Cyber Law and Cyber Security in Developing and Emerging Economies

Zeinab Karake Shalhoub
and Sheikha Lubna Al Qasimi

Cyber Law and Cyber Security in Developing and Emerging Economies

To Victor, my husband and friend
To Rana, Reem and Ruba
My daughters, my *raison d'être*.
To them all, I dedicate this book.

Zeinab

Cyber Law and Cyber Security in Developing and Emerging Economies

Zeinab Karake Shalhoub

Director of Research, Dubai International Financial Centre, Dubai, United Arab Emirates

and

Sheikha Lubna Al Qasimi

Minister of Foreign Trade, United Arab Emirates

Edward Elgar
Cheltenham, UK • Northampton, MA, USA

Published by
Edward Elgar Publishing Limited
The Lypiatts
15 Lansdown Road
Cheltenham
Glos GL50 2JA
UK

Edward Elgar Publishing, Inc.
William Pratt House
9 Dewey Court
Northampton
Massachusetts 01060
USA

A catalogue record for this book
is available from the British Library

Library of Congress Control Number: 2009937894

ISBN 978 1 84542 871 6

Printed and bound by MPG Books Group, UK

Contents

1. Establishing the context

INTRODUCTION

The advances of digital technology and the intertwined connections between computing and communications have set in motion many changes affecting the way we live. From 2000 to 2008, the Internet has expanded at an average annual rate of 290 percent on a global level, and currently an estimated 1.4 billion people are connected to the Internet, which is close to 25 percent of the world's population. The technology has advanced so fast and has become more and more user friendly; at the same time, people around the world have become more and more sophisticated in the use of technology. These inclinations have also created unparalleled opportunities for cyber criminals; criminal behaviors that were not imaginable a few years ago have become daily occurrences today. Digital technologies today make available to ordinary citizens tools which have the power and capability to inflict considerable damage. As never before, and at insignificant cost, criminals can cause calamitous harm to individuals, companies, and governments from places unheard of. The new advancement in technology, both hard and soft, is creating new opportunities for cyber criminals; and though, in principle, the same crimes considered illegal off-line are equally illegal in cyber space, online crimes take different forms in regard to the nature of the offender and the proof of crime. In order to create a control mechanism over cyber space and some form of deterrent for cyber criminals, a number of countries around the world have reformed their existing laws and legislation; however, these have proven to provide vague and inefficient solutions. It is argued in this book that in order for ethical standards to be established in cyber space, penal legislation must be developed and adopted which is clear and transparent; in other words, new laws have to be legislated to deal with cyber crimes. In addition, since cyber crime is borderless, where offenders can aim their attacks at many people, systems, and organizations in any country of the world regardless of their geographic location, international collaboration of law enforcement agencies and harmonization of cyber laws in the different countries are critical.

As information and computer technologies (ICTs) have developed, so have crimes related to their utilization; as a result of the move to the use

of computer networks in the online society in cyber space, new techniques of carrying out crimes have been exploited. Traditional laws were not developed with cyber society in mind. The main issue is how relevant these legislations are in dealing with cyber crime and to what degree. Traditional criminal laws describe qualified unethical behaviors which were developed over hundreds of years. The technological advancements of ICT networks have provided criminals with new opportunities to carry out attacks and commit fraud online. The costs incurred due to these attacks are considerable: loss of data and information, loss of revenues; losses associated with reputation and image of the entity affected, and damage to soft and hard infrastructure. Given the nature of cyber space in terms of lack of geographic boundaries, these attacks can cause instantaneous and inestimable devastation in a number of countries at once. Several individuals have been engaged in the fight against computer crime from its early development.

The pioneer in the area of computer crime is, by the account of many experts in the field, Donn B. Parker, a senior computer security consultant at the Stanford Research Institute in the United States. His journey with computer crime and cyber security started in the early 1970s; his first book on the subject was *Computer Crime* published in 1976.[1] Parker was also the lead author of *Computer Crime: Criminal Justice Resource Manual* (1979), the first basic US federal manual for computer-related law enforcement. In 1982, the Organisation of Economic Co-operation and Development (OECD) appointed an expert committee, the Information and Computer Communication Policy (ICCP) Committee, to discuss computer-related crimes and the need for changes in the legal systems. This committee presented its recommendations in 1986, stating that, given the nature of cyber crime, it was highly desirable to forge some form of international cooperation to reduce and control such activity. In addition, it recommended that member countries change their penal legislation to cover cyber crimes (OECD, 1986).

Cyber criminals have been very active both in developed and developing countries. While the developed world has moved at an early stage to enact laws to deal with cyber crime, the developing world has been very lax in moving in this direction. The 1980s and 1990s saw a great number of developing countries diversifying their economies from reliance on commodities. Many have elected to make use of information technology (IT) to become knowledge-based societies; to that end, there is a strong need for an appropriate legal foundation, or cyber laws. This is further necessitated by the fact that the Internet is difficult to regulate, given that no single, independent regulator has jurisdiction over international domains. The legal system, even in developed economies, has always had difficulties in keeping abreast with the advancement of technology.

One of the most disturbing trends in recent years has been the surfacing of an advanced, well-developed underground economy in which spam software, credit card information, and identity theft information are all available at affordable prices. Symantec, a security software company raised red flags about what it calls the 'underground server' economy in December 2008, with the publication of a report which estimates that nearly US$276 million worth of goods and information is available on online black markets. Credit card data accounted for 59 percent of the information available for sale on these underground market servers; further, Symantec reports that identity theft information constitutes 16 percent and financial information accounts for 8 percent (Symantec, 2008).

What is even more frightening than the accessibility of this information is its affordability. According to Symantec, bank account information is selling for US$10 to US$1,000, while information about financial websites' exposure is promoted for an average of US$740. If all the information available on the servers were made use of successfully it would net in close to US$5 billion, the report estimates. A primary reason why this data is more broadly available is that hackers have made hacking a full-time job, earning a living by stealing information and putting it on the market for sale on underground server systems. Malware has also extended its reach throughout the Internet. Google reports that close to 1.25 percent of all Internet search results in February 2008 had a minimum of one malicious URL, a large increase from the 0.25 percent of Internet search results in April 2007 that contained at least one malicious URL (Google, 2008).

The rise of malware and underground servers has resulted in alarming financial disasters for some businesses. This past summer (2008), the US Department of Justice announced that a group of hackers had used a combination of sniffer software and structured query language (SQL) injection attacks to gain access to more than 40 million credit and debit card numbers from TJX, OfficeMax, Barnes & Noble and other companies; they store them on underground server systems in the United States, Latvia, and Ukraine (Gross, 2008).

Given the financial crisis, financial crimes are expected to increase as cyber criminals take advantage of the predominant economic confusion and desperation of jobless people. The present global economic crisis will become a goldmine for cyber criminals and will most likely lead to more financial crimes in the next couple of years.

Businesses and governmental agencies around the world are being pressurized by the economic downturn, and the insecurity facing them is compounded by significant added risks due to data leakage, data loss, and outside attacks, all of which have increased significantly over the past couple of years. The current economic downturn has affected the ability of

organizations to safeguard crucial information such as intellectual property; a recent study sponsored by McAfee revealed the extent to which the economic downturn will negatively affect the security and confidentiality of vital information. The study finds that information is becoming an international sort of currency, and cyber criminals are targeting this new form of wealth. The report concludes with the findings that: (1) more and more essential information that is being digitally transferred between companies and continents is being lost; (2) the current financial crisis will set the stage to create an information security risk tsunami, as increased stress on businesses to reduce spending and downsize leads to weaker IT and increased opportunities for cyber criminals; (3) due to geopolitical perceptions, a number of countries are emerging as clear sources of threat to sensitive information and data; and (4) cyber criminals have moved beyond simple hacking aimed at stealing personally identifiable information and credit card data, to targeting intellectual property.

The first use of the term 'cyber space' was in 1984 in *Neuromencer*, a science fiction novel written by William Gibson; it described the virtual world of computers. Today, cyber space has become synonymous with the Internet; however, cyber space is not the World Wide Web alone. In addition to the hard infrastructure presented by the WWW, soft infrastructure is necessary in terms of regulatory mechanisms and cyber law.

The growth of electronic commerce and activities in cyber space in the past few years has created a need for vibrant and effective regulatory mechanisms to further strengthen the legal infrastructure that is crucial to the success and security of cyber space. All of these regulatory mechanisms and the legal infrastructure come within the domain of cyber law. Cyber law is important because it touches almost all aspects of transactions and activities concerning the Internet, the World Wide Web, and cyber space. Cyber law also concerns everyone; the most vigorous cyber gangs are using tried-and-true modus operandi to find Web applications containing major faults; they perform simple activities, such as overloading a badly written program with too much input, to break in. Usually, the intruder aims at taking control of the victim's personal computer and using it to proliferate infections and perform illegal activities. Meanwhile, all of the victim's important data are gathered and traded. In the past few years, e-mail, blog sites, social-network messages, search engine results, and popular webpages have become overloaded with such infections. In 2008 alone, a computer security firm traced in excess of 15 million malicious programs spread on the Internet (Nisen, 2009). One can only speculate the root cause of the proliferation of these attacks. Lately, phishers have been singling out smaller financial services companies and smaller banks worldwide, which may not be as prepared as the larger banking institutions; in

addition, phishing software is becoming more and more sophisticated, allowing the hijacking of a larger pool of Internet technologies.

KNOWLEDGE SOCIETIES

Rapid cycles of technological innovation, particularly with the advent of electronic commerce (e-commerce), have seen ICT become recognized by business owners/managers as a vital element of business. Perhaps most significantly, the Internet is praised as a unique and powerful form of ICT which, despite the collapse of the 'dot-coms', is continuing to advance at an ever-increasing pace and is making cyber space attractive to even the smallest of businesses, standing to gain tremendous business advantages from implementing Internet technology.

Similarly, despite the slow growth of mobile commerce, the importance of cellular or mobile phones as a form of business ICT is becoming more pronounced. While the emergence of the Internet, cellular phones, and other forms of ICT has significantly altered the way in which both small and larger businesses operate, divergent views exist as to whether the impact of such technological developments is indeed favorable or not. On the one hand, ICT may be considered 'a tool to enhance life', given its desirable direct impacts. In particular, it is claimed that ICT improves productivity, enables business to be conducted outside of an office, and creates new industries. The correlation between ICT and business growth is noted for a number of developing countries; however, the direction of this effect is unclear. A growing literature examines the link between growth and the convergence of communication and computer technology, particularly within the United States. The 1980s, 1990s and the start of the twenty-first century are seen as periods of advanced development. These periods witnessed major processes of transition from industry-based to knowledge-based economies. There are a number of indicators, both quantitative and qualitative, that point to these transition processes – such as the increasing number of knowledge workers, the shifting of importance between human capital and fixed assets, the investment in information technology, the creation of new knowledge-based businesses, the creation of new professions, and the introduction of institutional changes at the macro level. These changes are described as two interwoven society-wide development processes: (1) transformation of knowledge for economic and social development, and (2) the emergence of the Internet as the core of a worldwide digital information infrastructure. The concept of the division of knowledge is a determinant in analysing and describing the dynamics of societal processes of interaction by which knowledge is effectively

generated and used. In the new millennium, the information and the speed with which corporate executives receive it will be extremely important to charting the course of any company. John Donovan, professor at the Massachusetts Institute of Technology and chair of the Cambridge Technology Group, maintains that information executives are the only people who can improve the competitive position of US corporations as we venture into the twenty-first century (Donovan, 1989). The Internet has opened up avenues for commerce that were unimaginable just a few years ago. In essence, the Internet has created opportunities for seamless business collaboration between buyers and sellers as well as the collection of service companies that have constituted traditional supply chains. New business models inspired by the new technology break down traditional boundaries between business partners, in essence making all participants in a business transaction part of an expansive extranet. In theory, these business partners will be able easily and securely to communicate and complete end-to-end transactions from within their respective companies – streamlining communications, increasing the precision of forecasts, and driving cost out of day-to-day operations. The changes brought about by the Internet have even broader implications. With the advent of Internet technology, every company becomes a global company, with the means and opportunity to buy and sell from, or strike an alliance with, any company, anywhere, anytime. This golden opportunity brings with it a level of complexity that surpasses anything that all but the most far-flung global enterprises have experienced to date.

The recent explosion of information and IT has induced corporate management to utilize its ingenuity in creating the best available means to manage the flow of information, control flow channels, and integrate the different assets (both hardware and software) of IT utilized by the different departments and divisions of the corporation. As companies invest heavily in information-based systems, they are vesting more control in technology strategies and new business models, especially those related to e-commerce. E-commerce is considered the star of the IT revolution and the Internet. The most established components of e-commerce – electronic data interchange and electronic corporate payments – have been growing for over a decade at rates of around 20 percent a year and are rapidly reaching critical mass. As that happens the use of cyber space becomes a competitive necessity not an option. In the 1990s, those proven and steady applications of e-commerce were accelerated and extended by the combination of low-cost, high-performance telecommunications and personal computers plus the astonishing emergence of the Internet as a marketing channel, a telecommunications infrastructure that opens up e-commerce to small firms, and a vehicle for companies to rapidly develop internal

and external information and communication systems. The conundrum is whether or not the recent growth in use of the World Wide Web signals that the Internet will be a massive mass market for just about every type of business or if its already overloaded communications, with all the delays and frustrations that every Internet user has to deal with, and its demographics, will limit it to a narrow e-commerce community of mainly professional males, with well above average incomes, who use it largely for electronic mail. E-commerce and e-government are the most effective way to do business in an era where telecommunications allow more and more options for customer contact, elimination of documents and all the overheads and administration associated with them, computer-to-computer processing of transactions between customers and suppliers, and, though to a far lesser extent as yet, between companies and customers. If it's the best way to do business, then it's obviously something that every manager needs to make part of his or her thinking. That is what this book is about: providing business managers with a non-hype, non-technical, reliable, and interesting guide to this new business territory.

The adoption of the Internet and e-commerce has rapidly spread across the world. Most countries, especially in the developing nations category, are making substantial investments in modernizing and boosting IT infrastructure, building a strong telecommunications infrastructure, and promoting the Internet and use of cyber space in businesses, government, and various communities. This wide use of ICTs has accelerated the growth of cyber activities in many parts of the world. Information and communication technologies have transformed businesses, increased economic prosperity, and facilitated communication within a country and among countries around the world. The world is rapidly moving toward Internet-based economic structures and knowledge societies, which comprise networks of individuals, firms, and countries linked electronically in interdependent and interactive relationships (United Nations Conference on Trade and Development, 2003). In addition, cyber space activities promise to be the drive behind a new surge of economic growth and development. To examine the impacts of adopting new information technologies including cyber activities, two independent schools of thought have developed over the last decade. Proponents of the first school have emphasized models of diffusion of technology, integrating theories from change management, innovation, and technology diffusion literature (Larsen, 1998). The second school of thought identifies the impact of innovation or new technologies where innovations are the means of changing an organization, either as a response to change in the external environment or as a pre-emptive action to influence the environment (Rogers, 1995).

The spatial implications of the communication revolution are profound

but still uncertain for the developing world. Lower transaction and communication costs, combined with goods production that is increasingly based on flexible specialization, tend to favor the dispersion of economic activities. Yet, real-time information about consumers, easier outsourcing, and the proliferation of producer-support services tend to favor locating production near to large markets and urban centers. Concerning services, the ICT revolution is likely to promote the dispersal of services that can be delivered remotely and effectively, even while inducing further concentration of others, such as activities that are driven by innovation, tacit knowledge, and face-to-face interactions. Location-independent work or telecommuting is growing in industrial countries. One estimate suggests that about 5 percent of all service sector jobs in industrial countries will be contestable by developing countries (International Labour Organization, 2001).

The United Nations has been very active in promoting the diffusion of information communication technology as a means of economic development. This was illustrated through the Declaration of Principles of the World Summit on the Information Society that specifically states that information technology and communication are fundamental social processes, a basic human need and the foundation of all social organization; they are central to becoming members of the information society. Further, a number of United Nations initiatives affirm that the difficulties associated with the digital revolution make it necessary for emerging and developing economies to identify the major challenges facing them as active participants in a knowledge economy. Specifically, the challenges they face in creating wealth and making optimum use of the new development opportunities offered by the information society in various priority sectors; and the vitality of creating a trust framework through appropriate regulation of new social, economic, and cultural phenomena, as well as prevention and control of the dangers and risks associated with the information revolution.

PARADIGMS OF CYBER SOCIETIES

Cyber attacks are no longer a simple annoyance; cyber criminals in many instances could interrupt the critical mechanisms of the economy, affecting individuals and entities across the country. Despite controversies surrounding the problems and challenges associated with cyber space and its use in conducting business and commerce, and the burst of the 'dot.com' bubble at the start of the twenty-first century, many economies continue to make use of cyber space and deploy e-commerce extensively in their

economic activities. Many countries have developed Internet-enabled initiatives to manage the various aspects of economic activities, to strengthen online integration, and to design and customize products and services in an effort to serve citizens more effectively. While sizeable investments in e-commerce are being made, researchers and practitioners are struggling to determine whether and how these expenditures improve the performance of an economy both at the micro and macro levels. There has been much guesswork but little empirical data to determine the magnitude and distinctiveness of e-commerce initiatives and their impact on economic performance, especially of developing countries. Due to the complexity of determining what data to assemble, and of essentially collecting them, most of the existing literature regarding what determines the success of e-commerce initiatives tends to be fragmented and qualitative in nature. Case studies on countries such as Costa Rica, Bolivia, Egypt, Nepal, and Uganda have provided insights into the benefits of e-commerce, but the findings of these case studies are specific to just a few firms in the particular economy. In this book, a series of hypotheses will be formulated and tested in an effort to determine the success factors of e-commerce in developing economies.

The rise of e-commerce, the World Wide Web, and the software to support the initiatives is so startling in its economic implications that it may reasonably be considered a breakpoint in the way that we do business. This breakpoint is an abrupt and defining moment that obliterates standards and accepted commercial practices and replaces them with the essential business paradigm for the new era. The immediacy and growth of the Web have profound implications for businesses of all sorts. If you are a business strategist in the e-commerce age, you are confronting the fact that, almost overnight, your potential customer base has exploded in size, the choices available to those customers have multiplied many times, and hundreds of new competitors are suddenly clamoring for their attention. To thrive in this world, you must be online, and your online presence must be a powerful one.

The adoption of e-commerce and e-government is occurring at a frenetic pace in companies of all sizes and countries with varied degrees of development. Success in an environment that changes so fast requires individuals who are generalists but who can penetrate down deep into the technological foundation when needed. The strategic challenge is to understand a broad range of technologies, judge them quickly – especially emerging ones – make decisions about them, champion a direction, and provide leadership, all without losing track of the core business objectives and the fundamental growth perspectives.

Many essays concerning the implications of IT in general and

e-commerce in particular assert that these implications take a particular form and that the broad outlines of the future with e-commerce can be discerned fairly rapidly. The literature reveals three distinct perspectives on the implications of IT, in general. These perspectives can be applied to the implications of adopting e-commerce and electronic government at the macro (country) level. The three viewpoints are labeled the *Continuity, Transformation*, and *Structural* schools. For Continuists, IT exemplifies an incremental step on a long course of technological development. The important determinant for IT innovation here is how technological changes can meet: (1) users' needs, (2) the structure of factor costs, and (3) the availability of managerial, technical, and workforce skills (Miles, 1989: 224). Countries that do not jump on the wagon of IT innovativeness will risk the problem of losing their competitive edge and jeopardize their potential for economic growth. This is the main reason that developed countries spend significant percentages of their budgets on technological research and development.

Transformationists tend to put less importance on structures and strategies than on their underlying values and perspectives (Miles, 1989). Consequently, there has been ample research into perceptions of the 'impact' of IT on the workplace. Following the 1982 Versailles Summit, a major program of research into the acceptance of new technologies was launched. This was particularly inspired by concerns that public resistance to change was the root of slow innovation (Miles, 1989: 225).

A major assumption of the Structuralists is that many of our current uncertainties relate to being at the point of transition between structural doctrines; the stagnation and limits of old structures can be clearly seen but the viabilities of new models are hard to assess. New technologies imply learning processes and organizational changes to capitalize on their potential; new areas of demand are needed to establish new patterns of growth. Structuralist analysis typically attempts to identify key features of an emerging paradigm and to outline the enabling constraining factors around appropriate changes.

These three schools of thought differ in assessing the implications of IT in general and e-commerce in particular on formal work in an economy (including different economic sectors), the social structure of a country, international interdependence among nations, and globalization. It would be inappropriate to draw many conclusions from existing research, however. What is apparent is that there has been uneven development of research and that this adds to the intrinsic difficulties associated with assessing the implications of e-commerce and a knowledge society. Most practitioners and theorists are in agreement that the majority of developing countries in the new millennium will continue moving from the

industrial society to the information/knowledge era, or the third wave. Many advocate the use of IT and e-commerce as an effective way of coping with the changing environment, locally, regionally, and globally. These authors go one step further by stating that the adoption of electronic commerce at the national level plays a critical role for countries to survive in a hostile, complex, and turbulent global environment.

CYBER SPACE AND GLOBALIZATION

Cyber space and e-commerce have become a driving force for the globalization of the world economy, and countries that do not engage in e-commerce may put the competitiveness of their economies at risk. As a result, many firms and organizations in developing countries have become integral parts of global networks of production supply chains that increasingly use e-commerce mechanisms. Through these networks, entities in more developed countries induce developing-country enterprises to adopt new information technologies, organizational changes, and business practices.

The diffusion of cyber use in developing/emerging economies is relatively low. The main stumbling blocks are associated with regulatory, cultural, and social factors, including (1) the lack of regulations dealing with data messages and recognition of electronic signature; (2) the absence of specific legislations protecting consumers, intellectual property, personal data, information systems, and networks; (3) the dearth of appropriate fiscal and customs legislation covering electronic transactions; and (4) the absence and/or inadequacy of laws dealing with cyber crimes.

Today's technological advances are faster (Moore's law) and more fundamental (breakthroughs in genetics). They are driving down costs (computing and communications) at a pace never before seen. Leading these transformations are the accelerated developments in ICT, biotechnology, and just-emerging nanotechnology. Information and communications technology involves innovations in microelectronics, computing (hardware and software), telecommunications, and optoelectronics – microprocessors, semiconductors, and fiber optics. These innovations enable the processing and storage of enormous amounts of information, along with rapid distribution of information through communication networks. Moore's law predicts the doubling of computing power every 18–24 months due to the rapid evolution of microprocessor technology. Gilder's law predicts the doubling of communications power every six months – a bandwidth explosion – due to advances in fiber optic network technologies.

Individuals, households, and institutions are linked in processing and executing a huge number of instructions in imperceptible timespans. This radically alters access to information and the structure of communication, thus extending the networked reach to all corners of the world. Today's technological transformations are intertwined with another major historic shift – economic globalization – that is rapidly unifying world markets. The two processes are mutually reinforcing. The late twentieth century integration of world markets was driven by trade liberalization and other dramatic policy changes around the world, such as privatization and the fall of communism in the former Soviet Union. The new tools of information and communications technology reinforced and accelerated the process. Globalization propels technological progress with the competition and incentives of the global marketplace and the world's financial and scientific resources. The global marketplace is technology based, with technology a major factor in market competition. Developing countries that can develop the requisite infrastructure can participate in new global business models of intermediation, business process outsourcing, and value chain integration. In developing countries, as the user base expands, costs fall and technologies are adapted to local needs, the potential of ICT will be limited only by human imagination and political will. The organization of work must be revamped if national economies are to perform more effectively in a global market. Practitioners, theorists, and futurists alike concur that the challenge for countries that want to maximize their global presence involves structuring relationships and the flow of information so that the right parties can obtain it at the right time. Information technology and e-commerce initiatives play critical roles in the strategy of global competition. Countries reap the biggest benefits not by superimposing computers on top of old work processes but by restructuring those processes and the national culture. This strategy, over time, develops entirely new economic and business capacities.

Through the standardization of messages and business processes, today's market makers will create interoperability among markets. They will serve also as guarantors of predictable, trustworthy behaviors among trading partners, giving entrepreneurs the confidence that they need to take their great ideas into the market and build virtual businesses. Another crucial step is to establish standard specifications for business processes – the ways in which messages are generated and acted upon once they are received.

Technology to support this vast interconnected global commerce network is maturing rapidly due, in large part, to the great progress being made in establishing standard specifications for building commerce messages – requests for quotes (RFQs), purchase orders (Pos), contracts,

invoices, and so forth. Soon there will be completed libraries from which businesses can build and dispatch electronic messages that any other businesses in the world can accept and act upon with ease. One of the global consequences of IT, however, is the international concern about the risks and dangers that developed as well as developing economies may face in the wide application of IT. One such risk may be found in the proliferation of criminal activities in cyber space.

ECONOMIC DEVELOPMENT, GROWTH, AND RULE OF LAW

Many studies suggest that the key determinants of economic development are the accumulation of physical and human capital and technological improvements. Traditional neoclassical growth theory emphasizes physical capital accumulation whereas endogenous growth theory presumes that investment in human capital and technological progress are the main sources of economic growth. More recently, and as an extension to neoclassical models, Mankiw et al. (1992) have shown that physical and human capital are important determinants of growth. Nevertheless, it remains an open question whether these factors are the real sources of economic development. There is reason to believe that if physical or human capital enrichment or technological improvements are taking place, the real growth factors must already have been unbound. Accordingly, physical and human capital and technology should be seen as proximate causes of growth.

The changing value proposition in the knowledge economy is triggering a revolution in the way businesses and governments carry out their jobs. The Internet always did have its own complicated ethics, and those ethics were set aside by old-style management. This is radically shifting. They are, in part, becoming the rules of the game. For example, not only does business-to-business supply-chain management provide huge efficiencies and significant bottom line enhancement, but its deep integration allows partners to see into and through other organizations. As a consequence, decision makers are often privy to their competitors' internal strengths and weaknesses, trade secrets, unique know-how, market positioning, key personnel, and other valuable economic assets.

In summary, perhaps the most profound ethical changes in the New Economy are going on internally, inside the organization and at the firm level. In the New Economy, where knowledge, not equipment, drives profits, employees can no longer be considered 'outsiders'. They are the source of competitive advantage. The traditional command-and-control

model of management is rapidly being replaced by decentralized teams of individuals motivated by their ownership in the corporation. Value in the New Economy is being fundamentally redefined. As a result, transparency and the rule of law are becoming two of the keys to success in the twenty-first century. In e-business circles, transparency is no longer a rhetorical word. It is the rule of the game. It is unarguably recognized that the IT revolution will have significant long-run effects on the economy and that the principal effects are more likely to be microeconomic than macroeconomic. As a result, the new information economy will require changes in the way the government provides property rights, institutional frameworks, and 'rules of the game' that underpin the market economy. Two main reasons underlie these changes; first is the pace of technological progress in the IT sector, which is very rapid and will continue to be very rapid for the foreseeable future. For example, at the end of the 1950s, there were 2,000 computers processing 10,000 instructions per second. Today, as estimated by Forrester Research, at the end of 2008, there are one billion computers processing several hundred million instructions per second. The number of personal computers will reach two billion by 2015. Forrester Research's forecast is based on the assumption that from 2003 to 2015 the total number of personal computers in the world will increase annually by 12 percent (Forrester Research, 2008). As the IT sector of the economy becomes a larger share of the total economy, the overall rate of productivity growth will increase toward the rate of productivity growth in the IT sector. Secondly, the computers, switches, cables, and programs that are the products of today's leading sectors are general-purpose technologies. As a result, advances in high-technology affect all aspects of the economy, thereby leading to larger overall effects. These microeconomic effects will have long-lasting and far-reaching impacts on the economy. As a result, the role of the government in developed and developing economy alike needs to be re-examined. Since the creation of knowledge is cumulative, the importance of intellectual property rights becomes more critical in the new information economy. Three issues are interrelated: property rights over ideas, incentives to fund research and development, and the exchange of information among researchers.

The new information economy is 'Schumpeterian' rather than 'Smithian'. In a Schumpeterian economy, the production of goods exhibits increasing returns to scale. Under these conditions, the competitive equilibrium is not the likely outcome – setting price equal to marginal cost does not allow the firm to recover the large fixed costs. However, government regulation or government subsidies to cover fixed costs destroy the entrepreneurial spirit and replace it with 'group-think and red-tape defects of administrative bureaucracy' (Hakkio, 2001). In addition, when innovation becomes the

principal source of wealth, temporary monopoly power and profits may be essential to stimulate innovation. In a recent Brookings study on the economic impact of the Internet, a group of scholars estimated that the increased use of the Internet could add 0.25 to 0.5 percent to productivity growth over the next five years. Most of the impacts come from reducing the cost of data-intensive transactions (ordering, invoicing, accounting, and recruiting), from improved management of supply chains, from increased competition, and from increased efficiency of the wholesale and retail trade. In addition, many of the benefits of IT may result in improved standards of living, even though measured gross domestic product is unaffected. Examples include reduced error rates in medical care delivery; a reduction in accidents, crime, and fraud prevention; and additional conveniences for consumers in the use of time and space.

The emergence of the information economy has been a key feature of faster productivity growth for many economies, developed and developing. Information technology has affected productivity in two ways. First, the IT sector itself has contributed directly to stronger productivity. Computers and other IT hardware have become better and cheaper, leading to increases in investment, employment, and output of the IT sector. Secondly, advances in technology have also increased productivity in the more traditional sectors of the economy – financial services, business services, and the retail and distribution industries. In the US, economic policy has contributed to a revival in productivity growth. Policies to maintain domestic competition and increase international competition have been stressed. Funds have been provided to support basic research and education. Also, and most importantly, the mix of monetary and fiscal policy has lowered interest rates and encouraged investment. The information economy can improve the effectiveness of monetary policy by allowing the private sector to better anticipate future central bank actions. Central banks typically operate by affecting overnight interest rates. By affecting current overnight rates and, most importantly, by affecting market expectations of future rates, monetary policy can affect financial market prices such as long-term interest rates, exchange rates, and equity prices. These prices will have the greatest effect on economic activity.

CYBER LAW AS AN IMPEDIMENT OF CYBER SPACE

Cyber space is one of the most complex legal frontlines today; it is estimated that from 2000 to 2008, Internet diffusion increased at an average rate of 290 percent globally, and presently an estimated 1.46 billion people per year are surfing the Internet. Developing/emerging countries in Africa

and Asia have accounted for the largest chunk of the increase; the expansion in Asia has been 406 percent and in Africa 1,031 percent.[2] Cyber security and cyber crime, including enormous and synchronized attacks against countries' vital information infrastructure and attackers' misuse of the Internet, are activities of major concern to society in general and developing economies in particular. In addition, the costs associated with cyber attacks are substantial, not only when it comes to lost revenues and inconvenience caused by network inoperability but, and most recently, in terms of lives affected due to identity theft.

Cyber crimes constitute a prime obstacle to the diffusion of e-commerce and e-government in developing economies. Thus governments have an important role in developing control mechanisms in the form of laws and legislation in order to minimize the rate and severity of cyber crimes to speed up Internet diffusion; setting appropriate policies and complementary services, particularly affecting the telecommunications sector, other infrastructure, human capital, and the investment environment, severely constrain Internet access in developing countries. The major impediment to the growth and success of cyber use in many developing and emerging economies is still poor telecommunications infrastructure. Required telecommunications facilities include transmission facilities connecting a country's domestic network to the greater Internet, the domestic Internet backbone, and connections from homes and businesses to the backbone network. The defects of domestic telecommunications services may be less important for the larger firms in developing countries; these firms may find it profitable to invest in telecommunications facilities (such as wireless) that bypass the local network. A growing number of African Internet sites, for instance, are hosted on servers in Europe or the US due to the poor infrastructure in those countries. Hence, even traffic that originates and terminates domestically can cost the same as international transmission. The high cost of Internet access, the lack of local loop infrastructure necessary for basic dial-up modem access, and the poor quality of the local loop infrastructure that does exist all impede connections to the domestic backbone. Country comparisons show a strong relationship between usage price and Internet penetration. For many developing countries, the most important issue is the lack of telephone service to homes and businesses. Despite increases in rates of telephone line penetration during the 1990s and the first half of the 2000s, the average per capita telephone lines is close to 5 percent for Africa.

The most popular alternatives by which developing countries can overcome inadequate local loop infrastructure are shared facilities or wireless local loop. Shared facilities, which involve local entrepreneurs selling the use of a computer with Internet access, are a fast and relatively cheap way

of increasing Internet use. Wireless and satellite technologies also provide an alternative to the high costs and inefficiencies of many domestic telecommunications systems. Although currently used primarily for voice, mobile phones are increasingly acting as better devices for many of the usual Internet applications. Cellular phones in some developing countries have experienced strong growth rates and relatively high penetration, similar to those in industrial countries. In the United Arab Emirates (UAE), for instance, the mobile phone penetration rate is 200 percent in 2008. On average, however, for developing countries as a group, mobile phone penetration remains well below industrial-country levels.

Poor infrastructure services (other than telecommunications) are an important constraint on the use of cyber space in developing economies. Frequent and long power interruptions can seriously interfere with data transmission and systems performance; many Bangalore software firms, as an example, have their own generators (Panagariya, 2000). Mail services can be unreliable, expensive, and time consuming in many developing countries. For example, the unreliability of postal services in Latin America has meant that more expensive courier services must be used to deliver goods ordered over the Internet and, in response, international courier services are setting up special distribution systems in Miami. The lack of safeguards against fraud can severely restrict credit card purchases, the most common means of conducting transactions over the Internet. For example, many consumers in the Gulf countries of Saudi Arabia, UAE, and Kuwait are unwilling to purchase goods over the Internet because credit card companies will not compensate holders for fraudulent use of cards (in many industrial countries, cardholders have only a limited exposure to loss). A critical mass of highly skilled labor is needed in developing countries to supply the necessary applications, provide support, and disseminate relevant technical knowledge for e-commerce. The workforce in many developing countries lacks a sufficient supply of these skills, and the demand for this specialized labor from industrial countries has further strained the supply of this labor in developing countries.

Several regulatory impediments to the widespread adoption of cyber space activities exist in many developing countries. Duties and taxes on computer hardware and software and communication equipment increase the expense of connecting to the Internet. For example, a computer imported into some African countries may be taxed at rates exceeding 50 percent (UNCTAD, 2003). The overall environment for private sector activities is a significant determinant of Internet service diffusion. An open foreign direct investment regime helps promote technology diffusion, which is important to the growth of e-commerce. Governments

must provide a supportive legal framework for electronic transactions, including recognition of digital signatures; legal admissibility of electronic contracts; and the establishment of data storage requirements in paper form, intellectual property rights for digital content, liability of Internet service providers, privacy of personal data, and mechanisms for resolving disputes.

A number of international organizations have undertaken the leadership in pushing toward cyber law development in both developing and developed economies. The International Telecommunication Union (ITU) is identified as a leader in this domain; it launched the Global Security Agenda in November 2007, and formed a High-Level Experts Group to look into the issues and develop proposals for long-term strategies to promote cyber security. This group is currently working with the International Multilateral Partnership Against Cyber-Threats (IMPACT), a group sponsored by the government of Malaysia, with the aim of putting together an early warning system for cyber attacks. Another initiative undertaken by the ITU is COP, Child Online Protection, to develop safe guiding principles of surfing the Internet for children.

The Council of Europe has developed what is thought by many to be the most comprehensive treaty to protect people against cyber criminals. It developed the Cyber Crime Convention to resolve legal disputes and take forward a universal, collective system to take legal action against cyber criminals. The idea for the Convention on Cyber Crime was founded on a number of studies carried out by the Council in 1989 and 1995. As a result, the Council created a committee to draft this Convention; once it was completed, it opened for signing and ratification in November 2001.

That most Internet business is conducted in English is currently an important constraint on using the Internet. Estimates of the share of English used on the Internet range from 70–80 percent, but only 57 percent of Internet users have English as their first language (ITU, 2007). Per capita Internet use averages about 30 percent in those industrial countries where English is common, compared with about 5 percent in other industrial countries. Conversely, Internet content is limited in the local language of most developing countries. From a commercial aspect, Schmitt (2000) found that just 37 percent of Fortune 100 websites support a language other than English. The amount of non-English material on the Web is growing, however. Spanish websites in particular are increasing, in part to serve the large Spanish-speaking community in the US (Vogel and Druckerman, 2000). Improvements in translation services (by people and machines), as well as Web browsers that recognize characters of different languages, should ease language constraints. There is growing recognition that English-only content is insufficient for a global economy.

RESOURCE-BASED VIEW

The resource-based view argues that the performance of a firm is a function of the resources and skills that are in place, and of those firm-specific characteristics which are rare and difficult to imitate or substitute (Barney, 1991). This concept is based on Coase's theory of the firm, which maintains that the firm is a combination of alliances that have linked themselves in such a way as to reduce the cost of producing goods and services for delivery to the marketplace (Coase, 1937). An enhancement of this resource-based view is that a firm or an economy can create a competitive advantage by building resources that work together to generate organizational capabilities (Bharadwaj, 2000). These capabilities permit firms and economies to adopt and adapt processes that enable them to realize a greater level of output from a given input or maintain their level of output from a lower quantity of input.

Capabilities afforded by ICT are one major component of organizations' and economies' capabilities; and recent studies have identified a number of specific ICT capabilities that provide competitive advantage. Bharadwaj (2000) classifies an entity's key ICT capability as comprising: (1) a physical IT infrastructure, (2) human IT resources (including technical IT skills and managerial IT skills), and (3) intangible IT-enabled resources (such as customer orientation, knowledge assets, and synergy).

Viewed from a growth perspective, resource-based theory is concerned with the origin, evolution, and sustainability of firms. Firms experiencing the highest growth have added new competencies sequentially, often over extended periods of time. Resource-based sequencing is important for achieving sustainable growth. In a changing environment, firms must continuously invent and upgrade their resources and capabilities if they are to maintain competitive advantage and growth (Agryris, 1996). This sequential development of resources and capabilities can make a firm's advantage inimitable (Barney, 1991). Competitors cannot simply buy these resources and capabilities without acquiring the entire firm. This is because the resources and capabilities are built over time in a path-dependent process that makes them inextricably interwoven into a firm. This facet of resources and capabilities development makes it theoretically impossible for competitors to imitate completely (Dierickx and Cool, 1989).

Until recently, little research using a resource-based-view framework has examined strategy differences in the social context of developing economies. As with most resources that create competitive advantage, resources for competitive advantage in developing economies are, on the whole, intangible. However, they are not necessarily market or product specific, as might be expected. Although some qualifications are standard

regardless of the level of development (for instance, first-mover advantages), others are particularly important in developing economies. Global and multinational firms that are able to manage some of the imperfect conditions in developing economies benefit from being first movers; some of the benefits include economic advantages of sales volume and domination of distribution and communication channels.

In developing economies, however, such advantages are difficult to establish without good relationships with home governments. Early relationships give tangible benefits, such as access to licenses, the number of which is often limited by a government. In addition, local competitors may have developed capabilities for relationship-based management in their environment that substitute for the lack of institutional infrastructure. Developing distribution mechanisms may protect a domestic firm in a developing economy against entry by foreign firms. Furthermore, focusing on a market that has not yet reached the globalization stage might allow a domestic firm in an emerging economy to dodge the onslaught of multinational rivals. Additionally, competing in a global market may be possible in a commodity area where natural resources or labor give a low-cost advantage (Aulakh et al., 2000).

In essence, a firm must understand that relationship between its company assets and the changing nature of the institutional infrastructure as well as the characteristics of its industry. In so doing, the emerging economy firm may be able to become an aggressive contender domestically or globally by using its resources as sources of competitive advantage.

The resource-based view of the firm or an economy sees a firm or an economy as a bundle of resources and capabilities. Resources are firm-specific assets and competencies controlled and used by firms to develop and implement their strategies. They can be either tangible (e.g. financial assets, technology) or intangible (e.g. managerial skills, reputation) (Barney, 1997). Resources are heterogeneous across firms, and some resources are valuable yet rare, difficult to imitate or non-substitutable, giving the firms that have them distinctive core capabilities. Resources that provide sustainable advantage tend to be: (1) causally ambiguous (e.g. transformational leadership), (2) socially complex (e.g. culture), (3) rare, or (4) imperfectly imitable (Barney, 1997). Capabilities are a firm's abilities to integrate, build, and reconfigure internal and external assets and competencies so that they enable it to perform distinctive activities (Teece et al., 1997). The resource-based approach focuses on the characteristics of resources and the strategic factor markets from which they are obtained.

Past research using the resource-based view associates rent potential, that is, greater than normal returns, with two possible paths. The first involves external factors, including buyer and supplier power, intensity

of competition, and industry and product market structure, that influence what resources the firm selects, as well as how they are selected and deployed. The second path to the capture of rents involves creating idiosyncratically productive combinations of resources.

Firms cannot expect to garner rents by merely owning and controlling resources. They should be able to acquire, develop, and deploy these resources in a manner that provides distinctive sources of advantage in the marketplace. The traditional conceptualization of the resource-based view has not looked beyond the properties of resources and resource markets to explain enduring firm heterogeneity. In particular, past research has not addressed or examined the process of resource development (Oliver, 1997).

Firms' decisions about selecting, accumulating, and deploying resources are characterized as economically rational within the constraints of limited information, cognitive biases, and causal ambiguity. Additionally, the traditional resource-based view is limited to relatively stable environments. Barney (1997: 171) warns, 'if a firm's threats and opportunities change in a rapid and unpredictable manner, the firm will often be unable to maintain a sustained competitive advantage.' Only recently have researchers begun to focus on the specifics of how some organizations first develop firm-specific capabilities and then how they renew competencies to respond to shifts in the business environment.

The dynamic capabilities approach (Teece et al., 1997) is an extension of the resource-based view of the firm that was introduced to explain how firms can develop their capability to adapt and even capitalize on rapidly changing technological environments. Dynamic capabilities emphasize the key role of strategic management in appropriately adapting, integrating, and reconfiguring internal and external organizational skills, resources, and functional competencies within a changing environment. The development of such capabilities is limited by the firm's existing base of capabilities, and is shaped by its current market position and past history of developing capabilities (Teece et al., 1997). The difference between the traditional conceptualization of the resource-based view of the firm (Barney, 1997) and the dynamic capabilities view (Teece et al., 1997) is that under the traditional view, current firm resources and capabilities are exploited to the opportunities in the marketplace, whereas under the dynamic capabilities view, the firm needs to develop new capabilities to identify opportunities and respond quickly to them. Although Teece et al. (1997) outlined the dynamic capabilities approach, they did not provide empirical evidence to help understand how these capabilities are developed. Following this approach, a handful of models have been proposed to explain how resources and capabilities are built up over time (see, for example, Oliver, 1997). All these models are empirically grounded; however, they have all

followed a factor-oriented, or variance theory, approach. Process theories are less common in the resource-based view of the firm literature, and have yet to be developed for explaining the resource and capability development process. Process theories focus on sequences of activities to explain how and why particular outcomes evolve over time.

The literature review undertaken did not identify a single process model of capability development. The prevailing wisdom seems to be that capability development is a lengthy, complex process influenced by multiple organizational dimensions.

CHAPTER OVERVIEW

Cyber Law and Cyber Security in Developing and Emerging Economies uses a theory-based, empirical investigation to describe the linkage between the development and implementation of mature cyber laws and economic growth and development and a number of country-specific characteristics (resources). The book's six chapters are organized as follows:

- *Chapter 1* This chapter has provided an overview of the entire book and has established the context for the whole book. Importance of the research at hand is emphasized, along with the theories used, the geographic area of implementation, the methods used, and the methodology applied.
- *Chapter 2* This chapter provides an overview of the move to the digital economy and the state of trust and security in cyber space. Coverage of the threat of cyber crime to economies and businesses, especially in the financial sector, is introduced in this chapter. The chapter also covers the types of cyber crimes, especially in the financial sector.
- *Chapter 3* This chapter reviews the literature on resource-based theory and diffusion of radical technologies in developing economies.
- *Chapter 4* This chapter is devoted to the development of hypotheses, discussion of methodology, identification of variables, and data collection. In addition, reliable measures of this construct are identified. This chapter also covers the experiences of the sample of emerging countries in developing and implementing cyber laws.
- *Chapter 5* This chapter is devoted to model testing, data analysis and presentation of the results; the analysis should reveal why some countries are more inclined to develop and implement what we refer to as mature cyber laws.

- *Chapter 6* This chapter consists of a summary, concluding remarks, practical implications of findings, and recommendations for future research.

BOOK SUMMARY

This book aims to take a step toward an empirical/theoretical framework for understanding the impact of cyber law and its determinants in terms of growth and development of emerging and developing economies. Basically, a framework that is grounded in strong theory is developed. The framework uses core constructs that appear central to resource-based and technology diffusion literature and provides a fine-grained understanding of cyber space adoption processes by public and private sector entities in developing and emerging countries. In so doing, this book considers how each exchange encounter is shaped by, and in turn shapes, relational characteristics, which form the bases for growth and development.

This book is aimed at the 'low to middle' level of rigor. It is not designed to compete with extremely sophisticated modeling or quantitatively oriented books. Actually, this book does not know of any competitor. This level of rigor makes the book attractive to any student, professional, practitioner, or policy maker interested in finding answers to questions such as:

1. What are the determinants to the development of mature and comprehensive cyber laws?
2. What countries have been more vigilant in the development and implementation of cyber laws?
3. What are the components of an ideal cyber law for developing economies?

The major thrust of the book, which evaluates the experience of cyber space laws and regulations in developing and emerging economies from a resource-based theory perspective, is unique and innovative in nature. The features of uniqueness and innovativeness, coupled with the radical changes in the use of governmental resources to improve the effectiveness and efficiency of an economy, and the effects of these changes on the economic structure of a country, make this book useful to many disciplines. The book is inspired by a number of factors, including (1) the importance of the subject at hand and (2) the lack of empirical research on the subject. Most of the work done by others is descriptive in nature. This book brings economic concepts into the picture of adopting a cyber law model by using resource-based theory as a vehicle of analysis.

As e-commerce and other cyber space activities mature and their tools and applications improve, greater attention is given to their use to improve the business of public institutions and governments. The main goal is to provide citizens and organizations with more convenient access to government information and services, and to provide delivery of public services to citizens, business partners and suppliers, and those working in the public sector. E-government applications extend over a wide spectrum: (1) government-to-citizens (G2C), (2) government-to-business and business-to-government (G2B and B2G), (3) government-to-government (G2G), and (4) government-to-employees (G2E). Cyber law is deemed a critical success factor for these initiatives.

As in the industrial age, in many instances it will be up to governments to lead the transformation to the new information/knowledge age, and as such the criticality of developing cyber laws to protect cyber activities and cyber users. Public sector organizations will have to adjust their relationships with citizens, businesses, employees, and other public agencies. To this end, the information/knowledge society has prompted many countries to adopt e-government initiatives. The value of the book is twofold. First, it will cover the experience of a number of developing countries and newly industrialized countries (NICs), or emerging countries that have enacted and implemented cyber law initiatives early on, such as Hong Kong and the UAE. Some fragmented literature exists on the experience of these countries, but there is no unique book evaluating those experiences from a comparative analysis, resource-based perspective. The book will add value to existing literature by accomplishing this goal. In addition, it will cover the different approaches governments in the various countries have taken based on their own social, cultural, and economic contexts. Some countries have adopted a gradual approach to regulating cyber activities by adapting their existing laws or have taken a more radical approach by enacting new cyber laws. Many countries embarking on enacting new cyber laws are utilizing the 2001 European Convention on Cyber Crime as a guideline; the Convention criminalizes:

- Offenses against confidentiality, integrity offenses against confidentiality, integrity and availability of computer data and availability of computer data;
- Computer-related offenses such as forgery;
- Content-related offenses such as child pornography; and,
- Copyright-related offenses.

The book will cover the experiences of those countries from the inception of the idea, to the setting of vision, to the formulation of strategy, through

implementation, and ending with assessment of the costs and benefits of the initiative from a resource-based theory perspective.

Second, the book aims to take a step toward an integrative theoretical framework for understanding the impact of the rule of law in cyber space on economic development from a resource-based perspective. A large stream of research in organization theory, information systems, organizational sociology, economics, and technology management has contributed substantially to our understanding of organizational adoption of innovations. A close examination of the research would suggest three broad themes: (1) a number of organizational and environmental factors which influence organizational adoption of innovations; (2) institutional pressures from the environment to influence technology adoption; and (3) firms and governments often fail to respond effectively to environmental changes, including new technology.

In this book, the authors extend theoretical developments in the resource-based view to investigate why some countries respond better to new technologies, in general, and cyber activities, in particular. Technological opportunism, a 'sense and respond' capability of decision makers with respect to new technologies, is an important determinant of e-commerce/e-government adoption. To assess the incremental contribution of technological opportunism in explaining e-commerce adoption, variables such as the perceived usefulness of e-commerce as a technology and complementary assets that help generate value from e-commerce are integrated in the model. Electronic marketplaces, e-commerce and e-governments are (and will be) playing a significant role in determining the success (or failure) of corporations, governmental agencies, and, even, nations. Management and government officials need to learn that the real challenge surrounding electronic marketplaces, in particular, and e-commerce, in general, is the task of making it happen. The book targets professionals, academicians, and researchers. It can be used as a recommended reading in Electronic Commerce classes, Information Economy classes, Management of Change classes, Economic Development classes, and Macroeconomic classes, as well as Marketing classes. The book is great reading for small and medium sized businesses that are considering moving into e-commerce and are looking for a real case study. In addition, the greatest benefit could be gained by governmental officials of developing and NICs contemplating e-government initiatives. The book's timeliness and insights into the changes in organizational and governmental practices make it appealing to a broad management and geographic market: (1) senior and mid-level managers and strategic planners who are charged with developing business strategies; (2) corporate executives who must drive their firm's competitive future; (3) government officials, especially in developing economies, and

(4) IT managers, both in the public and the private sectors, who need to lead their teams with strategic decisions.

The book is geared toward professionals in the private and public sectors, researchers, and academicians. It refrains from technical complexity and this makes it readable and understandable. With respect to competition, I do not know of any book analysing the empirical impact of cyber laws on e-marketplaces, and on the economic, cultural, and social texture of an economic entity from a strong economic theory such as the resource-based approach. The book is unique and I believe it will open the door to other researchers to explore research and study experiences of other economic entities.

A major competitive advantage of this book is the fact that it is the collective product of an academician/consultant who is knowledgeable of the latest developments in cyber space development and e-commerce theory and application; and a practitioner who is applying leading-edge e-government technology and policy making at the UAE national level.

CONCLUSION

The Internet and cyber space revolution is not only changing the technology of the workplace but fundamentally redefining the way that countries design their growth and development strategies. Electronic governments and the B2B world with its e-markets, customer focus, and deeply integrated corporate and economic relationships are driving growth and development of economies at e-speed and creating value in different ways. The key to survival in the relatively new world of cyber space depends upon governmental leaders' ability to adapt to a new, more collaborative, corporate-type, and transparent competition model. This new reality presents major challenges to traditional ways of governing and leading economic growth and development. Economic development is the process of creating wealth by mobilizing human, financial, physical, natural, and capital resources to produce (generate) marketable goods and services. The government's role is to influence the process for the benefit of the various stakeholders in the country. Economic development, then, is fundamentally about enhancing the factors of productive capacity – land, labor, capital, and technology – of a national, state, or local economy.

Early economic development theory was but merely an extension of conventional economic theory which equated 'development' with growth and industrialization. As a result, Latin American, Asian, and African countries were seen mostly as 'underdeveloped' countries, that is, 'primitive' versions of European nations that could, with time, 'develop' the

institutions and standards of living of Europe and North America. Economic growth is caused by improvements in the quantity and quality of the factors of production that a country has available, that is, land, labor, capital, and enterprise. Conversely, economic decline may occur if the quantity or quality of any of the factors of production falls. Increases in the supply of labor can increase economic growth. Increases in the population can increase the number of young people entering the labor force. Increases in the population can also lead to an increase in market demand, thus stimulating production. However, if the population grows at a faster rate than the level of GDP, the GDP per capita will fall. It is not simply the amount of labor and skills that will lead to economic growth. It is often the quality of that labor. This will depend on the educational provision in countries. Improving the skills of the workforce is seen as an important key to economic growth. Many developing countries have made enormous efforts to provide universal primary education. As more and more capital is used, labor has to be better trained in the skills to use it. It should always be remembered that education spending involves an opportunity cost in terms of current consumption and thus it is often referred to as investment spending on human capital.

NOTES

1. See www.cybercrimelaw.net for a list of his publications.
2. See World Internet Usage and Population Statistics, http://www.internetworldstats.com/stats.htm (June 2008).

REFERENCES

Agryris, N. (1996), 'Evidence on the role of firm capabilities in vertical integration decisions', *Strategic Management Journal*, **17**: 129–50.

Aulakh, Preet S., Masaaki Kotabe and Hildy Teegen (2000), 'Export strategies and performance of firms from emerging economies: evidence from Brazil, Chile and Mexico', *Academy of Management Journal*, **43**(3): 342–61.

Barney, J.B. (1991), 'Integrating organizational behavior and strategy formulation research: a resource based analysis', *Advances in Strategic Management*, **8**: 39–61.

Barney, J.B. (1997), *Gaining and Sustaining Competitive Advantage*, Reading, MA: Addison-Wesley.

Bharadwaj, A. (2000), 'A resource-based perspective on information technology capability and firm performance: an empirical investigation', *MIS Quarterly*, **24**(1): 169–96.

Brookings Institute (2007), 'The effects of broadband deployment on output and

employment: a cross sectional analysis of USA data', http://www3.brookings.edu/views/papers/crandall/200706/itan.pdf, accessed 5 October, 2008.
Coase, R.H. (1937), 'The nature of the firm', *Economica*, new series, **4**(16): 386–405.
Dierickx, P.J. and K. Cool (1989), 'Asset stock accumulation and the sustainability of competitive advantage', *Management Science*, **35**: 1504–11.
Donovan, J. (1989), 'From the back room to the boardroom', *Computerworld*, **17** (April), 83–4.
Forrester Research (2008), 'In 2008 the number of personal computers in the world will reach one billion', http://www.science-portal.org/in/71, accessed 2 August, 2009.
Google (2008), 'Malicious content injection', http://googleonlinesecurity.blogspot.com/2008/02/all-your-iframe-are-point-to-us.html, accessed 2 July, 2009.
Gross, G. (2008), 'ID theft ring attacked retailers on multiple levels', http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9111880, accessed 18 December.
Hakkio, C.S. (2001), 'Economic policy for the information economy', http://74.125.155.132/search?cache:jbDDYAS6Nx YJ: www.kansascityfka.com/publicat/q=sympos/2001/papers/S02/summ.pdf, accessed 11 September.
International Labour Organization (ILO) (2001), *World Employment Report – Life at Work in the Information Economy*, Geneva: ILO.
International Telecommunication Union (ITU) (2007), *Telecommunication Indicators Database*, Geneva: United Nations.
Larson, T.J. (1998), 'Information systems innovation: a framework for research and practice', in T.J. Larson and G. McGuire (eds), *Information Systems Innovation and Diffusion: Issues and Directions*, Hershey, PA Idea Group Publishing, pp. 411–34.
Larson, M. (1998), 'Search for the secure transactions: barriers to e-commerce falling', *Quality*, **37**(8): 61–3.
McAfee (2008), 'McAfee virtual criminology report: cybercrime versus cyberlaw', http://www.mcafee.com/us/research/criminology_report/virtual_criminology_report/index.html, accessed 12 December.
Mankiw, N.G., D. Romer and D.N. Weil (1992), 'A contribution to the empirics of economic growth', *Quarterly Journal of Economics*, **107**(2): 407–37.
Miles, I. (1989), 'Social implications of information technology', in M. Jussawalla, T. Okuma, and T. Araki (eds), *Information Technology and Global Interdependence*, Westport, CT: Greenwood Press, pp. 222–35.
Nisen, Jeremy (2009), 'Counteracting compromised computers: a conversation with Panda Security's Juan Santana, www.hispanicbusiness.com/news/2009/1/21/counteracting_compromised_computers_a_conversation_with.htm', accessed 30 January.
Organization for Economic Co-operation and Development (OECD) (1986), *Computer-related Criminality: Analysis of the Legal Politics in the OECD Area*, ICCP report no. 10, Paris: OECD.
Oliver, Christine (1997), 'Sustainable competitive advantage: combining institutional and resource-based views', *Strategic Management Journal*, **18**(October): 697–713.
Panagariya, A. (2000), 'E-commerce, WTO and developing countries', *The World Economy*, **23**(8), 959–78.
Rogers, E.M. (1995), *Diffusion of Innovations*, 4th edn, New York: Free Press.

Schmitt, E. (2000), 'The multilingual site blueprint', *The Forrester Report* June, accessed March, 2008 at www.eriksen.com/Portals/O/Multi_Lingual_Site_Blueprint.pdf.
Symantec (2008), Report on the underground economy', white paper, accessed at www.symantec.com.
Teece, D.J., G. Pisano and A. Shuen (1997), 'Dynamic capabilities and strategic management', *Strategic Management Journal*, **18**(7): 509–33.
United Nations Conference on Trade and Development (UNCTAD) (2003), *Ecommerce and Development Report*, New York: United Nations.
Vogel, T. and P. Druckerman (2000), 'Latin internet craze sets off alarm bells', *Wall Street Journal*, 16 February.

2. Security and trust in cyber space

INTRODUCTION

There is no doubt that the technology utilized by a large number of businesses, including financial institutions, noticeably in developing and emerging countries, is becoming more and more varied, advanced, and innovative. When measuring the gap between financial institutions that are technology centric and those that are not, one finds a notable difference.

The International Telecommunication Union (ITU) has identified five key factors to the success of a cyber security program at the national level; these are: (1) a national strategy; (2) collaboration between government and industry; (3) a sound legal foundation to deter cyber crime; (4) a national incident management capability; and (5) a national awareness of the importance of cyber security (Ennis, 2008).

Attacks and unauthorized uses on businesses and institutions include malicious acts such as theft or destruction of intellectual property, abuse by insiders, and unauthorized access to information that results in a loss of data integrity and confidentiality, as well as malware threats such as viruses, spyware, worms, and Trojans. These cyber attacks affect the trust of cyber users and, as such, lead to apprehension about using the Internet as a means to conduct transactions.

Philosophers when discussing 'trust' frequently refer to the party which displays trust in another as making itself vulnerable to the other party's behavior. In other words if you trust somebody then you are accepting that while it is a theoretical possibility it is not a realistic probability that they will act in a manner that would disadvantage you.

The concepts of trust and security have attracted a great deal of attention in recent management literature. There has been discussion of what trust is; what it means, its impact on online activities, its contribution to the diffusion of activities in cyber space, and so on. Much of the literature has been in the organizational behavior field. More importantly, there has also been a growing use of the concept of trust in Internet-based businesses.

The term 'trust' is used by people concerned with information security and cyber space; the most popular domain for its usage has been research regarding authentication and the infrastructure for public key technology

in a networked environment. The issue of how to exchange public keys and their certifications over the Internet has been important to the creators and users of public key application. However, the broader, more traditional usage of the word – beyond the specifications of certification formats for public keys – has increased with the rise of cyber activities.

Even though the term 'trust' is used, it is rarely defined; trust is defined, in part, by *Webster's Dictionary* as,

1. firm reliance on the integrity, ability, or character of a person or thing;
2. reliance on the intention and ability of a purchaser to pay in the future.

Both of these definitions speak to the commonsense understanding of trust. If I trust you, I am relying upon a quality or attribute of something, or the truth of a statement. It also hints at a logical treatment that could apply toward understanding trust in a relationship.

Trust is 'a state involving confident positive expectations about another's motives with respect to one's self in situations entailing risk' (Boon and Holmes, 1991: 194) and thus is an orientation toward others that is beyond rationality (Lewis and Weigert, 1985; Tyler and Kramer, 1996) because it increases one's vulnerability to opportunistic behavior (Cummings and Bromiley, 1996; Zand, 1972). In the same vein, McAllister explains trust as 'the extent to which a person is confident in, and willing to act on the basis of, the words, actions, and decisions of another' (1995: 25), and he empirically identifies cognitive- and affect-based trust as separate constructs. This combination of views and findings provides us with a definition of trust between individuals (i.e. interpersonal trust).

However, trust also occurs at the level of the organization (organizational trust), and has empirically been found to be different from interpersonal trust (Doney and Cannon, 1997). Zaheer et al. describe organizational trust as 'the extent to which organizational members have a collective trust orientation toward the partner firm' (1998a: 143). This definition closely matches the understanding of macro-level trust in sociology. For example, Coleman clarifies trust at the macro level as being 'a generalization of the two actor system of mutual trust, but [it] involves a greater number of actors' (1990: 188). Coleman also argues that there is some kind of feedback between the macro and micro, and micro and macro, levels.

Management research on organizational trust is largely in agreement that it is beneficial for performance, but the results of research on interpersonal trust are less clear. For example, Chow and Holden's (1997) research offers strong support for the significance of interpersonal trust, whereas Zaheer and colleagues (1998a, b) discovered that its function was less important than that of organizational trust. It is clear that more theory is

needed before the importance and effects of trust are more fully realized and distinguished.

Emerging empirical evidence, however, lends support to McAllister's (1995) finding that trust has both cognitive- and affect-based dimensions (Johnson et al., 1998; McAllister, 1995). Cognitive-based trust reflects technical competency and a fiduciary obligation to perform (Butler, 1983) and is based on predictability, past behavior, dependability, and fairness (Rempel et al., 1985). It relies on a rational evaluation of another's capability to carry out obligations. Unlike cognitive-based trust, affect-based trust is ingrained in emotional attachment and thoughtfulness and concern for the other party's well-being (Lewis and Weigert, 1985). There is an intrinsic value to the relationship itself and a conviction that the other party feels the same way (Pennings and Woiceshyn, 1987; Rempel et al., 1985).

The importance of trust in the use of the Internet as a means to transact business or a means of communications deserves special attention. The physical separation of the buyer and seller, the physical separation of the buyers and the merchandise, and the overall environment of perceived insecurity on the Internet provide unique challenges to Internet-based businesses to find ways in which to initiate and develop these cyber space relationships. Based on these limitations, the seller must develop a trustworthy relationship in order to make that initial sale, thus fostering customer loyalty.

The lack of physical presence of the product and the physical distance between the buyer and seller, make this a unique situation in which trust is of paramount importance. The development of this trust evolves over time as relationships grow between both parties. The pace at which customers are becoming connected to the Internet and the rate at which purchasing over the Internet is becoming conventional provide Internet-based businesses with greater opportunities in electronic commerce exchanges. Business, as conducted online, is positioned to pump up in the next few years. Conventional marketing models, however, may not be sufficient to explain consumer behavior online. Such differences between store retailing and online retailing include the physical separation of the buyer and seller, the absence of a salesperson, the separation of the product and the buyer, and the ability of marketers to immediately update product, price, and distribution information. These differences represent threats to e-marketers that must be overcome for consumers to initiate a purchase online.

Consumer loyalty is emerging as the marketplace currency for the twenty-first century. Marketers desire and seek it through building relationships with customers, yet it remains elusive. To acquire and hold this elusive currency would require a deep understanding of processes by

which consumers maintain relational exchanges with providers, and how these processes in turn influence loyalty. This is especially the case for services as their inherent intangibility, heterogeneity, and performance ambiguity pose challenges for forming and sustaining customer service provider relationships. Although this issue has received significant attention in the literature, some critical gaps remain.

First, the literature has tended to view consumer relationships from the perspective of the marketer/service provider. Few researchers have used the consumers' perspective to examine relational exchanges. Likewise, much theoretical work for understanding relational exchanges in service contexts has been shaped by conceptualizations of exchange mechanisms involving inter-organizational partners (Berry, 1995). By contrast, theoretical work for inquisitive relational means from a consumer's perspective is not there. Thus, Buttle (1996) states that customers have no say in relationship marketing, and since relationships are intrinsically two-sided, this unbalanced focus is awkward.

Second, the limited research that exists has tended to attack mainly either the economic or psychological approach; as such, integrative endeavors have been lacking. For instance, researchers have had some success in using the economic principles of agency theory to understand contracts between consumers and providers (Casson, 1997). Equally, psychological approaches have tended to look at the role of consumer–provider trust in promoting relational exchanges and building trust (Garbarino and Johnson, 1999). Although both approaches have provided interesting findings, little attention has been given to how the economic and psychological approaches might work together to shape and influence consumer trust and loyalty in relational exchanges.

There is little doubt that the Internet provides enormous potential benefits for consumers worldwide. Wider choice ranges, lower prices, and entirely new products have become available in many product categories such as books, CDs, and travel packages, to consumers who are physically far away from the world's centers of traditional commerce (*Economist*, 1997). Amazon.com sells 20 percent of its books to foreign destinations (Hamel and Sampler, 1998). Although favorable pricing might be a necessity to win orders by overseas customers, it may not be sufficient. Doney and Cannon (1997) label trust as an order qualifier for purchase decisions. That is, in order for a consumer to place an order, the consumer must trust the merchant first. Trust is a belief or expectation that the word or promise of the merchant can be relied upon and the seller will not take advantage of the consumer's vulnerability (Geyskens et al., 1996). Trust is a critical factor in any relationship in which the trustor (for example, consumer) does not have direct control over the actions of a trustee (for example,

merchant or store), and there are possible negative consequences of one party not fulfilling its promises (Deutch, 1958; Mayer et al., 1995).

Quelch and Klein (1996) speculate that in the early stages of Internet development, trust is a critical factor in stimulating purchases over the Internet. Keen (1997) warns that trust is not only a short-term issue but the most significant long-term barrier for realizing the potential of Internet marketing to consumers. An experiential survey of US-based online surfers, new to Internet-based shopping, found the shoppers fascinated by international shopping opportunities on the Web, but they were skeptical about actually purchasing from overseas sites (Jarvenpaa and Todd, 1997). Others report widespread distrust among consumers about Internet-based merchants.

Consequently, the role of trust throws up some uncertainties about Internet consumer merchandising. Consumers are unlikely to support electronic stores that fail to create a sense of trust. Trust can only exist if the consumer believes that the seller has both the ability and the motivation to deliver goods and services of the quality expected by the consumer. This belief may be more difficult for an Internet-based business to create than it is for a conventional business. In cyber space, providers depend on an impersonal electronic storefront to act on their behalf. Additionally, the Internet lowers the resources required to enter and exit the marketplace. Internet-based businesses might be considered fly-by-night as there are fewer assurances for consumers that the retailer will stay in business for some time. In traditional contexts, a consumer's trust has been found to be affected by the seller's investments in physical buildings, facilities, and personnel (Doney and Cannon, 1997). E-tailers thus face a situation in which consumer trust might be expected to be inherently low, and as such certain strategies have to be developed and adopted to increase the level of trust in Internet-based businesses.

THREAT OF CYBER CRIME IN THE FINANCIAL SECTOR

The banking sector environment is especially vulnerable to a wide range of cyber threats. Those in charge of information security have been investing significant resources into the implementation of diverse technologies designed to protect both data and information technology (IT) infrastructure from those threats. All of these investments can serve an important role in safeguarding today's highly IT-dependent financial institutions but, by themselves, they are insufficient. In fact, over-reliance on security technology can put a financial institution at risk because a large percentage of

information security breaches are in reality the outcome of flawed human behaviors, rather than hardware or software weaknesses.

The job of the regulatory agencies in these countries, dealing with developing, enacting, and dictating rules and directions to cover all types of institutions, utilizing all kinds of technology to varying degrees, becomes a challenge. Major trends affecting the security issue in banking and financial institutions in emerging/developing countries are: (1) the increased complexity and coverage of technology; (2) the expansion of the number of financial institutions utilizing cutting-edge technologies; (3) the steady increase in the number of cyber users, especially in conducting financial transactions; and (4) the lack of laws dealing with cyber crimes.

The electronic distribution of retail banking services emerged with the inauguration of automated teller machines (ATMs) by Barclays Bank in 1967 (Ba´tiz-Lazo and Wood, 2002; Ba´tiz-Lazo and Wardley, 2007). A marked proliferation of electronic banking occurred in the 1990s due to the spread of the Internet. It did not take banks long to realize the potential of the Internet as a medium to increase their depth and breadth of services, while at the same time reducing cost. The first bank to adopt online transactions was California-based Wells Fargo in 1995 and the establishment of the first virtual branchless bank, Security First Network Bank, occurred during the same year (DeYoung et al., 2007).

The main driver behind Internet banking is the massive benefits it offers to customers and businesses. A number of studies undertaken by researchers mainly in developed countries (the US, Spain, and Italy) show a positive relationship between banks' financial performance, the adoption of online banking, and the provision of online services (DeYoung et al., 2007; Hernando and Nieto, 2007; Hasan et al., 2005). In addition to the reduction of operational expenses, these studies found that the creation of an alternative distribution channel provides banks with the opportunity to increase their revenues by selling additional fee-based services.

The diffusion of cyber banking is slowed by a number of impediments, mainly security in cyber space. When one considers banking in cyber space, customer trust is absolutely vital and paramount; and, currently, this trust is being focused more and more on technology-centered services. Examples of issues associated with using cyber space to conduct banking/financial activities include, but are not limited to, concern over the hacking of passwords, theft of personally identifiable information (PII), gaining access to a person's bank account number and credit card number, and so on. It has to be emphasized here that in moving forward trust will be about ensuring the customer's investments, data, and identity are protected.

With respect to the state of the regulatory environment, the modus operandi for agencies is playing catch-up at this point. Cyber crime laws and

regulation, especially when it comes to the financial/banking sector, are not moving at the same pace as the technological advancement that has taken place within the past ten years. More and more banking services and transactions are moving away from the physical bricks-and-mortar space to embracing a new business model based on the philosophy of a customer gaining access to and utilizing his or her finances whenever and wherever he or she wants. Mobile banking and in general wireless data transmission appear like a target in the spotlight for cyber criminals. Advancement of Internet and computer technology has made cyber attacks easier for the attackers and worse for the victims. The size, extent, seriousness, and impact of technology-based fraud will continue to grow in the next few years. This will ultimately affect and shake customers' trust.

The threat to banks and financial institutions with online operations from Internet and cyber criminals was underlined in February 2008 when a number of Swedish hackers in the middle of planning an online robbery of a bank were arrested after having failed to steal millions from another bank the previous year. The attack was a reminder of the January 2007 online attack by Russian hackers who broke into a Swedish bank and made away with more than US$1 million through the use of a Trojan horse program; a program that seems genuine but executes some criminal activities when it is run (Krebs, 2008).

In September 2007, Deloitte surveyed 169 worldwide financial institutions on operational security and reported that standard, basic security measures such as encryption, access control, and network security are insufficient at protecting banking and financial institutions' online operations. The survey determined that 27 percent of respondents had become victims of security breaches in their international operations in 2007. Accordingly, foreign banks, especially those in Eastern Europe and Brazil, have applied more technologically based, radical measures to secure their online banking operations; it is indicated that, as a result, almost 100 percent of Brazilian Internet banking depends on secure website protocols and uses two personal identification log-in requirements.

Banks and financial institutions in developing and emerging countries are in need of more support and help when it comes to security and legislation. Security and data/information privacy, the global character of the provision of e-finance services, and entry by non-regulated new intermediaries are challenges faced by the financial regulators and financial services industry. The online environment leaves all the operations of a financial services firm susceptible to external and internal threats. Security of transactions and data privacy are increasingly matters of concern for regulators worldwide. Moreover, such threats can exist internally within the organization. Pre-employment checks and security and continuous education

become all the more pertinent in today's technology-intensive environment in which an employee can e-mail enormous amounts of information in a matter of seconds (Shahrokhi, 2008).

Cyber space has become a 'playing field' for cyber criminals, and it is the financial/banking sector institutions that offer online services to make it safe for consumers to transact online. A recent UK Parliamentary report on e-crime, titled *Personal Internet Security*, states that cyber banking fraud is one of the biggest problem areas of recent years. It also emphasizes that today's cyber criminals are not just lone hackers but belong to highly skillful and specialized organized crime groups (House of Lords, 2008). The UK government report assigns responsibility for fighting online financial fraud unequivocally to the banks and other financial institutions, contesting the point of view that cyber security is the primary responsibility of the user. Although the prevalence and cost of cyber crimes are thought to be enormous, no exact data on these costs exist. Cyber security provider VeriSign alleges that the level of bad traffic caused by cyber criminals (including denial of service (DoS) attacks, e-mail spam, and phishing) is reaching 170 times the basic level of Internet traffic; by 2010 it is predicted to be 500 times the basic level (Hawser, 2007).

Spamming refers to the sending of unsolicited bulk messages to users. Although various techniques exist, the most common is e-mail spam. Cyber criminals send out millions of e-mails to users, often including advertisements for services and/or products with malicious viruses attached to them. The first spam e-mail appeared in 1978, but the frequency and maliciousness of spam have increased dramatically since.[1] Today, e-mail provider organizations report that as many as 85–90 percent of all e-mails are spam. With respect to where spam originates, in 2007 the main sources were the US (19.6 percent of the recorded total), China (8.4 percent), and South Korea (6.5 percent).[2]

Last year (2008) was full of stories of cyber criminal activities all around the world, with hackers, spammers, and phishers causing chaos, and, in some cases, confusion on computer systems and consumers, causing credit and debit fraud numbers to soar. Experts and law enforcement officials worldwide who hunt down cyber crimes state that scams increased in the last half of 2008, as criminals took advantage of economic uncertainty and unease to attack both consumers and businesses. Cyber criminals are sending out false e-mails and putting up bogus websites pretending to be banks, mortgage-service financial institutions, and even government agencies. Mobile phones and Internet-based phone services have also been used to identify and attack victims, with the objective of stealing money or gaining information for identity theft. Cyber offensives on many banks doubled in the last half of 2008 in developed as well as emerging/developing countries

around the world, including Mexico, Taiwan, and Brazil. Although most of these institutions are protected by computer and network security defenses, such as spam filters and fraud-detection systems, that still leaves potentially millions of victims. Until recently, most cyber crimes were dispersed, with spam e-mails sent indiscriminately to thousands of computer users at once. Currently, criminals are beginning to identify specific targets through prior research, a tactic called 'spear phishing'. In these attacks, e-mails are targeting offices of wealthy families or their corporate money managers, for instance. Potential victims and/or their companies are addressed by name, and an e-mail seems to be coming from an associate.

A more recent study, the only one of its kind, by the University of Michigan, shows that 76 percent of online banking websites have at least one design error that could direct users to make what are considered 'bad security decisions'. The Michigan State study of online banking plans in 214 US financial institutions focused on the recurrence of five widespread design flaws that were documented in a previous pilot study. These flaws are not the symbolic software bugs that can be fixed with a patch, but they become apparent in websites that are designed by security experts and developed with the latest security protocols, such as Socket Security Layer (SSL), and can inadvertently make it easy for users to expose sensitive data to cyber criminals. The five reported flaws along with the frequency (in parentheses) of their occurrence are described below:

1. *Content information/security advice on insecure pages (55 percent).* Here the criminal only spoofs or alters the page, substituting bogus numbers for the customer service phone numbers. A cyber criminal might establish a fake customer service number with the dishonest intention of later collecting information from a customer when he/she calls in response to a false message informing the user of the need to reset his/her password, for instance. The user, taking for granted that the information is safeguarded, gives whatever information he/she is asked to supply. The study claims that the main design flaw here is overlooking the well-known security principle of protecting not only the data distribution channel, but also the environment used to create the session keys for the channel.
2. *Presenting secure login options on insecure pages (47 percent).* In this case, a domain name hijacker can impersonate the entire page, while a trusting user might not realize the nonexistence of a secure option, and will not be cognizant of the security risk caused by having protected and unprotected portions on the same page.
3. *E-mailing security-sensitive information insecurely (41 percent).* This is the basis of phishing attacks.

4. *Break in the chain of trust (30 percent).* If a website declares that it is SSL-protected, a user will likely trust its security; but the trust issue can have more understated aspects. Several sites analysed by the Michigan University team started a user's Web navigation off on the right track, but for some transactions the program redirected users to a site with different company names on the URL from the signed security certificate.
5. *Inadequate policies for user IDs and passwords (28 percent).* The most popular IDs are the user's e-mail address and user's Social Security Number (SSN); both present a security risk for the user. E-mail addresses are straightforwardly gathered from the Internet; cyber criminals do this all the time. A US SSN is easy to calculate: each has only nine digits within the range of 0–9. The risk is diminished if users are asked and mandated to change their passwords to more secure ones.[3]

Financial systems do not operate in a void and independently of external and internal environmental factors; instead, their execution and success depend on a suitable enabling environment, whose mechanisms include a sound and effective contractual structure that properly defines and enforces creditor and debtor rights; an efficient information framework, including accounting and auditing standards, and operative measures for debtor and collateral information sharing; satisfactory macroeconomic management, including a sensible fiscal policy, a clear and trustworthy monetary policy, and efficient government bond markets; and effective practical oversight, including a well-functioning safety net. Certainly, it is the enabling environment that is directly affected by policy; given the impact of size and externalities, important elements of financial development may be delayed in smaller economies, relative to bigger, well-established countries at similar levels of economic development (Beck et al., 2008).

TYPES OF CYBER CRIME IN FINANCIAL INSTITUTIONS

Cyber crimes are no longer the work of a teenage hacker creating viruses and worms from his basement; it is a flourishing industry. Now, the US Federal Bureau of Investigation (FBI, 2008) reports that, for the first time ever, revenues from cyber crime have exceeded drug trafficking as the most lucrative illegal global business, estimated at more than US$1 trillion annually in illegal profits; technological advancements in ICT have helped

this to flourish. Sophisticated password-stealing Trojans and keyloggers designed to discreetly sit on a user's computer and send important information and data into remote foreign servers have replaced viruses and worms.

Malware is frequently distributed through malicious links sent via e-mails, directing people to an infected website. Security experts have recently seen a rise in malware attacks on legitimate, but vulnerable website, which stay for a short period of time before they are identified and removed. Usually, the victims are people encouraged to click malicious links by some kind of appealing social engineering tactic sent through e-mail. Some of the widespread tactics consist of malicious eVites or e-cards, and links to websites or videos imitating high-profile events. Chinese cyber criminals have become experts at the art of creating effective social engineering techniques with widely targeted messages using biographical data collected from the various sources. In no time, an infected computer becomes part of a larger network used to distribute malware to other systems.

Cyber criminals are working very hard on finding techniques to evade most traditional security procedures by creating malware that sidesteps the antivirus programs.

The Council of Europe Convention on Cyber Crime of 2001 defines cyber crime in Articles 2–10 on substantive criminal law in four different categories: (1) offenses against the confidentiality, integrity, and availability of computer data and systems; (2) computer-related offenses, (3) content-related offenses; and (4) offenses related to infringements of copyright and related rights.

In many emerging and developing countries, content-related offenses such as copyright infringements, racism, xenophobia, and child pornography may normally not be defined, categorized, and/or understood as cyber crimes. Copyright infringements are based on civil agreements and contracts and are not traditionally criminal offenses; these will very often be enforced through civil remedies due to their many complicated issues. Child pornography has always been classified as criminal.

Massive and coordinated attacks against the information infrastructure of a country are a serious cyber crime. As an example, one can refer to the coordinated cyber attacks against critical information infrastructure in Estonia from 27 April to 18 May 2007. The severity of those attacks increased as time passed; at the start, the attacks were relatively simple Denial of Service (DoS) attacks against government organizations, webservers, and Estonian news portals; then much more sophisticated, massive (use of larger botnets) and coordinated attacks took place. The most serious were the distributed denial of service (DDoS) attacks against some of the critical infrastructure components, against data communication

network backbone routers, and attacks against domain name service (DNS) servers; these led to interruptions in data communication backbone networks. On 10 May 2007, attacks targeted two Estonian banks. For one of them the attack lasted for almost two days and Internet banking services were unavailable for an hour and 30 minutes. For several days, restrictions affected the access of Internet banking services from foreign countries.

The following section covers the most popular types of cyber criminal activities and tools.

Social Engineering

An expanding practice to violate information security that involves social engineering in which victims are tricked into revealing confidential information to perpetrators for illicit financial gains (Mitnick and Simon, 2002). Workman et al. (2008) created a comprehensive model of social engineering factors which were tested empirically. While information security managers must certainly use technology to prevent malevolent interloper or internal users from hacking their way into vulnerable systems, they must also act aggressively to ensure that bank employees do not unintentionally compromise sensitive data.

Phishing

The term 'phishing' is a short form of 'password harvesting fishing' and refers to a particular method of online identity theft. The cyber criminal, usually posing as a financial institution, sends spoof e-mails to a number of possible victims requesting verification or an update of their account details. The link incorporated in the e-mail redirects the recipient to a counterfeit webpage designed by the cyber criminal, which closely replicates that of a legitimate financial institution. Once the account details are disclosed, the cyber criminal will use them fraudulently to enrich himself/herself. It has been estimated that the response rates to this kind of spam e-mail range from 0.5 percent to 4 percent (Bielski, 2004). This fact is disturbing, given the frequency with which the phishing attacks are unleashed. Symantec (2007) reports that in the first half of 2007, its software blocked over 2.3 billion phishing messages. Some of the more complex phishing attacks have proven capable of circumventing complex two-factor authentication systems.[4]

In 2008, the financial services industry saw an increase in the numbers of phishing attacks that is expected to continue in the future, including sophisticated spear phishing (aimed at a specific company) and rock phish (multiple domain) attacks. The Anti-Phishing Working Group

reports that the financial services sector continues to be the most affected sector; with more than 90 percent of attacks being directed at financial services. Further, one area of growth for phishing attacks is 'smishing' or SMS (short messaging system) phishing, where phishing messages are sent over cell phones via text messages. This will cause confusion among online banking users, especially those using mobile banking services. This type of attack will pose credibility and trust issues, and will impact banks with mobile banking services, especially as more and more customers use these services. Phishing goes through a life cycle; the Financial Services Technology Consortium (FSTC) describes this cycle as a process consisting of six stages, namely Planning, Setup, Attack, Collection, Fraud, and Post-Attack (Wetzel, 2005).

Gartner estimated that 2 million people had been enticed to release their sensitive information (Ollman, 2004). Another emerging trend is phishing attacks via Internet Relay Chat. An effective method for deterring such phishing attacks is to adopt authentication of incoming e-mails. Mechanisms such as Sender Policy Framework, DomainKey, and SenderID have been suggested for providing authentication; making use of alias e-mail addresses is also useful for minimizing the consequences.

Another channel of phishing attacks is via bogus websites. In this case, phishers first build a website which looks very similar to that of a trusted third party and then invite the general public to log on to the bogus site by giving away confidential information for verification. In order to combat this attack, it is important to ensure that the digital server certificate exists for the site that is being visited. Measures such as trusted path-ensured browsers are also useful to deter such phishing attacks (Dhamija et al., 2005). After obtaining users' confidential information such as user name and password from an online banking website, phishers commit identity theft by impersonating the victim at the website of the bank they mimic. Two-factor authentication in the form of a hardware security token, one-time password, and digital certificate, and zero knowledge proof are effective in deterring identity thefts.

Spyware

Spyware is considered one of the most dangerous threats to Internet users since spam, yet most users do not even know spyware is on their personal computers. Spyware makes its way into the computer without the user's knowledge and steals the information as if it were a spy. A user can unsuspectingly install it even if he or she observes normal computer usage. Some kinds of spyware are benign but some are viciously planned to steal specific information.

Spyware categories are varied; the first category is related to advertising displays, where installed modules display ads by various means to the computer user. They show ads that are embedded with code to automatically redirect users to a different webpage or install software on a user's computer without their knowledge. The latest scheme is referred to as 'cookie surfing', where a window pops up at off-screen coordinates so it is not visible to the user; this is embedded with a code designed to intercept clicks on the advert to redirect the user to purchase the advertised item through alternate channels (Edelman, 2006).

The next category is automatic download software, which requires no interaction with the user. These 'Driveby download' programs are installed without the user's knowledge or consent, either by a compromised webpage or malware placed on the system by other means. Trojan droppers are intended to drop on to a system, unpack and install Trojans and other executables, and then delete themselves (Anti-Spyware Coalition, 2006).

The third type of spyware is the autonomous ones. These are programs run outside of the browser that are activated at system startup with the security access rights of the current user. They may operate as remote control programs, keyloggers, e-mail, packet sniffers, and more. These programs may modify operating system settings, files, or functionality. Some modules also disable protective software such as anti-virus/spyware programs (Hackworth, 2005).

The fourth group of spyware is browser hijackers; these are modules that change Web browser settings and affect browsing activities. This type of program changes browser security settings to compromise security and redirects users when they attempt to visit certain sites. Some modules even change user Internet connection preferences (Hackworth, 2005).

Keyloggers record the sentences and commands that the user inputs into the computer. There have been an increasing number of cases where this software is used to steal personal information, including the user's name, account number, PIN, and e-mail address. These programs record users' keystrokes, including passwords, personal data (name, address, ID no.), and financial information (bank accounts, credit card numbers) to send to an external server. The personal information may be used directly by the person who collected it, for purposes such as identity theft, or sold to information brokers for widespread use (Edelman, 2006).

Another group of spyware falls under the category of tracking software. The spyware distributor, or an agent, uses third-party cookies or other means to keep track of a user's Web browsing behavior and page visits. Tracking software may also record keystrokes, perform 'screen scrapes', and harvest passwords and personal information to send to an external server (Edelman, 2006).

ATM Frauds

There are a number of frauds associated with Automatic Teller Machines; these include skimming, peeping at an ATM, and having an imposter at an ATM. Skimming is a scam where the magnetic data on the cash card or credit card are illicitly read stealthily in order to make a counterfeit copy of the card. This does not steal the card itself but only the information; in most cases, the victim does not notice it until cash is withdrawn from his/her account. Criminals install a skimming device to the ATM which electronically records the customer's debit card number and a small camera in the device video records the ATM keyboard as the customer enters his or her password. The criminals then download the information to a computer and send it to an e-mail account, most probably in one of the black market areas; the fraudsters then receive an e-mail in return attaching a list of bank debit card numbers and passwords. It is expected that until financial institutions and credit card companies roll out either a contact or contactless-based smart card infrastructure, there won't be a great reduction in the amount of fraud being perpetrated against consumers (Bruene, 2009).

Peeping, also called 'shoulder surfing', involves cases where the user's PIN is stolen by peeping from behind the ATM; this crime is on the rise. There are even cases where a camera is secretly placed on the ATM.

With the imposter ATM scam, the fraudster impersonates a bank clerk or guard to deceive a customer using an ATM. Typical cases are where the imposter pretends to help an elderly user operate an ATM, and asks for the PIN.

The organization and sophistication of criminals are increasing, and so is the sophistication of their attacks. A focused approach targeting precision attacks on an institution's customers is the new scheme cyber criminals have adopted. Cyber criminal groups are compiling huge amounts of data in order to get consumers to share account information with them. This allows them to entice those customers to 'give up the goods' by divulging enough information so they feel comfortable with the scam.

Denial of Service

Another especially painful crime to online banking/financial institutions is the denial of service, or distributed denial of service attack. The architect of the attack directs a large number of computers to concurrently send communications to a bank's Web server. This floods the server with so much traffic that it cannot fulfill its legitimate user requests. The site becomes inaccessible to customers, shutting down the business. This can be very expensive in the banking/financial industry. A downed brokerage

firm can lose US$6.4 million per hour (Johnson-Edwards, 2005). Smaller financial institutions are actually more susceptible to these kinds of attacks, especially, 'pure click' ones. Online gaming sites present a well-known example of main DDoS targets. What is interesting to note here is that when targeted, most of these entities are reluctant to contact law enforcement, even those based in countries (unlike the US) where online gambling is legal, fearing a tarnished reputation.

Cryptovirology

This is a type of cyber extortion, whereby a ransom-ware program such as Trogan.Pgpcoder searches an infected financial institution system's hard drive and encrypts all common file types (.db2, .doc, .htm, .txt, .xls) on the system. It then leaves a text message instructing the institution how to contact the hacker to buy the key to unlock them (*PC Magazine*, 2005). The idea of cryptovirology, offensive encryption, is not something new.

Insider Threat

This is one of the most dangerous and often ignored threats that financial institutions are going to face in the coming years. During economic downturns, employees are going to be more tempted to steal inside data, to sell it or use it for their own purposes. The insider threat will be more widespread where there is more despondent players around badly secured data and information. Appropriate checks and balances of all employees, suppliers, and contractors will help reduce this threat, but as seen in the most publicized cases recently, such as the US$7.2 billion in fraudulent trades at the French bank Societe Generale, action by a tenacious insider is one of the toughest types to prevent.

Threats by insiders are real and not so uncommon; a survey conducted by the United States Secret Service, the CERT Coordination Center (CERT/CC), and CSO magazine found that in cases where respondents could identify the perpetrator of an electronic crime, 20 percent were committed by insiders. The losses from crimes and security breaches conducted by insiders can be substantial because these people know exactly what to look for and where to look to obtain access to the financial accounts or intellectual property, and how to evade existing security measures. CERT has documented several cases where the costs, both tangible and intangible, were quite high. In one case, a technical employee of a defense contractor wrote a logic bomb that resulted in US$10 million in losses and the layoff of 80 employees. CERT/CC has published a report called 'Commonsense Guide to Prevention and Detection of Insider Threats' (cert.org 2008).

The information is based on the analysis of more than 150 known cases of malicious insider activities, how they were executed, and what could have helped to prevent them. It also contains trends and patterns in the various malicious activities, which fall into categories including insider IT sabotage, fraud, and theft of confidential or proprietary information.

Contractors and consultants pose equal risk to security of banking/financial institutions. Failing to recognize this security threat has already had serious consequences for many organizations, especially in light of two major business trends – outsourcing and remote connectivity. Outsourcing key corporate functions to low-cost providers and employee access to corporate resources from around the globe have decreased costs and increased efficiency. However, they have also led to the transmission and storage of sensitive data beyond the corporate firewall, extending the security perimeter to places beyond an organization's control.

Insiders constitute a permanent threat; they have access to data, information, and systems and they know how the system and its security work. Most bank thieves and large-scale corporate frauds, and many of the most notorious and impressive criminal attacks, involve insiders. Insiders are especially pernicious attackers because they are trusted. They have access because they are supposed to have access. They have opportunity, and an understanding of the system, because they use it – or they designed, built, or installed it. They are already inside the security system, making them much harder to defend against. In offices, employees are trusted people given access to facilities and resources, and allowed to act – sometimes broadly, sometimes narrowly – in the company's name. In stores, employees are allowed access to the back room and the cash register; and customers are trusted to walk into the store and touch the merchandise. Banks and financial institutions could not operate without trusted people. Replacing trusted people with computers does not make the problem go away; it just moves it around and makes it even more complex. The computer, software, and network designers, implementers, coders, installers, maintainers, and so on are all trusted people.

Identity Theft

Koops and Leenes (2006) were the first to coin the term 'identity-related crime'. As they defined it, this term embraces all criminal activities having identity as a target or a principal tool, and liable to be punished by law. However, there is no common, universally accepted definition of identity-related cyber crime, as it frequently includes many forms and kinds of crime such as identity fraud, identity theft, intellectual property abuse, or other related crimes (UNODC, 2007a, 2007b, 2008a, 2008b).

The 2008 Kroll Report (krollfraudsolutions.com 2008) claims that up until October 2008, victims of identity theft were affected by four of the five most common techniques; these involve opening new credit card accounts, using existing ones, opening new deposit accounts, and obtaining loans. In the past in the United States, financial institutions have offered assistance to victims but, with the new federal 'Red Flags Rule', proposed in 2006, the financial institution must establish a written identity theft program with policies and procedures to protect the customer and the bank. This rule requires financial institutions to verify the identity of those opening new accounts. They will also have to establish a list of 'red flags' to catch conditions that might indicate or facilitate identity theft. Staff have to be trained to implement the Red Flags program. For credit and debit card issuers, policies have to be put in place to monitor and validate change-of-address requests and requests for additional cards.

Identity theft is the fastest-growing crime in the United States, affecting more than 55 million adults since 2000 and 8 million-plus in 2007 alone. Today data and information are the lifeblood of any firm or governmental agency, and as such must be protected, especially PII. Information classified as PII includes, but is not limited to: (1) full name; (2) national ID card; (3) credit card number; (4) telephone number; (5) address; (6) e-mail; (7) financial account number; and (8) face and fingerprint information. All of this is information which can help a criminal or someone malicious to identify a person when it is compiled together.

The world is seeing a steep rise in the incidence of identity thefts of all types, including phishing, pharming, and theft of corporate identity; in addition, one notices a rise in traditional fraud schemes, such as theft by employees, the use of fictitious prime bank instruments to deceive investors, and so on. The total number of data breaches in 2008 exceeded those reported in 2007 (ITRC, 2008). In 2007, 656 breaches were reported, as at the end of 2006; as of August 2008, the data breach total stood at 449, the report by the ITRC states, adding that more incidents are either unreported or under-reported. In the United States, for instance, only three common states publish such information. In addition, there has been a steep increase in the frequency and volume of major data breaches. The Bank of New York Mellon Corp., for instance, admitted that a recent security breach involved 12.5 million customers, instead of the 4.5 million it had originally announced had been affected. In another incident in February 2008, it lost a box of six to ten unencrypted backup tapes containing customer names, addresses, birth dates, and Social Security numbers while they were being transferred.

Identity theft rose by nearly 25 percent in 2008 in the United States, according to *The 2009 Identity Fraud Survey Report* by Javelin Strategy

& Research (2009). The report shows that the number of identity fraud victims increased 22 percent to 10 million people, at a total cost of US$48 billion. With the tough economy, cyber criminals have become more desperate, and identity theft in the financial services industry has gone up at an increasing rate (McGlasson, 2009). The report shows that because of identity fraud, 15 percent of all customers leave their credit card provider, 17 percent leave their current bank or credit union, and 40 percent of people defrauded through a debit card look for other providers.

Identity-related cyber crime is on the rise, both in developed and developing countries. The twenty-first century has witnessed a surge of identity-related cyber crimes which left tens of millions of victims around the world. Identity-related cyber crimes are carried out with ease when compared with identity-related crimes in the bricks-and-mortar space (Smith, 2007); further, the negative consequences of identity-related cyber crime are much more damaging. The global disposition of criminal cyber activities and their connections to other criminal activities, such as fraud and money laundering, were described by UNODC as the crime of the twenty-first century (UNODC, 2008a: para. 30). The most popular method of identity-related crimes is phishing, based on the use of social engineering and malware; this can take place through 'pharming', where crimeware is used to direct users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning; 'SMiShing', through the use of short messaging system (SMS) in cell phones; or 'ViShing', through the use of voiceover protocol (Acoca, 2008).

There are no systematic data and statistics on the incidence of identity theft; with the exception of the United States, international statistics on identity-related cyber crime are not systematically collected, analysed, or published. Countries like Australia and the United Kingdom have recently developed various reports on identity theft, which provide base-level statistics, but not on identity-related cyber crime. As with respect to emerging/developing countries, this kind of statistic does not exist. The efforts of the UNODC core group of experts on identity-related crime (UNODC, 2008b) are laudable and it has to further specifically look into identity-related cyber crime and provide solutions for its prevention and the protection of victims.

It is essential that law enforcement agencies, businesses, consumers, and legislators understand the causes of data breaches, so they can be dealt with and the occurrence of these incidents minimized. It is only when one understands how data are exposed or stolen that one can avert further breaches through improved security procedures and safer information handling.

Lost laptops and other digital media containing consumer data lead

to 21 percent of data breaches, and 14 percent of breaches involve the accidental publishing of sensitive consumer data. Because these are accidental occurrences, they are difficult to prevent; however, banks can help minimize the likelihood with employee education (Morrow, 2008). In the United States, for instance, customer data theft by company employees accounts for 15.6 percent of data breaches; and approximately two million identity thieves are hired every year using stolen credentials because of poor background screening processes (Morrow, 2008).

The problem is not so much recognizing the nature and severity of the problem caused by cyber-facilitated frauds of all kinds, but understanding just what to do to protect ourselves from them. Given the state of economic uncertainty in the world, identity theft does not seem to be a policing priority for most countries; there are insufficient numbers of trained personnel and specialists to deal with the amounts of fraud reported; consequently, a large number of reports dealing with identity theft go uninvestigated. In addition, some of the major frauds committed by employees and businesses go unreported or under-reported.

With the growth of online business, it has become common for users to disclose financial and personal information about themselves on websites that let other users identify them. In many cases, this information is used to target advertisements and promotions directly to users. The increased reach and richness of information collection has led to increased levels of fraud, identity theft, spam e-mail, and junk faxes. The good news, though, is that the increase of international criminal activity in the form of identity theft and the like has been followed by an increase in court cases and judgments facilitated by the cooperation of international law enforcement agencies led by the United States. The face of cyber crime is global; in 2008, for instance, members of an international organized crime group operating a 'phishing' scheme in the United States, Canada, Pakistan, Portugal, and Romania obtained private information to use in a credit card fraud. Among the financial institutions affected were Citibank, Capital One, JPMorgan Chase, Comerica Bank, Wells Fargo, eBay, and PayPal. In another incident, hackers were arrested for infiltrating cash register terminals at Dave & Buster's restaurants in the United States to acquire credit card information, which was resold to others for criminal purposes. The hackers were prosecuted with the cooperation of the Turkish and German governments. A third case involves a Nigerian who installed a spyware program on a NASA employee's computer to capture personal data, such as bank account numbers, Social Security number, driver's license information, home address, and passwords to various computer accounts, as well as to intercept private electronic communications. Another incident involves a global criminal ring who smuggled counterfeit luxury goods

into the United States from the People's Republic of China. Valued at more than US$100 million, the counterfeit handbags, wallets, purses, and carry-on bags were labeled with such 'name' brands as Nike, Burberry, Chanel, Polo Ralph Lauren, and Baby Phat. The defendants paid more than US$500,000 in bribes to an undercover agent.

Operation Phony Pharm investigated the illegal sale of anabolic steroids, human growth hormone, and other controlled substances over the Internet. Raw materials imported from China and manufactured in US, Canadian, and Mexican underground laboratories were distributed through a MySpace profile and a website. Collaboration with Operation Raw Deal has resulted in the seizure of 56 steroid labs across the United States. The US operation took place in conjunction with enforcement operations in Mexico, Canada, China, Belgium, Australia, Germany, Denmark, Sweden, and Thailand.[5]

Three surveys will be mentioned here (Morrow, 2008); the first is the empirical research conducted by the US Computer Emergency Response Team, which estimates that almost 40 percent of IT security breaches are carried out by people inside a company; perhaps the most common way for attackers to gain access to a network is by exploiting the trusting nature of employees. You can have the best technical system in place, but it is not effective if people aren't educated about the risks. The second is a more recent survey conducted by Deloitte, which found that 75 percent of companies have not trained their staff in the risks of information leakage or social engineering. And the third is based on research conducted by the Identity Theft Resource Center, which found that during the first seven months of 2008, the number of data breaches grew by 68 percent versus the same period in 2007. The same study acknowledges that some incidents are under-reported and multiple breaches are sometimes reported as a single event. The research shows that breaches are becoming more technology based; during 2008, electronic data breaches accounted for 81 percent of the total, versus 19 percent which were considered paper breaches. The good news is that there is increased awareness of identity theft among people, so opening fraudulent accounts with other people's information is becoming increasingly difficult. The bad news is that because of this increased awareness, more fraudsters take over accounts instead of trying to open new ones.

All of these studies confirm that our biggest threat is not from the outside; it is from within and we need to look no further than the recent event at Societe Generale to highlight the severity of this threat and its implications when lax security and poor password management gaps are exposed. In the case of Societe Generale, the second largest bank in France, you have the case of a trusted employee of six years who combined

the theft of his coworkers' passwords with his knowledge of the bank system to perpetuate 7 billion dollars worth of fraud. However, Societe Generale is not alone; many stories are published in the press, as the three recent studies cited earlier indicate.

Another survey conducted in early 2008 by Websense.com (2009) found that more than 75 percent of UK workers using PCs at work admit copying data on to mobile devices at least once a week. The advice here is to use software to specify policies on what devices can be connected to the corporate network and what data can be downloaded. This should be enforced by the company and employees should be educated about why the policies are in place – or they will simply find a way to work around them. You can advise what we call an 'Acceptable Use Policy' which spells out employees' responsibility for network security, ensure it is signed by everyone, and that employees fully understand the risks and their responsibilities.

In February 2008, McAfee, Inc. reported on findings from the first global study on the security of information economies.[6] The study analysed responses from more than 800 chief information officers (CIOs) in the United States, the United Kingdom, Germany, Japan, China, India, Brazil, and Dubai; questions in the survey dealt with important information such as sources of intellectual property, where it is stored globally, and how it is transferred and misplaced. The companies surveyed estimated that they lost a combined US$4.6 billion worth of intellectual property in 2007 alone, and spent approximately US$600 million repairing damage from data breaches. Based on these numbers, McAfee projects that companies worldwide lost more than US$1 trillion in 2008.

This study is a wake-up call, especially in the existing environment of the current economic crisis; this will possibly lead to a global meltdown in vital information. Increased pressures on firms to cut costs and reduce staffing, especially in the information/computer security area, have led to an increased opportunity for crime caused by weak security measures. The study calls for a corporate cultural change whereby companies would start looking at information security as a business enabler not as a cost center. The study further suggests that the ability to safely store data and information in the form of intellectual property is a key driver of security investment in Brazil, Japan, and China. The study reports that 60 percent of Chinese survey participants cited 'safer storage' as a reason for storing intellectual property and other sensitive information outside of their own country.

The study sheds light on the impact of the current financial crisis on the state of securing intellectual property. Businesses are evidently concerned about the global financial crisis and its effect on the security of critical information such as intellectual property. The McAfee study reports that

39 percent of respondents surveyed consider their intellectual property to be at risk given the current economic conditions.

The study also evaluated the commitment of the various countries to protecting critical information; the results suggest that emerging and developing countries are more enthused about protecting their valuable new wealth, as demonstrated by the money spent on protecting their intellectual property, than their Western counterparts. Results show that Brazil, China, and India spent more money on security than Germany, the UK, US, and Japan, combined.

It is becoming evident to executives and policy makers around the world that intellectual property is an emerging target for cyber criminals, as evidenced by the increased number of attacks by what are being referred to as cyber mafia gangs. One trend shows that phishing techniques are becoming more and more sophisticated. Another trend highlights the danger of insiders and shows that employees steal intellectual property for the purpose of financial gain and to improve their competitive advantage. A mounting number of employees, many executives believe; 42 percent of those who responded to the McAfee survey believe displaced employees constitute the principal threat to critical information. In addition, it appears that China, Pakistan, and Russia are still the main source of cyber threats for various legal, cultural, and economic reasons.

BASES FOR TRUST BUILDING

Some bases for trust building identified in the relevant literature are reviewed in the following section. Competence (Blomqvist, 1997) is believed to be a basic and profound source of trust in asymmetric technology partnerships. Competence may be divided into technological, economic, and partnering competencies. It may be evaluated as a soundness of organizational strategy and vision of management. Ability to perform and reputation for partnering are aspects of organizational competence as well. At the individual level competence is signaled in professionalism, capability to carry through, realistic judgment of a situation, and interpersonal skills. Already at the very first meetings the professionalism of the counterpart is evaluated. Self-reference and double-contingent relationships mean that parties are able to refer to themselves and their competencies as actors of the system and dependent on other actors. Organizational and personal self-reference describe the actor's ability to define her/himself, and appreciate, evaluate, and communicate the complementary needs to other actors. A large company with strong NIH ('not invented here') may not be able to appreciate complementary knowledge and resources. At an individual level the ability to tolerate dissimilarity

is needed in order to be able to enjoy the benefits of complementary (by definition dissimilar) actors. Equity (Das and Teng, 1998) is a profound base for cooperation. Open dialogue based on equity characterizes double-contingency relationships. Reciprocity is a vital manifestation for the development of trust. At organizational and inter-organizational levels it may be enhanced through norms and values promoting reciprocity. Shared values promote synergistic social behaviors and organization-specific investments (Jones and George, 1998). Shared values and subsequent trust also increase a person's will to stretch his/her roles in the organization. Resulting high personal involvement promotes joint effort. Identification with a group increases expectations that others will reciprocate (Tyler and Kramer, 1996). Social and character similarity breeds trust (Creed and Miles, 1996; Ladegard, 1997). Social similarity may be based on character, education, competence, and personality at the individual level. At the organizational level character similarity may be characterized by compatible organizational culture and values. In asymmetric partnerships, both personal and organizational dissimilarity may exist and cause inertia. Social dissimilarity in asymmetric partnerships may be managed with boundary-spanners able to cope with both worlds. Socialization and shared meaning (Zucker, 1986) create trust. Shared experiences and interaction at an individual level may enhance socialization. Building a wide interface and promoting partner visits may also enhance socialization.

Managerial philosophy reflects an attitude toward economic life, which becomes visual via consistency of management behavior and organizational norms of, for example, honesty, openness, and keeping promises. It actualizes in management behavior, which should be reflected very carefully in respect to its impact upon inter-organizational trust. At the individual level the propensity to trust involves the ability to accept risk and delegate as well as the will to communicate feelings and expectations openly. Organizational culture and values can be seen in consistency of organizational behavior, decisions, and values. Personal values are realized in attitudes and emotions and finalized in made choices. In management philosophy trustworthiness may be experienced at both cognitive (rational) levels of trust such as competence, fairness, or openness, and in affective (emotional) levels of experienced trust such as care and concern (see O'Brien, 1995).

Converging goals set jointly create trust and commitment (Das and Teng, 1998). Organizational structures may be quite difficult for partners to identify and understand. In volatile industries like telecoms organizations are in the middle of a change and development process, which is reflected in organizational structures. Some aspects of this change may be communicated without losing too-sensitive information. Organizational

structure and roles refer to the clarity and visibility of organizational structures to external parties and the authority of organizational actors to enact their roles. At the individual level role clarity brings predictability and role stretching creates a feeling of adjustment to needs. In order to create the sufficient feeling of openness and security necessary for trust to develop, the roles and relevant authority of large firm boundary-spanners should be made clear to potential partners.

Information and communication are perhaps the most common and in theory easy to manage sources of trust. However, in everyday life much distrust is created due to inappropriate communication of issues, feelings, intentions, and opinions. As argued by Zucker (1986), production of trust rests on a common base of knowledge, which increases the predictability of partner behavior through shared meanings. Relevant information should be given promptly and frequently (O'Brien, 1995) and also some negative aspects should be revealed. In addition to fact-based information, information on feelings, intentions, and opinions should also be communicated. In successful communication, building trust and creating knowledge, all these different types of information exist. Sydow (1998) refers to multiplexity of network relations, meaning that organizational actors transact for a variety of reasons and exchange different contents, that is, information and emotion. If a communicator is able to be clear and precise on an issue and simultaneously add and develop the dialogue, she/he is bound to develop a trusting relationship. Communication skills are especially important when natural socialization does not enhance trust building because asymmetric technology partners are working separately and in different contexts or cultures. Concern (O'Brien, 1995) shows care and is an emotional basis for trust. If this is shown honestly in the form of proactive information, advice, and social support, it may be a strong building block to trust. Openness and concern may be possible to the extent of not revealing proprietary information. Parties may be quite frank about their internal competencies and weaknesses (challenges). Informing of delays in schedules shows concern for the resource-constrained small party. In line with the above presented idea of organizational boundary-spanners with knowledge of both worlds, Zucker (1986) states the need to assign a 'translator' in order to gain access to highly specialized or idiosyncratic knowledge. Security and stability (Creed and Miles, 1996) create trust. Thus communicating clear organizational roles and repeated contacts create trust through security. Individual boundary-spanners and organizational principles should converge in order to meet the expectations set for the organization (Sydow, 1998) Changes are evident but informing the other party of possible changes in advance will show concern and subsequently enhance security and reliability.

Learning of mutual competencies and differences is bound to lessen the negatively experienced dissimilarity and thus increase mutual understanding. Understanding enhances the ability to take the role of the other, an important source of trust creation (Jones and George, 1998). Thus trust could be enhanced by increasing education to accept diversity and by stressing the perceived similarities. Asymmetric partners may organize inter-firm workshops and seminars, where both parties present and work in teams. Informal settings may also increase understanding if partners are seen in a different light. Asymmetric partnering may be easier if partners have had personal experience (Creed and Miles, 1996) of the other context, for example, an entrepreneur had previously worked in a large firm (Blomqvist, 1999). Inter-firm adaptation (Das and Teng, 1998) is a sign of commitment, enhancing trust. Adaptation may be quite unusual in the large party of an asymmetric partnership. Transfer of key personnel could increase the motivation for adaptation and potentially enables some consideration for learning and best practices. Commitment is a concrete base for trust. Commitment may materialize in the relation-specific investments, for example, time and sense of urgency, of the key boundary-spanners and management. Reputation (Zucker, 1986; Creed and Miles, 1996) is a focal source for trust both at organizational and at personal level. A reputation of a third party, that is, intermediaries, may be used for trust building (Zucker, 1986; Sydow, 1998). Internal norms, incentives, and threat of punishment may help to manage reputation.

NATIONAL CULTURE AND TRUST

Another antecedent of trust may be the cultural background of a consumer. Societal membership socializes people early in life into a national culture with a set of values. These values influence what information is processed and found credible. In consumer behavior, cultural values have been shown to affect consumers' motives, attitudes toward choices, intentions, and behavior although there is a scarcity of empirical research on cross-cultural consumer behavior (McCort and Malhotra, 1993).

One dimension of culture is individualism–collectivism. Hofstede (1980) found this dimension to have the strongest variation across cultures. In individualistic cultures, individuals take precedence over the group's cultures, needs, values, and goals. In collectivistic cultures, the needs, values, and goals of the group take precedence over those of the individual. Those high on the individualism scale are characterized as self-reliant, competitive, trusting of others, and focused on utilitarian views of exchange and competence. Because of the utilitarian view, others are trusted if the

circumstances suggest that it is in the other's own interest to behave well. Individualism also promotes a trusting stance; one gets better outcomes assuming that others are reliable. Hence, individualists are much more likely to trust others until they are given some reason not to trust. By contrast, those high on collectivism are more likely to base their trust on relationships with first-hand knowledge. Because of the emphasis on social relatedness and interdependence, collectivists are sensitive to the ingroup–outgroup boundary. Members of collectivist cultures are less likely to trust someone who is not part of their ingroup (Yamagishi and Yamagishi, 1994).

Some errors stemming from subtle language and cultural standards have become classic examples that are regularly used in training international businesspersons. General Motors could not understand why its Chevrolet Nova model was not selling well in Latin America until someone pointed out that *no va* means 'it will not go' in Spanish. Pepsi's 'come alive' advertising campaign fizzled in China because its message came across as 'Pepsi brings your ancestors back from their graves'. Another company sold baby food in jars adorned with the picture of a very cute baby. The jars sold well everywhere they had been introduced, except in parts of Africa. The mystery was solved when the manufacturer learned that food containers in those parts of Africa always carry a picture of their contents.

The cultural overtones of simple design decisions can be dramatic. In India, for example, it is inappropriate to use the image of a cow in a cartoon or other comical setting. Potential customers in Muslim countries can be offended by an image that shows human arms or legs uncovered. Even colors or webpage design elements can be troublesome. A webpage that is divided into four segments or that includes large white elements can be offensive to a Japanese visitor. Both the number four and the color white are symbols of death in that culture. Softbank, a major Japanese firm that invests in Internet companies, has devised a way to introduce cyber space to a reluctant Japanese population. The Japanese have resisted the US version of electronic commerce because they prefer to pay in cash or by cash transfer instead of by credit card, and they have a high level of apprehension about doing business online. In 1999, Softbank created a joint venture with 7-Eleven, Yahoo! Japan, and Tohan (a major Japanese book distributor) to sell books and CDs on the Web. This new venture, called eS-Books, allows customers to order items on the Internet, and then pick them up and pay for them in cash at the local 7-Eleven convenience store. By adding an intermediary – the exact opposite of the strategy used by US firms – that satisfies the needs of the Japanese customer, Softbank plans to bring Internet-based commerce to Japan.

Some parts of the world have cultural environments that are extremely

inhospitable to cyber activities initiatives. For example, a report issued in 1999 by Human Rights Watch stated that many countries in the Middle East and North Africa have been reluctant to allow their citizens free access to the Internet. The report notes that many governments in this part of the world regularly prevent free expression by their people and have taken specific steps to prevent the exchange of information outside of state controls. Saudi Arabia and Yemen, for instance, use proxy servers to filter content. Jordan has imposed taxes that put the cost of Internet access beyond the means of most Jordanians. Jordan also passed a 1998 law that prohibited publications in any media that conflict with the values of an Islamic nation.

In contrast, Algeria, Morocco, and the Palestinian Authority have not limited online access or content. In most North African and Middle Eastern countries, officials have publicly denounced the Internet for carrying materials that are sexually explicit, anti Islam, and that cast doubts on the traditional role of women in their societies. In many of these countries, Internet technology is so at odds with existing traditions, cultures, and laws that electronic commerce is unlikely to exist there at any significant level in the near future.

Some countries, although they do not entirely ban cyber activities, have strong cultural requirements that have found their way into the legal codes that govern business conduct. In France, an advertisement for a product or service must be in French. Thus, a business in the United States that advertises its products on the Web and that is willing to ship goods to France must provide a French version of its pages. Many US electronic commerce sites include in their webpages a list of the countries from which they will accept orders through their websites. By limiting sales in this way, these companies hope to limit their exposure to legal liability in the excluded countries.

TRUSTWORTHINESS: COULD IT BE DEMONSTRATED?

'It has been suggested that trust is one of the states that appear to have the property that they can only come about as the by-product of actions undertaken for other reasons. They can never, that is, be brought about intelligently or intentionally, because the very attempt to do so precludes the state one is trying to bring about' (Elster, 1983: 43). It may be possible though to prove one's reliability – which is sometimes a first step toward gaining another's trust. At a less philosophical level there is also the practical issue that the person who tries too hard to demonstrate their

trustworthiness often produces the opposite effect to that which they intended! Luhman has commented on the difficulty of convincing another that one is trustworthy, stating that where participants can infer that a process is being employed in order to build up trust 'motives are unavoidably put in question, and such questioning can easily turn into mistrust' (Luhman, 1979: 43).

The global context of the Internet further challenges engendering trust in a consumer. From traditional marketing contexts, it is learned that consumer trust is most readily developed when the consumer has a positive trusting stance in general, has had prior interactions with the merchant, interacts with a knowledgeable salesperson with similar or familiar background, is protected by strong social and legal structures, and expects to be patronizing the merchant for a prolonged period. When consumers are scattered around the world, these sources of trust are not readily available for the merchant to harness.

Moreover, the fundamental bases of trust might vary across nationalities. Those consumers coming from individualistic countries might have a higher trusting stance in general and be more willing to base their trust in the merchant on factors that are inferred from an impersonal website than consumers from collectivistic countries. Dawar et al. (1996) found that personal and impersonal sources of information had different impacts on individuals across cultures.

Jarvenpaa et al. (1999) developed and tested a theoretical model about the antecedents and consequences of trust in an Internet store. The model suggests that customers' evaluations of stores' reputation and size affect their trust in the store. In addition, Jarvenpaa et al. found that the degree to which consumers trust a Web store affects their perceptions of the risk involved in purchasing from the store and their attitudes toward the store. The study that Jarvenpaa et al. (1999) carried out in Australia was replicated in Israel and partially replicated in Finland. The replications enabled the authors to test for cross-cultural differences, and at the same time to assess the validity of the model across national borders.

However, it is possible to take actions to create the context within which trustworthiness might be perceived, and trustworthiness, regarding a particular issue, is more likely to be perceived in contexts where those involved demonstrate the capability of being able to fulfill a promise that is, of acting in a trustworthy manner. As Dasgupta (1988: 50–51) states, 'you do not trust a person (or an agency) to do something merely because he says he will do it. You trust him only because, knowing what you know of his disposition, his available options and their consequences, his ability and so forth, you expect that he will choose to do it'. So for a supplier the provision of evidence of those capabilities and competencies which its

customers believe to be relevant is both a demonstration of its commitment and a prerequisite to its being regarded as trustworthy.

Clearly the problems in providing such evidence vary a great deal: it is easier for a manufacturer of standard items to provide evidence that it is trustworthy regarding quality than for a firm specializing in customized products. In the case of service industries such evidence is even more difficult to provide and can seldom be more than evidence that quality control procedures are in place and are rigorously implemented. However, it is beneficial to stress again that the more customized the product is the greater the problem will be. Given that most people do not extend blanket trust to others then if someone wishes to demonstrate their reliability and/or trustworthiness it follows that – perhaps particularly in the early stages of a relationship – an important question is with which elements of behavior they should first try to demonstrate their trustworthiness. Being willing to make a promise or to enter into a contract is one way in which a firm can demonstrate to others its confidence in its own competence and reliability with regard to quite specific activities. So a firm may promise or enter into a contract to act in a certain way, believing that those who know of this action can be reasonably expected to rely upon them to fulfill their obligation.

A contract seldom states precisely what discretion the other party has and a person can, if they wish, make the operation of most contracts a near impossibility simply by working to contract (or, to use the industrial relations term, 'working to rule'). Where a contract does not or cannot fully specify the nature of a relationship between two parties then some trust will be necessary to make the relationship 'workable' and it is recognized that 'trust seems essential to commercial transactions that are not fully controlled by either legal constraints of contracts or the economic forces of markets' (Oakes, 1990: 674.) Baier states that 'Promises are a most ingenious social invention, and trust in those who have given us promises is a complex and sophisticated moral achievement' (Baier, 1986: 246). Promises, Baier suggests, enable us to trust with minimal vulnerability and promises and contracts are both an artificially contrived and secured case of mutual trust. However, the difference between contracts and promises is subtle given that some, but not all, promises are regarded as legally binding and only some contracts are considered to be legally enforceable. Contracts, though, have, given the legal system's ability to impose penalties for breach of contract (including those promises which are interpreted as being legally binding), a distinctive authority. The value of a promise is that the promising entity subjects 'himself to the penalty of never being trusted again in case of failure' (Hume, [1740] 1969: 574) by those who know of the incident. Consequently those who break promises may never

again have normal open relations with those people who accepted their promises and they will have to incur the costs of setting up and monitoring contracts in future dealings. In comparison, if a contract is broken due process may be pursued but there is no reason why future relationships will not continue to be organized on a contractual basis. Thus promises and contracts are a way of creating assurance in another's reliability and, because they reduce vulnerability, come close to an artificial creation of trust. As Fukuyama comments, 'contracts allow strangers with no basis for trust to work with one another' (Fukuyama, 1995: 150), though he goes on to state that 'the process works far more efficiently when trust exists' (p. 150). Indeed, where obligations are made explicit in promises or contracts then conditions are created which approximate to those created by the existence of trust.

ANTECEDENTS OF TRUST

Reputation and size have been most frequently suggested as factors that contribute to consumer trust in a seller organization. In consumer marketing, the long-term reputation of the seller has been found to be more important than short-term product quality movements. Reputation and size provide assurances of the other party's ability, integrity, and goodwill.

Reputation is the extent to which buyers believe that the selling organization is honest and concerned about its customers (Doney and Cannon, 1997). Reputation is a valued asset (Chiles and McMackin, 1996) and sellers usually try to avoid getting a bad reputation. Reputation requires a long-term investment of resources, effort, and attention to customer relationships. The better the seller's reputation, the more the seller has presumably committed resources to build that reputation, the higher the penalty from violating the consumer's trust, and hence the more trustworthy the seller is perceived to be. A good reputation also signals past forbearance from opportunism (Smith and Barclay, 1997). Similarly, a perception of a large organization size implies that the merchant has significant resources invested in the business and has much to lose by acting in an untrustworthy way. Hence, the larger the firm the more it is perceived by customers that it is in the firm's best interest to fulfill its promises to the consumer. Size and reputation are also likely to interact. Reputational effects are strengthened if associated with longevity (Landon and Smith, 1997). Because of natural growth limits, larger firms might be expected to be around longer and hence firms that are larger and more reputable might be more trusted.

In the Internet marketing context, Quelch and Klein (1996) speculate that the reputation of the store will influence perceptions of the online site. Indeed, some Internet merchants publish stories and customer testimonials on their sites attesting to their reputation, and invest in webpage banners boasting of their size.

The difference between having a good reputation and being trusted is subtle but important. While a person or organization with a good reputation can be relied upon to take action to protect their reputation this does not necessarily imply that they will, in any circumstances, go beyond what their reputation would imply. Yet a reputation is still useful because it 'provides us with some information about the sort of person we are dealing with, before we have had the chance to have contact with that person' (Miszral, 1996: 120–21). Thus, while the standard below which they are unlikely to allow their performance to fall is known, if we are to regard them as trustworthy, they must be expected to show goodwill and benign intent. Such a viewpoint is understandable in that while a person or organization can take action with the intent of establishing and maintaining their reputation it is the trusting person, even when fulfilling a role on behalf of others, who makes a personal interpretation of the situation and decides by which criteria to judge the other's trustworthiness.

Such interpretation will be influenced by their experience – particularly of the other party's behavior. The accolade of being perceived as trustworthy is something that the trusting party gives after assessing the circumstances and is not something that can be claimed as a right.

Perceived reputation, perceived size, and trust, then, are beliefs that the consumer has formed on the basis of information that the consumer has about the merchant.

MARKETING AND THE INTERNET

Organizations use various media to communicate with current and potential clients, often adopting an integrated approach to effectively reach their target audience. Despite the relative newness of the Internet, its unique capabilities and interactive nature have added a new dimension to this process. Websites are seen as something of a mix between direct selling and advertising and offer an alternative to mass media communication (Hoffman et al., 1995). The medium enables the reaching of a large audience at a relatively low cost; the delivery of full color virtual catalogs, the provision of on-screen order forms, and convenient elicitation of feedback from customers. Furthermore, it facilitates the targeting of high-income, well-educated audiences. The medium also enables mass customization,

the projection of a favorable corporate image, and the creation of stronger brand identities (Hoffman et al., 1995). There are problems however, including the evaluation of the effectiveness of Internet marketing efforts (Bush et al., 1998), which can be attributed, in part, to the complexity involved in measuring the flow of Web traffic and exposure patterns. Furthermore, the Internet is not an intrusive medium and requires the audience to be active in seeking out and viewing a message. Given that not all consumers have access to, or the knowledge of how to navigate, the Web, reaching a specific target audience can still be a difficult task (Bush et al., 1998).

Another barrier to marketing on the Internet relates to security and privacy issues and the perceived risk associated with online credit card transactions (Bush et al., 1998; Hoffman et al., 1995). Despite these problems however, it seems that the Internet and the World Wide Web will become ever more powerful tools in the marketing communication arsenal (Bush et al., 1998).

The diffusion process is one in which innovative ideas, products, or services spread through a population. It is widely accepted that not all people will adopt an innovation at the same time and on this basis, most models describe four categories of adopters. 'Innovators' and 'early adopters' tend to be the risk takers or opinion leaders and are generally the first to adopt new products. They tend to 'make' (or 'break') the innovation. The 'early and late majority' consumers are more cautious and only adopt new innovations after they have proven to be successful or as a response to social pressure. They might be said to observe or 'watch' innovators use the new product, and then begin to purchase and use it themselves. 'Laggards', on the other hand, adopt innovations with reluctance. They are generally more traditional in their outlook and base decisions on what has been done in the past. Frequently their attitude toward innovations is to wonder what all the fuss is about. When compared with non-adopters, innovators generally have a higher income level and occupational status, are better educated and are often younger (Hawkins et al., 1994).

The rate at which an innovation is adopted or accepted within a social system is influenced by numerous factors, including how a potential adopter perceives the performance, value, and benefit of an innovation. These perceptions, however, change as more is learned about the innovation from both internal and external sources (Mahajan et al., 1990). The rate of diffusion is also influenced by a number of factors, among which are the perceived relative advantage of the product's compatibility with values and objectives, perceived product complexity, observability of an innovation, fulfillment of felt need, marketing effort involved, and perceived risk in trying an innovation (Hawkins et al., 1994). These models may be useful

in describing how readily organizations assimilate the Internet into their environment. Even though its use is spreading at a phenomenal rate, there are still some organizations that have had limited exposure to the technology and have yet to incorporate it in their marketing communication programs. Other organizations, however, have established 'online storefronts' for their customers or have provided them with information-based sites (Hoffman et al., 1995).

CREATING TRUST IN CYBER SPACE

The nature of the Web, with its two-way communication features and traceable connection technology, allows firms to gather much more information about customer behavior and preferences than they could using micromarketing approaches. For the first time, companies can measure a large number of things that happen as customers and potential customers gather information and make purchase decisions. The idea of technology-enabled relationship management has become possible when promoting and selling via the Web. Technology-enabled relationship management occurs when a firm obtains detailed information about a customer's behavior, preferences, needs, and buying patterns and uses that information to set prices, negotiate terms, tailor promotions, add product features, and otherwise customize its entire relationship with that customer. In advertising, for instance, technology-enabled relationship management provides information to a particular customer in response to specific customer inquiries, while the traditional relationship uses 'push and sell' as a uniform message to all customers.

The rich literature on organizational trust drawn from diverse disciplines including sociology, psychology, and economics has led to numerous conceptualizations of the trust construct and can be extended to the issue of trust in cyber-based businesses. Rousseau et al. (1998: 395) were able to extract common themes in the different conceptual definitions of trust to propose a consensus definition as follows: 'Trust is a psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or behaviors of another'.

Applying this definition to trust in cyber space, we can identify two parts to this definition. First, trust in cyber space relates to certain expectations about the intentions and/or behaviors of the exchange partner. Often referred to as the 'expectancy' conceptualization of trust, it focuses on one's beliefs that the exchange partner will act in a manner that is responsible, evidences integrity, and is not potentially injurious. Secondly, trust in cyber space relates to one's intentions to rely on the exchange partner

accepting the controversial disadvantage of not being seen face-to-face. Referred to as the 'behavioral' conceptualization of trust, it focuses on one's action tendencies toward exchange partners. Indeed, these conceptualizations are related as implied by the preceding definition, since behavioral intentions involve weighing expectations of a partner's behaviors against an individual's vulnerability in the exchange. In the marketing literature, however, researchers have argued against combining the expectancy and behavioral conceptualizations of trust, presumably because keeping them separate provides opportunities to study trust processes (Morgan and Hunt, 1994). In conformity with this, throughout this book, a distinction is maintained between expectations and behavioral intentions among the trading partners in cyber space.

Although efforts toward a consensual definition of trust have been successful, some researchers have argued that the resulting conceptualizations are so 'stretched' that they have limited usefulness for conceptual and/or empirical work. Following Osigweh (1989), the notion of stretching relates to a construct that is defined at a high level of abstraction and has both a broad coverage and a wide connotation. Problems in range and connotative specification of trust conceptualizations can lead different researchers working with different conceptual meanings of trust to accumulate a common body of work. Recognizing the confusion that this might create, Bigley and Pearce (1998: 406) have implored researchers to shift their focus from such questions as 'what is trust?' to 'which trust and when?'. Heeding this call, we further specify the domain and connotative meaning of the trust construct in the context of our study. Following this, we discuss the implications of trust for agency problems in consumer exchanges.

Three sources of specification are identified with regard to the consumer trust construct in cyber space. First, situational and contextual factors are likely to determine the relevance of the trust construct in cyber space exchanges. That is, trust is not a necessary ingredient for consummating consumer–firm exchanges, just as the presence of distrust does not, in and of itself, preclude consummation. Rather, situations will vary by the degree to which they evoke the relevance of trust and trigger mechanisms that are affected by the level of trust. Specifically, trust-relevant exchanges are characterized by (a) a high level of performance ambiguity, (b) vital consequentiality, and (c) greater interdependence (Sitkin and Roth, 1993).

Secondly, connotative specification is likely to bias the conceptualization of the consumer trust construct; that is, specifying the attributes with an appropriate level of precision so that the trust construct achieves meaningfulness across multiple domains. Defining trust in global terms without any attribute specification may be problematic because different consumers may score such items equivalently even when they use distinctly

different attributes to judge trust. By contrast, a highly precise specification may yield a trust construct with so many attributes that it is pragmatically cumbersome. Often, an intermediate precision level involving specification of salient attributes is thought to be desirable.

Several researchers have provided an intermediate level of connotative specification for the trust construct. For instance, in the context of buyer–seller relationships (for bricks-and-mortar businesses), Ganesan and Hess (1997: 440) propose two dimensions of trust: (1) credibility, or the focal partner's intention and ability to keep promises; and (2) benevolence, or evidence of the focal partner's genuine concern for the partner through sacrifices that exceed a purely egocentric profit motive. These two dimensions can be extended to the world of cyber space. Ganesan and Hess also provided empirical support for the discriminant validity of these trust dimensions. Using the notion of competence instead of credibility, McAllister (1995) defined a cognition-based trust and distinguished it from affect-based trust that stems from affective bonds among individuals. We focus on cognition-based trust to maintain consistency with our expectation conceptualization of trust. In an earlier work, Barber (1983) had proposed that trust expectations are likely to include evaluations of (1) technically competent role performance, and (2) carrying out obligations and responsibilities by placing others' interests before their own. Although none of these attempts has conceptualized the trust construct specifically for consumer exchanges, the consistent themes of competence and benevolence emerging from the inter-organizational literature appear relevant for the connotative specification of the consumer trust construct as well.

Thirdly, acknowledging the wide range of the trust construct, one recognizes that the trust construct is a linear continuum that is bounded by high levels of distrust and trust, and that these states are qualitatively different. Clearly, the distrust and trust states differ in terms of the valence of held expectations. Empirically, Sitkin and Roth (1993) demonstrate that trust and distrust are maintained by different mechanisms. Specifically, in the context of organization–employee relationships, they show that while unmet expectations of 'task reliability' generate violations of trust, it is the 'value incongruence' that engenders distrust. As such, the distinction between the positive and negative domains of the trust–distrust continuum is plausible and appears to cohere with the current notion of asymmetric effects in the marketing literature.

Thus, for cyber space businesses, in specifying the trust construct for understanding its role in agency relationships, one recognizes that (1) the relevance of trust is situation specific, (2) competence is a distinct dimension that forms overall trust expectations, and (3) trust–distrust expectations fall along a continuum with potentially asymmetric effects.

TRUST ISSUES IN CYBER SPACE

Trust issues in cyber space have not been fully researched and explored, despite the fact that trust itself has been proven to be imperative in relational exchanges. Morgan and Hunt (1994) argue that trust is a key component in the development of lasting marketing relationships. Trust has been identified in much of the literature as a key component of exchange, and as a catalyst for relationship development. With this in mind, Internet marketers must find ways to gain trust and initiate relationships with customers. A review of literature on trust in establishing and evolving marketing relationships found many research papers, both theoretical and empirical, tackling this issue. Most, however, identify and refer to variables that are experience related. That is, a customer must first take part in an exchange and then make judgments regarding the level of trust possessed by the provider.

That may not be at all practical for cyber space providers without the customer's frame of reference. In addition, this would suggest that only customers who had some kind of offline relationship with the company would be willing to make online purchases.

Three studies of importance in the area of experience-related trust variables are those conducted by Frazier et al. (1988), Czepiel (1990), and Beatty et al. (1996). The results of each of the research papers are discussed below.

Frazier et al. (1988) point out that the three variables that improve trust are personal integrity, upheld promises, and foregone opportunistic behavior. Personal integrity is a perceptual matter, and deals with the perceived level of honesty the buyer has for the service provider. This level of integrity is affected by past experiences and whether the provider has been known to keep promises. In general, personal integrity is determined by the provider's reliability as demonstrated in previous business exchanges. Additionally, levels of trust would be influenced by the provider's likelihood of taking advantage of the buyer's situation. Foregoing the opportunity to take advantage of the buyer increases levels of trust, according to Frazier et al. (1988). These are variables that will be determined over time, and can only be experienced after satisfactory exchanges have occurred.

Czepiel (1990) argues that relationships progress and vary over time and parties to relational exchanges develop greater trust and dependence as the relationship progresses. Czepiel developed a number of stages of creating and enhancing relationships for exchange; these include: (1) accumulation of satisfactory encounters and the expectation of future purchases; (2) active participation based on mutual disclosure and trust; (3) creation of a double bond (personal and economic), and (4) psychological loyalty to the

relationship. Again, these stages are based upon a consumer's perception of trust following a completed business (or non-business) exchange.

In research conducted by Beatty et al. (1996) three aspects were found to influence trust: (1) Sales associates continually demonstrating they had the customer's best interest at heart, (2) skills to meet customer needs, and (3) customer problems solved honestly. In their study of retail sales associates in a store situation, Beatty et al. (1996) argued that the sales associates developed trust by exhibiting extensive product knowledge and availability, and by choosing products to meet customer needs. In addition, the authors suggest that repeat exchanges are based upon trust, friendship, and functionality, and that relationships of the various parties strengthen directly with these three factors. The sales associates involved in the study identified several activities as developing trust. These activities include keeping the customer's best interest at heart, honesty, respectfulness, extensive product knowledge, and the availability of merchandise. Customers also identified the importance of trust and honesty in their relationships with the sales associates. Beatty et al. (1996: 239) found that: 'high performing salespeople place more emphasis on establishing trust between themselves and their clients than do lower performing salespeople'.

So, as evidenced by the findings of the last three studies reviewed, indicators of trust are based on the past experience of the buyer. The literature, however, fails to examine any factors that may imply the trustworthiness of the seller prior to an exchange. For the purposes of this chapter, these factors are referred to as cue based. Therefore, indicators of trust may be twofold: (1) those that are experience based, and (2) those that are cue based. Experience-based trust indicators are the result of an exchange. Based on an exchange, the consumer makes judgments regarding the perceived level of trust of the seller. This represents learned behavior. The literature summarized here revolves around the experience-based side of trust. There seems to be, however, less research in the area of trust cues. A trust cue would include any outward symbol that exists prior to the exchange and would indicate to a customer that a marketer is trustworthy. The challenge for e-marketers is to determine what these trust cues are in order to initiate that first experience. With all of the concerns of consumers specific to Internet marketing, cyber space must find ways to 'cue' consumers to trust the company in order to initiate the first transaction. Once started, it is up to the e-marketer to be sure the transaction is smooth and implemented in an environment of honesty and integrity. The following section explores some of the possible cues which may initiate consumer feelings of trust in the world of Internet marketing.

Several cues may cause potential buyers to infer a certain amount of

trust in the seller and initiate contact so that a relationship may be formed. In the world of Internet marketing, a business's communication tool is its website. It is through this medium that marketers must directly communicate product offerings, services, and company information, and must indirectly foster an environment of trust. These trust cues that are placed on the company website serve as a promotional tool to encourage online purchasing. These cues, which may serve as indicators of a trustworthy seller, may consist of return policies, name recognition, professional appearance of website, privacy and security policy, availability of company address and telephone number for alternative ordering procedures, and the references of existing customers. Each of these potential trust cues is explored below.

An extended warranty and/or guarantee is a cue of trustworthiness, whereas a policy of 'no returns' is considered less trustworthy. If a seller does not guarantee his or her product, then a purchaser may doubt the credibility of a quality purchase and hesitate to buy. The buyer assumes risk in making an Internet purchase. If the marketer can reduce the risk involved in making an online purchase, the consumer may presume a higher level of trust in that marketer. The responses to trustworthy cues and successful and satisfactory exchanges are the first steps to developing an initial buyer–seller relationship. For this reason, companies such as Lands' End have adopted liberal return policies that are prominently displayed on their website and in their advertising in order to increase consumer comfort and decrease consumer risk. The aforementioned Dell Computer guarantee also serves as an example of this cue.

The ability of the consumer to recognize the company name of the seller may also be an important trust cue. Consumers who identify a company name may have a higher comfort level, resulting in higher levels of trust. For that reason, many e-merchants are now advertising in traditional media such as newspapers and magazines to increase overall name recognition among consumers. This improves the e-marketer's visibility and recognition in the marketplace, even among non-Internet users. Recent examples include advertising by Shopping.com, Amazon.com, E-loan, and E-trade in newspapers such as *The New York Times* and *USA Today*; and Hotjobs and Ebay on network television. None of these businesses has any corresponding offline retail site, and as such has little or no name recognition among non-Internet users and new Internet users. These offline traditional media campaigns aim to increase name recognition, and therefore comfort levels, among all consumers.

Another indicator of trustworthiness among Internet websites is the appearance of the site. Those websites that have a professional appearance imply more trustworthy sellers. The professional appearance of a website

would include using proper grammar, correct spelling, appropriate references and citations where necessary, appropriate product line, and good use of graphic design. This would also extend to the website's listing with other sites, such as hyperlinks and search engines. Additionally, registration with search engines should foster appropriate responses.

As mentioned earlier in this chapter, security issues are of the utmost importance to Internet shoppers, and were the primary reason among Internet users for not becoming online shoppers. Credibility is a measure of honesty and ethical behavior. Higher levels of credibility create higher levels of trust. The consumer in a cyber space exchange wants to deal with a seller who is honest. Dishonest behavior, as evidenced in previous transactions, will lead to low trust levels. This dishonest behavior in electronic exchange may include such serious violations as intentional overcharges, misrepresenting merchandise, and fraudulent use of credit cards or other sensitive consumer information. This dishonest behavior also includes taking advantage of opportunities to do wrong to the other member in the exchange. Dwyer et al. (1987) refer to this as 'opportunistic behavior' and discourage its use. Online merchants recognizing this hesitance in consumers must provide assurance that security issues are important to the marketer as well, and must provide some manner of combating the consumer's fear. Security issues may be dealt with by offering a secured server over which all personal information and credit card numbers are transmitted. This information should be encrypted during transmission for the safety of the consumer. Additionally, privacy policies should be developed for all websites, explaining to the consumer why the data must be gathered, how they will be used, how they will be stored, and who will have access to them. The data gathered should be essential to the task at hand. For example, the customer understands why the marketer must have his or her name, address, phone number, and credit card number in order to process and ship an order. The need for the marketer to know how many children are in the household may not be understood by the consumer and may need to be explained. Additionally, consumers want to know how the data will be stored and who will have access to them. Consumers seem particularly concerned about whether the information will be sold to another party. A well-written privacy policy predominantly displayed on the website can address these issues and calm consumer worries. Another way to deal with security and privacy issues is through company guarantees and personal testimonials.

Online businesses such as Amazon.com offer evidence of their online safety track record. Amazon.com's website states that 'You'll be one of the 10 million customers who have safely shopped with us without credit card fraud.' Amazon.com uses secure server software which not only

encrypts credit card information but all personal information recorded during a transaction. So, even for those who have not previously dealt with Amazon.com, this evidence of safe and successful transactions provides a level of trust and commitment for consumers.

Companies such as American Express offer guarantees if their credit card is used during any online purchase. The company promises that 'When you use an American Express Card to purchase online, you will not be held responsible for any unauthorized charges. Guaranteed.' American Express has gone as far as communicating guarantees in the traditional media such as *The New York Times*, in order to assure the consumer of safety and satisfaction in purchasing online.

A traditional direct-marketer that has expanded its customer service to reflect concerns in online shopping is Lands' End. Its guarantee statement indicates that 'you can return anything, at any time, for any reason'. In response to the Internet age, Lands' End has added two new sections to its guarantee. The first addition offers secure protection against mistaken or fraudulent credit card use. The second addition protects users against the misuse of customer information and the opportunity to opt out of the reselling of personal information.

Finally, electronic merchants must be prepared to provide service to those who do not wish to submit their orders electronically. The website should include alternative ways in which the consumer is able to place an order. Some consumers just feel more secure talking to a representative over the phone, placing their order by mail, or visiting a retail store. With that in mind, online marketers must be prepared to accept alternative ordering procedures. A website that only allows online ordering will miss opportunities to serve customers who are not yet prepared to provide personal and financial information electronically. Offering the consumer alternative ordering procedures shows the consumer that the business is responsive to their needs, and is a real business with real employees and a real mailing address. Websites that offer customer employee contact names further emphasize the viability of the business.

E-operations opportunities are uses of Web technology that are directed at strategic change in the way a business manages itself and its supply chain, culminating in the production of its core product or service. For example, technology underpins BP Amoco's initiatives to troubleshoot more effectively by sharing the learning of its businesses around the world. General Electric Co. improved its purchasing by posting requirements on a website and having suppliers submit bids electronically.

E-marketing opportunities cover Web-based initiatives that are designed to achieve strategic change in downstream activities, either through direct interaction with the customer or through a distribution channel. In

e-marketing, a traditional product remains the focus of the business and its revenue generation, but the way the product is delivered or the scope of support services changes. The provider may be a traditional incumbent or a new pure-play entrant: a Barnes & Noble or an Amazon.com, a Toys 'R' Us or an eToys. The financial services sector is illustrative. In that arena, established companies and new competitors are forging links to established intermediary channels, to new intermediaries, and to the customer directly – while continuing to focus on the delivery of traditional financial services products such as savings accounts, credit cards, and mortgages.

E-service opportunities give companies new ways to address an identified set of customer needs. Rather than promoting proprietary products, the e-service business acts as the customer's agent in achieving a desired outcome. Most current examples are New Economy businesses: Chemdex, the information intermediary in the biosciences sector; OneMediaPlace (formerly Adauction.com), which provides buyers and sellers of advertising space with a radically new set of services; and shopping robots such as mySimon.com, which scour the Internet to find the best deals available. Some Old Economy businesses float an e-service business as a new venture – for example, Overseas Chinese Bank Corporation's Bank of Singapore has a financial services venture called finatiQ.com. Others may begin to redefine their core business, as Ford Motor Co. is doing in seeking to become 'the world's leading consumer company for automotive service'.

Defining e-opportunity domains using a business-oriented perspective and language illuminates the role of new technology in competitive advantage. Technology prompts new business practices rather than new business theories. In other words, successful e-strategies translate established strategic concepts into contexts in which they previously were not economically viable. In the 1960s and 1970s, IBM won the loyalty of major corporate customers through highly paid account executives who provided what IBM called 'relationship management'. That approach to supporting individual consumers is now technologically based.

Distinguishing between the three e-opportunity domains is critical. Each requires its own distinctive framework for identifying ideas that can bring competitive advantage to a given context. Every business should be considering opportunities across all three domains, but the potential significance of each domain, and of individual ideas within it, will vary widely across businesses and industry sectors. Although it is tempting to begin with the excitement of e-service – the Brave New World of the New Economy – in practice, the e-operations and e-marketing layers require the most urgent attention and provide the most certain rewards. As so many dot.coms have demonstrated, if you have e-vision but a single marketing approach and a poor fulfillment capability, you do not really have a business.

CONCLUSION

This chapter has presented an overview of the literature on cyber security issues and trust and their role in enhancing cyber activities.

The term malware (*mal*icious soft*ware*) refers to a program with malicious intention planned to damage the machine on which it operates or the network over which it communicates. The growth in the complexity of modern computing systems makes it difficult, if not impossible, to evade bugs, which, in turn, leads to an increase of the likelihood of malware attacks, acting on the vulnerabilities of the system. Consequently, the threat of malware attacks is an inevitable problem in computer security, and therefore it is critical to discover the existence of malicious codes in software systems. Information is the lifeblood of any bank and it must be protected, especially PII. There are many ways in which customer information could be stolen from you: dumpster diving, social engineering, phishing, pharming.

There are a staggering number of ways that information could be taken from computer networks and released outside an organization's boundaries. Whether it is MP3 player, CD-ROM, a digital camera, or USB data stick; today's employees could easily take a significant chunk of an organization's intellectual property out of the door in their back pocket. These types of devices are effectively very portable, very high-capacity hard drives; someone could take away up to 60 gigabytes of data on a USB stick.

Observing current computer security practices in banking and financial institutions leads one to question whether the state of cyber security in these institutions is adequate. Each week brings yet another news story of a major security breach; one reason for our failure in what concerns cyber privacy and security is that these problems are difficult to resolve. In systems development, in the haste toward releasing a product, there is little economic motivation to spend the time properly designing privacy and security into systems. While a number of developed countries have enacted, passed, and enforced laws that require notification in the case of data exposure, and call for the criminalization of hackers and system attackers, legal and policy systems simply have not kept up with the advancement of technology. While information and communication technology keeps evolving at an ever-increasing pace, our networked systems pose new threats and present new challenges.

We without a doubt have become information-/knowledge-based societies; being connected 24/7 has radically reformed the way we work and play, and how we interact with the inner and outer environments. Over the last 12–14 years, the topmost security objective was how to safeguard and

defend the network boundary from hackers who are determined to violate our information systems from the outside, compromise data, and to wreak havoc with our systems. Billions of dollars have been spent in the development and deployment of firewalls, intrusion detection devices, antivirus spyware, and the like.

For the most part, the battle against these hackers has been largely sorted out; however, today the biggest danger is not to the company's hardware or software, it is rather related to soft issues related to people, mainly internal, who are trying to compromise our data and information. The list of targets of cyber attackers is a mile long, ranging from individuals, banking and financial institutions, communication systems, infrastructures, government agencies, hospitals, universities, and many others. The growing intricacy and interdependence of the various networks of these entities make them more susceptible to cyber attacks and increase the reach, depth, and range of an attack's effects. A recent study by Symantec, the world's largest maker of security software, found that the fraud industry is worth a potential US$7 billion. McAfee's more recent study estimates the loss of intellectual property and adjusting the damage at about US$1 trillion.

Researchers at Verizon studied and analysed 500 cases of corporate data breaches over a period of four years; they concluded that different regions of the world are developing different types of hacking expertise. Hackers from Asia are inclined to target personal information in common software applications, and Eastern Europeans seem to be experts in identity theft (Fitzgerald, 2008). To protect themselves, many firms and governmental agencies have developed advanced IT asset use policies and procedures while others have put together policies with encryption technology to better protect their networks and secure vital information. While these are necessary steps, reality shows us they are not sufficient. Organizations still wrestle to counterbalance the human element from within and the outside. According to a recent survey of 1,400 enterprises, more than 60 percent of data breaches are the work of those operating within the firewall – insiders such as employees, contractors, and others with ready access to sensitive information (*Information Age*, 2007).

The relationship between systems' security and trust is well documented; it is demonstrated that the common denominator between the trust dimensions presented in the literature is the emphasis on issues that may directly influence the trust in an individual or an organization. In addition, the focus is on unidirectional trust dimensions. Research has been dedicated to regard trust as a unidirectional and direct relationship concept, though some authors have lately emphasized the importance of mutuality between firms in a business relationship. Still, trust is often regarded as an isolated

phenomenon in a marketing channel context, despite the fact that we know that other indirect factors certainly or most probably are important, and will influence the trust in a dyadic business relationship.

In research literature, different trust scenarios have been used in the study of relationships between individuals and/or organizations. These identified trust scenarios can tentatively be classified into four broad categories: (1) mutual trust, (2) upstream trust, (3) downstream trust, and, finally, (4) distrust. These trust scenarios are influential determinants of the trust in a dyadic business relationship. The existence of trust, according to one trust scenario or another, will certainly affect a dyadic business relationship. Therefore, the outcome of a dyadic business relationship is to a certain extent dependent upon the trust scenario. It is a completely different matter if both actors in a dyadic business relationship have trust in each other (that is, a mutual trust scenario), than if either party lacks trust in the other party (that is, an upstream trust scenario or a downstream trust scenario), or if there is no trust at all between the actors (that is, a distrust scenario). Research tends to ignore trust issues beyond the dyadic business relationship at focus. A marketing channel consists of a series of interdependent relationships, causing a necessity to broaden the significance of the conceptualization of the trust and mutual trust in dyadic business relationships to embracing upstream and downstream dyadic business relationships in the marketing channel, at least toward customers' customers and suppliers' suppliers.

Trust is based on competence, goodwill, and behavior. In order to build trust a wide scope of information is needed as different types of information (rational–emotional, economic–social, tacit–explicit) affect the trust experienced. Even in the business context the emotional level has a great impact on organizational trust building. Personal feelings and emotions are intertwined with more rational factors. In order to be able to communicate needs and expectations precisely and efficiently, both rational and emotional information is needed. Overly emotional information is not believable since it may seem subjective, lacking facts. Pure rational information of objective facts lacks emotional depth, ensuring the other party of the commitment and true intentions of the speaker.

Trust in cyber space relates to certain expectations about the intentions of the exchange partner. Often referred to as the 'expectancy' conceptualization of trust, it focuses on one's belief that the exchange partner will act in a manner that is responsible. In addition, trust in electronic commerce relates to one's rationale to rely on the exchange partner accepting the contentious disadvantage. This concentrates on one's action predisposition toward exchange partners. Undeniably, these conceptualizations are linked since behavioral intentions entail weighing expectations of

a business associate's behaviors against a person's susceptibility in the exchange. In the marketing literature, however, researchers have argued against combining the expectancy and behavioral conceptualizations of trust, presumably because keeping them separate provides opportunities to study trust processes. This notion is strongly held up in the management literature as well.

NOTES

1. Refer to Sunner, 'Security Landscape Update 2007', page 3, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may 2007.pdf.
2. '2007 Sophos Report on Spam-relaying countries', available at: http://www.sophos.com/pressoffice/news/ articles/2007/07/dirtydozjul07.html.
3. The full study is available at http://cups.cs.cmu.edu/soups/2008/proceedings/p117Falk.pdf.
4. For a further description of phishing refer to Butler (2007).
5. Source: US Department of Justice, www.usdoj.gov.
6. The study, titled 'Unsecured Economies: Protecting Vital Information', was done by a number of Purdue University professors.

REFERENCES

Acoca, B. (2008), 'Scoping paper on online identity theft of OECD', presentation at OECD Ministerial Meeting on the Future of the Internet Economy, 17-18 June, Seoul, Korea.

Anti-Spyware Coalition (2006, 26 June), 'Final working report: definitions', accessed 12 July at www.antispywarecoalition.org/documents/documents/ASCDefinitionsWorkingReport20060622.pdf.

Ba'tiz-Lazo, B. and P. Wardley (2007), 'Banking on change: information systems and technologies in UK high street banking 1919–1969', *Financial History Review*, **14**(2): 177–205.

Ba'tiz-Lazo, B. and D. Wood (2002), 'Historical appraisal of information technology in commercial banking', *Electronic Markets*, **12**(3): 1–12.

Baier, A. (1986), 'Trust and antitrust', *Ethics*, **96**(2): 231–60.

Barber, Bernard (1983), *The Logic and Limits of Trust*, New Brunswick, NJ: Rutgers University Press.

Beatty, S.E., M. Mayer, J. Coleman, K.E.E. Reynolds and J. Lee (1996), 'Customer-sales associate retail relationships', *Journal of Retailing*, **72**(3): 223–47.

Beck, Thorsten, Erik H.B. Feijen, Alain Ize and Florencia Moizeszowicz (2008), 'Benchmarking financial development', World Bank policy research working paper series no. 4638, accessed at http://ssrn.com/abstract=1149571.

Berry, Leonard L. (1995), 'Retailers with a future', *Marketing Management*, **5**(Spring): 39–46.

Bielski, L. (2004), 'Phishing phace-off', *ABA Banking Journal*, **96**(9): 46–54.

Bigley, Gregory and Jone Pearce (1998), 'Straining for shared meanings in

organization science: problems of trust and distrust', *Academy of Management Review*, **23**(3): 405–21.
Blomqvist, K. (1997), 'The many faces of trust', *Scandinavian Journal of Management*, **13**(3): 271–86.
Blomqvist, K. (1999), 'The role and means of trust creation in partnership formation between small and large technology firms: a preliminary study of how small firms attempt to create trust in their potential partners', in Wim During and Ray Oakey (eds), *New Technology-Based Firms in the 1990's*, vol. IV, London: Paul Chapman Publishing, pp. 81–98.
Boon, S.D. and J.G. Holmes (1991), 'The dynamics of interpersonal trust: resolving uncertainty in the face of risk', in R.A. Hinde and J. Grobel (eds), *Cooperation and Prosocial Behavior*, *Cambridge: Cambridge University Press*, pp. 190–211.
Bruene, J. (2009), 'How can online banking develop its own black card?', accessed at www.netbanker.com/creditdebit_cards/.
Bush, A.J., V. Bush and S. Harris (1998), 'Advertiser perceptions of the Internet as a marketing communication tool', *Journal of Advertising Research*, **38**(2): 17–27.
Butler, J.K. (1983), 'Reciprocity of trust between professionals and their secretaries', *Psychological Reports*, **53**: 411–16.
Butler, R. (2007), 'A framework of anti-phishing measures aimed at protecting the online consumer's identity', *The Electronic Library*, **25**(5): 517–33.
Buttle, Frances (1996), 'Unserviceable concepts in service marketing', *Quarterly Review of Marketing*, **11**(3): 8–14.
Casson, Mark (1997), *Information and Organization*, New York: Oxford University Press.
cert.org (2008), 'Insider threat research', accessed 22 January at www.cert.org/insider_threat/more.html.
Chiles, T.H. and J.D. McMackin (1996), 'Integrating variable risk preferences, trust, and transaction cost economics', *Academy of Management Review*, **21**: 73–99.
Chow, S. and R. Holden (1997), 'Toward an understanding of loyalty: the moderating role of trust', *Journal of Managerial Issues*, **9**: 275–98.
Coleman, J.S. (1990), *Foundations of Social Theory*, Cambridge, MA: Belknap Press of Harvard University Press.
Creed, D. and R.E. Miles (1996), 'Trust in organizations – a conceptual framework linking organizational forms, managerial philosophies, and the opportunity costs of control', in Roderick M. Kramer and Tom Tyler (eds), *Trust in Organizations, Frontiers of Theory and Research*, Thousand Oaks, CA: Sage, pp. 16–39.
Cummings, L.L. and P. Bromiley (1996), 'The organizational trust inventory', in R. Kramer and T. Tyler (eds), *Trust in Organizations*, Thousand Oaks, CA: Sage, pp. 302–30.
Czepiel, J.A. (1990), 'Service encounters and service relationships: implications for research', *Journal of Business Research*, **20**(1): 13–21.
Das, T.K. and Teng, Bing-Sheng (1998), 'Between trust and control: developing confidence in partner cooperation in alliances', *Academy of Management Review*, **23**(3), 491–512.
Dasgupta, P. (1988), 'Trust as a commodity', in D. Gambetta (ed.), *Trust: Making and Breaking Cooperative Relations*, Oxford: Basil Blackwell, pp. 49–72.
Dawar, N., P.M. Parker and L.J. Price (1996), 'A cross-cultural study of

interpersonal information exchange', *Journal of International Business Studies*, **27**: 497–516.
Deloitte (2007), 'Global security survey: the shifting security paradigm', accessed at www.deloitte.com/dtt/cda/doc/content/ca_en_Global_Security_Survey.final.en.pdf.
Deutsch, M. (1958), 'Trust and suspicion', *Journal of Conflict Resolution*, **2**: 265–79.
DeYoung, R., W.W. Lang and D.L. Nolle (2007), 'How the internet affects output and performance at community banks', *Journal of Banking and Finance*, **31**(4): 1033–60.
Dhamija, R. and J.D. Tygar (2005), 'The battle against phishing: dynamic security skins', *Proceedings of the 2005 Symposium on Usable Privacy and Security*, Pittsburg, PA: ACM Press, pp. 77–88, and accessed 23 December 2007 at http://people.ischool.berkeley.edu/~rachna/papers/securityskins.pdf.
Doney, P.M. and J.P. Cannon (1997), 'An examination of the nature of trust in buyer–seller relationships', *Journal of Marketing*, **61**: 35–51.
Dwyer, F.R., P.H. Schurr and S. Oh (1987), 'Developing buyer–seller relationships', *Journal of Marketing*, **51**(April): 11–27.
Edelman, B. (2004), 'Cookie-stuffing targeting major affiliate merchants', accessed July 15 2006 at www.benedelman.org/cookiestuffing/.
Elster, J. (1983), *Sour Grapes: Studies in the Subversion of Rationality*, Cambridge: Cambridge University Press.
Ennis, J. (2008), 'Best practices for organizing national cyber security efforts', presentation made at regional workshop organized by the ITU in collaboration with *ictQATAR* and *Q-CERT*, 18-21 February.
Federal Bureau of Investigation (FBI) (2008), 'Cybercrime exceeds drug trade', accessed 29 January at www.theregister.co.uk/2008/03/27/cyber crime_mythbusters.
Fitzgerald, P. (2008), 'The crash of civilizations', *Foreign Policy*, Sept./Oct.: 122.
Frazier, G.L., R. Spekman and C.R. O'Neal (1988), 'Just-in-time exchange relationships in industrial markets', *Journal of Marketing*, **52**(October): 52–67.
Fukuyama, F. (1995), *Trust*, London: Hamish Hamilton.
Ganesan, S. and R. Hess (1997), 'Dimensions and levels of trust: implications for commitment to a relationship', *Marketing Letters*, **8**: 439–48.
Garbarino, Ellen and Mark Johnson (1999), 'The different roles of satisfaction, trust and commitment in customer relationships', *Journal of Marketing,* **63**(April): 70–87.
Geyskens, I., J.-B.E.M. Steenkamp, L.K. Scheer and N. Kumar (1996), 'The effects of trust and interdependence on relationship commitment: a trans-atlantic study', *International Journal of Research in Marketing*, **13**: 303–17.
Hackworth, A. (2005), 'Spyware' retrieved 9 July 2006 from www.uscert.gov/reading_room/spywarehome_0905.pdf.
Hamel, G. and J. Sampler (1998), 'E-corporation; more than just web-based, it's building a new industry order', *Fortune*, 7 December, pp. 52–63.
Hasan, I., C. Zazzara and R. Ciciretti (2005), 'Do internet activities add value? Evidence from the banking industry', Rensselaer Polytechnic Institute, unpublished manuscript.
Hawkins, D., C. Neal, P. Quester and R. Best (1994), *Consumer Behaviour Implications for Marketing Strategy*, Irwin: Sydney, Australia.
Hawser, A. (2007), 'Banks on the spot over Internet fraud', *Global Finance*

Magazine, accessed 5 June, 2008 at www.gfmag.com.archives/37-37-September-2007/1164-newsmakers-few-cities-attain-knowledge-hub-status.html.
Hernando, I. and M.J. Nieto (2007), 'Is the internet delivery channel changing banks' performance? The case of Spanish banks', *Journal of Banking and Finance*, **31**(4): 1083–99.
Hoffman, Donna L., Thomas P. Novak and Patrali Chatterjee (1995), 'Commercial scenarios for the web: opportunities and challenges', *Journal of Computer Mediated Communication,* special issue on Electronic commerce, 1(December), http://shum.huji.ac.il/jcmc/coll/issue3/vollno3.html.
Hofstede, G. (1980), *Culture's Consequences: International Differences in Work-related Values*, Beverly Hills, CA: Sage.
House of Lords (2008), *Personal Internet Security: Follow Up Report*, published by the Authority of the House of Lords, London: The Stationery Office.
Human Rights Watch (1999), '1999: censorship, restrictions stunt internet growth in Mideast', accessed 23 February 2008 at www.hrw.org/reports/2005/mena1105/5.htm.
Hume, D. ([1740] 1969), *A Treatise on Human Nature*, Harmondsworth: Penguin Books.
Information Age (2007), 'The inside job', 13 August, accessed at www.informationage.com.
ITRC (2008), 'Data breach report', accessed 9 January 2009 at www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml.
Jarvenpaa, S.L. and P.A. Todd (1997), 'Consumer reactions to electronic shopping on the World Wide Web', *Journal of Electronic Commerce*, **1**(2): 59–88.
Jarvenpaa, S.L., N. Tractinsky and M. Vitale (1999), 'Consumer trust in an internet store', *Information Technology Management*.
Javelin Strategy Research (2009), 'The 2009 identity fraud survey report', accessed 1 March at www.javelinstrategy.com/2009/02/09/latest-javelin-research-shows-identity-fraud-increased-22-percent-affecting-nearly-ten-million-americans-but-consumer-costs-fell-sharply-by-31-percent.
Johnson-Edwards, D. (2005), 'Zombies and bots – tools for cyber extortion', accessed 20 May at www.richmond.com/sci-tech/output.aspx?ID=3683718andVertical_ID=53andtier=1andposition=1.
Johnson, J.L., T. Sakano, K. Voss, H. Takenouchi (1998), 'Marketing performance in U.S.–Japanese cooperative alliances: effects of multiple dimensions of trust and commitment in the cultural interface', published in Washington State University, working paper, *Journal of the Academy of Marketing Science*, **23**(4): 255–71.
Jones, G. and J. George (1998), 'The experience and evolution of trust: implications for cooperation and teamwork', *Academy of Management Review*, **23**: 3.
Keen, P.G.W. (1997), 'Are you ready for "trust" economy?', *Computer World*, 21 April, p. 80.
Kirda, E. and C. Kruege (2006), 'Protecting users against phishing attacks', *Computer Journal*, **49**(5), 554–61.
Kline, R.B. (no date), *Principles and Practice of Structural Equation Modeling*, New York: The Guilford Press.
Koops, B. and R. Leenes (2006), 'Identity theft, identity fraud and/or identity-related crime: definitions matter', *Datenschutz und Datensicherheit* – **30**(9) (September), 553–6.
Krebs, B. (2008), 'More cyber security regulations recommended', accessed at

http://worldanalysis.net/postnuke/html/index.php?name=Newsandfile=articleandsid=1725.
krollfraudsolutions.com (2008), 'Kroll global fraud report', accessed 5 January 2009 at www.krollfraudsolutions.com/. . .kroll/pdf-form-global-fraud.aspx.
Ladegard, G. (1997), 'Forming strategic alliances: the role of social compatibility', dissertation submitted to the Institute of Organization Sciences, Norwegian School of Economics and Business Administration.
Landon, S. and C.E. Smith (1997), 'The use of quality and reputation indicators by consumers: the case of Bordeaux wine', *Journal of Consumer Policy*, **20**: 289–323.
Lewis, D.J. and Andrew Weigert (1985), 'Trust as social reality', *Social Forces*, **63**(4) (June): 967–85.
Luhman, N. (1979), *Trust and Power*, New York: John Wiley and Sons.
Mahajan, V., E. Muller and F.M. Bass (1990), 'New product diffusion models in marketing: a review and directions for research', *Journal of Marketing*, **54**(1): 1–26.
Mayer, R.C., J.H. Davis and F.D. Schoorman (1995), 'An integrative model of organizational trust', *Academy of Management Review*, **20**(3): 709–34.
McAllister, D.J. (1995), 'Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations', *Academy of Management Journal*, **38**: 24–59.
McCort, D.J. and N.K. Malhotra (1993), 'Culture and consumer behavior: toward an understanding of cross-cultural consumer behavior in international marketing', *Journal of International Consumer Marketing*, **62**(2): 91–127.
McGlasson, L. (2009), 'Identity fraud survey shows ID theft up 22 percent', *BankSecurity*, 9 February.
Mizral, A. (1996), *Trust in Modern Society*, Oxford: Polity Press and Blackwell Publishing.
Mitnick, K. and W. Simon (2002), *The Art of Deception*, New York: Wiley.
Morgan, R. and S. Hunt (1994), 'The commitment–trust theory of relationship marketing', *Journal of Marketing*, **58**(4) (July): 20–38.
Morrow, B. (2008), 'No one is immune', *Texas Banking*, **97**(11): 16–17.
Oakes, G. (1990), 'The sales process and the paradox of trust', *Journal of Business Ethics*, **9**: 671–97.
O'Brien, R.C. (1989), 'Is trust a calculable asset in the firm', *Business Strategy Review*, 39–54.
Ollman, G. (2004), 'The phishing guide – understanding and preventing', Next Generation Security Software Ltd, accessed at www.technicalinfo.net/papers/Phishing.html.
Osigweh, Chemezie (1989), 'Concept fallibility in organization science', *Academy of Management Review*, **14**(4): 579–94.
PC Magazine (2005), 'Newest infection applies extortion', accessed 28 April from www.pcmag.com/article2/0,1759,1821782,00.asp.
Pennings, J.M. and J. Woiceshyn (1987), 'A topology of organizational control and its metaphors', *Research in the Sociology of Organization*, **5**: 75–104.
Quelch, J.A. and L.R. Klein (1996), 'The Internet and international marketing', *Sloan Management Review*, **37**(3): 60–75.
Rempel, J.K., J.G. Holmes and M.P. Zanna (1985), 'Trust in close relationships', *Journal of Personality and Social Psychology*, **49**: 95–112.
Rousseau, Denise, Sim B. Sitkin, Ronald Burt and Colin Camerer (1998), 'Not

so different after all: a cross-discipline view of trust', *Academy of Management Review*, **23**(3): 393–404.
Shahrokhi, M. (2008), 'E-finance: status, innovations, resources, and future challenges', *Managerial Finance,* **34**(6): 365–98.
Sitkin, S.B. and N.L. Roth (1993), 'Explaining the limited effectiveness of legalistic "remedies" for trust/distrust', *Organization Science*, **4**: 367–92.
Smith, J.B. and D.W. Barclay (1997), 'The effects of organizational differences and trust on the effectiveness of selling partner relationships', *Journal of Marketing*, **61**: 3–21.
Smith, R. (2007), 'Biometric solutions to identity-related crime', in Jewkes Y. (ed.), *Crime Online*, Portland, Oregon: Willan Publishing, pp.44–59.
Sydow, Jörg (1998), 'Understanding the constitution of interorganizational trust in trust within and between organizations', in Christel Lane and Richard Bachman (eds), *Conceptual Issues and Empirical Applications*, Oxford: Oxford University Press.
Symantec (2007), 'Symantec internet security threat report – trends for January–June 2007', vol. 12, September, accessed at www.symantec.com.
The Economist (1997), 'Survey of electronic commerce: in search of the perfect market', 10 May, pp. 3–26.
Tyler, Tom R. and Roderick M. Kramer (1996), 'Whither trust?', in *Trust in Organizations, Frontiers of Theory and Research*, in Roderick M. Kramer and Tom Tyler, Thousand Oaks, CA: Sage.
United Nations Office on Drugs and Crime (UNODC) (2007a), 'Study on "Fraud and the criminal misuse and falsification of identity"', accessed 21 September 2008 at www.unodc.org/documents/organized-crime/E_CN_15_2007_8.pdf.
UNODC (2007b), 'Report of the first meeting of the core group of experts on identity-related crime', 29-30 November, Courmayuer, Italy, accessed 21 September 2008 at www.unodc.org/documents/organized-crime/Courmayeur_report.pdf
UNODC (2008a), 'UNODC and organized crime: identity-related crime', accessed 21 September at www.unodc.org/unodc/en/organized-crime/index.html.
UNODC (2008b), 'Report of the second meeting of the core group of experts on identity-related crime', Vienna, Austria, 2-3 June, accessed 21 September, at www.unodc.org/documents/organized-crime/Final_Report_ID_C.pdf.
Viira, T. (2008), 'Cyber attacks against Estonia: what happened and conclusion', accessed 12 February at www.riso.ee/en/files/IT_yearbook_2007_final.pdf.
websense.com (2009), 'Desk top security', accessed 11 February at www.websence.com/docs/WhitePapers/DesktopSecurity.pdf.
Wetzel, R. (2005), 'Tackling phishing', *Business Communications Review*, **35**(2): 46.
Workman, M., W. Bommer and D. Straub (2008), 'Security lapses and the omission of information security measures: an empirical test of the threat control model', *Journal of Computers in Human Behavior*, **24**: 2799–816.
Yamagishi, T. and M. Yamagishi (1994), 'Trust and commitment in the United States and Japan', *Motivation and Emotion*, **18**: 129–65.
Zaheer, A., B. McEvily and V. Perrone (1998a), 'Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance', *Organization Science*, **9**: 141–59.
Zaheer, A., B. McEvily and V. Perrone (1998b), 'The strategic value of buyer–supplier relationships', *International Journal of Purchasing and Materials Management*, **34**(3): 20–26.

Zand, D.E. (1972), 'Trust and managerial problem solving', *Administrative Science Quarterly*, **17**: 229–239.
Zucker, L.G. (1986), 'Production of trust: institutional sources of economic structure, 1840–1920', in *Research in Organizational Behavior*, **8**: 53–111.

3. Resource-based view and theory

INTRODUCTION

One of the fundamental missions of strategic management research is to investigate and explain differences in performance among firms. The reigning incumbent explanation for the heterogeneity of firm economic performance is based on the concept of competitive advantage. More work has focused on the expanded concept of sustained competitive advantage, which, simply put, is the idea that some forms of competitive advantage are very difficult to imitate and can therefore lead to persistent superior economic performance. Popular extant theories of competitive advantage in strategic management research, based on industrial organization economics (Porter, 1980, 1985) and the resource-based view (RBV) of the firm (Barney, 1991; Conner, 1991), predict that the factors that sustain competitive advantages will generate superior economic performance that persists over time. On the other hand, historical economic theories such as those arising from neoclassical economics and the work of the Austrian school of economics (Schumpeter, 1934), as well as the hypercompetitive model (Brown and Eisenhardt, 1997, 1998; D'Aveni, 1994) of strategy, predict the opposite: that temporal dynamics, resulting from factors such as imitation, entry, and the introduction of substitutes, will erode almost all competitive advantages, and thus prevent superior economic performance from persisting. More recently, Foster and Kaplan (2001) have presented an empirically based, managerial view of the transitory nature of competitive advantage and some of the economic and management mechanisms that generate it.

The central questions addressed by the resource-based view concern why firms differ and how they achieve and sustain competitive advantage. Penrose (1959) argued that heterogeneous capabilities give each firm its unique character and are the essence of competitive advantage. Wernerfelt (1984) suggested that evaluating firms in terms of their resources could lead to insights different from the traditional I/O (industrial/organization) perspective (Porter, 1980). Barney (1986) suggested that strategic resource factors differ in their 'tradability' and that these factors can be specifically identified and their monetary value determined via a 'strategic

factor market'. Barney (1991) later established four criteria to more fully explicate the idea of strategic tradability. He suggested that firm resources and capabilities could be differentiated on the basis of value, rareness, inimitability, and substitutability.

The RBV is one of the latest strategic management concepts to be enthusiastically embraced by information technology (IT) and information management scholars. This book and the empirical analysis carried out maintain that the RBV holds much promise as a framework for understanding strategic information/knowledge economy issues but cautions that, before it is adopted, it needs to be fully understood. This chapter charts the development of the RBV from its origins in early economic models of imperfect competition, through the work of evolutionary economists to the contributions of strategy economics scholars over the past two decades. This broad literature base has given rise to a great deal of ambiguity, inconsistent use of nomenclature, and several overlapping classification schema. The book seeks to draw together common themes of firm heterogeneity, barriers to duplication, sustainable competitive advantage, and Ricardian rents within an overall model of resource-based competitive advantage.

The second part of the chapter describes three aspects of strategic information technology likely to benefit from adoption of the resource-based perspective in developing countries, namely strategic analysis, positioning of an economy, and globalization through cyber activities. In terms of the former, it is argued that the RBV helps to overcome some of the frequently cited problems of the SWOT (strengths, weaknesses, opportunities and threats) framework. Similarly, it contends that understanding a firm's resource base is central to effective positioning while applications in the area of globalization through the diffusion of the Internet highlight important differences between firm-specific and country-specific resources. The chapter concludes by noting some important conceptual and methodological issues that need to be addressed by future research adopting the RBV perspective.

PRINCIPLES OF RBV THEORY

A central principle of the RBV is that performance is a function of an entity's unique resource bundle. Resources are broadly defined to encompass specific assets as well as human competencies and intangible abilities. Ideally, managers will strive to build up resources that are valuable, rare, without substitutes, and structured in a manner so that the organization's resources are unique and difficult to replicate by competitors. Accumulating such resources requires that significant acquisition barriers

be overcome. Thus, managers who overcome these barriers place their organizations in a desirable competitive position. Over time, the most successful organizations may develop such a strong competitive advantage that their competitors will cease their attempts toward imitation through resource accumulation.

The RBV is primarily interested in the extent to which strategies are distinctive. Differences that yield superior organizational performance are determined by the distinct abilities of an organization and its management to accumulate and implement strategic resources. Thus, while generic strategies may be used to label an organization's basic strategic focus, broad generalizations alone are not useful for understanding differences that lead to a sustained competitive advantage.

The resource-based theory provides an explanation to understand why firms do obtain strategic advantage and are able to keep it. It has been used previously in IT to explain how information technology could be used to gain competitive advantage. It also gives an interesting framework to assess whether an activity should be kept within the firm or given to a supplier. It focuses on the strategic resources that firms develop and nurture. Even though they are not always readily discernible, these resources are important investments for organizations and should be leveraged for strategic advantage (Barney, 1991).

The key elements on which the resource-based theory is constructed are simple deviations from the perfect market environment. Resource-based theory argues that, in many situations, three hypotheses of a perfect market are not met: the firms are constrained by their past choices (history matters), the resources are not perfectly mobile, and expertise is not easy to reproduce or imitate. These elements are discussed in sequence. These can be applied at the macro level to a country's economy.

Recent work in the area of resource-based strategy has sought to more clearly explicate the role of resource value in determining firm competitiveness and performance (Barney, 2001; Bowman and Ambrosini, 2000; Priem and Butler, 2001). Bowman and Ambrosini (2000: 1) note that 'a more precise and rounded underpinning theory of value is required to help us identify "valuable resources"'. These authors then proceed to set out a process model that distinguishes between creating new 'use value' and capturing 'exchange value'. We are concerned with both in this chapter, as use value of goods is perceived by potential buyers (e.g. managers), and exchange value is a key determinant in the profitability of resource-based strategies. As we focus mostly on managers' perceptions of value in this chapter, we specifically define value to be that (or those) characteristics of a good that makes the firm better off (more capable, more efficient, more effective, and so on; Barney, 1991) with than without the good. These

characteristics are embodied in the components of our model discussed later. Naturally, there are several ways to define 'value' in this context (Bowman and Ambrosini, 2000; Priem and Butler, 2001). As we are interested in valuation decisions, we agree with Bowman and Ambrosini (2000) that it is the 'use value' perceived by managers that is important, and not value inherent in the good under consideration. Valuable resource bundles are heterogeneous not so much because of inert physical characteristics of the assets but because of their unique employment in the creation of use value. The uniqueness of such employment arises from the initial perceptual differences upon which our model elaborates.

These perceptual insights cannot be easily transferred across firm boundaries. What implications does this have for price and value? Resource-based scholars suggest that value/price discrepancies form the first step in the development of sustainable competitive advantages, as some firms 'see' opportunities that elude others (Barney, 1986; Bowman and Ambrosini, 2000; Kirzner, 1979). Above normal returns accrue in such scenarios as ultimate values are not fully imputed into the costs of procurement (Rumelt, 1987). Sellers in the resource-based scenario may fail to recognize this value, and thus fail to incorporate true asset value into the prices they charge (Barney, 2001); competitors may also fail to grasp these insights and, therefore, will provide less than adequate competition necessary to drive the knowledge-rich firm's returns to 'normal' levels. It is this learned, tacit valuation capability that provides the potential for resource-based competitive advantage (Nelson and Winter, 1982; Penrose, 1959).

Viewed from a growth perspective, resource-based theory is concerned with the origin, evolution, and sustainability of firms (Conner, 1991; Peteraf, 1993). Firms experiencing the highest growth have added new competencies sequentially, often over extended periods of time (Hall, 1992, 1993). Although everyone seems to agree that resources are developed in a complex, path-dependent process (Barney and Zajac, 1994; Dierickx and Cool, 1989), no resource-based theorist has explained or predicted this growth path. With the exception of work investigating the direction of firm diversification (Montgomery and Hariharan, 1991), analysis of the sequential development process of a firm's resource base over time is lacking in the literature.

Resource-based sequencing is important for achieving sustainable growth (Heene and Sanchez, 1997; Montgomery, 1995). In a changing environment, firms must continuously invent and upgrade their resources and capabilities if they are to maintain competitive advantage and growth (Argyris, 1996; Robins and Wiersema, 1995; Wernerfelt and Montgomery, 1998). This sequential development of resources and capabilities can

make a firm's advantage inimitable (Barney, 1991; Lado et al., 1997). Competitors cannot simply buy these resources and capabilities without acquiring the entire firm. This is because the resources and capabilities are built over time in a path-dependent process that makes them inextricably interwoven into a firm. This facet of resources and capabilities development makes it theoretically impossible for competitors to imitate completely (Dierickx and Cool, 1989; Reed and De Fillippi, 1990).

GROWTH AND DEVELOPMENT IN EMERGING COUNTRIES

Going into the twenty-first century, it seems that almost every country wants to be an active participant in the 'New Economy'. This trend is not hard to understand. Many emerging economies have made technology-led economic development a primary goal. Moving beyond technology parks (Egypt), incubation projects (Singapore), and other real-estate-based initiatives (Dubai), developing countries now look to promote information technology entrepreneurs, increase the amount of venture capital, improve basic and applied research, encourage the development and commercialization capacity of higher educational institutions, and attract and retain talented workers and research personnel.

Whatever the state of the IT and life science industries, no one expects technology to become a minor economic concern any time soon. Skills have become the currency of competitiveness for businesses, people, and communities. Information- and knowledge-based technology can only help a country so much if its workforce does not have the skills to apply it. Technology tends to create a demand for more highly skilled workers. Much of labor market research in developed economies shows us that most of the new jobs being created both now and in the future require training beyond a high school level.

To deal with this, some developing economies are looking at ways that universities can partner with industry to provide skills training (American University of Sharjah and American University of Dubai). Some countries target high school education, using school-to-work and other models to start building twenty-first century skills early on (United Arab Emirates (UAE), Mexico, Brazil, India). The key to workforce initiatives is creating business partnerships that can leverage resources and, more importantly, jointly identify skill and training needs for the industry as a whole. A number of developing countries ahead of the learning curve are implementing full-blown human capital investment strategies (India, Singapore, UAE).

Michael Porter and numerous other gurus and researchers have recently been preaching the doctrine of economic 'clusters' that are groupings of economic activity focused on a particular industry within a particular region. These can be high-tech oriented or not; however, as Porter states, there is no such thing as a truly 'low-tech' industry any more. New technological applications can enhance productivity in almost any field, be it agriculture or automobile manufacturing. In a number of developing countries, information technology cluster development has been underway, either with government involvement or only at the regional level (Bangalore, Dubai).

The dawn of the twenty-first century came with a digital revolution and economic globalization with a New Economy. We are moving toward a global knowledge society where information, skills, and competence become the driving forces of social and economic development. Information technology and greater competition at all levels of business and government are transforming the goals and practice of economic development. Beginning in the 1980s, private/public partnerships helped revitalize key industries. Now, a new generation of such partnerships is being formed to focus on technology innovation. These twenty-first century partnerships link technology-based economic development to an area's competitive advantage, providing important models for economic development in the coming years.

As we navigate the new millennium, information technology is driving the key economic development challenges. At the same time, competition has become a daily fact of life at every level of business and government. Consequently, developing countries have realized that to compete in the twenty-first century they must design new ways to turn these dynamics to their advantage. While technology has the power to transform industries, it cannot do so alone. Successful transfer and insertion of new technologies into the workplace are tremendously dependent on other factors, especially an exceptionally skilled workforce willing to suspend conventional practices and recalibrate its skills for new technologies.

Various viewpoints on the development process have been advanced by the many development economy scholars and observers. The leading work of Sen (1999) singles out freedom as both the primary end and principal means of development. Others have paid more attention to poverty reduction and the empowerment of poor people. All approaches regard economic growth as a critical component of the development process and stress that development is about more than growth. Growth in real income is a significant determinant of development but it is not the basic objective. The means and ends of the development process should not be mystified. As a matter of fact, it may thus be possible to improve the human

condition without requiring significant growth in real incomes. In the end the development process is about providing people with real opportunities. Closely linked to this broader definition of development is the importance of poverty reduction in the development process. It is estimated that of the world's 6 billion people, 2.8 billion live on less than US$2 a day and 1.2 billion live on less than US$1 a day (World Bank, 2000). Poverty not only includes material insufficiency but it is also coupled with low levels of education and health, greater weaknesses, possible ill treatment by institutions of the state and society, and powerlessness to influence key decisions. A major objective of poverty alleviation is to enable people to take greater control of their own future. Empowerment requires that people have access to information, participate in decisions that affect them, hold public and private institutions accountable, and develop organizational abilities; information technology and the digital economy make all of these possible. In the 1960s and early 1970s, concern about the impact of economic growth on the environment came to the fore. As a consequence, the concept of sustainable development gained ground. Sustainable development means that the needs of the present should be met without jeopardizing the ability of future generations to meet their own needs The eight Millennium Development Goals (MDGs), adopted by the UN Millennium Summit held in September 2000, exemplify the holistic approach to development. The MDGs are a set of time bound and measurable goals for combating poverty, hunger, disease, illiteracy, discrimination against women, and environmental degradation. The fact that economic growth is not listed as a goal reflects the accepted view that has been described above, namely that growth is a means to achieve development goals, not an end in itself. The MDGs involve eight goals and 18 targets. Economic growth can generate the resources necessary to meet these development challenges. In addition, these goals tie human and economic development together. The MDGs are based on the premise that human and economic development often move in concert. The interdependence of human and economic development suggests that human development is unlikely to be sustained in the face of enduring economic stagnation. Economic growth is driven by two major forces: finding new and better ways of utilizing existing resources, and generating new productive resources through investment. Better utilization of existing resources (especially information technology resources) appears to be the more important of the two factors. Countries utilize resources differently because they have different histories, institutions, cultures, and geographical circumstances. Early research on economic growth focused on the accumulation of capital, such as investment in machinery, equipment, and infrastructure. That is why during the 1950s and 1960s the development strategy in newly independent countries

and other struggling countries stressed investment and speedy industrialization. Other factors and resources have been proven to be major determinants of growth and development. Human capital is one of these factors. Human capital acquired through education and work experience is clearly required in order to operate efficiently and effectively. A better educated labor force makes investment in physical capital more profitable and therefore attracts more of it. However, not all countries with a well-educated labor force and a high investment rate grow. The Eastern European countries during the 1980s are a case in point and again illustrate that it is not the accumulation of capital (human and physical) that is most important, but the way it is utilized. As a conclusion, high-yielding investment opportunities become exhausted if not complemented by other factors such as education and research and development (R&D).

Knowledge has two characteristics which make it a significant contributor to the development process. The first is its permanence, implying that it can be used over and over again. The second is its non-exclusive nature. More than one person can take advantage of knowledge without lessening its value to others. Yet there are huge technology gaps between developed and developing countries. The key questions for understanding the linkage between knowledge and growth are how far ideas spread; how ideas affect behavior and technology; and to what extent a large stock of knowledge makes it easier to discover or create new ideas. When individuals, firms, and governments are able to act upon new ideas in terms of changing behavior, improving technologies, or changing policy respectively, ideas affect economic growth. From the R&D side, common knowledge of technologies – for example how a computer works – can be used by all producers of computers once the innovation has been made. Obviously reproducing what has already been invented is less costly than inventing the product. New innovations create new investment opportunities while the prospect of capitalizing on new inventions motivates further R&D. Capital investment and R&D thus feed on each other in much the same way as investment in human and physical capital feed on each other. Furthermore, R&D prevents investment from running into diminishing returns, as new technologies are more productive than those they replace and new products often fetch higher prices than comparable existing products.

Economic activities are not equally distributed among countries and regions, but tend to cluster in certain areas. In these clusters each activity benefits from access to inputs produced by others located in the same area and to a pool of skills, infrastructure, and business services. A sufficiently large market allows for extensive specialization while each company is still able to exploit economies of scale. Furthermore, when manufacturers have

access to a broad variety of specialized inputs their productivity improves, their costs are reduced, and they can expand sales. As the market expands, room for more specialized producers is created with a further lowering of costs. It is entirely possible for this process to create a self-sustained virtuous cycle.

The forces driving growth and development operate within a social, cultural, geographical, and institutional context. The notion of an institution embodies several elements – formal and informal rules of behavior, ways and means of enforcing these rules, procedures for mediation of conflicts, and sanctions in the case of breach of the rules. Institutions are more or less developed, depending on how well these different features operate. Institutions can create or destroy incentives for individuals to invest in human and physical capital, and the incentives to engage in R&D and work effort. One feature of institutions that is of particular relevance for economic development and growth is the treatment of property rights. In addition to the rule of law, the enforcement of contracts and payment of debts are important. Property rights, combined with access to credit and education, increase in importance with the degree of complexity of the industrial and technological environment. An industrial society, for instance, requires entrepreneurship and creativity. The distribution of such talents in the population is independent of the distribution of income. Limiting economic opportunities to a small percentage of the population represents a huge waste of resources. Conversely, when entrepreneurs have access to funding and can expect to receive a return on their investments, society will be better able to benefit from new technologies and continue to upgrade its industrial base as new technologies arrive. Transparent and efficient institutions that facilitate the establishment and enforcement of contracts therefore become more important as development proceeds. This does not mean that institutions are not important in developing countries. To the contrary, the rule of law and the enforcement of contracts are equally important in developing countries. It is, however, important that the complexity of regulations matches the institutional capacity to enforce the regulations.

A current issue in the development debate is the relative role of institutions and geography in explaining the fact that poor countries tend to be located near the equator. The question is whether a tropical climate per se is detrimental to growth, or whether countries in the tropical climate zone tend to have less development-friendly institutions. The direct impact of the tropical climate on development goes through agriculture and health. While tropical conditions were favorable to agriculture in the very early history of mankind, the invention of heavy ploughs, systems of crop rotation, and the introduction of new crops favored temperate zones. Tropical

diseases are found to have both a direct and an indirect impact on development. They represent higher health risks, and consequently a lower stock of human capital. Furthermore, the demographic transformation toward lower mortality and fertility rates has been slower in tropical areas due to higher health risks. This transformation is part of the development process toward sustained growth. The suggested linkage from climate to institutions is that the prevalence of tropical diseases prevented Europeans from settling, but not from exploiting, the natural resources in tropical areas. They therefore imposed institutions with the exclusive purpose of extracting resources. These institutions concentrated wealth and power within a small elite and the associated structures tended to prevail after independence. A number of empirical analyses suggest that institutions are indeed important determinants of the growth and development process. The concept of institutions is at present rather abstract and the discussion of their role in growth and development has much in common with the discussion in the 1980s of the role of technology, following the first publications on endogenous growth. An understanding of how economic agents and the institutional framework interact in the growth process, and how geography benefits or impedes the process, is emerging. But there are still gaps in our knowledge about what aspects of the institutional framework are the most relevant for growth, to what extent and how the optimal institutional framework depends on geography, culture, religion, and the level of development in each case, and how far and how quickly 'getting institutions right' would generate growth and development. We do know, however, that corruption, severe impediments to trade, and unclear and non-transparent regulations are detrimental to growth and development. Yet the brief discussion above has illustrated the sheer complexity of the growth and development process. No quick fixes have been identified. Nevertheless, in the section that follows, we discuss fairly well-established propositions about the circumstances in which engagement in the world economy can contribute to improved economic performance (UNCTAD, 2003).

Recent research by Thompson et al. (2007) focuses explicitly on information telecommunications networks and the effect they have on business transactions costs, information distribution, and organizational efficiency. Making use of a stochastic-frontier production function approach, the researchers separate the factors responsible for determining frontier production for subsets of countries while simultaneously exploring the impact of communication networks and economic reform on economies below the frontier. The findings are important in their own right and they are that the institutional reforms and the growth in information networks were shown to positively impact the world as a whole, in general, and

the least developed nations, in particular, by improving the efficiency of how these and other resources are used. These findings indicate that comprehensive communication networks work synergistically with economic reforms to build up and enhance business and government relations. However, the study provided evidence indicating that some types of institutional reform, if enforced and applied inadequately, could result in unsuitable consequences. The study concludes that in Africa, with the least developed countries, recent efforts to improve the diffusion of the Internet and telecom penetration, especially mobile phones, have paid off, and that some of this increased 'information communication' is adding to the political stability in that region (Thompson et al., 2007).

THE RESOURCE-BASED VIEW AND ECONOMIC GROWTH

The resource-based view is very insightful and, originally, is centered on the economic entity itself (Porter, 1991). It argues that the origins of competitive advantage are core competencies (valuable resources) that the entity possesses. Most of these resources tend to be intangible assets such as skills, customer and supplier relationships, and reputations, and are viewed as relatively immobile (Khosrow-Pour, 2004). The literature further suggests that successful entities are successful because they are unique resources and they count on these resources to be successful. Furthermore, resources are not valuable unless they allow firms to perform activities that create advantages in particular markets. The competitive value of the resource can be improved or wiped out by changes in technology, competitive behavior, or buyer needs (Porter, 1996).

Ansoff (1965) was one of the first scholars to address sequential stages of firm growth. Ansoff's product–market expansion grid identified stages that a firm would follow to generate growth. The firm would first attempt to gain more market share from its existing products in existing markets (market penetration). Next, its leaders would consider whether the firm could find new markets for its current products (market development). Third, the firm would develop new products for its existing markets (product development). Fourth, the firm would develop new products for new markets. Since Wernerfelt (1984) viewed products and resources 'as two sides of the same coin', it is possible to substitute resources for products in Ansoff's original matrix. This substitution implies the following resource-based arguments: Firms are collections of unused productive services (Penrose, 1959). These unused productive services provide excess capacity. This excess capacity provides an internal mechanism for growth

that allows the firm to better utilize the excess capacity to service existing markets (Penrose, 1959). This utilization of excess capacity may be especially relevant when a firm experiences a transition from an environment of regulation to one of deregulation.

In a regulated environment, a regulatory agency controls the scale and scope of firm operating authority (Hambrick and Finkelstein, 1987; Smith and Grimm, 1987). Thus firms may be constrained from achieving maximum efficiency from their resource base. For example, Johnson et al. (1989) showed that prior to the deregulation of the airline industry, airlines did not pursue strategies that would enhance their efficiency. Upon deregulation, these firms had the option of more fully and creatively using their existing resource bases (Gruca and Nath, 1994), Kelly and Amburgey (1991) empirically demonstrated this change in firm behavior in their study of the deregulation of the airline industry. Utilization of excess capacity increases in a deregulated environment. The use of excess capacity gives the firm an internal mechanism for growth and an opportunity to extract the maximum leverage that its existing resource base can provide (Penrose, 1959). Firms would be expected to utilize excess capacity as their first resource response to deregulation.

Resource-based theory suggests the existence of 'focus effects' (Montgomery and Wernerfelt, 1988). Montgomery and Wernerfelt argued that a given resource will lose more value when transferred to markets that are dissimilar to that in which the resource originated. In their 1988 study, they found that narrowly diversified firms received higher rents (measured as Tobin's Q) than widely diversified firms. This result supports the resource-based hypothesis that expansion by firms into activities in which they have comparative advantages is likely to yield rents (Penrose, 1959). As Wernerfelt pointed out, 'It is better to develop the resource in one market and then enter other markets from a position of strength' (1984: 176). Wernerfelt also asserted that firms will follow a path of sequential entry, first fully using their resource bases in existing domestic markets and then leveraging these existing resources in international markets. Specifically, Wernerfelt discussed the fact that production capacity can be used to support both domestic and international markets. Resources that can be 'dual-utilized' to service international markets provide increasing economies of scale. So firms would tend to make a focus on using existing resources in international markets (gaining international economies of scale) the second resource-sequencing phase after deregulation.

A fundamental idea in resource-based theory is that a firm must continually enhance its resources and capabilities to take advantage of changing conditions (Barney, 1991; Kraatz and Zajac, 1997). Optimal growth involves a balance between the exploitation of existing resource

positions and the development of new resource positions (Chatterjee and Wernerfelt, 1991; Ghemawat and Costa, 1993; Hansen and Wernerfelt, 1989; Itami and Numagami, 1992; Rubin, 1973). Thus, a firm would be expected to develop new resources after its existing resource base has been fully utilized. Building new resource positions is important if the firm is to achieve sustained growth. When unused productive resources are coupled with changing managerial knowledge, unique opportunities for growth are created (Castanias and Helfat, 1991; Cohen and Levinthal, 1990; Henderson, 1994; Henderson and Cockburn, 1994; Teece et al., 1997).

Only recently have scholars begun to focus on how firms first develop firm-specific resources and then renew these to respond to shifts in the business environment (Henderson, 1994; Iansiti and Clark, 1994; Teece et al., 1997). Firms in essence develop dynamic capabilities to adapt to changing environments (Dierickx and Cool, 1989; Chandler, 1990; Teece and Pisano, 1994). The term 'dynamic' refers to 'the capacity to renew resource positions to achieve congruence with changing environmental conditions' (Teece et al., 1997: 515). A 'capability' refers to 'the key role of strategic management in appropriately adapting, integrating, and reconfiguring internal and external organizational skills, resources, and functional capabilities to match the requirements of a changing environment' (Teece et al., 1997: 515).

When a firm has extracted the maximum value it can from its existing resource base, then it must develop dynamic capabilities to maintain growth in a dynamically changing environment. From a dynamic capability perspective, the firm continually replaces previously defined sources of competitive advantage with new sources of advantage to provide for dynamic firm growth (Bogner and Thomas, 1994; Hamel and Heene, 1994).

If firms are to develop dynamic capabilities, learning is crucial. Change is costly; therefore, the ability of firms to make necessary adjustments depends upon their ability to scan the environment to evaluate markets and competitors and to quickly accomplish reconfiguration and transformation ahead of the competition (Teece et al., 1997). However, 'history matters' (Nelson and Winter, 1982). Thus, opportunities for growth will involve dynamic capabilities closely related to existing capabilities (Teece and Pisano, 1994). As such, opportunities will be most effective when they are close to previous resource use (Teece et al., 1997). Firms would develop dynamic capabilities within existing markets in the third resource-sequencing phase.

After dynamic capabilities have been developed, resource-based theory suggests, there are managerial limits to the rate of firm expansion (Penrose, 1959). Existing managers must train new managers, in the so-called

Penrose effect (Morris, 1964; Shen, 1970; Slater, 1980). Penrose stated this: 'Managerial resources with experience within the firm are necessary for the efficient absorption of managers from outside the firm. Thus, the availability of inherited managers with such experience limits the amount of expansion that can be planned and undertaken in any period of time' (1959: 49). Empirical evidence shows that firms that have grown rapidly in one period typically regress to the average growth rate in the next time period (Ijiri and Simon, 1977; Shen, 1970). On the basis of the Penrose effect, we would expect firms to utilize the excess capacity provided by the dynamic capabilities as the fourth resource-sequencing phase.

Responding to environmental change is not sufficient to generate long-term growth. As Penrose pointed out, 'The environment is not something out there, fixed and immutable, but can itself be manipulated by the firm to serve its own purposes' (1985: xiii). Building new resource sets to service emerging markets is one way of generating long-term firm growth (Hamel and Heene, 1994; Hamel and Prahalad, 1994; Sanchez et al., 1996). This view of firms as being able to interpret and lead environmental change extends the traditional position of the firm beyond responding to environmental change ex post. By acquiring new resources to service new markets, a firm can shape environmental change that may alter the competitive environment in its favor to provide for long-term growth (Hamel and Heene, 1994). The capability to lead environmental change is related to the concept of 'creative destruction'.

Schumpeter (1942) first developed this concept, stating that '[gales of creative destruction] revolutionized the economic structure by destroying the old and creating a new one' (Schumpeter, 1942: 83). The new focus of the RBV is firms' ability to create the 'rules of the game' by developing new resources to service new markets (Hamel and Prahalad, 1994; Levinthal and Myatt, 1994; Sanchez et al., 1996). This is a core competence perspective. It extends the traditional notion of the fit of a firm's capabilities to its environment to embrace the idea that a firm can change to acquire new competencies that can shift the competitive environment in its favor (Collis, 1991, 1994; Hamel and Heene, 1994). This ability of the firm to lead environmental change depends upon its managerial resources (Penrose, 1959).

The resource-based view of organizations can be used as a theoretical perspective to explain how IT infrastructure and electronic government may be viewed as a source of competitive advantage. According to this theory, the internal resources of any economy can be one source of sustained competitive advantage. If one country has a particular resource not easily created, bought, substituted, or imitated by others, then this resource confers some degree of sustained competitive advantage on the economy

that possesses it. The speed of change in the competitive landscape coupled with increasing hyper-competition necessitates the development of global dynamic capabilities, which is the creation of difficult-to-imitate combinations of resources on a global basis that provide a competitive advantage (D'Aveni, 1999; Eisenhardt and Martin, 2000; Teece et al., 1997). The RBV has traditionally focused on firm-level resources (i.e. internal factors semi-permanently linked to the organization) providing a firm with a unique competitive posture (Barney, 1991; Dierickx and Cool, 1989; Wernerfelt, 1984). But recently, researchers have demonstrated that a RBV of idiosyncratic inter-firm linkages can be a source of relational rents and competitive advantage (Dyer and Singh, 1998), thus extending the RBV.

Powerful forces for change are re-mapping the economic and business environment but they have also led to a key alteration in organizational processes. The fundamental drivers of change comprise globalization, higher degrees of complexity, new technology, intense competition, volatile customer demands, and movements in the economic and political structure. These evolutions mean companies must strive to learn quickly, respond faster, and proactively adapt and shape their organizations. Firms are beginning to perceive that the conventional product-based competitive advantages are transient and that the only sustainable competitive advantages they possess are their resources (Barney, 1991). This means a greater focus, in practice, on intangible assets. To maintain competitive momentum and to endure over time in a competitive market, organizations need to measure, assess, and manage their strategic potential with incomparable efficacy.

Country-Specific Factors

Evaluating country-specific factors such as the political system, the regulatory framework, and the cultural variables will help us assess the level of economic growth. Supposedly, the level of economic development of the country will be associated with a higher interest in strategic issues in information technology management, and therefore investment and management of electronic governments. Among the strategic issues in IT we can mention IT-based business process redesign, planning, and managing telecommunications networks, improving information systems strategic planning, and so on (Brancheau et al., 1996). On the other hand, issues such as the scarcity of qualified human resources and obsolescence of computing equipment are still of a great importance in under-developed countries (Palvia et al., 1992). A few countries such as the United Arab Emirates have developed very useful policies and adopted strategies to (1)

develop their indigenous workforce through training and education, and (2) attract talents from neighboring countries by facilitating movement of skills into the country (Karake Shalhoub and Al Qasimi, 2003).

Political and regulatory factors in different countries also have an effect on key IT management issues such as the transformation into electronic government. Chepaitis (1996) emphasizes the problems caused by the effect of a political system that includes control and pressure by the authorities, poor public data stores, and a lack of competitive market experience. The political and governance philosophy (socialism, capitalism, communism, democracy, or dictatorship) affects therefore the conditions in which electronic government is managed and developed (Palvia et al., 2002).

Differences in national cultures also play an important role in the success or failure of e-government initiatives. The study of Hofstede (1980) has provided the basis for analysing the cultural impact on key IT issues, including electronic governments. Hofstede (1980) defined four dimensions of national culture: individualism/collectivism, power distance, uncertainty avoidance, and masculinity–femininity. There are important precedents in the study of the effect of national culture on IT management. Nelson and Clark (1994) proposed a research agenda of the cross-cultural impact on managing information systems; Shore and Venkachalam (1995) analysed differences in systems analysis and design related to culture. In other cases, the relationship between culture and technology acceptance (Kwon and Chimdambaran, 1998) and between culture and group support systems adoption (Davison and Jordan, 1998) has been the object of analysis. This question is still a very open line of investigation, because other studies do not find a direct relationship between different national cultures and IS management issues.

Firm-Specific Factors

Firm-specific factors can also impose upon key IT management issues, including the management of electronic governments. Most information technology research has considered the type of industry a firm competes in as an independent variable (Palvia et al., 2002). The level of development, the composition, and the objective of the IT portfolio can differ depending on the type of industry. Niederman et al. (1991) studied the differences in information technology management in manufacturing, service, and non-profit organizations. Service and manufacturing firms seem to manage some IS issues in a different manner, as has been suggested by Deans et al. (1991). They found that computer-integrated manufacturing, local cultural constraints, and vendor support in foreign subsidiaries were more important for manufacturing companies. On the other hand, data

security, data utilization, currency restrictions, and exchange rate volatility were more important for service firms (Palvia et al., 2002).

Global strategies is the second firm-specific element included in the study of Palvia et al. (2002). Based on the model of Bartlett and Ghoshal (1989), it is possible to analyse the relationship between the four basic strategies of internationalization (multinational, global, international, and transnational) and IT architecture. As Palvia et al. (2002) point out, most previous work suggests that aligning IT architecture strategies with each type of global business strategy is a critical success factor for global firms.

Global business and IT strategy is the fourth firm-specific factor that can affect key IT issues. Several IT management issues may have an important impact on the firm strategy definition and implementation. The utilization of IT as a driver of the firm's strategy has been a topic in business management since the early 1980s (Parsons, 1983; Porter and Millar, 1985) that has been revisited in the 1990s (e.g. Henderson and Venkatraman, 1993). Given that IT can delimit the firm strategy, the global strategy of the firm can also be shaped by IT issues. The means of introduction and expansion in new markets or the defense strategies against external competitive pressures can be interrelated to IT utilization and development choices. As an example, some multinational firms use new logistics and commercialization electronic devices to quickly cut costs and therefore to oust national, non-technological competitors from the markets in which they enter/participate.

Country-specific variables and firm-specific variables will be used in the next sections to explain the relationship between global issues and the main theoretical frameworks developed in IT general management.

THE RESOURCE-BASED VIEW AND GLOBAL ISSUES

The RBV (Wernerfelt, 1984) has been the dominant view in the development of the strategic approach in recent times (Hoskisson et al., 1999). According to the RBV, a firm that possesses a valuable, rare, and difficult-to-imitate or to -substitute resource will achieve a sustainable competitive advantage. A large number of studies have related the creation of value by means of IT with the gaining and maintenance of competitive advantage (for example Powell and Dent-Micallef, 1997; Bharadwaj, 2000). The options for further study in this area consist of the identification of new resources complementary to IT and the description of the conditions under which IT behaves as a valuable resource. Additionally, it would be useful to supplement the RBV with other approaches, such as the abovementioned institutional theory (Selznick, 1957) or that of the appropriation

of value by stakeholders (Coff, 1999). Despite this weakness, the RBV, complemented by the dynamic capabilities framework (Teece et al., 1997) can serve as a basis from which to explain the competitive impact of IT over a time period, an area with little empirical evidence so far.

The RBV has a number of points in common with other theoretical frameworks, such as the upper echelon (Hambrick and Mason, 1984; Karake, 1995), knowledge management (Kogut and Zander, 1992; Nonaka, 1994), and the organizational stakeholders approach (Coff, 1999). Apart from the knowledge management view, which has already added significantly to the study of IT, the upper echelon and the stakeholders approach can be further developed in the future. The first (Pinsonneault and Kraemer, 1997; Pinsonneault and Rivard, 1998) may be able to explain the interrelation between the characteristics of management (age, previous experience, technological knowledge, and international experience) and the effective introduction of the new technologies. It should be noted that there is a strong parallel between this approach and the RBV because the personal and career characteristics of the executives can be resources that are valuable, scarce, and difficult to imitate, and in combination with IT they may have a positive and lasting effect on competitive position. The second may be able to explain the situations in which IT generates value although the organization cannot take advantage of it in the form of income, benefits, or in general, increase in competitive advantage. In these cases there are certain powerful groups in the organization (stakeholders) that might absorb the resource's capacity for creation of value.

Other research questions arise if we consider approaches related to RBV, such as the knowledge management view and the stakeholders view. First, more research is needed to fully understand the relationship between IT utilization and competitive advantage using knowledge management practices by the same firm in different parts of the world. As an example, firms that try to compete in new markets could find difficulties implementing knowledge-sharing practices in countries with a high individualistic orientation. Secondly, the stakeholder approach can be used to explain specific situations in which branches of multinational firms that introduce a valuable IT-based system do not achieve better economic results. In these cases, the parent company might be appropriating the economic rents generated by the IT.

To turn the new elements of e-commerce technology and Internet information systems into competitive advantage, the firm must find some way to turn them into an invisible asset that other firms cannot easily copy (Barney, 1991). Yet the very nature of the cyber space revolution, its openness and the ability of all players to access the new technologies, means that hard aspects alone are not going to be easily transformed into

a competitive advantage for the firm. Customers may still benefit from lower costs and increased bargaining power, yet firms will have to find something extra if they are to find competitive advantage in these new technologies and systems. This can be found in the soft aspects of information management. Even if hard elements are easily accessible, two possible sources of competitive advantage remain: effective utilization of these hard technologies within the wider organization of the firm, and unique combinations of the soft organizational and hard systemic aspects of the cyber space revolution.

When a firm does make use of these organizational skills, the resulting information flows are more likely to be an invisible asset than those based purely on information technology or information systems. These flows can be from the firm to its environment, from customers to the firm, and internally within the firm. Competitors cannot easily duplicate the 'experiences of working together'. These assets are not easily purchased in the market, and even when created within the firm, take time to develop. A firm that responds quickly to the challenge of new technologies and systems has an organization with an advantage in dealing with technological change.

Combinations of assets can often be used to set a firm's strategy apart from competitors' strategies (Itami and Roehl, 1987). Firms that might not have a single outstanding technology may still be able to create a portfolio of invisible assets that allows them to be competitive.

International business literature also addresses this issue. Mathews (2002) argues that firms from developing countries can still become multinationals by combining the skills and relationships available globally with a dynamic internal company organization. In the case of e-commerce, it is the combination of hard and soft elements that can produce a portfolio of assets that is hard for competitors to copy easily. Firms that combine the hard elements of e-commerce technology and systems effectively are likely to find themselves strongly positioned in the marketplace (see Globerman et al., 2001 for examples from electronic brokerage).

Systems for knowledge development work best when the firm has created an atmosphere in which organizational innovation can easily take place (Nonaka and Takeuchi, 1995). Thus, a firm that has taken the first step of establishing an organization that is able to create soft elements is also able to create new combinations of assets that further strengthen its position (Brynjolfsson and Hitt, 2000; Itami and Roehl, 1987).

RBV theory has shed light on the hidden side of competitive assets: the soft, invisible, or intangible assets. They are at the heart of the key capabilities of the innovative firm (Christensen and Overdorf, 2000), for example, leadership and change management as resources, new knowledge creation as processes, and reciprocity and information sharing as values. Ideally,

these assets should be created in the course of regular operations, since doing so reduces the cost of acquiring the assets and tests them against the day-to-day issues faced by all employees of the firm. Hard resources alone are often easily available to competitors, as Globerman et al. (2001) have shown in the case of the electronic brokerage industry.

Nature and Categories of Resources

According to Wernerfelt, resources can include 'anything that might be thought of as a strength or weakness of a given firm' and so 'could be defined as those [tangible and intangible assets] which are tied semi permanently to the firm' (1984: 172). Resources are said to confer enduring competitive advantages to a firm to the extent that they are rare or hard to imitate, have no direct substitutes, and enable companies to pursue opportunities or avoid threats (Barney, 1991). The last attribute is the most obvious: resources must have some value – some capacity to generate profits or prevent losses. But if all other firms have them, resources will be unable to contribute to superior returns: their general availability will neutralize any special advantage. And for the same reason, readily available substitutes for a resource will also nullify its value. Thus, resources must be difficult to create, buy, substitute, or imitate. This last point is central to the arguments of the resource-based view (Barney, 1991; Lippman and Rumelt, 1982; Peteraf, 1993). Unusual returns cannot be obtained when competitors can copy each other. Thus, the scope of this study will be limited strictly to non-imitable resources.

Clearly, there are many resources that may meet these criteria, albeit with differing effectiveness under different circumstances: important patents or copyrights, brand names, prime distribution locations, exclusive contracts for unique factors of production, subtle technical and creative talents, and skills at collaboration or coordination (Black and Boal, 1994). There are a number of ways in which the resource-based view can be further developed. First, it may be useful to make some basic distinctions among the types of organizational resources that can generate unusual economic returns. By specifying the distinctive advantages of different types of resources, it may be possible to add precision to the research. Such distinctions will help avoid vague inferences that impute value to a firm's resources simply because it has performed well (cf. Black and Boal, 1994; Fiol, 1991).

Secondly, to complement its internal focus, the resource-based view needs to delineate the external environments in which different kinds of resources would be most productive. Just as contingency theory attempts to relate structures and strategies to the contexts in which they are most appropriate (Burns and Stalker, 1961; Thompson, 1967), so too must the

resource-based view begin to consider the contexts within which various kinds of resources will have the best influence on performance (Amit and Schoemaker, 1993). According to Porter, 'Resources are only meaningful in the context of performing certain activities to achieve certain competitive advantages. The competitive value of resources can be enhanced or eliminated by changes in technology, competitor behavior, or buyer needs which an inward focus on resources will overlook' (1991: 108).

Thirdly, there is a need for more systematic empirical studies to examine the conceptual claims of the resource-based scholars. Such studies, although growing in number (cf. Henderson and Cockburn, 1994; McGrath et al., 1995; Montgomery and Wernerfelt, 1988; Robins and Wiersema, 1995), remain too rare, perhaps because of the difficulties of pinning down the predictions of the resource-based view and even of operationally defining the notion of resources (Black and Boal, 1994; Fiol, 1991; Peteraf, 1993).

Several researchers have attempted to derive resource categorization schemes. Barney (1991) suggested that resources could be grouped into physical, human, and capital categories. Grant (1991) added to these financial, technological, and reputation creative resources. Although very useful for the purposes for which they were designed, these categorizations bear no direct relationship to Barney's (1991) initial criteria for utility, namely value, rarity, difficulty of imitation, and unavailability of substitutes. In this chapter we revisit a pivotal one of these criteria-barriers to imitability to develop our own typology. Imitability may be an important predictor of performance as, indeed, it is a central argument of the resource-based view that a firm can obtain unusual returns only when other firms are unable to imitate its resources (Barney, 1991; Lippman and Rumelt, 1982). Otherwise these resources would be less rare or valuable, and substitutability would become irrelevant.

Property-based versus knowledge-based resources

There appear to be two fundamentally different bases of nonimitability (Amit and Schoemaker, 1993; Hall, 1992, 1993; Lippman and Rumelt, 1982). Some resources cannot be imitated because they are protected by property rights, such as contracts, deeds of ownership, or patents. Other resources are protected by knowledge barriers – by the fact that competitors do not know how to imitate a firm's processes or skills.

Property rights control 'appropriable' resources: those that tie up a specific and well-defined asset (Barney, 1991). When a company has exclusive ownership of a valuable resource that cannot be legally imitated by rivals, it controls that resource. It can thereby obtain superior returns until the market changes to devalue the resource. Any rival wishing to obtain

the resource will have to pay the discounted future value of its expected economic returns. Examples of property-based resources are enforceable long-term contracts that monopolize scarce factors of production, embody exclusive rights to a valuable technology, or tie up channels of distribution. Property-based resources apply to a specific product or process. And many such resources buffer an organization from competition by creating and protecting assets that are not available to rivals – at least not under equally favorable terms (Black and Boal, 1994: 134). Typically, it is only the fortunate or insightful firms that are able to gain control over valuable property-based resources before their full value is publicly known.

Most competitors will be aware of the value of a rival's property-based resources, and they may even have the knowledge to duplicate these resources. But they either lack the legal right or the historical endowment to imitate successfully. Indeed, it might be argued that in order for property-based resources to generate unusual economic rents, they require protection from exclusionary legal contracts, trade restrictions, or first-mover pre-emption (Conner, 1991; Grant, 1991).

Many valuable resources are protected from imitation not by property rights but by knowledge barriers. They cannot be imitated by competitors because they are subtle and hard to understand because they involve talents that are elusive and whose connection with results is difficult to discern (Lippman and Rumelt, 1982). Knowledge-based resources often take the form of particular skills: technical, creative, and collaborative. For example, some firms have the technical and creative expertise to develop competitive products and market them successfully. Others may have the collaborative or integrative skills that help experts to work and learn together very effectively (Fiol, 1991; Hall, 1993; Itami, 1987; Lado and Wilson, 1994).

Knowledge-based resources allow organizations to succeed not by market control or by precluding competition, but by giving firms the skills to adapt their products to market needs and to deal with competitive challenges. Economic rents accrue to such skills in part because rivals are ignorant of why a firm is so successful. It is often hard to know, for example, what goes into a rival's creativity or teamwork that makes it so effective. Such resources may have what Lippman and Rumelt (1982) called 'uncertain imitability': they are protected from imitation not by legal or financial barriers, but by knowledge barriers. The protection of knowledge barriers is not perfect – it may be possible for competitors to develop similar knowledge and talent. But this normally takes time, and by then a firm may have gone on to develop its skills further and to learn to use them in different ways (Lado and Wilson, 1994).

The respective advantages of property-based and knowledge-based

resources are quite different. Property rights allow a firm to control the resources it needs to gain a competitive edge. They may, for example, tie up advantageous sources of supply, keeping them out of competitors' hands. Such control of a specific asset, in effect, is the only source of value for property-based resources. Knowledge-based resources typically are better designed to respond and adapt to the challenges facing an organization. Creative skills, for instance, can be used to interpret customer desires and respond to developing market trends. Of course, property- and knowledge-based resources are not always independent, as the latter may sometimes be used to develop or procure the former. A key theme of this chapter is that the benefits of property-based resources are quite specific and fixed, and thus the resources are appropriate mostly for the environment for which they were developed. For example, a process patent ceases to have value when it has been superseded by a new process; a prized location becomes useless when customers move away. In short, a particular property right stops being valuable when the market no longer values the property. As a result, when the environment changes, property-based resources may lose their advantage. This is especially true if the environment alters in ways that could not have been predicted when the property was developed or acquired or when the fixed contract was made (Geroski and Vlassopoulos, 1991). Thus, an uncertain environment – one that is changing and unpredictable – is the enemy of property-based resources. Knowledge-based resources, on the other hand, often tend to be less specific and more flexible. For example, a creative design team can invent products to meet an assortment of market needs Such resources can help a firm respond to a larger number of contingencies (Lado and Wilson, 1994). Many knowledge-based resources are in fact designed to cope with environmental change. Unfortunately, these resources are not protected by law from imitation, and many are unduly expensive in predictable settings, where more routine but far cheaper response mechanisms can be equally effective. Also, in placid environments a firm's knowledge may evolve so slowly as to be subject to imitation by rivals. In short, property-based resources will be of the greatest utility in stable or predictable environments, whereas knowledge-based resources will be most useful in uncertain, that is, changing and unpredictable, environments.

Some property-based resources are in the form of systems and their interwoven components; these typically include physical facilities and equipment. By themselves, most concrete facilities are easily imitable: thus, much of their value relies on their role within and their links to an integrated system whose synergy is hard to duplicate (Barney, 1991; Black and Boal, 1994). This is true of some integrated supply, manufacturing, and distribution systems. The units of a distribution network, for example,

may be valuable because of their connection with a steady source of supply or with economies of administration and promotion engendered by a well-respected parent company (Barney, 1991; Brumagin, 1994).

In the case of systemic resources, managers do not aim to tie up more and more individual assets, but to enhance the range and comprehensiveness of a pre-existing system. Resources are added not to substitute for existing assets but rather to strengthen a system or competence that is already in place. For example, one might acquire more distributors or outlets to bolster a distribution system (Lado et al., 1992). The more elaborate the system, the more market penetration it can provide, the more economically it can allocate marketing, administration, and even operating expenses, and the more it can make use of an established brand image or reputation.

Like discrete property-based resources, systemic resources will be more useful in predictable than in uncertain competitive environments. When an environment is predictable, it is easier to appraise the value of systems and to augment them in an orderly way with the aim of increasing the scope of market control. Predictability also allows a firm to determine the steps that it needs to take to fortify its system. Indeed, it is only when the environment is predictable and the existing system is secure that it makes sense for a firm to develop that system.

When the environment is changing unpredictably, however, managers may be reluctant to build on to a system whose longevity is difficult to estimate or that is at risk of becoming obsolete. For example, if distribution technology changes unpredictably, one cannot build on to existing networks. And in an uncertain environment in which clients' demands are ever changing and hard to anticipate, most property-based systems are threatened with obsolescence (Wernerfelt and Karnani, 1987). Here the useful life of systemic resources may be short and hard to predict, and a firm may find itself controlling assets that generate little revenue (Geroski and Vlassopoulos, 1991).

To parallel our analysis of property-based resources, we examine both discrete and systemic knowledge-based resources (Black and Boal, 1994; Brumagin, 1994). Discrete knowledge-based resources may take the form of specific technical, functional, and creative skills (Itami, 1987; Winter, 1987). Such skills may be valuable because they are subject to uncertain imitability (Lippman and Rumelt, 1982). It is often hard to discern just what it is about these skills that generates economic returns or customer loyalty. Therefore, competitors do not know what to buy or imitate. This advantage is protected precisely because it is in some way ambiguous and mysterious, even to those who possess it (Lado and Wilson, 1994; Reed and DeFillippi, 1990). As with discrete property-based resources, firms

can benefit from simultaneously developing as many of these knowledge resources as possible. For example, firms can at the same time pursue expertise in design, production, and marketing. Although unforeseeable changes in markets may render many property-based resources obsolete, knowledge-based resources such as unusual creative and technical skills may remain viable under varying conditions. Indeed, they may actually help a firm adapt its offerings to a changing environment (Wernerfelt and Karnani, 1987). Some creative skills are also quite flexible as they apply to different outputs and environments. And this makes them especially useful in a changing, uncertain setting. For example, where the environment is particularly competitive and rivals are introducing many new offerings, the skills of experts who can adapt and create better products will be especially valuable. In a stable or predictable environment, firms may also benefit from discrete skills. But these afford less effective, less efficient, and less secure advantages than do discrete property-based resources. Where a firm can enforce its legal property rights, it possesses almost perfect protection against imitation. This is not true of the protection given by knowledge, which can be lost, especially in stable settings in which knowledge and its application evolve more slowly and are thus easier to copy. Moreover, the high costs of retaining very talented employees may not produce much net benefit in stable contexts that do not demand the full exploitation of their unusual abilities.

Predictable settings do not typically call for as deep or extensive a set of skills for product or process innovation and adaptation as do uncertain and changing environments (Miller, 1988; Miller and Friesen, 1984).

Systemic knowledge-based resources may take the form of integrative or coordinative skills required for multidisciplinary teamwork (Fiol, 1991; Itami, 1987). Some organizations not only have a depth of technical, functional, and creative expertise but are also adept at integrating and coordinating that expertise. They invest in team-building and collaborative efforts that promote adaptation and flexibility. Indeed, it is not just skills in any one domain, but rather the way skills from several domains complement one another in a team that gives many firms their competitive advantage (Hall, 1993; Itami, 1987; Teece et al., 1990; Winter, 1987).

Collaborative skills are most subject to uncertain imitability (Hall, 1993; Peteraf, 1993: 183). According to Reed and DeFillippi, 'ambiguity may be derived from the complexity of skills and/or resource interactions within competencies and from interaction between competencies' (1990: 93). There is much subtlety in effective teamwork. The systemic nature of team and coordinative skills makes them especially firm specific – more valuable to a firm than to its competitors (Dierickx and Cool, 1989: 1505). Team talents, therefore, are difficult for rivals to steal as they rely on the

particular infrastructure, history, and collective experience of a specific organization.

Collaborative skills typically do not develop through programmed or routine activity. Instead, they require nurturing from a history of challenging product development projects. These long-term projects force specialists from different parts of an organization to work together intensively on a complex set of problems. And such interaction broadens both the technical and social knowledge of organizational actors and promotes ever more effective collaboration (Itami, 1987; Schmookler, 1966).

The above arguments suggest that team building is apt to be more necessary, more rewarding, and perhaps even more likely in uncertain than in predictable environments (Hall, 1993; Porter, 1985). Collaborative talents are robust – they apply to a wide variety of situations and products. In contrast with fixed routines, teamwork enables companies to handle complex and changing contingencies (Thompson, 1967). Moreover, 'unlike physical assets, competencies do not deteriorate as they are applied and shared . . . They grow' (Prahalad and Hamel, 1990: 82). Collaborative skills not only remain useful under changing environments, but they also help firms to adapt and develop new products for evolving markets (Lawrence and Lorsch, 1967; Thompson, 1967). Indeed, the flexibility born of multifunctional collaboration will help firms to respond quickly to market changes and challenges (Mahoney and Pandian, 1992; Wernerfelt and Karnani, 1987).

In stable environments, on the other hand, the returns to collaborative and adaptive skills may be small. Where tasks are unvarying, coordination can be routinized very efficiently, and thus coordinative or team skills will be less important (Thompson, 1967). Moreover, when customer tastes and rivals' strategies are stable, there is little need to constantly redesign or adapt products. In such contexts, the benefits of intensive collaboration may not justify the costs.

THE RESOURCE-BASED VIEW, STRATEGY, AND ECONOMICS

The resource-based view (RBV) approaches the firm as a historically determined collection of assets or resources which are tied semi-permanently to the firm's management (Wernerfelt, 1984). Some users of the RBV distinguish fully appropriable resources, such as physical capital or brand names, from less tangible assets, such as organizational routines and capabilities. Similarly, distinctions may be drawn between static and dynamic resources. The former are those that, once in place, may be considered to

represent a stock of assets to be utilized as appropriate over a finite life. Dynamic resources may reside in capabilities, for example, such as an organization's capacity for learning, that generate additional opportunities over time. It is worth noting that the crucial requirements of the RBV are that the relevant resources, whatever their nature, are specific to the firm and not capable of easy imitation by rivals (Barney, 1991). Therefore, such resources constitute the source of Ricardian rents that comprise a firm's competitive advantage and, to the extent that their replication by others is problematic, imply a sustainable advantage over the longer term. Since each firm's resource bundle is unique, the consequence of its past managerial decisions and subsequent experience, it follows that so is each firm's opportunity set.

Thus it would appear that the RBV directly addresses issues that are of central interest to researchers in strategy and economics alike. Strategy may be considered as the process of determining, exploiting, and developing a firm's opportunity set. Here the RBV would appear to offer direct insights. Economics is fundamentally concerned with the efficiency of resource allocation to productive users. This includes, or certainly should include, a consideration of the behavior of the firm, as the principal productive unit in capitalist economies, as well as comparative institutional assessments of alternative configurations of economic activity (for example vertical integration versus out-sourcing, franchising versus ownership, etc.). Here we would contend that the RBV offers important insights into the delineation of appropriate boundaries of the firm and hence for firm performance and economic organization. However, when we compare *explicit* interest in the RBV across the disciplines of strategy and economics there is a clear and obvious asymmetry. In strategy the RBV has been highly influential. Hoskisson et al. (1999) point out that from the 1960s until the late 1980s, the subject was dominated by consideration of external (that is, product market) sources of competitive advantage. This reflected the influence of structure, conduct, performance (SCP) work, in general, and the particular success of Michael Porter (1980, 1985) in synthesizing this in a strategy context. Hoskisson et al. (1999) suggest that the growing popularity of the RBV since the late 1980s has refocused attention on internal sources of competitive advantage.

In the economics journals, by contrast, explicit references to the RBV are scarce. A citation search, covering 165 economics journals, revealed that only a very small proportion of cites of the leading RBV papers occurs in the economics literature. For example, in not one of the key papers by Wernerfelt (1984), Barney (1991), and Conner (1991) did the proportion of citations in the economics literature rise above 5 percent. Restricting attention to the ten leading 'core' influential economics journals, following

Stigler et al. (1995), produces an even bleaker picture, with a total of three citations. However, a concentration on the lack of explicit attention given to the RBV in economics conceals the very considerable influence that has been achieved by many of the ideas that underpin it. The same contributions that informed the architects of the RBV, particularly those of Penrose (1959), Richardson (1972), and Teece (1980), who at the time of these publications would have been considered mainstream economists, have received much greater attention in the economics literature than the subsequent RBV papers. Papers of the three above-mentioned authors appear to have helped economists trained in the neoclassical tradition to accept the importance of path dependency in firm evolution. The result is that over the last decade or so, a period corresponding to the diffusion of the RBV in strategy, there has been a very substantial output of applied economics research that has sought to explain firm decision making and firm performance in a context in which history matters. Firm behavior is typically modeled as a consequence of existing firm-level attributes, many of which, (for example size, diversification, vertical integration, market and technological experience, etc.) may be considered as proxies for the firm-specific assets discussed by proponents of the RBV.

This growing economics literature on the importance of path dependency in firm development is reviewed below. That it has largely bypassed any explicit consideration of the RBV does not, in our opinion, invalidate the conclusion that its findings provide a systematic body of evidence that is both largely supportive of the predictions of the RBV and, as such, worthy of the interest of strategy scholars. That is not to say, of course, that many of the papers reviewed would not have benefited from insights drawn from the RBV. This point is developed below.

THE RESOURCE-BASED VIEW AND NEW INSTITUTIONAL ECONOMICS

As stated by North (1990), the New Institutional Economics is an attempt to incorporate a theory of institutions into economics. However, in contrast to the many earlier attempts to topple or take the place of neoclassical theory, the New Institutional Economics builds on, amends, and broadens neoclassical theory to allow it to come to grips and deal with an entire range of issues beyond its domain. What it maintains and builds on is the fundamental assumption of scarcity and hence competition. What it leaves behind is instrumental rationality – the assumption of neoclassical economics that has made it an institution-free theory. Institutions are formed to reduce uncertainty in human exchange. Together with the technology

utilized they determine the costs of transacting. Coase (1937) made the central connection between institutions, transaction costs, and neoclassical theory. As he stated, 'the neoclassical result of efficient markets only obtains when it is costless to transact; when it is costly to transact, institutions matter' (p. 391). And because a large part of our national income is devoted to transacting, institutions and specifically property rights are crucial determinants of the efficiency of markets.

Practically, there is still a tendency for the resource-based theory and the branches of New Institutional Economics to be used in isolation from one another. For example, much research in financial economics still assumes away firm heterogeneity, except perhaps for industry membership, and concentrates upon the agency problem, while some strategy research ignores agency considerations as belonging to a lower level or strategy implementation dimension. This division is far from universal and it was seen above that the analysis of corporate refocusing issues has drawn liberally upon both traditions. However, one consequence of the bifurcation is the relative neglect of governance–RBV interactions. It was noted earlier that the internal governance devices adopted by the firm (the composition of its board, the control systems covering its divisional management, etc.) do not merely have implications for the level of agency costs, but have implications for the optimal configuration of the firm's activities.

The firm's governance mechanisms (both internal and external) are to be considered as a relevant resource. For example, in the USA or UK these could include the skills of the non-executive directors and in Germany could include the firm's interlocking directorships with suppliers and customers and its banker relationships (Cable and Dirrheimer, 1983). Similarly, the firm's set of transactional arrangements with suppliers and customers is not simply a cost-minimizing device, in terms of transaction cost economics (TCE), but a resource that may yield competitive advantage. In general, this suggests that firms may need to secure an appropriate fit between the set of activities undertaken and the governance mechanisms and transactional arrangements in place. For example, external factors, such as the debt–equity funding mix and the extent of equity ownership concentration, may influence the optimal mix of activities (Demsetz and Lehn, 1985). Similarly, internal factors, including the choice between strategic and financial control systems, may determine the appropriate extent of diversification.

The authors share the view that in the early stages of market development, institutional theory is unmatched in illuminating the impact on government strategies. This is because government and societal pressures are stronger in developing economies than in developed countries. Institutional theory underlines the influences of the social and

organizational behavior of organizations. These systems might be internal or external to the company, and they do affect an organization's processes and decision making. Perspectives derived to examine these institutional pressures have both an economic orientation and a sociological orientation. This new theory focuses on the interaction of institutions and organizations resulting from market imperfections (Harris et al., 1995), North (1990) maintains that institutions provide the rules of the game that shape interactions in societies and that economic entities are the players constrained by those rules (formal and informal). The role of institutions in an economy is to reduce information costs and information asymmetry through minimizing uncertainty and crafting a stable structure that facilitates interactions. Palmer et al. (1993) examined the institutional constraints on American corporations in developing countries. The authors tested the institutional, political, and economic accounts of adoption of the multidivisional form (MDF) among large US industrial corporations in the 1960s, most notably by elaborating the institutional account. Their results suggested that institutional processes, including coercive and normative dynamics, substantially underpinned the MDF's diffusion during the 1960s. Firms producing in industries that had shunned the MDF earlier in the twentieth century were slow to adopt this form in the 1960s, an effect mediated by the percentage of firms in a corporation's sector using the MDF at the time. Firms with high debt-to-equity ratios, whose chief executives had elite business school degrees, and whose directors had non-directional corporate board contracts with the directors of MDF firms, adopted the MDF more frequently than other firms. Peng and Heath (1996) argued that the internal growth of transition economies is limited by institutional constraints. As a result, it was concluded that a network-based growth strategy was more appropriate in developing economies. Child and Lu (1996) maintained that economic reform of large state-owned enterprises was moving very slowly because of relational and cultural constraints. Following the same rationale Suhomlinova (1999) found that government institutions had a negative impact on Russian enterprise reform. In a study done on Chinese enterprises, Lau (1998) concluded that market and political forces were the institutional constraints that hindered the effective functioning of chief executive officers (CEOs) in these enterprises. Many firms in developing and emerging economies are influenced by existing institutional mechanisms and realities.

From a strategic perspective, institutions can also facilitate the process of strategy formulation, alignment, and implementation. Enterprises can play a more active role in an institutional environment when these institutional mechanisms allow them to maneuver and move beyond imposed constraints. A number of studies dealing with institutional effects on

developing countries have focused mostly on state-owned enterprises. In 1996, Lee and Miller studied the changes of institutional mechanisms and their impact on firms in various industries in Korea. They found that firms benefited to various degrees from a number of institutional and cultural changes in the country. Soulsby and Clark (1996) showed how institutional changes in the Czech Republic have led to a revamping of how managers think about and do their jobs in terms of acquiring new strategic thinking skills and other managerial techniques which are more appropriate to their new semi-open market environment. In an earlier article, Jefferson and Rawski (1995) concluded that the success of industrial reform in China was attributed to relaxing institutional constraints, market-leaning institutional change, development of property rights, and gradual relaxation of state ownership and control. In the case of China, these institutional changes provided appropriate incentives and the necessary changes in corporate culture that motivated firms and enabled them to take steps forward.

The number of studies using resource-based and institutional perspectives in developing economies is scarce, even though some theorists have argued that these perspectives are the most applicable for explaining economic behavior in developing economies. Characterized by trends toward market liberalization and privatization but still heavily regulated, developing and emerging economies provide the necessary institutional and resource influences in testing the theories.

THE RESOURCE-BASED VIEW AND DEVELOPING ECONOMIES

Until recently, little research using a RBV framework has examined strategy differences in the social context of developing economies. As with most resources that create competitive advantage, resources for competitive advantage in developing economies are, on the whole, intangible. However, they are not necessarily market or product specific, as might be expected. Although some qualifications are standard regardless of the level of development (for instance, first-mover advantages), others are particularly important in developing economies. Global and multinational firms that are able to manage some of the imperfect conditions in developing economies benefit from being first movers; some of the benefits include economic advantages of sales volume, knowledge of domestic markets and economies of scale. In general, many of the developing countries use the economics of free markets as the primary engine for growth. Hoskisson et al. (2000) investigated two groups of emerging

and developing countries: (1) the developing countries in Asia, Latin America, Africa, and the Middle East; and (2) the transition countries in the former Soviet Union and China. Both private and public enterprises have had to take different paths and use different strategies in dealing with the two distinct groups of developing countries. The research has examined the different strategies and implementation paths used by private and public businesses from a number of theoretical perspectives. One of these perspectives is the resource-based view of the firm.

In most developing and emerging economies, the postcolonial period saw the materialization of a state-centric form of governance, especially due to the lack of private capital and the absence of sophisticated market forces. More significantly, the role of the state expanded a great deal as a result of governments' national developmental agendas. Furthermore, many economic entities were brought under the management of the state through gigantic nationalization programs in order to end foreign economic dominance (cases in point are Egypt and Algeria). These programs brought with them immediate needs for basic services such as education and health that had to be provided by government in the absence of private sector initiatives (Haque, 2002). In fact, most of these initiatives were often supported by international aid agencies prior to the 1980s. But since the early 1980s the mode of governance has changed in developing and emerging countries. This is due to the impact of globalization demanding the substitution of state agencies by market-driven mechanisms supported by economic policies and institutions under a new political economy model.

In responding to the New Political Economy, developing and emerging governments have attempted to reduce the range of public governance through various measures such as privatization, deregulation, and downsizing, and to restructure its functions by emphasizing the state's role as a facilitator while assigning the main role to the private sector (Haque, 2002). For instance, as a result of pressure from international agencies such as the World Bank and the International Monetary Fund, gigantic privatization and deregulation initiatives have been undertaken in most Asian, African, and Latin American countries. Some of the well-known examples include Argentina, Brazil, Chile, Indonesia, Malaysia, Mexico, Nigeria, Pakistan, the Philippines, South Korea, and Thailand. In these countries different approaches of privatization have been adopted in major sectors such as telecommunications, airlines, electricity, petroleum, automobiles, television, fertilizers, tobacco, banking, insurance, and so on (Haque, 1999). This unparalleled process of privatization has significantly reduced the state's economic control in these countries. In addition, most governments have also taken initiatives to directly downsize the public sector to create greater avenues for the private sector. For example,

under the influence of the World Bank and the Asian Development Bank, Malaysia has implemented measures to downsize the public sector; the Philippines has adopted the strategy of 'streamlining the bureaucracy' to reduce staff by 5–10 percent; Singapore has applied a zero manpower growth policy in order to ultimately reduce the number of public employees by 10 percent, and Thailand has put on hold new employment (Haque, 2002). Similarly, India has decided to downsize the public sector by reducing public employment by 30 percent, and Sri Lanka has introduced an early retirement policy and retrenched thousands of government employees (Haque, 2001). In Latin America, governments have elected to reduce or freeze public sector employment, such as in Argentina, Bolivia, Brazil, and Mexico. A recent study shows that between the early 1980s and 1990s, as a percentage of total population, the number of central government employees decreased from 2.6 to 1.1 percent in Asia, 1.8 to 1.1 percent in Africa, and 2.4 to 1.5 percent in Latin America (Schiavo-Campo, 1998: 465). These downsizing exercises express the growing tendency of developing and emerging economies to reorganize public governance in line with the overall agenda for its diminishing role in socioeconomic activities. In recent years, the governments in India, Malaysia, Pakistan, Singapore, Sri Lanka, and Thailand have de-emphasized the role of public bureaucracy as the primary actor in socioeconomic development, redefining its role to facilitate or enable the business sector to take more active initiatives to deliver services (Haque, 2002). According to the World Bank (1996), in Arab countries such as Algeria and Jordan the recent structural adjustment programs have led to a greater role for private enterprises and investors, while the public sector has to enable rather than constrain such enterprises and investors. The overall objective of this restructuring of the role of public governance vis-à-vis business sector management has been to reduce the prominence of interventionist states and to expand the sphere of national and global market forces.

In line with the assumption of the New Political Economy, there have emerged a number of reform initiatives to restructure the organization and management of public governance based on the experiences of the private sector. The trends are toward commercializing government entities, adopting corporate practices, managing public agencies like private companies, and forming partnerships with business enterprises (Haque, 2001). These worldwide trends in restructuring governance can be observed today in many Asian, African, and Latin American countries. More specifically, various government ministries and departments have been converted into businesslike 'autonomous agencies' enjoying considerable operational autonomy in financial, personnel, and administrative matters. Following the examples of developed nations many developing

and emerging countries have introduced these structural changes in governance. In South Asia, Pakistan has introduced such a structure in specific sectors such as railway, telephone, and rural energy. In Southeast Asia, Singapore has introduced the most complete program to convert almost all government departments into autonomous agencies based on comprehensive restructuring of the budget and personnel systems. In various degrees, managerial autonomy in governance has also emerged in Indonesia, Malaysia, the Philippines, and Thailand. These new structural movements in governance represent an unmatched shift from the traditional bureaucratic model practiced in developing countries. In addition to these internal restructuring initiatives, there have been external structural changes, especially in terms of increasing partnership between the public and private sectors. In embarking on new projects, initiating new policies, and delivering services, such public–private partnership or alliance has expanded in Asian countries including India, Indonesia, Malaysia, Pakistan, the Philippines, Singapore, Thailand, and Vietnam, although this deeper public–private alliance often creates potential for conflict of interest between public agencies and business firms (Haque, 2001). The number of joint ventures has also increased in various African and Latin American countries such as Argentina, Mexico, and South Africa. This businesslike restructuring of public agencies and expansion of public–private collaboration implies diminishing boundaries between the public and private sectors.

THE INTERNET AS A SOURCE OF RADICAL TECHNOLOGY

The worldwide trends of globalization, deregulation, technical evolution, and market liberalization are restructuring markets and challenging traditional approaches to gaining competitive advantage (Chakravarthy, 1997; Hamel, 2000). It is becoming harder for firms to retain a competitive advantage based on physical or financial assets, or even on a new technology, as competitors with access to the same open market conditions can easily acquire similar assets and technologies, and even leapfrog to newer technologies. Consequently, firms need to concentrate on developing distinctive capabilities that are more difficult for competitors to imitate (Barney, 1997; Wernerfelt, 1984). Such development has become the focus of attention not only among academics, but also among business consultants, journalists, government officials, and business leaders (Miyazaki, 1995).

A prevailing paradigm for understanding how and why firms gain

and sustain competitive advantage is the resource-based view of the firm (Mahoney and Pandian, 1992; Schendel, 1994). From this perspective, capabilities and resources enable firms to conceive and implement strategies to generate above-normal rates of return (Barney, 1997; Dierickx and Cool, 1989). Sustainable competitive advantage is viewed as the outcome of discretionary rational managerial choices, selective capability accumulation and deployment, strategic industry factors, and factor market imperfections. Notwithstanding its important insights, the existing literature has concentrated on explaining the exploitation of existing firm-specific capabilities and on the attributes of firm resources (for example, their rarity, uniqueness, difficulty to copy, or non-substitutability).

The emergence of pervasive digital networks – especially the public Internet – has created business opportunities in both established and emerging sectors of the economy. Firms that have embraced these digital networks – net-enabled organizations (NEOs) (Straub and Watson, 2001) – can execute transactions, rapidly exchange information, and innovate through new business processes at an unprecedented pace (Weill and Vitale, 2001). NEOs have new channels for accessing customers, real-time integration with supply-chain partners, new efficiencies in internal operations, and offer new digital products or services. These net-enabled business innovations, which are the first step in an organization-wide process of net-enablement, require timely and ongoing reconfiguration of firm resources.

Opportunities for net-enablement are also creating a strategic and tactical quagmire for many firms. They struggle to assimilate the rapid pace of innovation in information technologies and the emerging business practices they make possible. It is in this context that business leaders must often make defensive and offensive strategic investments in new net-enabled business practices before credible measurement of prior investments can be ascertained (Sambamurthy, 2000; Sambamurthy et al., 2000).

On face value, some firms seem to be better at managing and executing net-enabled business innovation than other firms. Some firms with outstanding brands in the physical world have net-enabled their products and services to the delight of their customers, while other great brands have suffered from tardy and dismal efforts at net-enablement. Our research question asks, are there measurable, organizational capabilities that comprise the ongoing work of net-enablement? If so, what are these capabilities? Do these capabilities distinguish successful NEOs from less successful organizations?

The need for net-enablement (and the development of NEOs) is most visible in hypercompetitive environments. Hypercompetitive industries

are characterized by rapid changes in technology, relative ease of entry and exit by rivals, ambiguous consumer demands, and fleeting periods of competitive advantage (Bogner and Barr, 2000). Others refer to similar market dynamism as 'high-velocity markets' where successful business models and industry structure are unclear (Eisenhardt and Martin, 2000). These competitive conditions fuel a demand for innovation and speed while digital networks offer both speed and an opportunity for innovating (Sambamurthy et al., 2001). Both require firms to develop reliable capabilities for continual IT innovation for competitive necessity and to exploit short-term competitive advantage.

The utility of net-enablement is also applicable in non-hypercompetitive environments. Even mature industries, where competitive advantage may still flow from industry position or ownership of unique resources, are subject to opportunities, new efficiencies, or even competitive threats posed by digital networks. Net-enablement can provide new growth opportunities or establish defensive positions with customers and suppliers. Firms can pre-emptively become NEOs even though they do not currently experience the pace of competitive change in hypercompetitive environments. Alternatively, they may use a series of net-enabled innovations to erode the existing basis of long-term competitive advantage while they reap a series of irritable, short-term gains.

The dominant business configuration for NEOs is a network, web, or hub connected via IT. Suppliers, customers, complementors, and alliance partners engage in 'coopetition' as they collaborate via alliances and compete via coalitions (Brandenburger and Stuart, 1996; Moore, 1996; Singh and Mitchell, 1996; Afuah, 2000). As firms become net-enabled, their competitive advantage may rest on tacit, inimitable, collaborative relationships as a network or hub with its coopetitors. These coopetitors provide a critical source of innovations (Allen, 1977; von Hippel, 1988; Ahujah, 1996), knowledge transfer (Kogut, 1988), complementary products (Grove, 1996), and critical resources (Bower, 1970) for collectively garnering competitive advantage as a network of resources or complementary competencies. We believe that participation in these network relationships provides greater potential to lead in net-enabled business innovation.

CONCLUSION

This chapter was dedicated to the coverage of resource-based theory. The central questions addressed by the resource-based view deal with why firms and economies differ and how they achieve and sustain competitive

advantage. It has been argued that the heterogeneous competences that give economic entities their unique characters are part of the fundamental nature of competitive advantage.

For our purpose, resources are based in an environment and, depending on the characteristics of that environment, focusing on one resource or another could create strategic (dis)advantage which might lead to positive (negative) outcomes. Few scholars have analysed the issue of an economic entity's sustainable advantage in terms of resource-based and institutional factors and suggested that entities are able to create or develop institutional capital to enhance optimal use of resources (Oliver, 1997). Consequently, economic entities have to manage the social context of their resources and capabilities in order to be profitable.

Research using resource-based theory and examining macro strategy difference in the social context of developing economies is absent. Similarly to most resources that create competitive advantage at the micro level, resources for competitive advantage at the macro level in developing economies are mainly intangible. Although some capabilities are standard across all economies (e.g. first-mover advantage), others are particularly significant in developing economies (Hoskisson et al., 2000). The economic literature has paid attention to the revenue-generating promises of developing economies, and as such has focused mainly on big developing and emerging economies such as China, India, and Russia. Firms which are able to manage the discouraging environments in developing economies grab hold of the benefits of first-mover advantages. In developing economies, however, such advantages are very difficult to harness without good institutional infrastructure. Consequently, it is essential to understand the relationship between economic success (failure) and the changing nature of the institutional environment.

REFERENCES

Afuah, A.N. (2000), *Innovation Management: Strategies, Implementation and Profits*, London: Oxford University Press.

Ahujah, G. (1996), 'Collaborations and innovation: a longitudinal study of inter firm linkages and firm patenting performance in the global advanced material industry', dissertation, University of Michigan.

Allen, T.J. (1977), *Managing the Flow of Technology*, Cambridge, MA: MIT Press.

Amit, R. and P. Schoemaker (1993), 'Strategic assets and organizational rent', *Strategic Management Journal*, **14**: 33–46.

Ansoff, H. (1965), *Corporate Strategy*, New York: McGraw-Hill.

Argyris, N. (1996), 'Evidence on the role of firm capabilities in vertical integration decisions', *Strategic Management Journal*, **17**: 129–50.

Barney, J.B. (2001), 'Is the resource-based "view" a useful perspective for strategic management research? Yes', *Academy of Management Review*, **26**(1): 41–56.
Barney, J.B. (2002), *Gaining and Sustaining Competitive Advantage*, 2nd edn, Upper Saddle River, NJ: Prentice Hall.
Barney, J.B. and E.J. Zajac (1994), 'Competitive organizational behavior: towards an organizationally-based theory of competitive advantages', *Strategic Management Journal*, **15**: 5–9.
Barney, J.B. (1986), 'Strategic factor market: expectation, luck and business strategy', *Management Science*, **32**(10): 1231–41.
Barney, J.B. (1991), 'Firm resources and sustained competitive advantage', *Journal of Management*, **17**(1): 99–120.
Barney, J.B. (1992), 'Integrating organizational behavior and strategy formulation research: a resource based analysis', in P. Shrivastiva, A. Huff and J. Dutton (eds), *Advances in Strategic Management*, vol. 8, 39–62, Greenwich, CT: JAI Press.
Barney, J.B. (1997), *Gaining and Sustaining Competitive Advantage*, Reading, MA: Addison-Wesley.
Bartlett, C. and S. Goshal (1989), *Managing Across Borders: The Transnational Solution*, Boston, MA: Harvard Business School Press.
Bharadwaj, A.S. (2000), 'A resource-based perspective on information technology capability and firm performance', *MIS Quarterly*, **24**(1): 169–98.
Black, J.A. and K.B. Boal (1994), 'Strategic resources: traits, configurations and paths to sustainable competitive advantage', *Strategic Management Journal*, **15**: 131–48.
Bogner, W.C. and P.S. Barr (2000), 'Making sense of hypercompetitive environments: a cognitive explanation of high velocity competition', *Organizational Science*, **11**(2): 212–26.
Bogner, W.C. and H. Thomas (1994), 'Core competence and competitive advantage: a model and illustrated evidence from the pharmaceutical industry', in G. Hamel and A. Heene (eds), *Competence-Based Competition*, 111–44, New York: Wiley.
Bowman, C. and V. Ambrosini (2000), 'Value creation versus value capture: towards a coherent definition of value in strategy', *British Journal of Management*, **11**: 1–15.
Brancheau, J.C., B.D. Janz and J.C. Wetherbe (1996), 'Key issues in information systems: 1994–1995 SIM Delphi results', *Management Information Systems Quarterly*, **20**(2): 225–42.
Brandenburger, A. and H. Stuart (1996), 'Value-based business strategy', *Journal of Economics and Management Strategy*, **5**(1): 5–24.
Brown, S.L. and K.M. Eisenhardt (1997), 'The art of continuous change: linking complexity theory and time-paced evolution in relentlessly shifting organizations', *Administrative Science Quarterly*, **42**: 1–34.
Brown, S.L. and K.M. Eisenhardt (1998), *Competing on the Edge: Strategy as Structured Chaos*, Boston, MA: Harvard Business School Press.
Brumagin, A.L. (1994), 'A hierarchy of corporate resources', in P. Shrivastava and A. Huff (eds), *Advances in Strategic Management*, vol. lOA, Greenwich, CT: JAI Press, pp. 81–112.
Brynjolfsson, E. and L.M. Hitt (2000), 'Beyond computation: information technology, organizational transformation and business performance', *Journal of Economic Perspectives*, **14**(4): 23–48.

Burns, T. and G. Stalker (1961), *The Management of Innovation*, London: Tavistock.
Cable, J. and M. Dirrheimer (1983), 'Hierarchies and markets: an empirical test of the multidivisional hypothesis in West Germany', *International Journal of Industrial Organization*, **1**(1), 43–62.
Castanias, R.P. and C.E. Helfat (1991), 'Managerial resources and rents', *Journal of Management*, **17**: 155–71.
Chandler, A. (1990), *Scale and Scope: The Dynamics of Industrial Capitalism*, Cambridge, MA: Harvard University Press.
Chakravarthy, B. (1997), 'A new strategy framework for coping with turbulence', *Sloan Management Review*, **38**(2): 69–78.
Chatterjee, S. and B. Wernerfelt (1991), 'The link between resources and type of diversification: theory and practice', *Strategic Management Journal*, **12**: 33–48.
Chepaitis, E.V. (1996), 'The problem of data quality in a developing country', in P. Palvia, S. Palvia and E.M. Roche (eds), *Global Information Technology and Systems Management*, Marietta, GA: Ivy League Publishing.
Child, J. and Y. Lu (1996), 'Institutional constraints on economic reform: the case of investment decisions in China', *Organization Science,* **7**: 60–67.
Christensen, C.M. and M. Overdorf (2000), 'Meeting the challenge of disruptive change', *Harvard Business Review*, **78**(2) (March–April): 67–76.
Coase, R.H. (1937), 'The nature of the firm', *Economica*, **4**: 386–405.
Coff, R.W. (1999), 'When competitive advantage doesn't lead to performance: the resource-based view and stakeholder bargaining power', *Organization Science*, **10**(2): 119–33.
Cohen, W.M. and D.A. Levinthal (1990), 'Absorptive capacity: a new perspective on learning and innovation', *Administrative Science Quarterly*, **35**, 128–52.
Collis, D.J. (1991), 'A resource-based analysis of global competition: the case of the bearings industry', *Strategic Management Journal*, **12**(Summer special issue), 49–68.
Collis, D.J. (1994), 'How valuable are organizational capabilities?', *Strategic Management Journal*, **15**(Winter special issue), 143–52.
Conner, Kathleen (1991), 'A historical comparison of resource-based theory and five schools of thought within industrial organization economics: do we have a new theory of the firm?', *Journal of Management*, **17**(1) (March), 121–54.
D'Aveni, R.A. (1994), *Hypercompetition: Managing the Dynamics of Strategic Maneuvering*, New York: The Free Press.
D'Aveni, Richard (1999), 'Strategic supremacy through disruption and dominance', *Sloan Management Review*, **40**(3): 127–36.
Davison, E. and E. Jordan (1998), 'Group support systems: barriers to adoption in a cross-cultural setting', *Journal of Global Information Technology Management*', **1**(2): 37–50.
Deans, P.C., K.R. Karwan, M.D. Goslar, D.A. Ricks and B. Toyne (1991), 'Identification of key international information systems issues in US based multinational corporations', *Journal of Management Information Systems*, **7**(4): 27–50.
Demsetz, H. and K. Lehn (1985), 'The structure of ownership: causes and consequences', *Journal of Political Economy*, **93**: 1155–77.
Dierickx, Ingemar and Karel Cool (1989), 'Asset stock accumulation and sustainability of competitive advantage', *Management Science*, **35**(12): 207–23.
Dyer, J.H. and H. Singh (1998), 'The relational view: cooperative strategy and

sources of interorganizational competitive advantage', *Academy of Management Review*, **23**: 66–79.
Eisenhardt, Kathleen M. and Jeffrey A. Martin (2000), 'Dynamic capabilities: what are they?', *Strategic Management Journal*, **21**(10/11), 110–21.
Fiol, C.M. (1991), 'Managing culture as a competitive resource', *Journal of Management*, **17**: 191–211.
Foster, R. and S. Kaplan (2001), *Creative Destruction: Why Companies That Are Built to Last Underperform the Market – And How to Successfully Transform Them*, New York: Doubleday.
Geroski, P. and T. Vlassopoulos (1991), 'The rise and fall of a market leader', *Strategic Management Journal*, **12**: 467–78.
Ghemawat, P. and J. Costa (1993), 'The organizational tension between static and dynamic efficiency', *Strategic Management Journal*, **36**(Winter special issue), 59–73.
Globerman, S., T.W. Roehl and S. Standifird (2001), 'Globalization and electronic commerce: inferences from retail brokerage', *Journal of International Business Studies*, **32**: 749–68.
Grant, R.M. (1991), 'The resource-based theory of competitive advantage: implications for strategy formulation', *California Management Review*, **33**(3), 114–35.
Gruca, T. and D. Nath (1994), 'Regulatory change, constraints on adaptation, and organizational failure: an empirical analysis of acute care hospitals', *Strategic Management Journal*, **15**: 345–63.
Hall, R. (1992), 'The strategic analysis of intangible resources', *Strategic Management Journal*, **13**: 135–44.
Hall, R. (1993), 'A framework linking intangible resources and capabilities to sustainable competitive advantage', *Strategic Management Journal*, **14**: 607–18.
Hambrick, D.C. and S. Finkelstein (1987), 'Managerial discretion: a bridge between polar views of organizational outcomes', in L.L. Cummings and B. Staw (eds), *Research in Organizational Behavior*, vol. 9, Greenwich, CT: JAI Press, 369–406.
Hambrick, D.C. and P.A. Mason (1984), 'Upper echelons: the organization as a reflection of its managers', *Academy of Management Review*, **9**: 193–206.
Hamel, G. (2000), *Learning the Revolution*, Boston, MA: Harvard Business School Press.
Hamel, G. and A. Heene (1994), *Competence-Based Competition*, New York: Wiley.
Hamel, G. and C.K. Prahalad (1994), *Competing for the Future*, Boston: Harvard Business School Press.
Hansen, G.S. and B. Wernerfelt (1989), 'Determinants of firm performance: the relative importance of economic and organizational factors', *Strategic Management Journal*, **10**: 399–411.
Haque, M.S. (1999), 'Globalization of market ideology and its impact on Third World development', in A. Kouzmin and A. Hayne (eds), *Essays in Economic Globalization, Transnational Policies and Vulnerability*, Amsterdam: IOS Press, pp. 75–100.
Haque, M.S. (2002), 'Globalization, new political economy, and governance: a third world view', *Administrative Theory and Praxis,* **24**(1), 103–24.
Harris, J., J. Hunter and C.M. Lewis (1995), *The New Institutional Economics and Third World Development*, London: Routledge.
Heene, A. and R. Sanchez (eds) (1997), *Competence Based Strategic Management*, Chichester: Wiley.

Henderson, J. and N. Venkatraman (1993), 'Strategic alignment: leveraging information technology for transforming organizations', *IBM Systems Journal*, **32**: 4–16.
Henderson, R.M. (1994), 'The evolution of integrative capability: innovation in cardiovascular drug discovery', *Industrial and Corporate Change*, **3**: 607–30.
Henderson, R. and I. Cockburn (1994), 'Measuring competence: exploring firm-effects in pharmaceutical research', *Strategic Management Journal*, **15**: 63–84.
von Hippel, E. (1988), *The Sources of Innovations*, London: Oxford University Press.
Hofstede, G.H. (1980), *Culture's Consequences: Comparing Values, Behaviours, Institutions, and Organizations Across Nations*, Thousands Oaks, CA: Sage.
Hoskisson, R.E., M.A. Hitt, W.P. Wan and D. Yiu (1999), 'Theory and research in strategic management: swings of a pendulum', *Journal of Management*, **25**(3): 417–56.
Hoskisson, Robert R, Lorraine Eden, Chung Ming Lau and Mike Wright (2000), 'Strategy in emerging economies', *Academy of Management Journal*, **43**(3), 249–68.
Iansiti, M. and K.B. Clark (1994), 'Integration and dynamic capability: evidence from product development in automobiles and mainframe computers', *Industrial and Corporate Change*, **3**: 557–605.
Ijiri, Y. and H. Simon (1977), *Skew Distributions and the Size of Business Firms*, Amsterdam: North Holland.
Itami, H. and T. Numagami (1992), 'Dynamic interactions between strategy and technology', *Strategic Management Journal*, **13**: 119–35.
Itami, H. and T. Numagami (1992), 'Dynamic interactions between strategy and technology', *Strategic Management Journal*, **13**: 119–35.
Itami, H. and T. Roehl (1987), *Mobilizing Invisible Assets*, Cambridge, MA: Harvard University Press.
Johnson, N.B., R.B. Sambharya and P. Bobko (1989), 'Deregulation, business strategy, and wages in the airline industry', *Industrial Relations*, **28**: 419–30.
Karake, Z.A. (1995), 'Information technology performance: agency and upper echelon theories', *Management Decision*, **33**(9), 30–38.
Karake Shalhoub, Z. and L. Al Qasimi (2003), *The UAE as an Information Society*, Beirut: ESCWA.
Kelly, D. and T.L. Amburgey (1991), 'Organizational inertia and momentum: a dynamic model of strategic change', *Academy of Management Journal*, **34**: 591–612.
Khosrow-Pour, M. (2004), *The Social and Cognitive Impacts of E-Commerce on Modern Organizations*, Hershey, PA: Idea Group Publishing.
Kirzner, I.M. (1979), *Perception, Opportunity, and Profit*, Chicago, IL: University of Chicago Press.
Kogut, B. and U. Zander (1992), 'Knowledge of the firm, combinate capabilities, and the replication of technology', *Organization Science*, **3**(3): 383–97.
Kraatz, M.S. and E.J. Zajac (1997), 'Resource heterogeneity and its effects on strategic change and performance in turbulent environments', University of Illinois at Urbana-Champaign working paper.
Kwon, H.S. and A. Chimdambaran (1998), 'A cross cultural study of communication technology acceptance: comparison of cellular phone adoption in South Korea and in the United States', *Journal of Global Information Technology Management*, **1**(3): 43–58.

Lado, A.A. and M.C. Wilson (1994), 'Human resource systems and sustained competitive advantage: a competency-based perspective', *Academy of Management Review*, **19**: 699–727.
Lado, A.A., N.G. Boyd and P. Wright (1992), 'A competency model of sustained competitive advantage', *Journal of Management*, **18**: 77–91.
Lado, A.A., N.G. Boyd and S.C. Hanlon (1997), 'Competition, cooperation, and the search for economic rents: a syncretic model', *Academy of Management Review*, **22**: 110–41.
Lau, C.M. (1998), 'Strategic orientations of chief executives in state-owned enterprises in transition', in M.A. Hitt, J.E. Ricart I. Costa and R.D. Nixon (eds), *Managing Strategically in an Interconnected World*, Chichester: Wiley, pp. 101–17.
Lawrence, P. and J. Lorsch (1967), *Organization and Environment*, Boston, MA: Harvard University Press.
Lee, J. and D. Miller (1996), 'Strategy, environment and performance in two technological contexts: contingency theory in Korea', *Organization Studies*, **17**: 729–50.
Levinthal, D. and J. Myatt (1994), 'Co-evolution of capabilities and industry: the evolution of mutual fund processing', *Strategic Management Journal*, **15**: 45–62.
Lippman, S.A. and R.P. Rumelt (1982), 'Uncertain irritability: an analysis of interfirm differences in efficiency under competition', *Bell Journal of Economics*, **13**: 418–38.
Mahoney, J.T. and J. Pandian (1992), 'The resource-based view within the conversation of strategic management', *Strategic Management Journal*, **13**: 363–80.
Mathews, J. (2002), *Dragon Multinational: A New Model for Global Growth*, Oxford, UK: Oxford University Press.
McGrath, R.G., I.C. MacMillan and S. Venkatraman (1995), 'Defining and developing competence: A strategic process paradigm', *Strategic Management Journal*, **16**: 251–75.
Miller, D. (1988), 'Relating Porter's business strategies to environment and structure', *Academy of Management Journal*, **31**: 280–309.
Miller, D. and P.H. Friesen (1984), *Organizations: A Quantum View*, Englewood Cliffs, NJ: Prentice-Hall.
Miyazaki, K. (1995), *Building the Competencies of the Firm*, London: Macmillan.
Montgomery, C.A. (1995), 'Of diamonds and rust: a new look at resources', in C.A. Montgomery (ed.), *Resource-Based and Evolutionary Theories of the Firm: Towards a Synthesis*, Boston: Kluwer Academic, pp. 251–68.
Montgomery, C.A. and S. Hariharan (1991), 'Diversified entry by established firms', *Journal of Economic Behavior and Organization*, **15**: 71–89.
Montgomery, C.A. and B. Wernerfelt (1988), 'Diversification, Ricardian rents, and Tobin's q', *Rand Journal of Economics*, **19**: 623–32.
Moore, J.E. (1996), *The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems*, New York: Harper Collins.
Morris, R.L. (1964), *The Economic Theory of 'Managerial' Capitalism*, New York: Free Press.
Nelson, K.G. and T.D. Clark Jr. (1994), 'Cross-cultural issues in information systems research: a research program', *Journal of Global Information Management*, **2**(4): 19–28.

Nelson, R.R. and S.G. Winter (1982), *An Evolutionary Theory of Economic Change*, Cambridge, MA: Belknap Press.
Niederman, F., J.C. Brancheau and J.C. Wetherbe (1991), 'Information systems management issues for the 1990's', *MIS Quarterly*, **17**(4): 475–500.
Nonaka, I. (1994), 'A dynamic theory of organizational knowledge creation', *Organization Science*, **5**(1): 14–37.
Nonaka, I. and H. Takeuchi (1995), *The Knowledge-Creating Company*, New York: Oxford University Press.
North, D. (1990), *Institutions, Institutional Change and Economic Performance*, New York: Cambridge University Press.
Oliver, C. (1997), 'Sustainable competitive advantage: combining institutional and resource based views', *Strategic Management Journal,* **18**: 697–713.
Palmer, D.A., P.D. Jennings and X. Zhou (1993), 'Late adoption of the multi-divisional form by U.S. corporations: institutional, political, and economic accounts', *Administrative Science Quarterly,* **38**: 100–131.
Palvia, P., S. Palvia, and R.M. Zigli (1992), 'Global information technology environment: key MIS issues in advanced and less developed nations', in S. Palvia, P. Palvia and R.M. Zigli (eds), *The Global Issues of Information Technology Management*, Harrisburg, PA: Idea Group Publishing.
Palvia, P.C., S.C.J. Palvia and J.E. Whitworth (2002), 'Global information technology: a meta analysis of key issues', *Information and Management*, **39**: 403–14.
Parsons, G.L. (1983), 'Information technology: a new competitive weapon', *Sloan Management Review*, (Fall): 3–14.
Peng, M.W. and P.S. Heath (1996), 'The growth of the firm in planned economies in transition: institutions, organizations, and strategic choice', *Academy of Management Review,* **21**: 492–528.
Penrose, Edith (1959), *The Theory of the Growth of the Firm*, New York: John Wiley & Sons.
Peteraf, Margaret (1993), 'The cornerstone of competitive advantage: a resource-based view', *Strategic Management Journal,* **14**(3, March): 179–91.
Pinsonneault, A. and K.L. Kraemer (1997), 'Middle management downsizing: an empirical investigation of the impact of information technology', *Management Science*, **43**: 659–79.
Pinsonneault, A. and S. Rivard (1998), 'Information technology and the nature of managerial work: from the productivity paradox to the icarus paradox', *MIS Quarterly*, (September): 287–311.
Porter, M.E. (1980), *Competitive Strategy*, New York: Free Press.
Porter, M.E. (1985), *Competitive Advantage*, New York: Free Press.
Porter, M. (1991), 'Towards a dynamic theory of strategy', *Strategic Management Journal*, **12**: 95–117.
Porter, M. (1996), 'What is strategy?', *Harvard Business Review*, **74**: 61–78.
Porter, M. and V.E. Millar (1985), 'How information gives you competitive advantage', *Harvard Business Review*, **63**(4): 149–60.
Powell, T.C. and A. Dent-Micallef (1997), 'Information technology as competitive advantage: the role of human, business and technology resources', *Strategic Management Journal*, **5**(18): 375–405.
Prahalad, C.K. and G. Hamel (1990), 'The core competence of the corporation', *Harvard Business Review*, **68**(3): 79–91.
Priem, R.L. and J.E. Butler (2001), 'Tautology in the resource-based view and

the implications of externally determined resource value: further comments', *Academy of Management Review*, **26**: 57–66.
Rawski, Thomas G. (1995), 'Implications of China's reform experience', *China Quarterly*, **144**: 1150–73.
Reed, R. and R.J. DeFillippi (1990), 'Causal ambiguity, barriers to imitation, and sustainable competitive advantage', *Academy of Management Review*, **15**: 88–102.
Richardson, G.B. (1972), 'The organization of industry', *Economic Journal,* **82**: 883–96.
Robins, J.A. and M.F. Wiersema (1995), 'A resource-based approach to the multi-business firm: empirical analysis of portfolio interrelationships and corporate financial performance', *Strategic Management Journal*, **16**: 277–99.
Rubin, P.H. (1973), 'The expansion of firms', *Journal of Political Economy*, **81**: 936–49.
Rumelt, R.P. (1987), 'Theory, strategy, and entrepreneurship', in D.J. Teece (ed.), *The Competitive Challenge: Strategies for Industrial Innovation and Renewal*, Cambridge, MA: Ballinger, pp. 137–58.
Sambamurthy, V. (2000), 'The organizing logic for an enterprise's IT activities in the digital era: a prognosis of practice and a call for research', *Information Systems Research*, **11**(2): 105–14.
Sambamurthy V., A. Bharadwaj and V. Grover (2001), 'Shaping agility through digital options: re-conceptualizing the role of IT in contemporary firms', *MIS Quarterly*, **27**(2): 237–63.
Sanchez, R., A. Heene and H. Thomas (1996), *Dynamics of Competence Based Competition*, Oxford: Elsevier Press.
Schendel, D. (1994), 'Introduction to competitive organizational behaviour: toward a competitive-based theory of competitive advantage', *Strategic Management Journal*, **13**(5): 363–80.
Schiavo-Campo, S. (1998), 'Government employment and pay: the global and regional evidence', *Public Administration and Development*, **18**: 457–78.
Schmookler, J. (1966), *Invention and Economic Growth*, Cambridge, MA: Harvard University Press.
Schumpeter, J.A. (1934), *The Theory of Economic Development*, Cambridge, MA: Harvard University Press.
Schumpeter, J.A. (1942), *Capitalism and Democracy*, Cambridge, MA: Harvard University Press.
Selznick, P. (1957), *Leadership in Administration: A Sociological Interpretation*, New York: Harper & Row Publishers.
Sen, A. (1999), *Development as Freedom*, New York: Oxford University Press.
Shen, T.Y. (1970), 'Economies of scale, Penrose-effect, growth of plants and their size distribution', *Journal of Political Economy*, **78**: 702–16.
Shore, B. and A.R. Venkachalam (1995), 'The role of national culture on systems analysis and design', *Journal of Global Information Management*, **3**(3): 5–14.
Singh, K. and W. Mitchell (1996), 'Precarious collaboration: business survival after partners shut down or form new partnerships', *Strategic Management Journal*, **17**(Summer): 99–115.
Slater, M. (1980), 'The managerial limitations to the growth of firms', *Economic Journal*, **90**: 520–28.
Smith, K.G. and C.M. Grimm (1987), 'Environment variation, strategic change

and firm performance: a study of railroad deregulation', *Strategic Management Journal*, **8**: 363–76.
Soulsby, A. and E. Clark (1996), 'The emergence of post-Communist management in the Czech Republic', *Organization Studies*, **17**(2): 227–47.
Stigler, G.J., S.M. Stigler and C. Frieland (1995), 'The journals of economics', *Journal of Political Economy*, **103**(2): 331–59.
Straub, D.W. and R.T. Watson (2001), 'Research commentary: transformational issues in researching IS and net-enabled organization', *Information Systems Research*, **12**(4): 337–45.
Suhomlinova, O. (1999), 'Constructive destruction: transformation of Russian state-owned construction enterprises during market transition', *Organization Studies*, **20**(3): 451–84.
Teece, D.J. (1980), 'Economies of scope and the scope of the enterprise', *Journal of Economic Behavior and Organization,* **1**: 223–47.
Teece, D.J. and G. Pisano (1994), 'The dynamic capabilities of firms: an introduction', *Industrial and Corporate Change*, **3**: 537–56.
Teece, D., G. Pisano and A. Shuen (1997), 'Dynamic capabilities and strategic management', *Strategic Management Journal*, **18**: 509–33.
Thompson, H. and G. Garbacz (2007), 'Mobile, fixed line and Internet service effects on global productive efficiency', *Information Economics and Policy*, **1**(2), 189–214.
Thompson, J.D. (1967), *Organizations in Action*, New York: McGraw-Hill.
United Nations Conference on Trade and Development (UNCTAD) (2003), *e-Commerce and Development Report 2003*, New York and Geneva: UNCTAD, accessed 12 July 2008 at www. unctad.org/Templates/Download.asp?docid=4228&lang=1&intItemID=1528.
Weill, P. and M.R. Vitale (2001), *Place to Space: Migrating to Ebusiness Models*, Boston, MA: Harvard Business School Press.
Wernerfelt, Birger (1984), 'A resource-based view of the firm', *Strategic Management Journal*, **5**: 171–80.
Wernerfelt, B. and A. Karnani (1987), 'Competitive strategy under uncertainty', *Strategic Management Journal*, **8**: 187–94.
Wernerfelt, B. and C.A. Montgomery (1998), 'Tobin's q and the importance of focus in firm performance', *The American Economic Review*, **78**(1): 246–50.
Winter, S. (1987), 'Knowledge and competence as strategic assets', in D. Teece (ed.), *The Competitive Challenge*, Boston: Harvard Business School Press, pp. 159–84.
World Bank (1996), *World Bank Annual Report 1996*, Washington, DC: International Bank for Reconstruction and Development.
World Bank (2000), *Attacking Poverty*, World Bank report, Washington, DC: World Bank.

4. Methodology and development of hypotheses

INTRODUCTION

The resource-based view (RBV) of the firm argues that the performance of an economic entity is, inter alia, a function of the resources and skills that are in place and of those economic entity-specific characteristics which are rare and difficult to imitate or substitute. This concept is in essence based on Coase's theory of the firm, which maintains that the firm is a combination of alliances that have linked themselves in such a way as to reduce the cost of producing goods and services for delivery to the marketplace (Coase, 1937). An enhancement of this resource-based view is that an economy can create a competitive advantage by building resources that work together to generate organizational and country-based capabilities (Bharadwaj, 2000). These capabilities permit economic entities and economies as a whole to adopt and adapt processes that enable them to realize a greater level of output from a given input or maintain their level of output from a lower quantity of input.

In this chapter we will develop a set of hypotheses with the objective of conducting a systematic cross-country analysis of cyber laws in a sample of developing and emerging economies. Based on resource-based theory, the overall premise is that in addition to the physical infrastructure which explains much of the variation in basic Internet use and country e-readiness, cyber activities, especially e-commerce and e-government, also depend significantly on a supportive institutional environment such as national respect for the 'rule of law', the availability of credible payment channels such as credit cards, the support of top leadership, and the existence of cyber law.

Despite its widely cited potential to transform global economies, the use of cyber space, especially commercially, is as yet predominantly a North American phenomenon. Estimates vary, but it is generally accepted that more than 75 percent of online transactions are confined within US borders. The slow development of cyber activities in other countries is paradoxical, given the intuitive appeal of the notion that the digital age brings with it the 'death of distance' (Cairncross, 1997). In addition, some

developing and emerging countries such as the United Arab Emirates (UAE), Singapore, and Bahrain have done much better than others in digitizing their economies. While this puzzle has been the subject of much speculation, systematic analysis is sparse. In particular, to our knowledge there has been little empirical analysis of the conditions necessary for the development of viable online markets in developing countries.

In general, research on information technology (IT) and the impact on the economy of the electronic commerce, in terms of productivity and business value, can be classified into two categories: (1) the production-economics-based approach and (2) the process-oriented approach (Barua and Mukhopadhyay, 2000). The production-economics-based approach employs production functions to examine the relationship between output events and production inputs such as IT and non-IT classified capital and labor. Notwithstanding the many years of debate on the contested 'productivity paradox', several researchers were able to estimate production functions and to find a, somehow, positive relationship between investment in information technology, including investment in electronic commerce technology, and productivity. These findings were supported by several other studies and prompted a large stream of literature in this area (Brynjolfsson and Yang, 1996). As Hitt and Brynjolfsson (1996) point out, while the theory of production envisages that lower prices for information technology will generate benefits in the form of lower production costs for a given level of output, it is unclear on the question of whether economic entities will raise their performance advantages in terms of supra-normal profitability.

The process-oriented approach aims at explaining the process through which information technology investments improve intermediate operational performance, which in turn may affect higher levels of financial performance. An early study by Mukhopadhyay et al. (1995) assessed the business value of electronic data interchange (EDI) in a manufacturing setting. Their findings indicate that EDI facilitated the effective use of information to systematize material movements between manufacturers and their suppliers, which resulted in considerable cost savings and inventory cutback. As an inter-organizational information system, EDI has some features in common with the Internet-based initiatives, but it also shows signs of important differences as EDI is, by and large, a more expensive, proprietary technology under the control of one large manufacturer or supplier. In contrast, Internet technologies may induce large-scale variations within an organization as well as in its dealings with customers and suppliers. It is important to note that most of these studies were carried out before the extensive use of the Internet, and as such they logically did not include variables associated with Internet initiatives and e-commerce capabilities.

A promising framework for enhancing the theoretical basis of cyber activity value is the resource-based view of the economy, which links economic performance to economic and organizational resources and capabilities. Economic entities create performance advantages by assembling resources that work together to create added capabilities (Penrose, 1959; Wernerfelt, 1984; Peteraf, 1993). To create sustainable advantages, these resources, or resource combinations, would have to be economically valuable, relatively scarce, difficult to imitate, or imperfectly mobile across economic entities (Barney, 1991). Resources can be combined and integrated into unique clusters that enable distinctive abilities within an economic entity firm. In the information systems literature, the resource-based view has been used to explain how firms can create competitive value from information technology assets, and how sustainability resides more in the available skills to leverage IT than in the technology itself. Information technology payoffs depend heavily on how the various IT resources work together in creating synergy. Computers, databases, technical platforms, and communication networks form the core of an entity's overall IT infrastructure resources. Although the individual components that go into the IT infrastructure are commodity-like, the process of integrating the components to develop an integrative infrastructure tailored to a firm's strategic context is complex and imperfectly understood (Milgrom and Roberts, 1990; Weill and Broadbent, 1998). The resource-based view has been extended with the dynamic capabilities perspective (DCP) to tackle the practicality of unstable markets and swift technological change. DCP refers to the ability of a firm to achieve new forms of competitive advantage by renewing technological, organizational, and managerial resources to fit with the changing business environment (Eisenhardt and Martin, 2000). In this environment, capabilities that enable rapid and purposeful reconfiguration of a firm's resources are the means through which both industry position and timely unique resources can be obtained. This model implies that dynamic capabilities are essentially change-oriented capabilities that help economic entities reconfigure their resource base to meet growing customer demands and competitor strategies. The ability to anticipate technological change and adopt the appropriate strategies may create a path of growth that would generate a performance advantage (Teece et al., 1997). Resources are dynamic because the economic entities are continually building, adapting, and reconfiguring internal and external competences to attain congruence with the changing business environment when the rate of technological change is rapid, time-to-market is critical, and the nature of future competition and markets is difficult to determine (Teece et al., 1997). Dynamic capabilities create resource configurations that generate value-creating strategies (Eisenhardt and Martin, 2000).

Consistent with DCP, cyber space can be considered to be a dynamic capability. Internet-enhanced organizations continually reconfigure their internal and external resources to employ digital networks to exploit business opportunities. Thus, Internet-enhanced organizations exemplify the characteristics of dynamic capabilities as they engage routines, prior and emergent knowledge, analytic processes, and simple rules to turn IT into customer value (Wheeler, 2002; Bharadwaj et al., 2000; Sambamurthy et al., 2001).

Because this book seeks to extend the IT value literature to the domain of Internet-enabled e-commerce and e-government initiatives in developing countries, it is natural to ask if Internet initiatives are different from pre-Internet technologies (e.g. PC, mainframe, legacy systems). In fact, the economic characteristics of the Internet are significantly different from those of pre-Internet computer technologies. The Internet is unique in terms of connectivity, interactivity, and open-standard network integration (Shapiro and Varian, 1999; Kauffman et al., 2001). These characteristics have very different bearings on customer reach and richness of information. Prior to the Internet, firms often used stand-alone, proprietary technologies to communicate inadequate data. It was difficult and/or costly for a firm to relate to its customers, suppliers, and business partners. In contrast, the Internet facilitates a two-way, real-time information exchange between a firm and its customers and suppliers.

Given these unique potentials of the Internet, many countries have adopted e-commerce as a strategy for growth and development. Yet, the way that e-commerce is ingrained in business processes differs from one country to another. In fact, it is how economic entities leverage their investments to generate unique Internet-enabled resources and entity-specific competence that determines overall effectiveness of online activities. Economic entities, in the public or private sectors, benefit from the Internet when they embed online capability in their fabric in a way that creates sustainable resource synergy. For instance, the integration of online capability and IT infrastructure may improve connectivity, compatibility, and responsiveness of an economic unit at the micro level, which results in better efficiency and lower costs at the macro level.

The connectivity and open-standard data exchange of the Internet may help remove incompatibility of the legacy information systems. A mainframe-based legacy IT system (such as EDI) that only marginally improves performance under ordinary conditions may produce substantial advantages when combined with the Internet. The Internet's greater connectivity allows more direct interaction with customers and tighter data sharing with suppliers. Internet-based e-commerce can be adopted to enhance traditional IT systems in many ways, for example using a Web-

based, graphical interface to improve the user-friendliness of enterprise resource planning (ERP) systems; implementing Internet-based middleware to make EDI connections more flexible and affordable for smaller businesses; connecting various legacy databases by common Internet protocol and open standard; using eXtensible markup language (XML)-based communication to increase the ability of exchanging invoice and payment documents online between companies; and analysing online data to better understand customer demand.

Based on the above, it is vital to concentrate on resource synergy as a promising path to cyber space effectiveness. The resource-based view provides a solid theoretical foundation for studying the contexts and conditions under which cyber, Internet-based economies may produce more productivity and performance improvements in emerging and developing economies. In particular, it directs us toward a well-adjusted and stable position, one that recognizes the commodity view of the technology per se, while permitting the possibility of synergetic associations arising from combining the capabilities of electronic commerce, other information technology infrastructure, and other resources.

Unarguably, the most significant impediment to the development of commerce in cyber space in many developing countries is the lack of necessary physical infrastructure, particularly household access to personal computers and a cost-effective telecommunications system. However, indications from New Institutional Economics (NIE) support the notion that we should look beyond these immediate indicators to examine how the institutional environment in a country contributes to (or undermines) confidence in a new market such as e-commerce/e-government and supports private investment in the new medium. Empirical evidence has revealed that the integrity of the institutional environment, particularly with respect to the 'rule of law', is important for the development of e-commerce and e-government. Only in such an environment can participants in electronic transactions have confidence in a satisfactory performance or adequate legal recourse should the transaction break down.

Research done by Oxley and Yeung (2001) discusses the issue of transactional reliability in online markets and explores the role of institutions in supporting the growth of commercial online activities. The authors develop an analytical framework for cross-country comparisons of the environment for e-commerce, focusing on both the direct facilitators of growth – such as physical infrastructure – and on the underlying, intangible features of the institutional environment.

Based on the above, it is fair to assume that capabilities afforded by information communication technology (ICT) are one major component of economies' capabilities, and recent studies have identified a number of

specific ICT capabilities that provide competitive advantage. Bharadwaj (2000) classifies an entity's key ICT capability as comprising (1) a physical information technology infrastructure, (2) human information technology resources (including technical IT skills, and managerial IT skills), and (3) intangible information technology-enabled resources (such as customer orientation, knowledge assets, and synergy). We add to these other intangible factors, such as those identified by Oxley and Yeung, above.

THE NATURE OF RESOURCES

According to Wernerfelt, resources can include 'anything that might be thought of as a strength or weakness of a given firm' and so 'could be defined as those [tangible and intangible assets] which are tied semi permanently to the firm' (1984: 172). Applying Wernerfelt's ideas to the setting of a developing country, resources are said to give long-term competitive advantages to a country to the extent that they are rare or hard to imitate, have no direct substitutes, and enable economic entities to pursue opportunities or avoid threats (Barney, 1991). But if all other economic entities have those resources, they will be unable to contribute to superior returns and their general availability will defuse any special advantage. Thus, resources must be difficult to create, buy, substitute, or imitate. This last point is central to the arguments of the resource-based view (Barney, 1991; Lippman and Rumelt, 1982; Peteraf, 1993).

Evidently, there are many resources that may satisfy these criteria, though with differing effectiveness under different circumstances: important patents or copyrights, brand names, prime distribution locations, exclusive contracts for unique factors of production, subtle technical and creative talents, and skills in collaboration or coordination (Black and Boal, 1994).

There are a number of directions in which the resource-based view can be directed, when applied to developing economies. Of paramount importance is to make some fundamental distinctions among the different categories of resources that can produce unusual economic returns. In addition, to supplement its internal focus, the resource-based view needs to define the external environments in which various resources would be largely beneficial (Burns and Stalker, 1961; Thompson, 1967). In addition, the resource-based view must start to consider the circumstances within which various kinds of resources will have the best influence on performance (Amit and Schoemaker, 1993). According to Porter, 'Resources are only meaningful in the context of performing certain activities to achieve certain competitive advantage. The competitive value of resources can be

enhanced or eliminated by changes in technology, competitor behavior, or buyer needs which an inward focus on resources will overlook' (1991: 108).

Based on the resource-based theory literature, resources can be thought of in two broad categories: property-based and knowledge-based resources. Property-based resources are tangible – land, building, equipment, machinery, and so on while knowledge-based resources are intangible – skills, competences, experience, relationships, alliances, and intra-organizational structures and systems.

A number of researchers have attempted to classify resources based on various criteria and schematic frameworks. Barney (1991) argued that resources could be classified as physical, human, and capital. Grant (1991) added to the classification list financial, technological, and reputation-based resources. Other researchers revisited some of these initial criteria to come up with new typologies.

As stated above, a pivotal criterion in resource-based theory is barriers to imitation of resources. Some resources cannot be imitated because they are protected by property rights, such as contracts, deeds of ownership, or patents. Other resources are protected by knowledge barriers preventing competitors from imitating an entity's processes or skills.

Property rights deal with control of resources that bind a specific and well-defined asset (Barney, 1991). When an entity has exclusive ownership of a precious resource that cannot be legally imitated by competitors, it controls that resource. It can in that way acquire higher returns until conditions change to bring down the value of the resource. Any competitor desiring to have a hold of the resource will have to pay the discounted future value of its expected economic returns (Barney, 1991). Enforceable long-term contracts that monopolize scarce factors of production, embody exclusive rights to a valuable technology, or tie up channels of distribution are examples of property-based resources. Such resources shield an organization from competition by creating and protecting assets that are not available to competitors or would-be competitors (Black and Boal, 1994).

Most rivals will be conscious of the value of a competitor's property-based resources, and they may even have the knowledge to replicate these resources, but they do not have the legal right to imitate them successfully. In fact, one might make the case that in order for property-based resources to generate unusual economic return, they require protection from exclusionary legal contracts, trade restrictions, or first-mover pre-emption (Conner, 1991; Grant, 1991).

Property rights resources are protected from imitation by property rights, and knowledge-based resources are protected from imitation by knowledge barriers. These resources cannot be duplicated because they

are, to a large degree, unique and hard to understand since they require talents that are elusive and whose connection with results is difficult to determine (Lippman and Rumelt, 1982). Knowledge-based resources often take the form of specific skills, including technical, creative, and collaborative. They allow organizations to flourish not by preventing competition, but by providing entities with the skills to adapt their products to market needs and to deal with competitive challenges. It is important to point out here that the protection of knowledge barriers is not absolute; it may be possible for others to develop similar knowledge and talent, but this usually takes time, and by then a firm may have gone on to develop its skills further and to learn to use them in distinct ways (Lado and Wilson, 1994).

In addition to property-based and knowledge-based resources, insights from the NIE suggest that we should look beyond these direct indicators to look into how the institutional environment in a country contributes to (or damages) confidence in a new market and supports private investment in the new means. Not only institutional physical resources, but knowledge resources are important determinants of how successful Internet-based initiatives can be applied in a developing economy.

The New Institutional Economics is an attempt to integrate a theory of institutions into economics. However, in contrast to the many earlier attempts to overturn or replace neoclassical theory, the New Institutional Economics builds on, transforms, and extends neoclassical theory to allow it to deal with a host of issues beyond its knowledge. What it maintains and builds on is the basic assumption of scarcity. What it discards is instrumental rationality. New Institutional Economics views economics as a theory of choice subject to constraints; it makes use of price theory as a crucial part of the analysis of institutions.

INSTITUTIONAL ENVIRONMENT

It is likely that cyber space will be among the most powerful transmission mechanisms through which technology-induced change will spread across many developing and emerging countries. The application of ICT to, for instance, health or education can certainly contribute to the achievement of basic development objectives and can, in the long term, lead to productivity increases. However, the upward movement of economic growth that the Internet and cyber activities can bring about would probably result in a more immediate and sustainable contribution to the reduction of poverty and economic progress, one of the Millennium Goals specified by the United Nations.

Addressing the comparatively low levels of productivity in a large number of developing countries, the adoption of e-commerce in these countries can yield particularly to large relative improvements in productivity. In most cases, these gains are not derived directly from the technology itself but through incremental improvements resulting from organizational changes in the production process that are made possible (or indispensable) by the technology. An encouraging factor is that e-commerce seems to be spreading in a number of developing countries faster than was the case in previous technological revolutions. To grease the wheels of e-commerce and e-government and facilitate their spread, the institutional environment in developing and emerging economies has to be favorable.

According to Davis and North (1971: 6–7), the institutional environment is '[that] set of fundamental political, social and legal ground rules that establishes the basis for production, exchange and distribution. Rules governing elections, property rights, and the right of contract are examples.' There is now an established tradition of research within NIE connecting characteristics of the institutional environment to the extent and nature of private investment. Some of this work has examined the impact of general characteristics of the nation-state (e.g. Levy and Spiller, 1996; Henisz and Zelner, 2001), while some has focused on specific aspects of the legal or regulatory environment (e.g. Oxley, 1999).

An important question needs to be addressed is what aspects of the institutional environment are most important for promoting transactional integrity in cyber space and hence in supporting investment in these new markets? From an institutional perspective, this question can be analysed from the following key features: (1) the overall integrity of the nation's legal system, related to the degree to which the economy is governed by the rule of law; and (2) the credibility of payment channels available to cyber activity participants, which in turn is a function of the country's financial institutions and regulations and the existence of a law that governs electronic commerce transactions, that is, cyber law.

Developing and emerging countries can profit from the opportunities provided by e-commerce for exploiting competitive advantages not achievable in the 'old economy'. E-commerce gives small and medium-sized enterprises (SMEs) the ability to access international markets that used to be difficult to enter due to high transaction costs and other market access barriers. Labor-intensive services can now be delivered using cyber space as a medium, providing new opportunities for developing countries with relatively cheap labor. The emergence of successful industries such as software development or tele-servicing in several countries is an example of this. Thanks to e-commerce, entrepreneurs in developing countries can

also access cheaper, better-quality trade-related services (for instance, finance or business information), thus escaping local de facto monopolies. Finally, cyber activities can stimulate growth in developing countries by helping to improve the transparency of the operation of markets and public institutions. For instance, by simplifying business procedures, cyber activities not only reduce the cost for businesses of complying with domestic and international trade-related regulations, but also reduce the cost of corruption, a burden that often most severely affects SMEs and other weaker players in the economy.

For all these promising benefits to happen, a number of institutional measures and mechanisms are required in order to create an enabling environment for e-commerce, and address areas such as infrastructure, applications, payments systems, human resources, the legal framework, and taxation.

The following analysis of cyber security issues in a cross-section of developing countries should prove that not only physical infrastructure measures are important in explaining variations in basic cyber activity adoption and Internet use, but also intangible institutional measures are critical to the success of online business. The book will examine the strengths of cyber crime laws in a number of developing countries from an institutional, resource-based perspective.

WHAT IS HAPPENING ON THE GROUND?

Countries and economies are interconnected. If information systems in one economy are not effectively protected, then the underlying infrastructures of all the interconnected economies are threatened. Thus, the fight against cyber attacks is primarily dependent on the legal frameworks of every country. Specifically, cyber security is contingent upon every economy having (1) sound laws that criminalize attacks on systems and networks and ensure that law enforcement officials have the authority to investigate and prosecute crimes made possible by technology; and (2) laws and policies that permit international collaboration with other parties in the fight against computer-related crime. In addition, for these laws to work given the nature of cyber crimes, they have to be coordinated and harmonized across borders. In order to reach a global harmonization of cyber crime legislation, and a common understanding of cyber security and cyber crime among countries, whether developed, emerging, or developing, a global agreement at the United Nations level should be established that incorporates resolutions designed to tackle the global challenges. A convention is generally a more air-tight arrangement, where

parties may be held legally responsible for violations under international law. The most active UN entity in arriving at comprehensive and global cyber crime legislation is the International Telecommunications Union (ITU). This institution is exceptionally positioned to develop a global agreement on cyber crime.

In 2001, the UN initiated the World Summit on the Information Society (WSIS) and put the ITU in charge to lead and coordinate the multi-phased activities of WSIS. The work of WSIS got off the ground with Phase one in Geneva in December 2003; Phase two took place in Tunisia in 2005. Following these summits, the ITU took on the central role in coordination and harmonization of the activities among UN member countries in order to build confidence and security in cyber space. The responsibility of the ITU is to seek agreement on a framework for international cooperation in cyber security, in order to reach a common understanding of cyber security threats among countries at all stages of economic development (that includes developing and emerging economies) and put into action solutions aimed at addressing the global challenges to cyber security and cyber crime.

In May 2007, a Global Cyber security Agenda (GCA) was launched by the United Nations Secretary-General, as a global framework for dialogue and international cooperation aimed at proposing strategies for solutions to enhance security in the information society. The main goal of the GCA is the elaboration of strategies for the development of a 'model of cyber crime legislation' that is globally applicable and interoperable with existing national and regional legislative measures. In order to support the ITU's Secretary-General in developing strategic proposals to Member States, a High Level Experts Group (HLEG) was set up in October 2007. In June 2008, the HLEG group of more than 100 international experts provided its recommendations on strategies in the following five work areas: legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation. These recommendations are being adapted by a large number of developing and emerging economies in their effort to enact their cyber laws.

The Council of Europe's Convention on Cyber Crime

The 2001 Council of Europe's Convention on Cyber Crime[1] was a significant achievement in combating cyber crime. It entered into force on 1 July 2004, and by January 2008 45 countries had signed the Convention and 23 of those had ratified it. The Convention sets forth a comprehensive framework for international cooperation against computer crimes and requires member states to outlaw specific activities. These international agreements

acknowledge that the boundless nature of many illicit activities compels individual states to cooperate to restrain emerging threats.

Europe's Convention on Cyber Crime is perceived to be the best legislation to deal with what is referred to as cyber crime havens. It is based on the principle that harmonizing national laws will facilitate cooperation between law enforcement officers investigating crimes in cyber space and eliminate the haven scenario by ensuring that cyber criminals can be prosecuted and extradited for prosecution. Countries are called on to sign and ratify the Convention to outlaw cyber crime offenses, to ensure that their laws provide the facility to help officers from other countries investigating cyber crimes, and to ensure they have jurisdiction to prosecute such crimes. The Convention acts as a preventive measure by criminalizing actions that endanger the confidentiality, integrity, and availability of computer systems, networks, and computer information/data.

The Convention was opened for signature on 23 November 2001. Any member of the Council of Europe can sign and ratify the Convention; several non-member states, including the United States, can do so because they were involved in drafting the Convention. The parties to the Convention can allow other countries to sign and ratify it as well. The Convention consists of four chapters:

1. Chapter I covers the use of terms and definitions on computer systems, computer data, service providers, and traffic data.
2. Chapter II deals with actions that have to be taken at the national level and covers areas of substantive criminal law, procedural law, and jurisdiction. The section on substantive criminal law identifies offenses against the confidentiality, integrity, and availability of computer data and systems (such as illegal access, illegal interception, data interference, system interference, and misuse of devices). Computer-related offenses include forgery and fraud. Content-related offenses are offenses related to child pornography, and offenses related to infringements of copyright and related rights. The section on procedural law includes common provisions that apply to the Convention's articles on substantive criminal law, and to other criminal offenses committed by means of a computer system, and to the collection of evidence in electronic form relating to criminal offenses. There is a provision on expedited preservation of stored computer data, covering expedited preservation and partial disclosure of traffic data. The section includes also provisions on production order, search and seizure of stored computer data, real-time collection of traffic data, and interception of content data. Provisions on jurisdiction are dealt with in a separate section.

3. Chapter III covers international cooperation, and consists of general principles dealing with international cooperation, extradition, mutual assistance, and spontaneous information. This chapter includes procedures relevant to requests for mutual assistance in the absence of applicable international agreements, and to confidentiality and limitation on use, including specific provisions on mutual assistance on the subject of provisional measures, mutual assistance regarding investigative powers, and a provision for a 24/7 network.
4. Chapter IV deals with final provisions and includes the final clauses, mainly in accordance with standard provisions in Council of Europe treaties. In accordance with Article 40, any state may declare that it avails itself of the possibility of requiring additional elements, as provided for under certain articles. In accordance with Article 42, any state may declare that it avails itself of the reservations provided for in certain articles.

By ratifying or acceding to the Convention, countries agree to ensure that their domestic laws criminalize the conducts described in the section on substantive criminal law, and establish the procedural tools necessary to investigate and prosecute such crimes.

As shown in Table 4.1, nine countries from our sample (Bulgaria, Croatia, Czech Republic, Hungary, Poland, Romania, Slovakia, South Africa, and Ukraine) have signed, ratified, and/or entered the Convention into force. Russia has refused to sign the Convention on Cyber Crime because it did not manage to agree upon appropriate terms for cross-border access to data-processing networks.

Table 4.1 Sample countries, members of the Convention

Country	Signature	Ratification	Entry into force
Bulgaria	23/11/2001	07/04/2005	01/08/2005
Croatia	23/11/2001	17/10/2002	01/07/2004
Czech Republic	09/02/2005	–	–
Hungary	23/11/2001	04/12/2003	01/07/2004
Poland	23/11/2001	–	–
Romania	23/11/2001	12/05/2004	01/09/2004
Slovakia	04/02/2005	08/01/2008	01/05/2008
South Africa	23/11/2001	–	–
Ukraine	23/11/2001	10/03/2006	01/07/2006

Source: www.convention.coe.int.

The United Nations Resolutions

The United Nations has been very active in combating cyber criminal activities. Two resolutions are worth mentioning here: UN Resolution 57/239 (2002) and UN Resolution 58/199 (2004). The first resolution deals with the creation of a global culture of cyber security; in doing so, it identifies the following nine criteria:

1. *Awareness*: Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.
2. *Responsibility*: Participants are responsible for the security of information systems and networks in a manner appropriate to their individual roles. They should review their own policies, practices, measures, and procedures regularly, and should assess whether they are appropriate to their environment.
3. *Response*: Participants should act in a timely and cooperative manner to prevent, detect, and respond to security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective cooperation to prevent, detect, and respond to security incidents. This may involve cross-border information sharing and cooperation.
4. *Ethics*: Given the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests of others and recognize that their action or inaction may harm others.
5. *Democracy*: Security should be implemented in a manner consistent with the values recognized by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness, and transparency.
6. *Risk assessment*: All participants should conduct periodic risk assessments that identify threats and vulnerabilities; are sufficiently broad based to encompass key internal and external factors, such as technology, physical and human factors, policies, and third-party services with security implications; allow determination of the acceptable level of risk; and assist in the selection of appropriate controls to manage the risk of potential harm to information systems and networks in the light of the nature and importance of the information to be protected.
7. *Security design and implementation*: Participants should incorporate security as an essential element in the planning and design, operation, and use of information systems and networks.

8. *Security management*: Participants should adopt a comprehensive approach to security management based on risk assessment that is dynamic, encompassing all levels of participants' activities and all aspects of their operations.
9. *Reassessment*: Participants should review and reassess the security of information systems and networks and should make appropriate modifications to security policies, practices, measures, and procedures that include addressing new and changing threats and vulnerabilities.

UN Resolution 58/199 (2004) further emphasizes the 'promotion of a global culture of cyber security and protection of critical information infrastructures'. Specifically, it recognizes the growing importance of information technologies for the promotion of socioeconomic development and the provision of essential goods and services. It also addresses the increasing links among most countries' critical infrastructures and that these are exposed to a growing number and a wider variety of threats and vulnerabilities that raise new security concerns. It encourages member states and relevant regional and international organizations that have developed strategies to deal with cyber security and the protection of critical information infrastructures to share their best practices and measures that could assist other member states in their efforts to facilitate the achievement of cyber security.

Among others, these two resolutions act as guiding principles to countries around the world and place the issue of cyber security in the limelight.

Association of Southeast Asian Nations

The Association of Southeast Asian Nations (ASEAN)[2] is the first regional organization to adopt a harmonized cyber space legal framework consistent across jurisdictions. By mid-2009, all ASEAN member countries will have enacted consistent national e-commerce legislation. Part of the success of the ASEAN E-Commerce Project is due to its focus on global harmonization and international interoperability, rather than merely on regional harmonization. This focus on international interoperability included the selection of international models and templates, particularly the UN Convention on Electronic Contracting, for the implementation of domestic e-commerce law in ASEAN member countries. This ensured that ASEAN's e-commerce legal infrastructure would also be compatible with international developments, providing greater certainty for consumers and greater consistency for businesses.

In dealing with cyber crime legislation, ASEAN member states have

established the high-level Ministerial Meeting on Transnational Crime (AMMTC). Of the ten member countries of the ASEAN Group, five are part of our sample; these are Indonesia, Malaysia, the Philippines, Singapore, and Thailand. The ASEAN countries have been pioneers in the fight against cyber crime, with the e-ASEAN Reference Framework for Electronic Commerce Legal Infrastructure as a good starting point for such development. However, the e-ASEAN reference framework is strictly limited to basic e-commerce laws. Despite recognizing the need for implementation, the laws do not provide any guidelines for adopting legislation or codes of practice to address data and privacy protection, consumer protection, cyber crime, intellectual property, admissibility of computer outputs as evidence in court, or Internet content. The e-ASEAN reference framework also excludes issues of cross-border e-commerce such as conflicts of laws or taxation.[3] Early in 2004, cyber crime and the need for cooperation to fight against it were recognized as an important activity for the ASEAN member states. In July 2006, the ASEAN Regional Forum (ARF) issued a statement stressing that an effective fight against cyber crime and terrorist abuse of cyber space requires increased, swift, and well-functioning legal and other forms of cooperation. The ASEAN states pledged to act to develop, enact, and implement cyber crime and cyber security laws well suited to their national conditions and by relying on relevant international guidelines for the detection, prevention, combat, and mitigation of cyber attacks. They further recognized the added-value of a national framework for cooperation and partnership in dealing with criminality in cyber space, and advanced the creation of such a framework. In November 2007, ASEAN member states realized the value of wider cooperation in this area from China and South Korea. A joint APEC–ASEAN workshop on network security was held in the Philippines in 2007 to share knowledge and experience in capacity building in cyber security and cyber crime. The Convention on Cyber Crime developed by the ITU was introduced as a reference legal model for APEC and ASEAN members. Discussions were also held on legislation and building technical expertise in digital forensics. More recently, in May 2008, member states adopted a set of resolutions on cyber crime. At present, seven out of the ten ASEAN countries have cyber crime laws in place, and Indonesia has a draft law. Legislations contains similar offenses, but varies slightly. Offenses covered concentrate on unauthorized access, unauthorized access with the intent of committing an offense, and unauthorized modification of computer material. The legislation also contains provisions which make it a crime to disclose computer access codes without authorization.

Two ASEAN countries shine in their effort to fight cyber crime; these are Singapore and Malaysia. Malaysia was a pioneer in this respect by

enacting the Cyber Crime Act early in 1997, followed by the Digital Signatures Regulations in 1998. Singapore followed suit by enacting its Electronic Transactions Act 1998. The e-transaction laws in Malaysia and Singapore follow international conventions and European countries. Further, the Singaporean Electronic Transactions Act of 1998 has elaborate articles concerning, among others, the recognition of foreign certification authorities, revocation of certificates, and revocation without the consent of subscribers (MarketResearch.com, 2001).

ASEAN member states have committed to the establishment of an integrated ASEAN Economic Community (AEC) by 2015. A significant target within this commitment is the development of a harmonized legal infrastructure for e-commerce, as set out in the *Roadmap for Integration of e-ASEAN Sector*.[4] This roadmap calls for ASEAN countries to adopt the best practices and guidelines on cyber law issues (i.e. data protection, consumer protection, intellectual property, Internet service provider (ISP) liability, etc.) in order to support regional e-commerce activities; the time frame is specified as 2010–13.

On another related topic and in a recent development, there is a clear and strong trend in the ASEAN region to protect privacy through comprehensive legislation that is closely aligned with the European Union approach.

Asian Pacific Economic Cooperation

In 2002, the countries of Asian Pacific Economic Cooperation (APEC)[5] pledged to fight cyber crime at a meeting in Mexico. Member countries declared their intention to make an effort to enact a comprehensive set of laws dealing with cyber security and cyber crime. In 2005, this pledge was renewed by encouraging all APEC countries to consider the European Convention on Cyber Crime as a model, and attempt to develop and pass cyber laws compatible with international legal instruments, including the Convention on Cyber Crime. As for individual countries, China, the Philippines, and South Korea have specifically addressed certain aspects of cyber crime in their criminal codes, e-commerce enabling laws, other legislative instruments, and in case law. With respect to copyright offenses, penalties are imposed for online copyright infringement in the countries that have copyright protection laws explicitly extending to the online environment.

In response to this call from leaders the Security and Prosperity Steering Group (SPSG) was formed with the mandate of focusing on capacity building and legislative drafting of comprehensive cyber crime laws. Further assistance was provided to individual countries to tackle their specific

requirements and needs in developing wide-ranging legal frameworks and forming effective law enforcement and cyber crime investigative units. A Judge and Prosecutor Cyber Crime Enforcement Capacity Building Project is also in progress for APEC countries to help with capacity building in legal expertise on cyber crime (APEC, 2008).

As for individual countries, in December 2008 India passed the Information Technology (Amendment) Bill that provides for imprisonment, which could extend to a life term, for those indulging in cyber crimes and cyber terrorism and a jail term of up to five years for publishing or transmitting obscene material in electronic form. The Bill seeks addition of provisions to deal with cyber crimes such as transmitting sexually explicit materials in electronic form, breach of confidentiality, disclosure of data by intermediary, and e-commerce fraud. It also addresses issues related to stolen computer resources, identity theft, violation of privacy, and transmitting sexually explicit materials. The Bill also proposed the establishment of a special body, the Cyber Appellate Tribunal, to deal with cyber crime (*The Hindu*, 2008).

Organization of American States

In 1999, member countries of the Organization of American States (OAS)[6] approved the setting up of a group of governmental experts on cyber crime. The following countries in our sample are members of the OAS: Argentina, Bolivia, Brazil, Chile, Columbia, Ecuador, Mexico, Peru, Uruguay, and Venezuela. Brazil boasts the most advanced Internet and e-commerce industry in Latin America and the fifth largest telecom infrastructure worldwide. This is due to privatization of Brazilian telecom services and associated advancements (IBLS, 2009). As of 2007, 15 of the 35 Latin American states had substantive cyber crime legislation in place, with only 12 states having enacted procedural cyber crime legislation.[7] Some countries in Latin America have started to adapt their legal and regulatory systems to address e-commerce and cyber crime in order to take full advantage of the role ICT can play in development. Internet use in the Latin American region has been climbing steadily since 2002. The impact of the development and application of laws on the development of e-commerce activities is reported by many countries to be encouraging, leading to increased ICT-related business opportunities and greater level of foreign direct investment. This applies especially to Argentina, Brazil, and Chile (the ABC countries). Since 2002, these countries have developed and implemented laws on such issues as digital signatures, privacy, e-contracts, consumer protection, and intellectual property rights (IPRs). These actions are directed at removing barriers to the progress and growth

of e-commerce, e-government, and the use of ICT by raising the level of trust among users of e-platforms. The adaptation of national legal structures is an important development in ICT-related policies and procedures that the various governments should establish to promote e-commerce. Brazil's financial sector is the regional leader in adopting information technologies; the country is widely considered the regional leader of Internet marketing and online sales, service, and support. It appears that the Brazilian financial sector has capitalized on its IT experience to adopt e-commerce technologies and integrate them with existing information systems.

Brazil is considered the largest networked economy in Latin America. In 2006 it was ranked fifth highest in world market cellular phone users and seventh in world market software (estimated to be US$9 billion annually, with an average consistent annual growth of 10 percent) (IBLS, 2009). In addition, Brazil is among global leaders in the development of e-government applications, such as e-learning, e-procurement, online tax applications, and the national election system. Given the foregoing facts, one expects cyber laws in Brazil to be well ahead of other emerging economies; this is not the case, however. The only development has come out of the industry as self-regulating. In 2007, the Brazilian Association of Internet Service Providers (ABRANET) published a self-regulatory code for ISPs describing the roles of the ISPs in terms of facilitating communications and protecting users.

As for Argentina, in mid-2008 it approved law 26388 that updates its criminal code and sanctions against cyber crime. On 4 June 2008 and after numerous debates, Argentinean 'Camara de Diputados' characterized as crimes the following conducts: (a) distribution and possession with the intent to distribute child pornography; (b) e-mail violations; (c) illegal access to information systems; (d) distribution of virus and damage to information systems; (e) aggravated crimes against information systems; and (f) interruption of communications. According to these updates, it is now a crime in Argentina to access e-mails without authorization; the new law also makes illegal the deletion of electronic communications by persons other than their addressee. The law also criminalizes the interception or capture of private electronic communications (this may cover Voice over Internet Protocol (VoIP) communications). In addition, unauthorized access to private or public databases and information systems became a new type of crime in Argentina, punishable by a prison term. Breach of data and information, including revealing information to third parties, is now punishable under the new law. Further, the new law criminalizes those who change, damage, or improperly use information systems, including documents, or infect systems with viruses.

Notwithstanding the comprehensiveness of the provisions of the Argentinean cyber law, the sentences are not harsh enough to deter persistent cyber criminals. In other words, the law does not have enough teeth to make it successful in combating cyber crime.

At the regional level, the working group established by the countries of the OAS made a number of recommendations in 2004, 2005, and 2006 urging member countries to continue to strengthen cooperation with the Council of Europe; to give consideration to applying the principles of the Council of Europe's Convention on Cyber Crime; and to adopt the legal and other measures required for its implementation. Further, the group encouraged member states to continue their efforts in establishing mechanisms for the exchange of information and cooperation with other international organizations and agencies, such as the United Nations, the European Union, ASEAN, APEC, the OECD, the Commonwealth, and Interpol. These recommendations were adopted in June 2007.[8]

The adoption of cyber crime laws becomes a necessary condition with the increased diffusion of e-commerce in the economy; this is the case for many of the Latin American countries. According to a new study by Visa Incorporated, business to consumer (B2C) e-commerce in Latin America, including retail, travel, and tourism, rose to nearly US$11 billion in 2007, up from about US$5 billion in 2005 and US$7.78 billion in 2006, and is expected to surpass US$30 billion by 2010 (Achille, 2008).

Late in 2008, government representatives from 18 Latin American countries gathered in Columbia to discuss ways to strengthen their national legislations against cyber crime.

Countries of the ESCWA Region

The members of the Economic and Social Commission for Western Asia (ESCWA) include Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, the Syrian Arab Republic, the UAE, and Yemen. Cyber crime is still a foreign concept for the majority of the ESCWA member countries; the only two exceptions are the UAE and Saudi Arabia. The UAE was the first country in the region to adopt cyber crime legislation, with its Cyber Crime Law No. 2, enacted in June 2006. In January 2008, Saudi Arabia unveiled 16 articles for prosecuting technology-assisted crimes, specifically mentioning identity theft and running extremist websites. Under the new law, people found guilty of using computers to commit crimes could face up to ten years in prison and fines of up to 5 million Saudi riyals. The Law establishes that website defacement is a crime worthy of punishment, while data theft could carry a significant fine of more than US$130,000 or even a maximum one-year

prison sentence. The same punishment could apply to those found guilty of defamation using electronic means or those who unlawfully break into private electronic networks. Users spreading malware could find themselves paying US$800,000 and spending up to four years in a Saudi jail, less than those found guilty of spreading immorality. People setting up websites with pornographic content or content that defames humanity, or sites with information promoting drug use, may be punished with fines of up to US$1.3 million and five years of jail time.

The Gulf Cooperation Council (GCC) (which includes Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the UAE) recommended at a conference in June 2007 that the GCC countries draft a treaty on cyber crime. In February 2008, a workshop sponsored by the ITU was held in Doha Qatar, stressing the role of cyber legislation in combating cyber attacks on the region.

More recently, the government of Abu Dhabi has been making bold moves in the fight against white-collar crime; a new initiative states that cases of bribery, money laundering, abuse of power, embezzlement, and the misuse of funds are to be overseen by a special new prosecution body (23 February 2009). The Finance Public Prosecution body would cover both public and semi-public organizations. The move is part of a widespread strategy to improve financial accountability and transparency in the public sector in the emirate of Abu Dhabi. The new body will be specialized in investigating financial crimes and referring those cases to relevant courts in accordance with the laws concerning public fund-related crimes, such as breaches of trust and abuse of public office. Its main objective will be to provide a framework to protect public and private funds in line with the Judicial Department's five-year strategy.

The African Union

The African Union (AU) is an intergovernmental organization made up of 53 African states. The following countries in our sample are members of that Union: Algeria, Egypt, Nigeria, South Africa, and Tunisia. Currently, there are eight regional economic communities (RECs) within the Union, each established under a separate regional treaty. One REC, the Southern African Development Community (SADC), including Zambia, Zimbabwe, South Africa, Malawi, and Mozambique, initiated efforts to enact compatible cyber crime laws in 2005 (ITU, 2008).

A summit was held in October 2007 (The Connect Africa Summit) with the objective of launching a global multi-stakeholder partnership, aimed at promoting the development of secure and reliable high-quality ICT infrastructure in Africa. Even though progress on this front has been

very slow, some individual African countries have taken the initiative and moved ahead with legislation to address cyber crime; South Africa is the most advanced in this respect and its cyber crime legislation is regarded as a model law for the region.

Chapter XIII of the Electronic Communications and Transactions Act of South Africa, passed in 2002, among other things defined cyber crime to included: (1) unauthorized access to, interception of, and interference with data; (2) computer-related fraud, extortion, and forgery; and (3) aiding or abetting a cyber criminal. In addition, the Act specifies the penalties associated with these crimes to include a jail sentence and fines. According to the Act, the Director-General can appoint a cyber inspector who will have the power to inspect any website or activity on any information system in the public domain and report any unlawful activity to the appropriate authority. The inspector has the power to investigate the activities of a cryptography service or authenticating service provider to see if they are compliant with the Act. The inspector may also demand the production and inspection of relevant licenses and registration certificates as provided for in any law.

Examining the South African Act, one can safely state that it is fairly advanced legislation but it is not sufficient to deal with the critical issues of cyber security. This has lately been recognized by the South African authorities, and they are planning to introduce a more comprehensive and integrated legislative framework to promote collaboration between the various stakeholders in the government and the private sectors. Consequently, South Africa is currently using the strategies developed by the ITU in the process of developing a South African National Cyber Security Policy Framework. In developing this framework, the authorities are evaluating the country's laws that currently address the threat of cyber crime against the international best practices envisaged in the model cyber crime legislation that is recommended as globally applicable and interoperable. This work will necessitate reviewing existing national laws that deal with cyber crimes.

Internet-based attacks and crimes are increasing in Nigeria as cyber criminals continue to steal data from businesses and individuals. Cyber criminals are becoming more and more sophisticated, which has led cyber experts to issue a warning that if the government fails to do something to stop them, many Nigerians may be in danger of fresh attacks. This is because cyber criminals are now discovering new ways to exploit people, networks, and the Internet and many people are very vulnerable to such attacks. Nigeria is third in the top ten countries which are highly susceptible to fraudulent attacks through electronic mail and webpages. Statistics from the Internet Crime Complaint Center highlight an ever-increasing

concern around the nature and dynamics of the fraudulent attacks taking place. Further, financial services continue to be the most targeted sector at 91.7 percent of all attacks recorded during December 2007 (*Daily Trust*, 2009). According to the 2007 Internet Crime Report, Internet crime resulted in nearly US$240 million in reported losses in Nigeria in 2007, a US$40 million increase over reported losses in 2006. As countries move more and more online, the retrieval of consumers' personal identity data and financial account credentials is often achieved by stealing details directly using key-logging mechanisms and phisher-controlled proxies or by misdirecting users to non-authentic websites. To effectively tackle the problem of economic and widespread Internet fraud in Nigeria, there must be enabling legislation, as the absence of enabling legislation to properly spell out punishment for offenders has been responsible for the increasing rate of cyber crime in the country. Until the government does that, cyber crime will continue to increase in the country (*Daily Trust*, 2009).

DEVELOPMENT OF HYPOTHESES

The set of hypotheses in the current research addresses the determinants of the comprehensiveness of the legal system in deterring, combating, and criminalizing cyber crime in developing and emerging economies. The following section will identify economic resources and constraints that might support (undermine) the development of the cyber legislative environment in developing and emerging countries. Chapter 5 will cover the choice of the sample of countries, methodology, and operational variables which will be included in the analysis.

Human Resources

The first type of constraint faced by an emerging or developing country is the quantity and quality of its human resources available to society. Since financial resources are only a means to acquire productive assets, resources critical to cyber activities are primarily embedded in technical infrastructure and human skill sets. Most policy makers agree that unless businesses and consumers in a country are educated about the opportunities and benefits offered by information/communication technologies and unless they are trained to use the Internet, cyber activities will not be successful. Some go further to argue that training and education are the main challenges for most developing and emerging countries seeking to participate in the digital economy (ILO, 2001). Training and education are fundamental to the effective use of the Internet as a medium, and consequently

to regulating activities in cyber space. In a networked society, many of the benefits relate directly to the capability to use data and information to create new knowledge. Therefore, information technology skills of the human resource component are considered to be a core component of a successful information society strategy. In many developing countries, the literacy rate is low and the level of education is insufficient for full implementation of the changes required to move into an information society. In addition, given the fast technological change related to information and communication technologies, continuous learning is required, which means that employees and citizens of any country need to improve skills or acquire new ones on a continuous basis. Governments can play an important role in enhancing information and technological literacy through the country's education system. Training teachers in the use of the Internet and communications technologies in the classroom will lead to a new generation of IT-literate children. The United Arab Emirates is a good example of government support of education in this respect. In 2003, one of the authors was appointed by the Minister of Education and Youth to head a committee charged with revamping the K-12 education system in order to incorporate ICT and Internet technologies into the curriculum of schools. The work of the committee was completed in June 2004 with a report and a list of recommendations to the Ministry. This document was adopted by the Ministry in October 2004, and was put into effect for implementation in 2007.

The quantity and quality of the country's existing skilled personnel limit the expansion of its economic base; what is referred to as the 'Penrose effect' (Marris, 1963), Edith Penrose has been credited by several authors espousing a resource-based perspective as having been instrumental in the development of this perspective. Penrose's much-cited work on the theory of the growth of the firm provides arguably the most detailed exposition of a resource-based view in the economics literature. She notes that a firm is more than an administrative unit; it is also a collection of productive resources, the disposal of which, between different users and over time, is determined by administrative decision. When we regard the function of the private business firm from this point of view, the size of the firm is best gauged by some measure of the productive resources it employs (Penrose, 1959).

The Penrose effect is more pronounced in an emerging or developing economy than it is in a developed one. In the former, the new staff, either nationals or expatriates, have to go through a time-consuming integration process before they become productive team players. The constraint is a result of the intimate relationship between human (especially managerial at the executive level) and organizational resources. The two types

of resource have to be well balanced in order that successful measures by local and federal governments can be taken. Hence the first hypothesis:

Hypothesis 1: A country's cyber law maturity is positively related to the level of skills of its human resource component.

Financial Resources

Another common resource constraint is the country's existing financial base. The resource-based view of the firm regards the firm (in our case, the unit of analysis is the economy) as a collection of resources and capabilities that are derived internally by factors such as its assets, skills, knowledge, or culture. The RBV has been used by several authors in their research as a mechanism for understanding the manner in which firms operate. From the RBV perspective, resources are often copied by competitors – although cost may be a barrier to imitation. This research will use the economy as a unit of analysis from a resource-based perspective instead of a firm. In addition, the country's capabilities, which may be defined as complex interactions and coordination of people and other resources, are the means by which an economy reaches a competitive advantage. However, in order to achieve a competitive advantage, economic actors must enable it to perform value-creating activities, which are determined by market forces, better than its competitors. For e-business to be effective, there needs to be an appropriate infrastructure in place.

Even though the domestic financial sector and the capital account in developing countries were heavily regulated for a long time, Kaminsky and Schmukler (2002) show how the restrictions have been lifted over time. These authors developed an index of financial liberalization that takes into account restrictions on the domestic financial system, the stock market, and the capital account. They illustrate the gradual lifting of restrictions in both developed and emerging countries during the last 30 years. They also show that developed countries have tended to use more liberal policies than developing countries. Although there has been a gradual lifting of restrictions over time, there were periods of reversals in which restrictions were re-imposed. The most substantial reversals took place in the aftermath of the 1982 debt crisis, in the mid-1990s, and after the Argentine crisis in Latin America. Under the current financial conditions and the aftermath of the 2007–08 sub-prime crisis and the meltdown of financial systems around the world, we will see more restrictions and regulations being introduced in the various economic sectors, mainly the financial sector.

The literature identifies six main reasons to explain the new wave of

liberalization and deregulation of the financial sector by governments of different countries. First, governments found capital controls increasingly costly and difficult to maintain effectively. Second, as Errunza (2001) and the World Bank (2001) argue, policy makers have become increasingly aware that government-led financial systems and non-market approaches have failed. Of course that is debatable given the current market conditions! Third, recent crises have heightened the importance of foreign capital to finance government budgets and smooth public consumption and investment. In addition, foreign capital has helped governments capitalize banks with problems, conduct corporate restructuring, and manage crises. Fourth, opening up the privatization of public companies to foreign investors has helped increase their receipts. Fifth, although governments can also tax revenue from foreign capital, they might find this harder to do than with other factors of production because of its footloose nature. Finally, governments have become increasingly convinced of the benefits of a more efficient and robust domestic financial system for growth and stability of the economy and for the diversification of the public and private sectors' investor base.

Financial institutions, through the internationalization and globalization of financial services, are also a major driving force of financial liberalization. As discussed by the International Monetary Fund (2000), changes at the global level and changes in both developed and developing countries explain the role of financial institutions as a force of globalization and liberalization.

At a global level, the gains in information technology have diminished the importance of geography, allowing international corporations to service several markets from one location. As discussed in Crockett (2000), the gains in information technology have had three main effects on the financial services industry: (1) they have promoted a more intensive use of international financial institutions; (2) they have led to a major consolidation and restructuring of the world financial services industry; and (3) they have given rise to global banks and international conglomerates that provide a mix of financial products and services in a broad range of markets and countries, blurring the distinctions between financial institutions and the activities and markets in which they engage. Demographic changes and the increased sophistication of small investors around the world have intensified competition for savings among banks, mutual funds, insurance companies, and pension funds. Households have bypassed bank deposits and securities firms to hold their funds with institutions better able to diversify risks, reduce tax burdens, and take advantage of economies of scale.

In developing countries, liberalization of the regulatory systems has

opened the door for international firms to participate in local markets. The privatization of public financial institutions has provided foreign banks an opportunity to enter local financial markets. Macroeconomic stabilization, a better business environment, and stronger fundamentals in emerging markets have ensured a more attractive climate for foreign investment.

In recent years, then, there has been a revival of interest in the role played by financial development in long-term economic growth. A host of studies carried out over the past decade, beginning with King and Levine (1993), has found evidence in favor of the Schumpeterian view that a well-developed financial system promotes growth by channeling credit to its most productive uses. This has now become the conventional wisdom. Further, in the Information Age, the most productive use of finances is investment in cyber space and Internet-based technologies. Hence,

Hypothesis 2: A country's success in developing a legal framework dealing with cyber space is positively related to the strengths of its financial base.

Access and Technical Capabilities and Internet Penetration

Another related factor is the indigenous technical capability of the developing country, which is indicated by a number of variables such as national R&D expenditure, the rate of capital formation, national investment in education, and the number of technical personnel per capita. Technology and technical skills are driving growth at every level of any economy. For example, most economists now agree that three ingredients are essential to economic growth: capital, labor, and technology. Of these three components, technology and technical skills are the most important. Eminent economists estimate that technical growth and technological maturity have accounted for the bulk of economic growth in the most developed countries over the past 50 years. Of course, technology improves the productivity of labor. But leading economists who have analysed the role of technical progress in the postwar period found a greater influence on the productivity of capital.

The fact that more and more people are using the Internet, which is a must for the growth of cyber space activities and e-commerce, is not necessarily a sign of the survival of such expansion or of its speed. Some estimates of the numbers of Internet users count anyone (including, for instance, children) who has had access to the Internet in the previous 30 days. A much higher frequency of access is necessary in order to acquire the familiarity and generate the confidence that is needed in order to become a cyber space economic consumer. Particularly in the case of those

engaged in business-to-business (B2B) activities, the order of magnitude of their use of the Internet cannot be of some hours per month but must be of hours per day. Indeed, when asked about the use they make of the Internet, people in developing and emerging countries rarely mention e-commerce as a frequent online activity. E-mail is the most popular use of the Internet in developing countries. It is safe to assume that in developing countries the proportion of Internet users who are also e-commerce practitioners is lower than average, owing of course to lower per capita incomes but also to other well-known factors such as low credit card usage, lack of relevant products or services, and poor logistics and fulfillment services.

Without an appropriate technological infrastructure, there will be little use of electronic commerce and electronic means by the business community. The network infrastructure needs to be accessible, affordable, and of good quality. The telecommunications sector in many developing countries is run by the public sector, where the scope of and modalities of privatization and liberalization pose difficult problems. It is worth noting here that countries that have carried out telecommunications sector reforms have experienced significant improvements in their move towards information societies. For example, since adopting a new national ICT plan in 1999, Egypt has successfully increased telephone capacity and teledensity, the numbers of mobile phone subscribers and international circuits, and the capacity of international links to the Internet, while reducing access costs (OECD, 2007).

Developing and emerging countries need to take into consideration that establishing telecommunications infrastructure is costly, and that they might need inflows of foreign direct investment. In general, technological development and technical growth in a developing economy can take place through the transfer of technology and expertise from more advanced and developed countries. A study of 33 countries using American technology showed that there was a positive relationship between rate of development (i.e. as measured by the indigenous technical capability) and the proportion of licensing arrangements which were used as the means of technology absorption (Contractor, 1980). Furthermore, in transitional economies such as China, successful transfer of hard technology often has to be accompanied by the transfer of soft technologies such as management know-how (Hendryx, 1986). Overall, we see the growth-inducing power of technology at the industry level in developed countries. In the United States, for instance, research-intensive industries – aerospace, chemicals, communications, computers, pharmaceuticals, scientific instruments, semiconductors, and software – have been growing at about twice the rate of the economy as a whole in the past two decades. In developed countries, we also see technology's growth-inducing power at the level of

the individual firm. Recent studies show that firms with access to advanced technologies are more productive and profitable, pay higher wages, and increase employment more rapidly than firms that do not. The evidence is mounting. At the macroeconomic level, the industry level, and the firm level, access to technical resources constitutes the engine of economic growth.

In the realm of technology, the so-called enabling technologies are the most important factors in this economic growth equation. Throughout the twentieth century, enabling technologies – such as mass production, machine numerical control, and the transistor – were powerful engines of growth. The integrated circuit was, perhaps, the defining enabling technology of the twentieth century. Since its invention more than 40 years ago, it has enabled a whole range of new products and industries – from the computer to satellite communications – and it has had a profound impact on existing products and processes from automobiles, consumer electronics, and home appliances, to a broad range of advanced industrial systems. The integrated circuit sowed the seeds for the knowledge-based economy and the Information Age that are rapidly unfolding.

Without access to personal computers and Internet connections at a reasonable cost, consumers in developing economies are unable to migrate from traditional markets to electronic markets, and, hence, the need for a law to regulate these cyber activities would be much less imperative. However, even with access to the necessary equipment, people will not become active e-participants unless they have reasonable confidence in the truthfulness of transactions undertaken online. Thus, the presence of an adequate Internet infrastructure is a necessary but not sufficient condition for the development of e-economies:

Hypothesis 3: A country's cyber law maturity is positively related to its indigenous technical capability.

Rule of Law

Social theorists, legal scholars, and historians concur that law has played a central role in the transformation and industrialization of the West over the past 200 years. The mounting complexity of formal legal systems and the development of constitutionalism and the rule of law during this period are thought to have been key determinants of economic growth and prosperity. Max Weber went as far as affirming that a well-developed legal system was a prerequisite for the development of capitalism (Weber, 1981). Kinship relations, reputation bonds enforced by relatively closely united communities, and a multitude of self-enforcing mechanisms form

the most important governance and enforcement mechanisms. Several historical and comparative studies (Ellickson, 1991; Greif, 1989; Redding, 1990) have revealed that these mechanisms can be extremely successful.

For developing and emerging countries, providing an enabling legal framework is a determining factor to developmental success in cyber space, as it affects the ability to conduct transactions online. The main legal challenge of cyber activities is the dematerialization problem; that is, the lack of tangible information. Because of this and other unique characteristics of e-commerce, national legal frameworks need to be adapted to enable the development and success of e-commerce. It is important to remember, though, that adjusting the legislative framework to e-commerce will not solve fundamental problems inherent in the existing legal system of a country. Although it is known that commerce and technology often advance ahead of the law needed to regulate them, it is equally true that technology needs to take into account relevant legal requirements. Furthermore, efficient regulation of e-commerce issues such as spam and digital rights management requires that legislative solutions go hand in hand with technical solutions (UNCTAD, 2003).

It has been argued that an institutional and legal perspective would offer researchers a vantage point for conceptualizing the digital economy as an emergent, evolving, embedded, fragmented, and provisional social production that is shaped as much by cultural and structural forces as by technical and economic ones. Faced with new forms of electronic exchange, distribution, and interaction, information/communication technology researchers cannot reasonably confine their interests to the problems of developing and implementing technologies or even to studying a technology's impact on local contexts. A world of global networking (both technological and organizational) raises issues of institutional interdependence whose understanding requires an appreciation for how prior assumptions, norms, values, choices, and interactions create conditions for action and how subsequent action produces unintended and wide-reaching consequences (Orlikowsk and Barley, 2001). Recognition of the institutional implications of electronic commerce would focus attention on such complex issues as the blurring of corporate boundaries, national sovereignty, organizational control, intellectual property, individual privacy, and internetworking protocols. Without an institutional structure, electronic commerce and electronic government research might focus more narrowly on technological designs, economic imperatives, or psychological impacts, thus missing important social, cultural, and political aspects of technology diffusion.

A number of reasons have been put forward in the resource-based literature to explain why valuable resources, both tangible and intangible,

are imperfectly imitable by competitors (Dierickx and Cool, 1989; Grant, 1991; Lippman and Rumelt, 1992). The most well-known reason is casual ambiguity, which is said to exist 'when the link between the resources controlled by a firm's sustained competitive advantage is not understood or understood only very imperfectly' (Barney, 1991: 108–9). Discussions of casual ambiguity are usually focused on the core competences of a firm that account for its competitive advantage (Reed and DeFillippi, 1990). These competences are a complex combination of productive services offered by the firm's physical, human, and organizational resources. In view of the intricacies of the relationships and processes involved, even senior management of the firm may not fully understand the exact nature of the casual connections between actions and results.

However, the situation for a stand-alone technology would be very different. Casual ambiguity is less a problem here. Imitation by competitors can be a real danger, especially when the technology has been substantially codified. It is in the firm's interest to guard against the leakage of its crucial technical know-how. How far intellectual property rights are protected in the host country is a critical factor every economic agent should consider. Studies have found that the risk of patent infringement may provide an internalization motive for foreign direct investment (Caves, 1971; Dunning, 1979; Horstmann and Markusen, 1987). In developing countries where the record of patent protection is poor, the firm would prefer transfer modes such as joint ventures or even wholly owned subsidiaries so that it has more control over the use of the technology and can minimize the leakage. Of course, as mentioned earlier, public policy of the host country is an important factor as well. For instance, China has a preference for joint ventures as a means of importing foreign technology (Tsang, 1995). Firms using other transfer modes will lose the economic incentives offered to joint ventures.

A country with a strong rule of law is defined as one having a strong court system, well-defined political institutions, and citizens who are willing to accept the established institutions and to make and implement laws and arbitrate disagreements. North (1986) argues that the key to economic growth is 'efficient economic organization', involving, among other things, a well-specified legal system, an impartial judiciary, and a 'set of attitudes towards contracting and trading that encourage people to engage in [markets] at low cost' (North, 1986: 236).

The strength of the rule of law affects transactional integrity in cyber space, and thus investment in such markets, in three ways. First, a strong rule of law generates greater transparency and stability regarding the boundaries of acceptable behavior. This reduces the transactor's uncertainty about what legal protection they can expect, and enhances their

ability to successfully litigate at least the more serious cases of fraudulent online dealings. Wherever the rule of law is weak, that ability is undermined. Second, effective punishment of transgressors lowers the cost of reputation building for honest businesses, as signals are more credible when defectors face high sanctions. Third, a strong rule of law influences people's general attitudes, increasing the level of trust in markets and contracting. This trust is particularly important in e-commerce, given our earlier discussion of information asymmetries in online markets.

To illustrate the importance of these features of a strong rule of law, consider countries where citizens grant little legitimacy to legal contracts, relying on more informal approaches when conducting business. Here, personal relationships are important, and people will likely be leery of any business dealings with faceless strangers (and, conversely, may not hesitate to cheat a stranger with whom they *do* trade).

What is meant by rule of law, then, is the presence of a clear governance arrangement that respects individual and commercial rights and which is enforced consistently and fairly as an important prerequisite for promoting effective use of technology and knowledge. If commercial contracts are not respected, and if businesses can be arbitrarily seized and/or if bureaucratic red tape stifles creative energy, any incubation project will be doomed to failure.

The issue of the effect of law, mainly business law, on the economy and growth, has become the topic of hot discussion over the last several decades among policy makers, practitioners, and researchers, especially in economic development circles. For policy makers, this interest grew out of disappointment in the 1980s over the role structural adjustment policies played in growth and development, which has necessitated the need to reform institutions, especially the legal ones. In the late 1990s, a number of researchers linked the legal framework to the development of financial markets and, through finance, to growth and development. La Porta et al. started an effort to determine whether there was a correlation between the legal framework of a country and the development of its financial system, with the following underlying assumptions: (a) that there is a benchmark for 'good' financial markets (the US model); and (b) that extensive financial markets command growth (La Porta et al.: *supra* note 7, at 1117–26). The model was gradually transformed into a broad theory about the development of markets, culminating in a so-called 'New Comparative Economics'.

The World Bank, among other multinational institutions, got on the bandwagon of these ideas and turned them into normative guidelines for development (World Bank, 2008).

The pervasive growth in electronic commerce in recent years has raised concerns that existing legal and regulatory regimes are too inconsistent

or inadequate in dealing with the issues that electronic commerce raises. Most commentators have, however, noted that ironically it is the lack of substantial legal or regulatory infrastructure that has made the unbridled growth of electronic commerce possible and this has caused some to worry that the application of too much traditional regulation will stifle growth. Some other commentators have taken the point further and argue that modern information markets should largely be defined by agreements and other manifestations of market choice rather than by regulation. At various stages during the development of the Internet, several observers have also expressed disappointment with the inadequacy of domestic legal systems in dealing with issues in cyber space. This is hardly surprising as the principles developed to deal with legal issues in the physical world are sometimes inadequate in dealing with the emerging legal challenge thrown up by the Internet.

The fast growth of the Internet and consequently cyber space activities greatly increases the ease of accessing, reproducing, and transmitting information. This ease raises a host of legal issues including the risk of copyright infringement, the protection of patent rights, and the preservation of trade secrets. The Internet also raises privacy concerns and issues pertaining to the validity and enforcement of agreements entered into via the medium of the Internet. Conflict of law issues take on an added dimension of complexity and confusion due to the inherently fluid nature of the Internet. Users habitually trigger the application of the laws of multiple jurisdictions in a matter of seconds. It is becoming increasingly evident that the process of mapping existing legal concepts and tools into this new domain is not straightforward, and that a number of familiar legal concepts will need to be rethought and, perhaps, re-engineered before they can be efficiently applied in the new environment. Most governments act reactively and amend or create regulations after industry acceptance of these technologies has taken place. This gives rise to the maddening and steadily widening gap between new technologies and adequate government regulation. The existing body of law is, however, not entirely helpless and oftentimes the law is able to adapt and tackle some of the emerging legal issues thrown up by online activities. This is done through the process of drawing from precedents and on reasoning by analogy. There is, unfortunately and perhaps understandably, a limit to the ability of the law to adapt itself to emerging technologies: timely legislative intervention to supplant the existing law and to fill in the existing lacunae is often needed to ensure that the law remains current and relevant.

Many governments and regulatory bodies in developing and emerging countries are starting to recognize the economic potential of electronic commerce and electronic government and are considering a number of

policy initiatives designed to encourage further development and application of this technology. These initiatives include attempts to overhaul or effect amendments to existing laws to deal with the emerging legal issues that electronic commerce raises. In Singapore, for instance, various amendments to existing legislation and subsidiary legislation have been put in place rationalizing the existing law to cope with moves in various industries toward the electronic framework. The amendments have collectively dealt with computer and electronic evidence, copyright, income tax concessions for cyber trading, electronic dealings in securities and futures, electronic prospectuses, and deregulation of the telecommunications industry.

In Malaysia, the Multimedia Development Corporation has been working on a National Electronic Commerce Master Plan which is designed to facilitate the creation of a favorable environment for the development of electronic commerce. The four key elements in this Master Plan are to boost confidence in online trading, prepare a regulatory framework, build a critical mass of Internet users, and introduce an electronic payments system.

In the Philippines, the passage of the Electronic Commerce Act underpins the government's resolve to create an environment of trust, predictability and certainty in the Philippine system so as to enable electronic commerce to flourish. In India, there have been feverish attempts to update the legal and regulatory framework to make it more relevant in the face of rapid developments in information technology and communications. The Internet service provider and gateway markets have been liberalized and the national long-distance sector has been opened up. In addition, discussions are ongoing for the liberalization of the international long-distance sector and India's uplinking policies are slated to become more liberal.

A closer examination of the legislative activity in this area, however, leaves one with the uncomfortable feeling that what is taking place across a large part of the developing world is probably a reaction to perceived legal problems presented by electronic commerce rather than a careful and considered response to the actual issues that this new method of doing business raises.

Most countries have sought to respond to the novel legal problems that crop up in cyber space by enacting new legislation while others have sought to extend the ambit of their current laws to cover the novel scenarios occurring in cyber space. In this flurry of activity, it is not surprising that most countries have not addressed the fundamental issue of whether it would be wise or desirable to apply existing national laws, which have evolved mainly to deal with 'territorially based' concepts and rights, to the realm of cyber space. Accordingly, there have been calls to treat cyber

space as a separate jurisdiction for the purposes of legal analysis. Some analysts have suggested that a separate law of cyber space, similar to the law of the high seas, should be formulated. Others have proposed that the norms and practices of the users of the Internet could be relied upon in determining the applicable and appropriate legal principles that should apply to transactions conducted via the medium of the Internet. This would include 'netiquette', which has the potential to constitute the foundation pillars of a workable uniform cyber space law.

Based on the above, it is reasonable to assume cyber laws contribute to better diffusion of electronic commerce and electronic governments.

Hypothesis 4: A mature rule of law will more likely lead to a mature cyber law.

Level of E-government Maturity

In the past few years, governments in developed and developing economies have learned from the benefits that the private sector earned from using cyber space and have engaged in the development of their e-government initiatives. Some of these initiatives are still budding, such as those in Oman and Saudi Arabia; others have reached maturity, such as the e-government initiative in the UAE and Singapore. A mound of literature and case studies exists demonstrating the rise and growth of e-government initiatives all around the world (Singh et al., 2007).

Unlike conventional bricks-and-mortar-based activities, digital delivery procedures are non-hierarchical, non-linear, interactive, and available 24/7. The non-hierarchical nature of Internet delivery allows people to look for information at their own ease. The interactive features of e-government provide both citizens and policy makers with the capability to send as well as receive information.

Developments and progress of e-government initiatives in more than 200 countries around the world have attracted an increasing level of interest from academics, researchers, practitioners, and policy makers. Developing metrics to measure the diffusion, progress, and success of e-governments has been dominated by multilateral institutions such as the World Bank and the United Nations, consulting companies such as Accenture, and academic institutions such as Brown University and INSEAD. These organizations have independently created and outlined different metrics to measure the diffusion of e-government. However, a common denominator has emerged among the various attempts and that is the preponderance of nations with high gross national products in the top echelons (Singh, 2007); this might explain the leadership of developed economies in the

Table 4.2 Leaders in e-government

West (2008)	UN/DESA (2005)	Accenture Consulting (2005)
1. South Korea	USA	Canada
2. Taiwan	Denmark	USA
3. United States	Sweden	Denmark
4. Singapore	UK	Singapore
5. Canada	South Korea	Australia
6. Australia	Australia	France
7. Germany	Singapore	Japan
8. Ireland	Canada	Norway
9. Dominica	Finland	Finland
10. Brazil	Norway	Netherlands

development, implementation, and success of e-government. Table 4.2 shows the leaders in terms of e-government projects based on the results of three studies.

It is expected that we find a strong link between leadership or maturity of e-government and the inclination for countries to develop and enact cyber laws. The development of cyber laws is an indication of commitment of the leadership of a country to ensuring the success of its e-government initiatives. This link between the dedication of a country's leadership and the quality of governance, on the one hand, and the maturity of e-government initiatives on the other, would lead to the development of cyber laws as part of a broader trend toward better online governance.

Hypothesis 5: There is a positive relationship between the level of e-government maturity and the level of cyber law maturity.

CONCLUSION

This chapter has covered the nature of resources and the foundation of institutional environment theory. In addition, it has also analysed the state of cyber law in the countries in our sample.

A number of hypotheses, dealing with what is believed to lead to the development of laws governing cyber space in a country, were than developed. The first had to do with the quantity and quality of human resources available to society. It is believed that training and education are fundamental to the effective use of the Internet and hence to the success of electronic commerce. Since the quantity and quality of a country's existing

skilled personnel limit the expansion of its economic base (the Penrose effect), it is hypothesized that a country's success in cyber space and its effort in developing a comprehensive cyber law are positively related to the level of skills of its human resources. The second hypothesis has to do with the financial resources available to a country. In recent years, a host of studies have found evidence of a positive relationship between the strength of the financial base of a country and its economic growth. It is hypothesized that, in the information age, financial investment in Internet-based technologies is positively correlated with economic growth.

Access to Internet-based resources and technical capabilities constitutes the basis of the third hypothesis. Without access to computers and Internet connections at a reasonable cost, citizens in developing economies will be unable to migrate from traditional markets to electronic markets. The fourth hypothesis deals with the role the rule of law plays in facilitating the use of Internet-based technologies in a developing country. Scholars from all professional backgrounds agree that law plays a vital role in the transformation and development of societies. It is believed that, in the developed world, the development of constitutionalism and the rule of law have been the major drivers of economic growth and progress. A number of reasons have been advanced in the resource-based literature to highlight the role a strong rule of law plays in economic growth and development. The argument goes that a strong rule of law affects transactional integrity in an Internet-based society, and thus investment in such markets.

Cyber law is hailed to be one of the major drivers of cyber activities and Internet-based business. Because of the unique nature of the Internet, its use creates legal issues and questions, especially in areas related to intellectual property rights and cyber crime. Few countries in the developing world have drafted cyber law; and those that have are still struggling to perfect its implementation. In this study, the authors argue that the existence of cyber law leads to better diffusion of electronic commerce, and subsequently to economic growth and development. Hence, the fifth hypothesis was formulated to state that success in electronic commerce is positively related to the existence of cyber law.

The following chapter will cover the formulation of methodology, collection of data, and the testing of the five hypotheses formulated in this chapter

NOTES

1. See http://www.conventions.coe.int.
2. The ASEAN Group consists of ten states: Brunei Darussalam; Cambodia; Indonesia;

Laos; Malaysia; Myanmar; Philippines; Singapore; Thailand; Vietnam. See www.aseansec.org.
3. Please refer to http://www.apectelwg.org/apecdata/telwg/28tel/estg/telwg28-ESTG-14.htm.
4. *Roadmap for Integration of e-ASEAN Sector*, appendix to the *ASEAN Framework Agreement for the Integration of Priority Sectors*, November 2004, http://www.aseansec.org/16689.htm.
5. APEC includes Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong, Indonesia, Japan, South Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Taipei, Thailand, United States, and Vietnam; see www.apecsec.org.
6. See www.oas.org/juridico/english/cyber.htm.
7. See Latin American governments strengthen cooperation against cyber crime (2008); www.identitytheftdaily.com.
8. See www.oas.org/cyber.htm.

REFERENCES

Accenture Consulting (2005), 'E-government leadership: high performance, maximum value', accessed at www.accenture.com/NR/rdonlyres/D7206199-C3D4-4CB4-A7D8-846C94287890/0/gove_egov_value.pdf.

Achille, S. (2008), 'Visa predicts e-commerce in Latin America to surpass $16 billion this year', *The Hindu*, 11 July, accessed 11 November at www.multilingual-search.com/visa-predicts-e-commerce-in-latin-america-to-surpress-16-billion-this-year/11/07/2008

Amit, R. and P. Schoemaker (1993), 'Strategic assets and organizational rent', *Strategic Management Journal*, **14**: 33-46.

Asian Pacific Economic Cooperation (APEC) (2008), 38th APEC Telecommunications and Working Group Meeting, plenary session, 15-17 October accessed 12 November at www.apecte/wg.org/jsp/download.jsp?seq=5096&board.

Baker and McKenzie (2004), 'Singapore to introduce jail terms, fines, for software and Internet Piracy', accessed at www.channelnewsasia.com.

Barney, J. (1991), 'Firm resources and sustained competitive advantage', *Journal of Management,* **17**(1): 99–120.

Barua, A. and T. Mukhopadhyay (2000), 'Information technology and business performance: past, present and future', in R. Zmud (ed.), *Framing the Domains of IT Management: Projecting the Future through the Past*, Cincinnati, OH: Pinnaflex Educational Resources.

Bharadwaj, A. (2000), 'A resource-based perspective on IT capability and firm performance: an empirical investigation', *MIS Quarterly*, **24**(1) 169–96.

Black, J.A. and K.B. Boal (1994), 'Strategic resources: traits, configurations and paths to sustainable competitive advantage', *Strategic Management Journal*, **15**: 131-48.

Brynjolfsson, E. and S. Yang (1996), 'Information technology and productivity: a review of the literature', *Advanced Computing*, **43**: 179–214.

Burns, T. and G. Stalker (1961), *The Management of Innovation*, London: Tavistock.

Cairncross, F. (1997), *The Death of Distance*, Boston, MA: Harvard Business School Press.

Caves, R.N. (1971), 'International corporations: the industrial economics of foreign investment', *Economica*, **38**: 1–27.
Coase, R.H. (1937), 'The nature of the firm', *Economica*, **4**: 386–405.
Conner, K.R. (1991), 'A historical comparison of resource-based theory and five schools of thought within industrial economics', *Journal of Management*, **17**: 121–54.
Contractor, F.J. (1980), 'The composition of licensing fees and arrangements as a function of economic development of technology recipient nations', *Journal of International Business Studies*, (Winter): 47-62.
Crockett, A. (2000), 'Commentary: how should financial market regulators respond to the new challenges of global economic integration?' in *Global Economic Integration: Opportunities and Challenges*, proceedings of a symposium sponsored by the Federal Reserve Bank of Kansas City, Jackson Hole, WY, 24-26 August pp. 121–8.
Daily Trust (2009), 'The delay on cyber crime law is dangerous', 23 February, accessed 27 February at www.dailytrust.com/index.php?option=com_content&task=view&id=5029&Itemid=10.
Davis, L.E. and D.C. North (1971), *Institutional Change and American Economic Growth*, Cambridge: Cambridge University Press.
Dierickx, I. and K. Cool (1989), 'Asset stock accumulation and sustainability of competitive advantage', *Management Science*, **35**(12): 1504–11.
Dunning, J.H. (1979), 'Explaining changing patterns of international production: in defense of the eclectic theory', *Oxford Bulletin of Economics and Statistics*, **41**(4): 269–95.
Eisenhardt, K. and J. Martin (2000), 'Dynamic capabilities: what are they?', *Strategic Management Journal*, **21**: 1105–22.
Ellickson, Robert C. (1991), *Order without Law: How Neighbors Settle Disputes*, Cambridge, MA: Harvard University Press.
Errunza, Vihang R. (2001), 'Foreign portfolio equity investments, financial liberalization, and economic development', *Review of International Economics*, 9(November): 703–26.
Grant, R.M. (1991), 'The resource-based theory of competitive advantage: implications for strategy formulation', *California Management Review*, **33**(3): 114–35.
Greif, Avner (1989), 'Reputation and coalitions in medieval trade: evidence on the Maghribi traders', *Journal of Economic History*, **49**(3): 857–82.
Hendryx, S.R. (1986), 'Implementation of a technology transfer joint venture in the People's Republic of China: a management perspective', *Columbia Journal of World Business*, (Spring): 57–66.
Henisz, Witold J. and Bennet A. Zelner (2001), 'The institutional environment for telecommunications investment', *Journal of Economics and Management Strategy*, **10**(1): 123–47.
Hitt, L. and E. Brynjolfsson (1996), 'Productivity, business profitability, and consumer surplus: three different measures of information technology value', *MIS Quarterly,* **20**(2): 121–42.
Horstmann, I. and J.R. Markusen (1987), 'Licensing versus direct investment: A model of internalization by the multinational enterprise', *Canadian Journal of Economics*, **20**(3): 464–81.
Identity theft dailly.com (2008), 'Latin American governments strengthen cooperation against cyber crime', 9 September accessed at www.identitytheftdaily.com/index2.php.

IBLS (2009), The Impact of Telecom Sector Privatization on E-Commerce in Brazil, accessed 12 February at www.ibls.com/members/docview.aspx?doc=2343.
ILO (2001), *World Employment Report*, Geneva: ILO.
International Monetary Fund (2000), *International Capital Markets*, Washington, DC: IMF Publications.
International Telecommunication Union (ITU) (2008), *ITU Global Cybersecurity Agenda. A Global Strategic Report*, accessed 3 January 2009 at www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
Kaminsky, Graciela and Sergio L. Schmukler (2002), 'Short-run pain, long-run gain: the effects of financial liberalization', World Bank policy research working paper 2912.
Kauffman, R. and E. Walden (2001), 'Economics and electronic commerce: survey and directions for research', *International Journal of Electronic Commerce*, **5**(4): 5–16.
King, R. and R. Levine (1993), 'Finance and growth: Schumpeter might be right', *Quarterly Journal of Economics*, **108**(3): 681–737.
Lado, A.A. and M.C. Wilson (1994), 'Human resource systems and sustained competitive advantage: a competency-based perspective', *Academy of Management Review*, **19**: 699–727.
La Porta, R. (1998), 'Law and finance', *Journal of Political Economics*, **106**: 1113–55.
La Porta, R., F. Lopez-de-Silanes, A. Shleifer and R. Vishny (1998), 'Law and finance', *Journal of Political Economy*, **106**(6): 6, 1113–55.
Levy, Brian and Pablo T. Spiller (1994), 'The institutional foundations of regulatory commitment: a comparative analysis of telecommunications regulation', *Journal of Law, Economics, and Organization*, **10**(2): 201–46.
Levy, Brain and Pablo T. Spiller (1996), *Regulations, Institutions and Commitment*, Cambridge: Cambridge University Press.
Lippman, S.A. and R. Rumelt (1982), 'Uncertain imitability: an analysis of interfirm differences in efficiency under competition', *Bell Journal of Economics*, **13**: 418–38.
International Telecommunication Union (ITU) (2008), 'Report of the ITU Regional Cybersecurity Forum for Eastern and Southern Africa', 25-28 August, accessed at www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/lusaka-cybersecurity-forum-report-aug-08.pdf.
MarketResearch.com (2001), *CyberCrime and Business Security in Malaysia and Singapore*, accessed at MarketResearch.com, May.
Marris, R.L. (1963), 'A model of the "Managerial" enterprise', *Quarterly Journal of Economics*, **77**: 185-209.
Milgrom, P. and J. Roberts (1990), 'The economics of modern manufacturing: technology, strategy, and organization', *American Economic Review,* **80**(3) 511–28.
Mukhopadhyay, T., S. Kekre and S. Kalathur (1995), 'Business value of information technology: a study of electronic data interchange', *MIS Quarterly*, **19**(2): 137–56.
North, D.C. (1986), 'The new institutional economics', *Journal of Institutional and Theoretical Economics*, **142**(1): 230–37.
Organisation for Economic Co-operation and Development (OECD) (2007), *Communications Outlook*, Paris: OECD.

Orlikowski, W.J. and S.R. Barley (2001), 'Technology and institutions: what can research on information technology and research on organizations learn from each other?', *MIS Quarterly,* **25**(2): 145–65.
Oxley, Joanne Elizabeth (1999), 'Institutional environment and the mechanisms of governance: the impact of intellectual property protection on the structure of inter-firm alliances', *Journal of Economic Behavior and Organization*, **38**(3): 283–310.
Oxley, Joanne E. and Bernard Yeung (2001), 'E-commerce readiness: institutional environment and international competitiveness', *Journal of International Business Studies*, **32**(4): 705–24.
Penrose, E.T. (1959), *The Theory of the Growth of the Firm*, New York: Wiley.
Peteraf, M.A. (1993), 'The cornerstones of competitive advantage: a resource-based view', *Strategic Management Journal*, **14**(3) 179–91.
Porter, M. (1991), 'Towards a dynamic theory of strategy', *Strategic Management Journal*, **12**: 95–117.
Redding, S.G. (1990), *The Spirit of Chinese Capitalism: Studies in Organization*, vol. 22, New York: W. de Gruyter.
Reed, R. and R.J. DeFillippi (1990), 'Causal ambiguity, barriers to imitation, and sustainable competitive advantage', *Academy of Management Review,* **15**(1): 88–102.
Sambamurthy, V., A. Bharadwaj and V. Grover (2001), 'Shaping agility through digital options: re-conceptualizing the role of IT in contemporary firms', University of Maryland working paper, College Park, MD.
Shapiro, C. and H. Varian (1999), Information Rules: A Strategic Guide to the Networking Economy, Boston, MA: Harvard University Press.
Shleifer, A. (2003), 'The New Comparative Economics', *Journal of Comparative Economics*, **31**: 595.
Singh, H., A. Das and D. Joseph (2007), 'Country-level determinants of e-government maturity', *Communications of the Association for Information Systems*, **20**(40): 632–48.
Teece, D.J., G. Pisano and A. Shuen (1997), 'Dynamic capabilities and strategic management', *Strategic Management Journal*, **18**: 509–33.
Asian–Pacific Economic Cooperation (2008), The 27th APEC Telecommunications and Information Working Group, the Chair's Report, accessed at www.apectelwg.org/jsp/download.jsp?seq=5224&board_id=GPATEL_DOCUMENT&doc_seq=1.
The Hindu (2008), Parliament approves Cyber Crime Bill, 24/12/2008, accessed at www.thehindu.com/2008/12/24/stories/2008122456021400.htm.
Thompson, J.D. (1967), *Organizations in Action*, New York: McGraw-Hill.
Tsang, E.W.K. (1995), 'The implementation of technology transfer in Sino-foreign joint ventures', *International Journal of Technology Management*, **10**(7/8): 757–66.
United Nations Conference on Trade and Development (UNCTAD) (2003), *E-commerce and Development Report 2003*, New York and Geneva: United Nations.
United Nations Department of Economic and Social Affairs (UN/DESA) (2005), *Global e-government Readiness Report 2005: From E-government to E-inclusion*, (ITU Regional Cybersecurity Forum 2008) New York: United Nations.
Weber, Max (1981), *General Economic History*, New Brunswick, NJ: Transaction Books.

Weill, P. and M. Broadbent (1998), *Leveraging the New Infrastructure: How Market Leaders Capitalize on Information Technology*, Boston, MA: Harvard Business School Press.
Wernerfelt, B. (1984), 'A resource-based view of the firm', *Strategic Management Journal*, **5**: 171–80.
West, D. (2008), 'Global e-government 2008', accessed at http://insidepolitics.org/egovto7int.pdf.
World Bank (2001), *Finance for Growth: Policy Choices in a Volatile World*, Washington, DC: Policy Research Report.
World Bank (2008), *World Bank Doing Business 2008 Report*, Washington, DC: World Bank.

5. Data collection and empirical results

INTRODUCTION

Cyber space is disordered and chaotic, but its well-defined set of rules is becoming more vigorous every day. It is not confined or restricted by geographic boundaries, which makes it difficult for it to be successfully regulated by geographically defined legislative systems. The rapid expansion of the Internet holds substantial promise for emerging and developing countries, which can benefit, to a great extent, from the Internet's communication and information capacity to help meet their economic, social, and political needs. The increased speed of information generation to electronic media is making information resources generated anywhere in the world available to all global citizens of the world. Emerging and developing countries are the foremost beneficiaries of the recent revolution in communication and information technology. This revolution serves and can serve all sectors of society: the areas of education, health, social policy, commerce and trade, government, agriculture, communications, and research and development all are prime winners.

The correlation between information, communication, and economic growth is well known, making the usefulness of networks nearly self-evident. Electronic networking is a strong, speedy, and economical way to communicate and to exchange information. When networks are available, collaboration among various entities and individuals, as well as countries, seems to come into being almost spontaneously.

The growth of the online economy has been overwhelming, and is expected to reach US$10 trillion by 2010. In many countries, government and business entities have depended on the Internet to, among other things, decrease transaction costs, reach a wider audience, and improve profitability. In the world of the Internet, customers seem to be the main beneficiaries: they use the Internet as a way to gather information and increase their search efficiency and effectiveness. However, more reliance on the Internet would increase the necessity to develop laws to tackle cyber-related attacks and crimes. Unfortunately, not many emerging and developing countries have jumped on the bandwagon of developing comprehensive cyber laws, which has led to a widening legislative divide in the digital world.

The digital divide is a very serious matter for those who are currently behind in Internet access, for they are not able to enjoy many benefits of being wired and are handicapped in participating fully in society's economic, political, and social life. These benefits include finding lower prices for goods and services, working from home, acquiring new skills using distance learning, making better-informed decisions about healthcare needs, and getting more involved in the education of their children. These are only some of the myriad benefits conferred by Internet access. Thus, for citizens of developing countries, lagging behind in Internet access entails further lagging behind in economic progress in the quality of life. Emerging and developing countries lagging in cyber space find themselves in an increasingly difficult position as they attempt to promote their exports, attract capital investment and jobs, and transform their economies. A variety of reasons have been suggested for the digital, and consequently legislative, divide, from lack of telecommunications infrastructure, dearth of computer skills on the part of business and consumers, and failure of regulatory reform and standards, to the poor state of physical infrastructure, such as roads and rail.

The fastest-growing emerging and developing countries are those with the highest degree of openness to imports and exports (Sachs and Warner, 1995; Edwards, 1998); and cyber space is a medium that increases a country's openness. A similarity exists with trade liberalization and Internet adoption. The majority of the countries cited as failing to liberalize trade are found to have very low Internet penetration rates, mainly as a result of poor investment in their telecommunications infrastructure and availability of computers. The International Telecommunication Union (ITU) reports that within the Western hemisphere and some emerging countries, Internet use is highest in those countries where density of telephone use is greater, where the provision of telecommunications services is more competitive, and where the combined costs required to access and use the Internet are lower (ITU, 2009).

The literature on Internet diffusion and cyber activity adoption in emerging and developing countries is extremely limited, although some evidence exists describing the impediments (Travica, 2002). Petrazzini and Kibati (1999) report on cyber space impediments analysing the cases of Argentina, Kenya, India, and Armenia. These include limited Internet accessibility, a lack of competition in international telephone traffic that makes access to the international network expensive, a lack of intra-regional infrastructure, and a disproportionate penetration of the telephone in the urban as opposed to rural, more populated areas. South Korea shares the problems of customers' trust in online merchants (Lee, 1999). A number of researchers have identified obstacles to cyber activities, such as a lack of customer protection laws, tradition of remote shopping,

methods of non-cash payment, and Internet culture. Montealegre (1999) draws on King et al. (1994) and suggests that both society and culture must be considered for successful adoption of cyber activity in developing countries. He illustrates examples of Latin American countries that successfully adopted technology using varying combinations of government, non-governmental, and business organizations. Other cases (Peha, 1999; Clark, 1999) cite examples from Haiti and China, respectively, where successful adoption of telecommunications technology was achieved as a result of competition between government agencies (that formerly controlled the telecommunications networks) and private entities. Davis (1999) indicates that accessibility to technology is the limiting factor, while in reality it is a combination of infrastructure and organizational culture.

In recent years, economists have analysed the impact of a technology developed in an industrialized country that is copied by a developing country. They have shown that the rate of growth of the developing country depends on its initial stock of knowledge and the costs of imitation (Barro and Sala-I-Martin, 1995). They have further argued that if the costs of imitation are lower than the costs of innovation, the poorer country can grow faster than the richer one by leapfrogging technology development through participating and competing in global trade and sharing information globally (Srikantaiah and Xiaoying, 1998). For instance, countries with an underdeveloped telecommunications infrastructure can implement a digital telecom network and avoid the costs many developed countries incurred in first laying out an analog system. Yet, even when developing countries adopt cyber activity and electronic commerce, the technologies are not always optimized. A survey by the International Trade Center discovered that businesses in developing countries view their Internet connectivity as a valuable communications tool, but failed to incorporate the technology as an aspect of their competitive strategy (Barclay and Domeisen, 2001). Business perception contributes to the fact that less than a third of the surveyed countries included electronic trade as a component of their national export development strategies, an excellent indicator of the need for close cooperation between government and business during this technology adoption.

To facilitate the introduction of the Internet and eventually electronic commerce/services, the necessary condition is the creation of the communication's infrastructure, or the skeleton of cyber activity. For developing countries, financial resources needed to invest in communication infrastructure are one of the major barriers since most countries rely on foreign aid. A number of initiatives undertaken by developed countries are helping to narrow the digital divide, albeit limited in terms of scope and weight; the Leland Initiative, for instance, is a five-year US$15 million

project sponsored by the United States government to provide Internet connectivity in more than 20 African countries. In addition to developing infrastructure, the objective of the program is to create a sustainable supply of Internet services including training, marketing, and extension into rural areas, as well as support and training for small to medium sized businesses (USAID, 2003). The user-based initiative relies on partnerships of local banks, companies, and governmental entities. Expanding on the development of the communications infrastructure projects is the creation of community learning centers (CLCs) which have their roots in former post and telegraph offices that served as central points for public information and communication. These centers, widely popular in some countries in Africa and Latin America, provide inexpensive Internet access plus a variety of business services such as faxing, photocopying, word processing, and printing, reducing the cost of equipment and connection fees. In addition to these services, the CLCs provide training and education on both technology and business management issues.

A number of infrastructure development challenges include (1) development of physical telecommunications infrastructure; (2) provision of universal access at a reasonable cost; (3) achievement of interconnection and interoperability of telecommunications; and (4) establishment of networks and services.

While developing the ICT infrastructure is the necessary condition for economies to get on the cruise into cyber space, the sufficient condition to encourage people to venture into cyber space is the development of the legislative environment that will protect users on the cyber highways. Developing cyber laws act as an insurance policy for those who dare to venture into cyber space. A number of multilateral entities, such as the ITU and the European Union, have developed what is referred to as a 'model' set of laws for cyber space, and are providing the necessary support to emerging and developing countries to draft their cyber laws. However, many of these emerging and developing countries still lag behind in this area.

The remainder of this chapter deals with data collection on the various variables identified in the previous chapter, the proposed operational measurements of the independent variables and the dependent variable, discussion of methodology, and analysis of the empirical results.

DATA COLLECTION

In order to assess the significance of the various economic resources in explaining the development of cyber laws in emerging and developing countries, the authors assembled cross-sectional data for 44 emerging

and developing economies which are considered more advanced in their involvement in the information/knowledge society, and which have implemented electronic commerce initiatives. Data on Internet usage and other indicators of electronic commerce activities were collected from the Internet World Stats website (Table 5.1).

Table 5.2 shows our sample countries organized according to the World Bank classification in terms of development. In this classification, economies are divided according to their 2003 gross national income (GNI; formally referred to as GNP) per capita. The groups are: low income, with GNI of US$765 or less; lower middle income, with GNI of US$766–US$3,035; upper middle income, with GNI of US$3,036–US$9,385; and high income, with GNI of US$9,386 or more. In calculating GNI the World Bank uses the Atlas conversion factor. The purpose of this conversion factor is to reduce the impact of exchange rate fluctuations in the cross-country comparison of national incomes. The Atlas conversion factor, for any year, is the average of a country's exchange rate (or alternative conversion factor) for that year and its exchange rates for the two preceding years adjusted for the difference between the rate of inflation in the country, and through 2000, that in the G-5 countries (France, Germany, Japan, the United Kingdom, and the United States). For 2001 onwards, these countries include the Euro Zone, Japan, the United Kingdom, and the United States. A country's inflation rate is measured by the change in its gross domestic product (GDP) deflator.

The inflation rate for G-5 countries (through 2000, and the Euro Zone, Japan, the United Kingdom, and the United States for 2001 onwards), representing international inflation, is measured by the change in the special drawing rights (SDR) deflator. (Special drawing rights are the IMF's unit of account.) The SDR deflator is calculated as a weighted average of the G-5 countries' GDP deflators in SDR terms, the weights being the amount of each country's currency in one SDR unit. Weights vary over time because both the composition of the SDR and the relative exchange rates for each currency change. The SDR deflator is calculated in SDR terms first and then converted to US dollars using the SDR to dollar Atlas conversion factor. The Atlas conversion factor is then applied to a country's GNI. The resulting GNI in US dollars is divided by the midyear population to derive GNI per capita.

OPERATIONAL MEASUREMENTS

In the current research, the comprehensiveness of the cyber legislation and related activities is the dependent variable. The proposed measurements of the dependent and independent variables are presented below.

Table 5.1 2008 Internet usage in sample countries

Country	Number of Internet users (millions)	% of population using the Internet
Algeria	3.5	10.4
Argentina	16.0	39.0
Bolivia	1.0	10.8
Brazil	50.0	27.0
Bulgaria	2.4	32.6
Chile	7.4	44.9
China	298.0	22.4
Colombia	13.8	30.5
Czech Republic	4.9	48.8
Ecuador	1.1	8.0
Egypt	10.5	12.9
Hong Kong	4.9	69.5
Hungary	5.2	52.5
India	81.0	7.1
Indonesia	25.0	10.5
Iran	23.0	34.9
Israel	3.7	52.0
Jordan	1.1	18.2
Kazakhstan	1.9	12.4
Korea	36.8	76.1
Lebanon	0.95	23.9
Malaysia	15.9	62.8
Mexico	23.7	21.6
Nigeria	10.0	6.8
Oman	0.3	9.1
Pakistan	17.5	10.1
Peru	7.6	26.2
Philippines	14.0	14.6
Poland	20.2	52.0
Qatar	0.35	37.8
Romania	7.43	33.4
Russia	38.0	27.0
Saudi Arabia	6.2	22.0
Singapore	3.1	67.4
Slovakia	2.7	49.6
South Africa	4.6	9.4
Sri Lanka	0.77	3.7
Taiwan	15.2	66.1
Thailand	13.4	20.5
Turkey	26.5	35.0
UAE	2.3	49.8

Table 5.1 (continued)

Country	Number of Internet users (millions)	% of population using the Internet
Ukraine	6.7	14.6
Uruguay	1.1	31.6
Vietnam	20.8	24.2

Source: Internet World Stats, www.internetworldstats.com.

Maturity of Cyber Laws (Dependent Variable)

Frenetic activity in the past few years has ensured that lawyers and policy makers specializing in information technology law have been kept busy monitoring developments that are taking place in many parts of the world.

An examination of national laws covering the different legal facets and issues associated with cyber space, supported by an analysis of the existing international conventions and agreements which are relevant to this specific area, uncovered the following five main legislative topics:

- data protection and processing, including privacy rights;
- e-commerce, including e-governments;
- e-transactions, especially issues dealing with online banking;
- cyber crime;
- intellectual property.

In the developing and emerging countries in our sample, it is observed that while, in general, cyber laws have been enacted in a number of countries, a large chunk still fall short of what can be considered adequate and/or comprehensive cyber legislation; what we refer to in this book as mature cyber law. Generally, the majority of countries have enacted legislation relating to e-commerce/e-government, including e-signature and acceptance of e-documents and e-contracts; in addition, many have tackled intellectual property issues, which are largely addressed under general copyright laws, rather than under specific cyber laws related to intellectual property (United Nations Economic and Social Commission for Western Africa, 2008).

Broadly speaking, cyber space symbolizes a conceptual distinction between activities that take place in the physical or real world and those that occur online or in virtual reality. Beyond conceptual distinctions, we

Table 5.2 World Bank classification

Algeria	Lower middle income
Argentina	Upper middle income
Bolivia	Lower middle income
Brazil	Upper middle income
Bulgaria	Lower middle income
Chile	Upper middle income
China	Lower middle income
Colombia	Lower middle income
Czech Republic	Upper middle income
Ecuador	Lower middle income
Egypt	Lower middle income
Hong Kong	High income
Hungary	Upper middle income
India	Low income
Indonesia	Lower middle income
Iran	Lower middle income
Israel	High income
Jordan	Lower middle income
Kazakhstan	Lower middle income
Korea	High income
Lebanon	Upper middle income
Malaysia	Upper middle income
Mexico	Upper middle income
Nigeria	Low income
Oman	Upper middle income
Pakistan	Low income
Peru	Lower middle income
Philippines	Lower middle income
Poland	Upper middle income
Qatar	High income
Romania	Lower middle income
Russia	Lower middle income
Saudi Arabia	Upper middle income
Singapore	High income
Slovakia	Upper middle income
South Africa	Lower middle income
Sri Lanka	Lower middle income
Taiwan	Middle income
Thailand	Lower middle income
Turkey	Lower middle income
UAE	High income
Ukraine	Low income
Uruguay	Upper middle income
Vietnam	Low income

might say that the infrastructure of cyber space is basically digital code, and that this aspect of cyber space makes the virtual landscape unique. As a practical matter, both the increasing importance and the expanding utility of the Internet are making distinctions between real space and cyber space less noticeable. Even so, cyber space still presents a remarkable number of novel legal questions involving how computer users carry out various transactions involving cyber activities through the interconnection of computing and communications technologies. Although the lack of reliable or relevant precedent renders legal practice in this area difficult and, quite often, annoying, the challenges are also exciting.

Not surprisingly, because of the unique nature of the Internet, its use creates unique legal questions and issues, particularly with respect to intellectual property rights and cyber crime. In addition, e-government requires a regulatory and public policy environment conducive to electronic commerce, protection of rights, and an enabling legal framework for the digital transformation of government operations. Policy agendas include issues such as privacy, security, digital signatures, consumer protection, international trade, telecommunications, taxation, and the digital divide. Industrial age laws, their interpretation, and intent are many times not applicable or, worse, detrimental to a growing digital economy and society. Investment in the education of legislators around technology issues is a prerequisite to successful e-government. Without digital signatures, for instance, companies are hard pressed to engage in electronic commerce. Businesses require assurance that an electronically signed document can be enforced against the sender. At present, in most countries, there is no definitive court decision ruling that an electronic document can be 'signed' electronically in legal systems and in circumstances where the signature remains as a formal requirement of law. This 'signature' issue is intimately related to a technical, legal issue of proof. In a court case, a party seeking to enforce a contract has the burden of proving that (1) the document was signed by the person who it claims to have come from; and (2) the document presented is, in fact, the one that was signed.

Many developing and emerging countries have realized the importance and necessity of law to regulate cyber space. However, development of cyber law is still evolving in developing and emerging countries. The totality of the proposed Digital Signature and E-Commerce regime in Thailand, for instance, has been strongly criticized. The two separate laws – one on electronic transactions and the other on electronic signatures – have been merged into one following a review by the Office of the Juridical Council. This new draft, which was approved by the Cabinet, is opposed by the IT industry because the Cabinet's regulatory authority lies with digital signatures not the much broader issue of electronic commerce. Industry

feels strongly that these two areas are fundamentally different and should be clearly distinguished. Moreover, IT experts find the new draft overly broad and too vague. Notwithstanding the criticism, the Bill passed its first reading in Parliament on 23 August 2000. On 27 September 2000, a revised version of the Electronic Commerce law was scheduled for its second reading in Parliament. The draft law was rewritten to remove concerns about too much government control over electronic commerce and some unclear sections of the law. Basically it seemed that the responsibility of the e-commerce committee would be confined to regulating e-signatures instead of the broader issue of electronic commerce or enacting a cyber law dealing with cyber crime. In October 2000, it became clear, however, that the Bills would be stalled and delayed. In a recent development, one of the first orders passed by the military junta that took power in Thailand on 19 September 2006 was to appoint an Official Censor of the Military Coup whose responsibility is to censor the Internet and block controversial websites. In addition, the Computer-Related Crimes Act (CRCA) requires all state and private organizations to install log management systems that store and monitor computer data for the purpose of preventing Internet crime. Failure to comply with this provision carries a fine of up to US$14,500.

Other developing and emerging countries, however, have been very slow in, or reluctant to develop a cyber law. In 2003, Egypt, for instance, drafted an electronic signature law, which has been approved by the Cabinet (it is awaiting discussion by Parliament); however, Egypt is deferring a broader electronic commerce law that will address such issues as domain names, customs and duties, and creation of a certificate authority to verify electronic signatures. The development of electronic commerce in Egypt has been impeded by concern about the lack of security on computer networks, the relatively high prices charged by Internet service providers, and the somehow low number of Internet users in the country (12.9 percent in 2008). The country of Lebanon is a perfect example of disinclination and reluctance; Lebanon has not yet adopted an electronic signature law, which would allow companies to conduct business and keep records electronically, although a draft of the law has circulated in Parliament since 2000. In addition, a telecom liberalization and privatization law passed in 2002 remains unimplemented. Table 5.3 lists the countries in our sample, whether or not the country has enacted a separate cyber law, and, if so, the year the law was enacted.

In Latin America, Brazil and Argentina have been proactive in the development of cyber regulations. The laggards are countries such as Venezuela, Ecuador, and Bolivia, which are less developed and in some cases still have monopoly long-distance or local service providers and that really have not embraced liberalization on any front.

Table 5.3 Cyber law in sample countries

Country	Law (Y/N)	Year enacted
Algeria	No	
Argentina	Yes	2001
Bolivia	No	
Brazil	Yes	2001
Bulgaria	Yes	1999
Chile	Yes	2002
China	No	
Colombia	Yes	1999
Czech Republic	Yes	2000
Ecuador	Yes	2002
Egypt	No	
Hong Kong	Yes	2000
Hungary	Yes	2001
India	Yes	1998/2008 (amended)
Indonesia	Bill drafted	
Iran	No	
Israel	Yes	2001
Jordan	No	
Kazakhstan	No	
Korea	Yes	2001
Lebanon	No	
Malaysia	Yes	1997
Mexico	Yes	2000
Nigeria	Bill drafted	
Oman	Yes	2008
Pakistan	Yes	2008
Peru	Yes	2000
Philippines	Yes	2000
Poland	Yes	2001
Qatar	No	
Romania	Yes	2001
Russia	Yes	2001
Saudi Arabia	Yes	2009
Singapore	Yes	1998
Slovakia	Yes	2002
South Africa	Yes	2002
Sri Lanka	No	
Taiwan	Yes	2001
Thailand	Yes	2000
Turkey	No	
UAE	Yes	2006
Ukraine	No	

Table 5.3 (*continued*)

Country	Law (Y/N)	Year enacted
Uruguay	Yes	2000
Vietnam	Yes	2002

Source: Compiled by the authors from various resources.

As developing and emerging countries join the World Trade Organization (WTO) they have been adapting their legal and regulatory systems to accommodate trademark, patent, and intellectual property rights (IPR) protection. Some countries have been part of the early stages of IPR protection; others have retroactively signed the agreements and sought membership in the World Intellectual Property Organization (WIPO). As of February 2009, only five countries in our sample are not members of the WTO; these are Algeria, Iran, Kazakhstan, Lebanon, and Russia.

Developing and emerging countries' participation in interim treaties is uneven. These include the WIPO Copyright Treaty (WCT), the Trademark Law Treaty (TLT), and the Patent Law Treaty (PLT). As of January 2009, for instance, only 69 states worldwide were members of the WCT. Copyright protection extends to expressions and not to ideas, procedures, methods of operation, or mathematical concepts as such (WIPO, 2009). Twenty-four countries in our sample are members of the WCT, or 55 percent. Russia was the latest cosignatory, having become a member in November 2008.

As of January 2009, only 42 countries worldwide have brought the TLT into force. As Table 5.4 indicates, as of January 2009, only 13 countries, or 30 percent, in our sample have brought this treaty into force and an additional five countries have signed the treaty. As of January 2009, only 61 countries worldwide were cosignatories to the PLT, and only 19 of those have brought the treaty into force. Table 5.4 shows that only six countries in our sample are among those which have signed and enforced this treaty, with an additional seven having signed the treaty but have not yet entered it into force.

In its 2003–06 action plan, Singapore had adopted three outcomes for e-government: delighted customers, connected citizens, and networked government. Singapore is in the process of reviewing its current suite of online services against the needs of the public to identify opportunities for service innovation that will yield greater value. In some cases, these action plans are not supported by an all-encompassing approach to measuring value or progress; however, in many cases such a measurement framework

Table 5.4 Status of countries on IPR (2009)

Country	WTO member	WCT	TLT	PLT
Algeria				Signed
Argentina	1995	2002		
Bolivia	1995			
Brazil	1995			Signed
Bulgaria	1996	2002		
Chile	1995	2002		
China	2001	2007	Signed	
Colombia	1995	2002		
Czech Republic	1995	2002	1996	Signed
Ecuador	1996	2002		
Egypt	1995		1999	
Hong Kong	1995			
Hungary	1995	2002	1998	2008
India	1995			
Indonesia	1995	2002	1997	
Iran				
Israel	1995		Signed	Signed
Jordan	2000	2004		
Kazakhstan	2000	2004	2002	
Korea	1995	2004	2003	
Lebanon				Signed
Malaysia	1995			
Mexico	1995	2002		
Nigeria	1995			2005
Oman	2000	2005	2007	2007
Pakistan	1995			
Peru	1995	2002		
Philippines	1995	2002		
Poland	1995	2004	Signed	Signed
Qatar	1996	2005		
Romania	1995	2002	1998	2005
Russia		2008	1998	
Saudi Arabia				
Singapore	1995	2005		
Slovakia	1995	2002	1997	2005
South Africa	1995		Signed	
Sri Lanka	1995		1996	
Taiwan	2002			
Thailand	1995			
Turkey	1995	2008	2005	Signed
UAE	1996	2004		
Ukraine		2005	1996	2005

Table 5.4 (*continued*)

Country	WTO member	WCT	TLT	PLT
Uruguay	1995		Signed	
Vietnam				

Source: Collected by the authors from various sources.

is planned. Mexico, for example, is developing a new project management system for e-government that will include metrics, key performance indicators, and a scorecard to facilitate evaluating its e-Mexico initiative. Late in 2008, Pakistani President Asif Ali Zardari issued a decree making Internet crime punishable by death or imprisonment with heavy fines. The law, enforced at the time of signing, defines any cyber crime that causes a death as 'cyber terrorism', which will be punishable by death or imprisonment for life. Only crimes leading to death will be punishable with the death sentence; other crimes are punishable by imprisonment and/or heavy fines. As of February 2009, Pakistan has more than 10 million Internet users. According to the law, the offender, whether a person, a group, or an organization, will be deemed to have committed 'cyber terrorism' if accessing a computer, electronic system, or electronic device with a view to engaging in an act of terrorism.

According to the new Pakistani law, 'cyber crime' also includes 'stealing or copying' classified information or data required to make chemical, biological, or nuclear weapons. The law specifies various durations of imprisonment and fines for other crimes, such as cyber fraud, stalking, and spamming (Khan, 2008).

In a move toward creating a suitable environment for secure electronic transactions, Oman has issued the e-Transactions Law under Royal Decree 69/2008. One of the main purposes of this law is to facilitate electronic transactions that are considered vital to e-government and e-commerce applications in Oman. In order to support such transactions, any contract, agreement, or communication carried by electronic means as electronic messages is considered legally valid through this law. Further, the law regulates the transfer of electronic data and messages through various electronic channels such as the Internet and controls changes made to data. The creation of this regulatory environment in Oman has placed strict penalties on the misuse of electronic systems and data resident on these systems. Cyber criminal acts, such as hacking into computer systems and unauthorized capture or tampering with data, are punishable by jail terms not to exceed two years and/or hefty penalties not to exceed

5,000 Omani riyals (US$13,000). Promotion of this law sets up unified rules, regulations, and standards of authenticating electronic messages and records.

Oman Law no. 69 of 2008 consists of nine sections and 54 articles. It has been developed and refined over a period of three years, based on guidelines of the United Nations Commission on International Trade Law (UNCITRAL), the Organization for Economic Cooperation and Development, and e-laws of several countries such as the USA, France, Ireland, and Malaysia. The Law legalizes the use of digital signatures in electronic commerce and communications through letters and e-mails.

The authors developed a Cyber Law Index (CLI) for the 44 countries included in our sample. The Index was developed using a content analysis of the various laws enacted by the countries in addition to their engagement in a global world as international actors, indicated by their memberships in the WTO and the various WIPO initiatives such as the WCT, PLT, and TLT.

Given the lack of information on the soundness of cyber laws in the various countries, the authors will use the length of time the law has been enacted as a proxy. It is believed that countries that developed and implemented cyber laws early on (and based them on the European Convention model) have a better and strong commitment to moving their economies into the information/digital age, for the mere development of these laws is a signal or an indication to motivated businesses to move into cyber space.

Given the continuously developing nature of online activities due to new technological developments and convergence, in particular the development of the Internet and the ICT sector, and the large quantity and range of personal information involved, these developments afford a number of challenges that may not necessarily be dealt with by telecommunications laws or general traditional consumer protection laws. Therefore, many countries are enacting and implementing additional laws and regulations that are focused on consumer protection matters in cyber space, such as intellectual property rights, spam, privacy, fraud, identity theft, cyber crime, and e-commerce transactions. Such legislation protecting consumer activities in cyber space, and providing for the security of electronic networks and communications, is necessary to create trust and confidence in the use of digital networks and enhance online transactions.

The CLI variable is constructed in its composite form based on:

1. content analysis of the legal texts of national laws of the sample countries; we strived to isolate those provisions dealing with cyber legislation. We then conducted an analysis of existing cyber laws in the

sample countries in terms of whether such laws have covered the five areas mentioned above (data protection, e-transactions, e-commerce/e-government, intellectual property, and cyber crime);
2. a country's membership in the WTO;
3. a country's membership in the WCT;
4. a country's membership in the TLT;
5. a country's membership in the PLT.

These five components are not equally weighted. The authors judged component (1), content of the cyber law, to be the most important; consequently, it is given a 65 percent weight. Next in terms of importance is membership in the WTO, with a weight of 20 percent. The remaining three components (WCT, TLT, and PLT) are weighted at 5 percent each. Table 5.5 shows the Cyber Law Index for the sample countries.

Level of Technical Maturity

Countries are usually at very different starting positions in the task of building their digital infrastructure to facilitate the development and diffusion of e-commerce applications. E-commerce infrastructure determines the level of access and technical capabilities of an economy, and is defined as the share of total economic infrastructure used to support electronic business processes and conduct electronic commerce transactions. The innovation of the Internet technology, coupled with different environment and policy externalities, lead to distinctive arrangements determining specific diffusion paths among individual countries and regions. Identifying unique resources of countries is essential for understanding e-commerce diffusion in these countries. Some large developing countries, such as Brazil, are faced with obstacles and opportunities to diffuse the Internet across their economies and societies. Telecommunication infrastructure is often a stumbling block for developing countries. Based on this statement, countries lagging behind a certain level of telephone density would be severely handicapped for e-commerce diffusion.

Our access and technical capabilities measures focus on a number of indicators describing the availability of reasonably priced access to the Internet. For most current applications, Internet access requires a personal computer, plus a phone connection to the Internet, although access via mobile phone is becoming a viable alternative in some applications and in a number of countries in our sample such as the UAE. For the purpose of our study, we use the following infrastructure indicators: (1) total number of telephone subscribers, (2) number of Internet hosts, and (3) number of personal computers. Data for 2003 on the total number of personal

Table 5.5 Cyber Law Index

Country	Cyber Law Index
Algeria	0.20
Argentina	0.80
Bolivia	0.50
Brazil	0.80
Bulgaria	0.80
Chile	0.80
China	0.30
Colombia	0.80
Czech Republic	0.90
Ecuador	0.80
Egypt	0.40
Hong Kong	0.70
Hungary	0.90
India	0.70
Indonesia	0.60
Iran	0.10
Israel	0.80
Jordan	0.40
Kazakhstan	0.50
Korea	0.90
Lebanon	0.30
Malaysia	0.70
Mexico	0.80
Nigeria	0.40
Oman	0.50
Pakistan	0.50
Peru	0.80
Philippines	0.60
Poland	0.90
Qatar	0.60
Romania	0.90
Russia	0.40
Saudi Arabia	0.20
Singapore	0.80
Slovakia	0.90
South Africa	0.70
Sri Lanka	0.40
Taiwan	0.70
Thailand	0.70
Turkey	0.40
UAE	0.70
Ukraine	0.30

Table 5.5 (*continued*)

Country	Cyber Law Index
Uruguay	0.80
Vietnam	0.40

Source: Developed by the authors.

computers, phone lines, number of Internet users, and mobile phones in each country are taken from the *International Telecommunications Union Yearbook* of 2007 (ITU, 2007). We scale each of these totals by population to produce per capita measures: TLLINE, PCHOSTS, and PC #.

In a recent ICT published index (ITU, 2009), the UAE has significantly improved its information and communication technology or ICT levels, ranking sixth in the International Telecommunication Union's ICT price basket in 2008.

The country also ranks first in the ITU's new ICT Development Index in the Arab world. This index compares developments in ICT in 154 countries over a five-year period from 2002 to 2007, and shows that the UAE recorded a gain in index value of around 300 percent, among the highest in the world. This places the UAE at a rank of 32, up from 40 in 2002. Mobile phone broadband penetration in the country was already at 46.6 percent in 2007. Similarly, mobile cellular penetration reached one of the highest values globally in 2007 – 176 per 100 inhabitants. The UAE tops other Gulf Cooperation Council (GCC) countries in the index, which saw Bahrain and Qatar ranked 42nd and 43rd, Saudi Arabia and Kuwait at the 55th and 57th ranks, and Oman in 77th place.

The UAE also ranked third in the overall ICT price basket for 2008, together with Luxembourg, Denmark, Hong Kong, Taiwan, Sweden, and Norway. It ranked sixth in the mobile cellular sub-basket for 2008, third in the fixed telephone sub-basket and 22nd in the fixed broadband Internet sub-basket for 2008.

Monitoring the cost of ICT services is important because it influences or even determines whether people will subscribe to a certain service and use ICTs. Although ICT infrastructure is crucial in providing the basic prerequisite for citizens to access and use ICTs, the services offered have to be affordable. Almost 50 percent of the developing countries have an ICT price basket that corresponds to more than 10 percent of their GNI per capita. This suggests that countries with higher income levels pay relatively little for ICT services, while low-income countries pay relatively more. In addition, the high value of the ICT price basket in several developing

countries is partly explained by very high fixed Internet broadband prices. The results of the ICT price basket further suggest that the relative price of ICT services is linked to a country's ICT level. In other words, generally, countries with high prices have lower access and usage levels. The economies ranked at the top of the ICT price basket include some of the most advanced economies in terms of ICT uptake and use, such as Singapore, the United States, Luxembourg, Denmark, Hong Kong, Sweden, and Norway. These are the economies with the lowest relative price of ICTs. However, bucking this trend, the UAE shares the dubious distinction of having the highest cost of telephone and especially mobile phone calls, along with Egypt, Italy, and Hong Kong.

Developing practical measures of the reach and richness of cyber law in emerging and developing economies, as well as in the developed world, is a considerable challenge. At present only a few developed countries, such as the United States and the United Kingdom, have initiated national data collection on cyber crime; none of these countries, though has tested the effectiveness of their cyber laws, nor have they developed metrics to measure the reach and richness of these laws. The reach and richness of cyber laws are expected to be positively related to the penetration rate of Internet users in an economy; this is used as a proxy for e-commerce diffusion.

Data on the number of Internet users in a country in 2008 are available from the Internet World Stats website at www.internetworldstats.com. Based on Table 5.1, the four countries with the highest Internet penetration rates, South Korea (76.1 percent), Hong Kong (69.5 percent), Singapore (67.4 percent), and Taiwan (66.1 percent), are all in Asia. Among the Latin American countries, Chile (44.9 percent) and Argentina (39 percent) top the list there. In the Middle East, Israel (52.0 percent) and the UAE (49.8 percent) rank at the top.

The Technical Maturity (TECHMAT) Index is computed as:

$$\begin{aligned} TECHMAT = {} & 1/3\ (\text{Internet penetration}) + 1/6\ (\text{PC penetration}) \\ & + 1/6\ (\text{Internet host}) + 1/6\ (\text{Telephone penetration}) \\ & + 1/6\ (\text{Broadband penetration}) \end{aligned} \tag{5.1}$$

Table 5.6 lists the countries in our sample along with their broadband diffusion rate; it is noticeable that Korea, Hong Kong, and Israel are the top three performers in this category; the lowest performers are Iran, Bolivia, and Nigeria.

Table 5.7 depicts the computed technical maturity of the countries in our sample as defined by the formula (5.1) defined above.

Table 5.6 Broadband penetration, 2008

Country	Broadband/100
Algeria	0.85
Argentina	6.58
Bolivia	0.36
Brazil	3.54
Bulgaria	8.24
Chile	7.86
China	5.00
Colombia	2.62
Czech Republic	12.90
Ecuador	2.39
Egypt	0.63
Hong Kong	26.35
Hungary	14.25
India	0.27
Indonesia	0.11
Iran	0.00
Israel	22.06
Jordan	1.45
Kazakhstan	1.75
Korea	30.50
Lebanon	4.88
Malaysia	3.80
Mexico	4.27
Nigeria	0.10
Oman	0.78
Pakistan	0.03
Peru	2.04
Philippines	0.56
Poland	9.00
Qatar	8.37
Romania	9.09
Russia	2.81
Saudi Arabia	2.52
Singapore	20.18
Slovakia	8.76
South Africa	0.78
Sri Lanka	0.33
Taiwan	20.92
Thailand	1.43
Turkey	6.08
UAE	8.67
Ukraine	1.73

Table 5.6 (*continued*)

Country	Broadband/100
Uruguay	4.94
Vietnam	1.48

Source: ITU (2008).

Human Resources

The Human Development Index (HDI) is a widely discussed new measure of the effect of economic development on the well-being of the people. The United Nations Development Program (UNDP) developed the HDI during the early 1990s when in the economic literature 'per capita income' was considered as an inadequate measure of development (especially for emerging and developing countries). It was argued that 'real' gross domestic product per person growth is not necessarily a good guide to growth of living standards in the twentieth century; it is probably a considerable underestimate (Crafts, 1999). The HDI shifted the focus of economic development from (per capita) income to a much broader achievement in human life.

The HDI measures the overall achievement of a country in three basic dimensions of human development – longevity, knowledge, and a decent standard of living – all of which we consider as indigenous resources. Longevity is measured by life expectancy at birth; knowledge (or educational attainment) is measured by a combination of adult literacy (two-thirds weight) and the combined primary, secondary, and tertiary enrollment (one-third weight); and standard of living is measured by real GDP per capita ($PPP). To calculate the HDI score, first, for each indicator of human development, a range (a maximum and a minimum) is established. Then, the difference of score of a country on each indicator (actual score minus minimum of the range) is divided by the range itself. The HDI is a simple average of the three indicators so obtained.

Despite its popularity as an index, it is not free of criticism. The concept of human development has a broad meaning and cannot be captured by an index or a set of indicators (Streeten, 1994). The index has also been criticized on other grounds. These include the construction of the scale and measurement (Dasupta and Weale, 1992; Desai, 1991; Luchters, 1996; Shrinivasan, 1994), methodology (Shrinivasan, 1994), and data quality/limitations issues (McGillivray and White, 1993). Despite its limitations, the index is a useful measure to gauge the status of human development

Table 5.7 Technical maturity

Country	TECHMAT
Algeria	0.152525
Argentina	0.222659
Bolivia	0.06978
Brazil	0.14623
Bulgaria	0.280946
Chile	0.188673
China	0.123569
Colombia	0.156584
Czech Republic	0.270758
Ecuador	0.152825
Egypt	0.09264
Hong Kong	0.390909
Hungary	0.262808
India	0.039597
Indonesia	0.072235
Iran	0.126665
Israel	0.31653
Jordan	0.153741
Kazakhstan	0.188533
Korea	0.281279
Lebanon	0.088585
Malaysia	0.182219
Mexico	0.142954
Nigeria	0.047616
Oman	0.179401
Pakistan	0.069277
Peru	0.11231
Philippines	0.107017
Poland	0.243153
Qatar	0.313104
Romania	0.227265
Russia	0.248342
Saudi Arabia	0.22325
Singapore	0.329392
Slovakia	0.239641
South Africa	0.162761
Sri Lanka	0.093305
Taiwan	0.318505
Thailand	0.227667
Turkey	0.189732
UAE	0.363036
Ukraine	0.248989

Table 5.7 (*continued*)

Country	TECHMAT
Uruguay	0.207505
Vietnam	0.102892

Source: Developed by the authors.

in a country. Economists agree that while there is a strong relationship between development and income, human outcomes do not depend on economic growth and levels of national income alone. They also depend on how these resources are used. For instance, democratic participation in decision making and equal rights for men and women are two of the most important human development indicators but they do not depend on income or GDP.

The Human Development Index is derived from the 2004 *Human Development Index Report* published by the United Nations. This report presents an extensive set of indicators, including 33 tables and 200 variables, on important human outcomes realized in countries around the world.

The HDI focuses on three measurable dimensions of human development: living a long and healthy life, being well educated, and having a decent standard of living. Table 5.8 shows the values of the three dimensions of the HDI along with the HDI for each country in our sample. These figures are compiled from the 2004 *Human Development Report* published by the United Nations.

A close examination of Table 5.8 reveals that Israel is ranked number one in our sample with an HDI value of 0.908, closely followed by Hong Kong (0.903) and Singapore (0.902). The country that ranked at the bottom of the list in our sample is Nigeria, with an HDI of 0.466, followed by Pakistan (0.497) and India (0.595). The average HDI value for all countries in our sample is 0.766, with a standard deviation of 0.094. This small standard deviation indicates a narrow distribution where all values cluster around the mean.

In our statistical analysis the HDI will be utilized to measure human development in a country.

Financial Resources

As discussed in Chapter 4, information technology has led to the promotion of a more intensive use of international financial institutions and gave rise to global international conglomerates. In addition, previous studies have

Table 5.8 HDI values of sample countries

Country	Life expectancy index	Education index	GDP index	HDI value
Algeria	0.74	0.69	0.68	0.704
Argentina	0.82	0.96	0.78	0.853
Bolivia	0.64	0.86	0.53	0.681
Brazil	0.72	0.88	0.73	0.775
Bulgaria	0.77	0.91	0.71	0.796
Chile	0.85	0.90	0.77	0.839
China	0.76	0.83	0.64	0.745
Colombia	0.78	0.84	0.69	0.773
Czech Republic	0.84	0.92	0.84	0.868
Ecuador	0.76	0.85	0.60	0.735
Egypt	0.73	0.62	0.61	0.653
Hong Kong	0.91	0.86	0.93	0.903
Hungary	0.78	0.95	0.82	0.848
India	0.64	0.59	0.55	0.595
Indonesia	0.69	0.80	0.58	0.692
Iran	0.75	0.74	0.70	0.732
Israel	0.90	0.94	0.88	0.908
Jordan	0.76	0.86	0.62	0.750
Kazakhstan	0.69	0.93	0.68	0.766
Korea	0.84	0.97	0.86	0.888
Lebanon	0.81	0.84	0.63	0.758
Malaysia	0.80	0.83	0.75	0.793
Mexico	0.81	0.85	0.75	0.802
Nigeria	0.44	0.59	0.36	0.466
Oman	0.79	0.71	0.82	0.770
Pakistan	0.60	0.40	0.49	0.497
Peru	0.74	0.86	0.65	0.752
Philippines	0.75	0.89	0.62	0.753
Poland	0.81	0.96	0.78	0.850
Qatar	0.78	0.83	0.88	0.833
Romania	0.76	0.88	0.70	0.778
Russia	0.69	0.95	0.74	0.795
Saudi Arabia	0.79	0.71	0.81	0.768
Singapore	0.88	0.91	0.92	0.902
Slovakia	0.81	0.91	0.81	0.842
South Africa	0.40	0.83	0.77	0.666
Sri Lanka	0.79	0.83	0.60	0.740
Taiwan	0.78	0.79	0.77	0.780
Thailand	0.74	0.86	0.71	0.768
Turkey	0.76	0.80	0.69	0.751
UAE	0.83	0.74	0.90	0.824

Table 5.8 (*continued*)

Country	Life expectancy index	Education index	GDP index	HDI value
Ukraine	0.74	0.94	0.65	0.777
Uruguay	0.84	0.94	0.73	0.833
Vietnam	0.73	0.82	0.52	0.691

Source: UN Human Development Index Report (2004).

found evidence that a well-developed, sound financial system promotes growth in the economy by channeling credit to its most productive uses.

A robust, well-functioning financial sector is vital for economic growth and successful electronic activities, especially for developing economies. It is critical for vigorous sustained growth. As an economy grows and matures, its financial sector must grow with it. It must be able to fit with the increasingly sophisticated demands that are placed on it. To help in the process of development and changes in the structural underpinning of the economy, financial institutions must adapt as economies mature. However, as economies grow and become more digitized, their agricultural and manufacturing sectors expand, and their service sectors develop and grow, their banking sectors need to keep up. Decisions as to which activities to finance are crucial for rapid growth. Growing economic complexity is, of course, an inevitable consequence of growth. It means that the benefits of efficient credit allocation rise; that efficient credit allocation is financing investments where the payoff is highest. But it also means that the challenges for those assessing alternative loan applicants mount. They must develop means of allocating credit among competing needs. They must learn to assess business plans and identify and manage risk.

For our purpose, we will use the following two variables to assess the financial strength of an economy: (1) access to sound money, as related to monetary policy; and (2) banking and finance as they relate to credit market regulations. The ranking of the countries based on these four components is taken from the 2005 Heritage Foundation Index of Economic Freedom.

A country's monetary policy affects the stability of its financial base. With a stable monetary policy, people can rely on market prices for the foreseeable future. Hence, investments, savings, and other longer-term plans are easier to make, and individuals enjoy greater economic freedom. Inflation not only confiscates wealth, but also distorts pricing, misallocates resources, raises the cost of doing business, and undermines the movement of capital and investment into the society.

In the majority of countries, banks provide the essential financial services that facilitate economic growth; they lend money to start businesses, purchase homes, and secure credit that is used to buy durable consumer goods, in addition to furnishing a safe place in which individuals can store their earnings. The more banks are controlled by the government, the less free they are to engage in these activities. Hence, heavy bank regulation reduces opportunities and restricts economic growth and, therefore, the more a government restricts its banking sector, the lower its level of economic growth and the higher its score.

Table 5.9 shows the sample countries rated on the three components measuring the financial strengths of the economies. The two variables used to measure the soundness of the financial base in a country are (1) access to sound money (*ACSMNY*) and (2) credit market regulations (*CRDREG*).

Rule of Law

A major concern for scholars of development and growth is the 'rule of law' and related concepts from other legal systems. The rule of law is a concept that encompasses a number of consequences flowing from the law being the supreme ruler of a society. There are at least three distinct but connected elements:

1. All citizens are equal before the law.
2. The courts, not the state, should interpret and apply the law without fear or favor.
3. Citizens should have absolute respect for and faith in the law.

Economic growth, political adjustment, the protection of human rights, and other admirable objectives are all thought to revolve around the rule of law. Policy makers in developing and emerging economies are thus seeking ways to establish or strengthen the rule of law in their countries. Despite the assortment of definitions of the term rule of law, most can be classified according to whether they emphasize formal characteristics, substantive outcomes, or functional considerations. The differences between these three conceptions and the implications of each for efforts to establish, measure, or foster the rule of law can be found in Stephenson (2001).

Levy and Spiller (1996) have developed a framework to analyse the interaction of the institutional endowment of a country, the nature of its regulatory institutions, and the performance of the various sectors. They emphasize that the integrity and value of a regulatory framework differ with a country's political and social institutions. They also observe that performance can be adequate with a wide range of regulatory measures as soon

Table 5.9 Financial strengths of countries in the sample

Country	Size of government expenditures, taxes, and enterprises	Access to sound money	Credit market regulations
Algeria	4.93	6.33	5.86
Argentina	7.48	6.17	6.70
Bolivia	6.20	8.66	8.08
Brazil	6.65	7.77	5.74
Bulgaria	4.95	8.76	9.22
Chile	7.50	9.14	9.23
China	5.00	8.22	7.30
Colombia	4.44	7.85	8.54
Czech Republic	4.49	9.30	8.86
Ecuador	8.03	5.06	7.90
Egypt	7.29	8.74	6.10
Hong Kong	9.30	9.36	9.22
Hungary	5.70	9.48	9.01
India	7.14	6.70	6.29
Indonesia	6.36	7.18	7.52
Iran	6.79	8.24	6.52
Israel	3.83	9.14	7.50
Jordan	5.53	8.94	9.03
Kazakhstan	7.77	8.21	9.42
Korea	6.62	9.34	9.08
Lebanon[a]	–	–	–
Malaysia	5.50	6.02	9.36
Mexico	7.33	8.24	9.13
Nigeria	3.97	7.38	8.57
Oman	5.51	9.33	8.78
Pakistan	7.01	6.45	8.61
Peru	8.27	8.76	7.29
Philippines	7.12	8.13	8.12
Poland	5.34	9.54	8.35
Qatar[a]	–	–	–
Romania	5.54	8.69	7.34
Russia	5.64	7.46	7.99
Saudi Arabia[a]	–	–	–
Singapore	7.86	8.99	9.24
Slovakia	6.44	9.40	9.29
South Africa	6.97	7.76	9.32
Sri Lanka	7.03	6.10	7.42
Taiwan	7.44	9.71	7.85
Thailand	7.33	6.61	8.72
Turkey	7.82	5.42	6.64

Table 5.9 (*continued*)

Country	Size of government expenditures, taxes, and enterprises	Access to sound money	Credit market regulations
UAE	6.21	8.32	7.79
Ukraine	4.06	6.60	8.87
Uruguay	7.52	7.98	6.96
Vietnam	4.58	6.37	9.47

Note: [a] Not included in study.

Source: Heritage Foundation and *Wall Street Journal* (2006).

as three complementary means limiting arbitrary administrative action are all in place: (1) substantive restraints on the discretion of the regulator, (2) formal or informal constraints on changing the regulatory structure, and (3) institutions that implement and enforce the above formal constraints.

The basic political institutions of a country refer to the nature of its judiciary and its legislative and executive institutions. Specifically, a self-governing and professional judiciary is a natural candidate for fulfilling the condition of enforcing formal constraints. A dishonest, politically motivated judiciary will be unlikely to side against the government on sensitive matters. Thus, judicial independence and professionalism imply a more confident framework for enforcing contracts, hence increasing the confidence of customers in the economy. Levy and Spiller further emphasize the role of the contending social interests within a society and the balance between them. In actuality, the more controversial these social interests are, the higher the potential for a reversal of government policies. The higher the political instability of a country, the higher the potential for opportunistic behavior by governments, and hence the more inefficient will be the performance of the sector. Finally, Levy and Spiller stress the importance of administrative capabilities. Practically, the higher the administrative potential of the country, the higher the potential superiority of the regulatory system and, hence, the higher the performance of the sector.

For the sake of our study, we employ the most widely accepted measure of the rule of law, which was developed by the PRS Group, a country risk-rating agency, in its *International Country Risk Guide* (ICRG) (PRS Group, 2008a). This measure (LAW) takes on a value between one and ten; higher values indicate a stronger rule of law in a country.

The ICRG Risk Rating System assigns a numerical value (risk points) to a predetermined range of risk components, according to a predefined

scale, for each country covered in the analysis. Each scale is designed to award the highest value to the lowest risk and the lowest value to the highest risk. To allow for comparability, all countries are assessed on the same base scale. The risk components are grouped into three risk categories: economic, financial, and political. Each risk category is made up of a number of risk components. The sum of the risk points assigned to each risk component within each risk category determines the overall risk rating for that risk category. The objective of the political risk rating is to provide a means of assessing the political stability of the countries covered on a comparable basis. To produce the political risk ratings, the following risk components are used: government stability, socioeconomic conditions, investment profile, internal conflict, external conflict, corruption, the military in politics, and religion in politics. Each of these components is assessed, evaluated, and weighted and then they are all combined to produce the political risk factor.

The prime objective of the economic risk rating is to present a way of measuring a country's economic strengths and weaknesses. In general, if a country's strengths outweigh its weaknesses it will be classified as a low economic risk and if its weaknesses outweigh its strengths it will be classified as a high economic risk. Countries' strengths and weaknesses are evaluated and measured by assigning risk points to a number of economic risk components. The minimum number of points that can be assigned to any component is zero and the maximum number is assessed based on the weight that component is given in the overall economic risk assessment (PRS Group, 2008b). In all cases, the lower the number of points, the higher the risk. In addition, and to ensure comparability between countries, the components are based on accepted ratios between measured data within the financial and economic structures of the country. To produce the economic risk ratings, the following risk components are used: GDP per head, real GDP growth, annual inflation rate, budget balance as a percentage of GDP, and current account as a percentage of GDP.[1]

The financial risk rating provides a means of evaluating a country's ability to pay its way. Consequently, this entails a system of measuring a country's ability to finance its official, commercial, and trade debt obligations. The financial risk components identified and weighted by the ICRG are: foreign debt as a percentage of GDP; foreign debt service as a percentage of exports of goods and services; current account as a percentage of exports of goods and services; net international liquidity as months of import cover, and exchange rate stability. The method of calculating the composite index is based on a formula that assigns 50 percent to political risk and 25 percent each to financial and economic ratings. Table 5.10 represents the country risk ranked by composite risk rating for 2005.

Table 5.10 Country risk and ranking for our sample

Country	Composite risk	Rank in 2005	Category
Singapore	88.3	6	Very low risk
Kuwait	85.0	12	Very low risk
UAE	84.3	15	Very low risk
Taiwan	83.8	17	Very low risk
Hong Kong	83.0	19	Very low risk
Korea	82.0	23	Very low risk
Oman	82.0	23	Very low risk
Saudi Arabia	81.0	27	Very low risk
Chile	80.5	29	Very low risk
Bahrain	80.3	30	Very low risk
Malaysia	79.8	32	Low risk
Qatar	79.5	34	Low risk
Russia	77.0	41	Low risk
Czech Republic	76.5	46	Low risk
Slovakia	76.5	46	Low risk
Algeria	76.0	49	Low risk
China	75.5	51	Low risk
Mexico	75.5	51	Low risk
Hungary	75.3	54	Low risk
Jordan	75.0	56	Low risk
Poland	74.3	57	Low risk
Kazakhstan	73.5	60	Low risk
South Africa	73.3	61	Low risk
Thailand	73.0	62	Low risk
India	71.8	65	Low risk
Bulgaria	71.5	66	Low risk
Romania	71.5	66	Low risk
Uruguay	70.8	70	Low risk
Israel	70.5	71	Low risk
Brazil	70.0	73	Low risk
Egypt	70.0	73	Low risk
Iran	70.0	73	Low risk
Ukraine	69.8	76	Moderate risk
Vietnam	69.8	76	Moderate risk
Peru	69.3	80	Moderate risk
Philippines	69.0	81	Moderate risk
Argentina	67.5	86	Moderate risk
Turkey	67.3	88	Moderate risk
Ecuador	67.0	90	Moderate risk
Bolivia	66.8	91	Moderate risk
Columbia	64.0	103	Moderate risk
Indonesia	63.3	107	Moderate risk

Table 5.10 (*continued*)

Country	Composite Risk	Rank in 2005	Category
Pakistan	60.0	116	Moderate risk
Lebanon	59.3	120	High risk
Nigeria	58.0	125	High risk

Source: The PRS Group, *International Country Risk Guide*.

Our sample contains ten countries in the very low risk category, or 22.7 percent. The bulk of our countries, or 22 countries, in the sample fall in the low risk category; this constitutes 50 percent of the countries in the sample. The moderate risk category contains 11 countries or 25 percent of our sample. Only two countries, or 0.05 percent, fall in the high risk category, and these are Nigeria and Lebanon. We use the composite risk factor as defined by the ICRG to assess the rule of law in a given country. In our sample, this measure (LAW) takes on a value between 88.3 and 58.0; higher values indicate a stronger rule of law in a country.

Maturity of E-government

Countries vary enormously in their e-government diffusion; variations are the result of a number of factors, both tangible and intangible. West (2008) reports that the most highly ranked e-governments, in order, are South Korea, Taiwan, the United States, Singapore, Canada, Australia, Germany, Ireland, Dominica, Brazil, and Malaysia; on the other side of the spectrum, countries such as Tuvalu, Mauritania, Guinea, Congo, Comoros, Macedonia, Kiribati, Samoa, and Tanzania hardly have a presence online.

Among the countries in our sample, many governmental departments have welcomed the digital revolution and are incorporating a wide range of information and services online for their citizens. Websites as one-stop-shops are being set up to smooth the progress of tourism, citizen complaints, and improve business investment. Some of these have been very successful; Bulgaria and the Czech Republic, for instance, are attracting foreign direct investments through their websites.

In this study, we will use West's (2008) e-government maturity measures; this is deemed the most thorough quantitative indicator. To develop this index, West and his associates evaluated different features of the 1,782 government websites for the 198 countries under examination. Based on a thorough assessment of the attributes of these websites, West and his

colleagues at Brown University scored countries to a maximum of 100. Each of the following attributes was given four points: publications, databases, audio clips, video clips, foreign language access, not having ads, not having premium fees, not having user fees, disability access, having privacy policies, having security policies, allowing digital signatures on transactions, an option to pay via credit card, e-mail contact information, areas to post comments, option for e-mail updates, option for website personalization, and personal digital assistant (PDA) accessibility. These features provide a maximum of 72 points for particular websites. Each site was then eligible for up to 28 points based on the number of online services offered on that site (one point for one service, two points for two services, three points for three services, and on up to 28 points for 28 or more services). The overall e-government index runs along a scale from zero (having none of these features and no online services) to 100 (having all features plus at least 28 online services). Totals for each website within a country were averaged across all of that country's websites to produce a zero to 100 overall rating for that country. The 2008 ranking put South Korea at the top with 64.7 percent. Table 5.11 lists the countries in our sample along with their e-government index.[2]

Economic Development

Since several of our explanatory variables (e.g. rule of law, infrastructure measures) are likely to correlate significantly with the level of economic development in a country, it is important that we control for this aspect of country difference. We therefore include in our empirical model a control variable, the natural log of per capita in each country, *LPCI*. These data are for 2005 (the latest available) and are drawn from the 2007 *World Development Report* (World Bank, 2007).

CHOICE OF STATISTICAL METHODS

Multiple regression is used to account for (predict) the variance in an interval dependent, based on linear combinations of interval, dichotomous, or dummy independent variables.

The multiple regression equation takes the form:

$$y = \text{blxl} + \text{b2x2} + \ldots + \text{bnxn} + \text{c}$$

The b's are the regression coefficients, representing the amount that the dependent variable y changes when the independent changes one unit. The

Table 5.11 2008 e-government ranking

Rank	Country	Index
1	South Korea	64.7
2	Taiwan	58.7
4	Singapore	53.1
10	Brazil	43.6
11	Malaysia	42.8
20	Mexico	39.5
23	Columbia	38.4
24	Hong Kong	38.2
27	Chile	37.7
36	India	36.6
39	Qatar	36.1
40	UAE	36.1
53	Saudi Arabia	35.1
54	Kazakhstan	31.0
55	Czech Republic	34.8
58	Peru	34.7
61	Turkey	34.2
64	Nigeria	33.9
66	Israel	33.3
67	China	33.2
73	Egypt	32.6
86	Uruguay	31.8
88	Jordan	31.6
89	Philippines	31.3
90	Ukraine	31.2
94	Bulgaria	31.0
95	Russia	30.9
97	Ecuador	30.5
101	Lebanon	30.4
107	Pakistan	29.8
108	Vietnam	29.8
109	Iran	29.7
110	Poland	29.7
113	Argentina	29.4
114	Bolivia	28.7
116	Hungary	28.5
119	Oman	28.4
123	Algeria	28.3
138	Thailand	27.9
147	Romania	26.0
149	South Africa	25.9
153	Slovakia	25.7

Table 5.11 (*continued*)

Rank	Country	Index
169	Sri Lanka	24.0
175	Indonesia	24.0

Source: West (2008).

c is the constant, where the regression line intercepts the y-axis, representing the amount that the dependent *y* will be when all the independent variables are 0. The standardized versions of the b coefficients are the beta weights, and the ratio of the beta coefficients is the ratio of the relative predictive power of the independent variables. Associated with multiple regression is r^2, multiple correlation, which is the percentage of variance in the dependent variable explained collectively by all of the independent variables.

Multiple regression has a number of assumptions, including linearity of relationships, the same level of relationship throughout the range of the independent variable ('homoskedasticity'), interval or near-interval data, and data whose range is not truncated. In addition, it is important that the model being tested be correctly specified. The exclusion of important causal variables or the inclusion of extraneous variables can change markedly the beta weights and hence the interpretation of the importance of the independent variables.

The regression coefficient, b, is the average amount that the dependent increases when the independent increases one unit and other independents are held constant. Put another way, the b coefficient is the slope of the regression line; the larger the b, the steeper the slope, and the more that the dependent changes for each unit change in the independent. The b coefficient is the unstandardized simple regression coefficient for the case of one independent. When there are two or more independents, the b coefficient is a partial regression coefficient, though it is common simply to call it a 'regression coefficient' also.

Correlation is a bivariate measure of association (strength) of the relationship between two variables. It varies from 0 (random relationship) to 1 (perfect linear relationship) or −1 (perfect negative linear relationship). It is usually reported in terms of its square (r^2), interpreted as percentage of variance explained. For instance, if r^2 is 0.25, then the independent variable is said to explain 25 percent of the variance in the dependent variable.

There are several common pitfalls in using correlation. Correlation is symmetrical, not providing evidence of which way causation flows. If other variables also cause the dependent variable, then any covariance

that they share with the given independent variable in a correlation will be falsely attributed to that independent. Also, to the extent that there is a non-linear relationship between the two variables being correlated, correlation will understate the relationship. Correlation will also be attenuated to the extent that there is measurement error, including use of subinterval data or artificial truncation of the range of the data. Correlation can also be a misleading average if the relationship varies depending on the value of the independent variable ('lack of homoskedasticity').

Beside Pearsonian correlation (*r*), the most common type, there are other special types of correlation to handle the special characteristics of such types of variables as dichotomies, and there are other measures of association for nominal and ordinal variables. There is also 'multiple correlation', which is the correlation of multiple independent variables with a single dependent. Also, there is 'partial correlation', which is the correlation of one variable with another, controlling for a third or additional variables. The statistical method that will be used to estimate the model is ordinary least squares (OLS) multiple regression. Consider the general linear model

$$Y = XB + u$$

where y is a (n × 1) vector of observations on the dependent variable, X is a (n × p) matrix of observations on the p explanatory variables, B is a (p × 1) unknown fixed coefficient vector, and u is the (n × 1) vector of unknown random disturbances. OLS results in an estimate of the coefficient vector B that is unbiased and has minimal variance when the following standard assumptions hold:

$$E(u) = 0 \; E(ut \; us) = 0$$

ut is independent of all explanatory variables and normally distributed. Then, by the Gauss–Markoff theorem, OLS estimators are best linear unbiased estimates.

Interpretation of multiple regression results depends implicitly on the assumption that the explanatory variables are not strongly correlated. If there are no linear relationships among regressors, they are said to be orthogonal. Under such circumstances, it is usual to interpret a regression coefficient as measuring the change in the response variable when the corresponding explanatory variable is increased by one unit and all other explanatory variables are held constant. This interpretation may not be valid if there are strong relationships among the explanatory variables. When this ideal assumption of independent explanatory variables is

violated, the variables are said to be collinear, and the data are said to be multicollinear.

The problem of multicollinearity is often cited as a serious problem in many econometric studies and is highly pronounced in the time-series production function approach because of high correlations among inputs. In our case, the basic aggregates such as outputs, capital stock, and labor force exhibit relatively regular growth: capital and labor tend to move together and are both highly correlated with time, and hence with each other.

Multicollinearity is a critical statistical issue in any econometric time-series study, and it should be given special and careful attention for a variety of reasons. First, the presence of multicollinearity hinders the precise estimation of economic relationships because the impact of each independent variable on the dependent variable cannot be separated, and the regression results may be ambiguous. Secondly, when the explanatory variables are collinear, the estimated values of the coefficients will have large sampling errors that affect both inferences and forecasts that are based on the regression model. Thirdly, in the presence of multicollinearity, the estimated values of the coefficients become very sensitive to slight changes in the data and to the addition or deletion of variables in the equation.

Autocorrelation

The fundamental assumptions in linear regression are that the error terms have zero mean and constant variance, are uncorrelated, and are normally distributed. This assumption of uncorrelated or independent errors is often not appropriate for time-series data, since the errors in time-series data frequently exhibit serial correlation, that is, E(ut, us) is not zero for t different from s. Such error terms are said to be autocorrelated.

The presence of autocorrelation in the errors has several effects on the OLS regression procedure. These are summarized as:

1. The OLS estimates are still unbiased, but they are no longer minimum variance estimates. We say that these estimates are inefficient.
2. The confidence intervals and tests of hypotheses based on the t and F distributions are, strictly speaking, no longer appropriate.
3. When errors are positively autocorrelated, the residual mean square (MSE) may seriously underestimate the error variance. Consequently, the standard errors of the regression coefficients may be computed as being much smaller than their true values.

Various statistical tests can be used to detect the presence of autocorrelation. The test developed by Durbin and Watson (1971) is widely used.

This test is based on the assumption that the errors in the regression model are generated by a first-order autoregressive process at equally spaced time periods. Because most regression problems involving time-series data exhibit positive autocorrelation, the hypotheses usually considered by the Durbin–Watson test are:

$$\text{H0: rho} = 0 \quad \text{H1: rho} > 0$$

where rho is the autocorrelation parameter. A significant value of the Durbin–Watson statistic indicates a model specification error.

In this study the Durbin–Watson statistic is used to check for autocorrelation. In the case of the presence of autocorrelation, the problem would have been eliminated by using the method of Cochrane and Orcutt (1949) to estimate the parameters of the model, including rho.

Stability of the Estimates

Besides multicollinearity and autocorrelation, there is the issue of structural stability of estimated relations in a multiple regression analysis. When a linear regression is used to represent an economic relationship, the question often arises as to whether the relationship remains stable in two periods of time or whether the same relationship holds for two different groups of economic units.

The Chow (1960) test will be used to examine possible structural instability and parameter sensitivity. The Chow test results in conclusive evidence against instability and is based on the analysis of covariance. The method involved can be described very simply in the following way. Suppose that n observations are used to estimate a regression with p parameters. Suppose also that there are m additional observations, and one is interested in deciding whether they are generated by the same regression model as the first n observations. To perform the analysis of variance, we need the following sums of squares:

- A = sum of squares of $(n + m)$ deviations of the dependent variable from the regression estimated by the $(n + m)$ observations, with $(n + m - p)$ degrees of freedom.
- B = sum of squares of n deviations of the dependent variable from the regression estimates by the first n observations, with $(n - p)$ degrees of freedom.
- C = sum of squares of m deviations of the dependent variable from the regression estimated by the second m observations, with $(m - p)$ degrees of freedom.

Then the ratio $(A - B - C)/p$ to $(B + C)/(n + m - 2p)$ will be distributed as $F(p, n + m - 2p)$ under the null hypothesis that both groups of observations are generated by the same regression model.

Data Analysis

The initial analysis was conducted by calculating descriptive statistics including frequencies, mean scores, and standard deviations. Pearson's Production Moment Correlation analysis was used to determine the correlation of each of the independent variables with the Cyber Law Index at the 0.05 level of significance. After this, multiple regression analysis was performed to determine the weight of each variable in the prediction of developing a cyber law in a specific country.

EMPIRICAL RESULTS

Table 5.12 presents the definitions of the operational variables used in the regression analysis.

Table 5.13 presents the descriptive statistics of operational variables used in the statistical analysis.

The empirical results of the regression analysis are presented in Table 5.14. These OLS estimations were conducted to explore the relationships among the different variables defined in Table 5.14 and to test the five hypotheses formulated in Chapter 4. The main objective of our analysis is to identify those resources contributing to the success of electronic commerce initiatives in lesser developed and emerging economies. As stated in Chapter 4, the authors hypothesized that in addition to physical infrastructure resources, the success of electronic commerce initiatives depends on the existence of soft resources such as a well-established rule of law, cyber law, and credible payment systems. The results presented in

Table 5.12 Definition of all operational variables

TECHMAT:	Technical maturity of a country
LAW:	Rule of Law Index
CLI:	Cyber Law Index developed by the authors
PCINCOME:	Log per capita income
ACSMNY:	Country rating of access to sound money
CRDREG:	Country rating of credit market regulations
HDI:	Country rating on the Human Development Index
EGOVMAT:	E-government Maturity Index

Table 5.13 Descriptive statistics

Variable	*N*	Mean	Std Dev	Minimum	Maximum
EGOVMAT	44	33.92727	1.24202	24.0	64.7
LAW	44	6.15750	0.02324	3.794416	9.46323
CLI	44	0.620455	0.034344	0.1	0.9
PCINCOME	44	3.46893	0.07511	2.600967	4.43685
ACSMNY	44	7.7	0.25518	3.8	9.9
CRDREG	44	6.904545	0.17683	4.5	9.6
HDI	44	0.758	0.01386	0.463	0.905
TECHMAT	44	0.189941	0.013354	0.39091	0.03959

Table 5.14 are quite supportive of the authors' argument. The results of the regression analysis are presented below.

Given the nature of the variables, it is expected that they will be highly correlated. Another problem that presents itself in this case is the size of the sample. Results from multivariate statistical analysis based on a small sample may be questionable. However, it is well known that parameter estimates remain unbiased and consistent in ordinary least squares regression despite the presence of multicollinearity. In addition, as can be seen from Table 5.14 the F-statistics for the regression analysis (presented later) are found to be highly significant.

As can be seen from the results above, there are three variables significant at above the 90 percent confidence level; these are the per capita income of a country (*PCINCOME*); and the technical maturity of the country (*TECHMAT*) as represented by the computer, telephone, Internet, and broadband penetration rates. This variable was derived according to equation (5.1) above. The third significant variable is the rule of law in a country (*LAW*). The coefficient of determination for this model (R^2) is 71.20 percent, and the value of the F-statistic for the entire model is 13.36 with 3 degrees of freedom. On the whole, the model is significant at the 99 percent level.

Based on the results in Table 5.14, all variables are consistently signed; that is, as hypothesized, the model shows a positive relationship between the level of maturity of cyber law in an economy and the per capita income of a country. The results also support the hypothesis stating the positive relationship between a country's rule of law and the maturity of cyber law in a country. From Table 5.14, the Cyber Law Index (*CLI*) is positively related to the level of maturity of the rule of law. Also, as expected, the maturity of the cyber law is positively related to the level of technical maturity of the hard infrastructure in a country (*TECHMAT*).

Together these results provide support for our main argument that, in

Table 5.14 Results of regression analysis – model summary

Regression statistics	
Multiple *R*	0.711963518
R square	0.506892051
Adjusted *R* square	0.46896067
Standard error	0.161023595
Observations	43

ANOVA

	df	SS	MS	F	Significance F
Regression	3	1.03948235	0.34649412	13.36339573	3.8061E-06
Residual	39	1.011215325	0.0259286		
Total	42	2.050697674			

	Coefficients	Standard error	t-statistic	P-value	Lower 95%	Upper 95%
Intercept	0.022580605	0.121119413	0.1864326	0.853071942	0.267567739	0.22241
PCINCOME	0.152037457	0.034605058	4.39350394	8.30095E-05	0.082042122	0.22203
TECHMAT	0.034740785	0.019736005	1.76027444	0.086202635	0.005179053	0.07466
LAW	0.108340538	0.055805176	1.94140662	0.059459189	0.004536084	0.22122

Dependent Variable: Cyber Law Index (CLI).

general, the development and comprehensiveness of cyber laws in emerging or developing economies are dependent on the resources available in a particular economy. In particular, that physical resources in terms of telecommunications infrastructure are not the sufficient conditions to the development and success of cyber activities in an economy; they might be necessary but not sufficient conditions. As demonstrated in our analysis above, the strength of some institutional components such as the rule of law is an additional factor in the development of laws to govern cyber space.

The results of the stepwise regression analysis do not necessarily indicate that the other variables that were excluded from the model do not have an impact on the maturity of cyber law in developing and emerging economies. As explained earlier, the problem of multicollinearity among the independent variables may be a main reason why some of the variables were shown to be statistically insignificant from the multivariate analysis. Another problem that presents itself in this case is the size of the sample; results from multivariate statistical analysis based on a small sample may be questionable.

One expects to have a positive relationship between the level of e-government maturity and the maturity of cyber law as per the hypothesis formulated in Chapter 4 of this book. Our analysis, however, failed to support this hypothesis. One reasonable explanation is that countries with a high level of cyber crime, such as Pakistan, the Philippines, and some Eastern European and Latin American countries, have developed these laws as a reaction to the high level of cyber criminal activities; that is, in order to deter cyber criminals, and not as a proactive mechanism aimed at encouraging the diffusion of electronic commerce and electronic government activities.

Many developing and emerging economies have crafted cyber laws which are seen as the primary and leading statute for the development of their information/knowledge-based societies. No doubt, the cyber law in many of these countries has provided a new thrust and a base to the information society. The law will help materialize the concept of e-society in many of these countries; but much needs to be done if these countries are to become e-players in this global world. In many of these countries, the law has covered e-documentation and provisions for cyber crime; some Internet laws and policies covering aspects of IPRs are still needed.

CONCLUSION

The literature on cyber space use and adoption in developing countries is extremely limited, although some evidence exists describing the

impediments, which include limited Internet accessibility, a lack of competition in international telephone traffic that makes access to the international network expensive, a lack of intra-regional infrastructure, and a disproportionate penetration of the telephone in the urban as opposed to rural, more populated areas. To facilitate the introduction of the Internet and eventually the efficient use of cyber space, the necessary condition is the creation of a communication infrastructure, or what we refer to as a mature technical base. For developing countries, the financial resources needed to invest in communication infrastructure are one of the major barriers since most countries rely on foreign aid. As has been demonstrated in this chapter, physical infrastructural resources might be necessary for the creation of cyber laws in developing and emerging economies, but they are not sufficient. Our statistical analysis shows that institutional environment is as important as physical infrastructure as a driver for the development and implementation of cyber laws. These institutional environments, it is argued, facilitate the building of transactional integrity in online transactions.

The chapter dealt with data collection on the various variables identified in the previous chapter, discussed the proposed operational measurements of the independent variables and the dependent variables, laid out the methodology for the analysis, and presented and discussed the empirical results. Our analysis supported the main argument that the maturity of cyber law in developing and emerging economies depends not only on physical resources but on an important institutional mechanism, which we refer to as soft resources; that is, the maturity level of the rule of law in the economy. This is of central concern to researchers of New Institutional Economics.

NOTES

1. For a definition of these variables and their measurement proxies, please refer to the International Country Risk Guide (2003).
2. http://www.brookings.edu/~/media/Files/rc/reports/2008/0817_egovernment_west/0817_egovernment_west.pdf.

REFERENCES

Barclay, B. and N. Domeisen (2001), 'Trade opportunities: are developing countries ready?', *International Trade*, **2**(Forum)(1): 16–19.
Barro, R.J. and X. Sala-I-Martin (1995), *The Diffusion of Technology*, New York: McGraw Hill.

Chow, G. (1960), 'Tests of equality between sets of coefficients in two linear regressions', *Econometrica*, **28**(3): 591–605.
Clark, T. (1999), 'Electronic commerce in China', in F. Sudweeks and C.T. Rom (eds), *Doing Business on the Internet: Opportunities on the Internet*, London: Springer.
Cochrane, D. and G.H. Orcutt (1949), 'Application of least squares regressions to relationships containing auto correlated error terms', *Journal of the American Statistical Association*, **44**: 32–61.
Crafts, Nicholas (1999), 'Economic growth in the twentieth century', *Oxford Review of Economic Policy*, **15**(4): 18–36.
Dasgupta, Partha and Martin Weale (1992), 'On measuring the quality of life', *World Development*, **20**(1): 119–31.
Davis, C.H. (1999), 'The rapid emergence of electronic commerce in a developing region: the case of Spanish-speaking Latin America', *Journal of Global Information Technology Management*, **5**(1): 25–40.
Desai, Meghnad (1991), 'Human development, concepts and measurement', *European Economic Review*, **35**: 335–57.
Durbin, J. and G.S. Watson (1971), 'Testing for serial correlation in least squares regression III', *Biometrika*, **58**: 1–19.
Edwards, S. (1998), 'Openness, productivity, and growth: what do we really know?', *Economic Journal*, **108**(44): 383–98.
International Telecommunication Union (ITU) (2004), *International Telecommunication Union Yearbook*, Geneva: ITU.
ITU (2007), *International Telecommunication Union Yearbook*, Geneva: ITU.
ITU (2008), *International Telecommunication Union Yearbook*, Geneva: ITU.
ITU (2009), *International Telecommunication Union Yearbook*, Geneva: ITU.
Khan, Iliyas (2008), 'Pakistan unveils cybercrime law', *BBC News*, accessed 3 December at www.news.bbc.co.uk/2/hi/south_asia/7714714.stm.
King, J.L., V. Gurbaxani, K.L. Kraemer, F.W. McFarlan, K.S. Raman and C.S. Yap (1994), 'Institutional factors in information technology innovation', *Information Systems Research*, **5**(2): 139–69.
Lee, O. (1999), 'An action research report of an e-commerce firm in South Korea', in Fay Sudweeks and Celia T. Rom (eds), *Doing Business on the Internet: Opportunities on the Internet*, London: Springer, pp. 246–58.
Levy, B. and P. Spiller (eds) (1996), *Regulations, Institutions, and Commitment*, New York, NY: Cambridge University Press.
Luchters, Guido (1996), 'Human development as statistical artifact', *World Development*, **24**(8): 1385–92.
McGillivray, M. and H. White (1993), 'Measuring development? The UNDP's human development index', *Journal of International Development*, **5**: 183–92.
Montealegre, R. (1999), 'A temporal model of institutional interventions for information technology adoption in less-developed countries', *Journal of Management Information Systems*, **16**(1): 207–32.
Peha, J.M. (1999), 'Lessons from Haiti's Internet development', *Communications of the ACM*, **42**(6): 67–72.
Petrazzini, B. and M. Kibati (1999), 'The Internet in developing countries', *Communications of the ACM*, **42**(6): 31–6.
PRS Group (2008a), The 2008 International Country Risk Guide, accessed at www.prsgroup.com/ICRG.aspx.
PRS Group (2008b), 'International Country Risk Guide', accessed at www.prsgroup.com/icrg_methodology.aspx.

Sachs, J. and A. Warner (1995), 'Economic reform and the process of global integration', in W. Brainard and G. Perry (eds), *Brookings Papers on Economic Activity*, **1**: 1–118.
Shrinivasan, T.N. (1994), 'Human development: a new paradigm or reinvention of the wheel?', *American Economic Review*, **84**(2):238–43.
Srikantaiah, T.K. and D. Xiaoying (1998), 'The Internet and its impact on developing countries: examples from China and India', *Asian Libraries*, **7**(9): 199–209.
Stephenson, M. (2001), 'The rule of law as a goal of development policy', accessed at www1.worldbank.org/publicsector/legal/ruleoflaw2.htm.
Streeten, Paul (1994), 'Human development: means and ends', *American Economic Review*, **84**(2): 232–7.
Travica, B. (2002), 'Diffusion of electronic commerce in developing countries: the case of Costa Rica', *Journal of Global Information Technology Management*, **5**(1): 4–24.
United Nations Economic and Social Commission for West Africa (ESCWA) (2007), *Models for Cyber Legislation in ESCWA Member Countries*, E/ESCWA/ICTD/2007/8, Beirut: ESSWA.
ESCWA (2009), *Cyber Legislation in the ESCWA Region: Security Issues*, Beirut: United Nations.
United Nations Human Development Program (UNDP) (2004), *Human Development Report: Cultural Literacy in Today's Diverse World*, New York: New York University Press.
USAID (2003), 'Leland initiative', accessed at www.usaid.gov/regions/afr/leland/project.htm.
West, D.M. (2008), 'Improving technology utilization in electronic governments around the world', accessed 5 November at www.brookings.edu/~/media/Files/rc/reports/2008/0817_egovernment_west/0817_egovernment_west.pdf.
White, L.J. (2000), 'Reducing the barriers to international trade in accounting services: why it matters, and the road ahead', World Trade Organization working paper, accessed 11 May 2008 at www.stern.nyu.edu/eco/wkpapers/workingpapers00/00-04white.pdf.
World Bank (1997), *World Development Indicators*, Washington, DC: World Bank.
World Bank (2007), *World Development Report*, accessed 1 July, 2008 at http://econ.worldbank.org/WEBSITE/EXTERNAL/EXTDEC/EXTRESEARCH/EXTWDRS/EXTWDR2007/0_contentMDK:21055591~menuPK:1489854~pagePK:64167689~piPK:64167673~theSitePK:1489834,00.html.
World Intellectual Property Organization (2009), http://www.wipo.org.

6. Conclusion, recommendations, and future research

INTRODUCTION

In this book, we have provided a guiding framework for understanding the determinants of cyber law maturity in a number of developing and emerging economies from a resource-based theory perspective. The work performed here and the conclusions reached are unique in nature and have several characteristics, none of which has received attention in the legal, information technology (IT), or economics literature. The analysis of cyber law contents and guidelines in a cross-section of developing and emerging countries conducted in this study proved that not only physical infrastructure measures are important in explaining variations in cyber space activities and Internet use, but also intangible institutional measures are critical to the success of a country in utilizing cyber space. The book examined the degree of dependence of cyber law maturity on the strengths of a number of institutional, knowledge base, and physical resources. The adaptation of the Internet for commerce has widely stretched its reach globally, making access available to previously restricted markets. Specifically, developing and emerging countries' access to the Internet has been a source of economic value-added. The resulting shift to affordable networked computers and devices has made the Internet available to the masses. Given the growth of cyber activities, the absence of a coordinated, comprehensive control framework has added to the spread of cyber crime in all shapes and forms.

Information is being changed into a digital format at an exponential rate; an estimated 61 billion gigabytes of digital information was created in 2006 alone; this is equivalent to 3 million times the information in all books ever written (Gantz et al., 2007). This information is being shared and distributed around the world through the use of high-speed Internet technology. The volume of digitized information is expected to increase six-fold by 2010.

Given the economic value of the digital information and the ease of distribution via the Internet, as well as the lack of security of this medium, that has been a high level of cyber crime in recent years. Cyber crime is a

major challenge not only for developing and emerging countries but for developed ones as well; a congressional report released in 2007 states that the Unites States is suffering from a high rate of cyber crime and is paying enormous costs in terms of risk (Goodman and Lin, 2007). The report goes further to indicate that 'Cyber space in general, and the Internet in particular, are notoriously vulnerable to a frightening and expanding range of accidents and attacks by a spectrum of hackers, criminals, terrorists, and state actors (Goodman and Lin, 2007, p. 11)'. The high rate of cyber crime is an indication of lack of security, leading to an increased level of victimization.

Cyber space is a very complex environment and its security is not simply a technological question, but one with social and cultural dimensions that involve a number of actors: governments, law makers, the private sector, and citizens. Having said that, it is important to note here that little is known about the holistic picture of cyber security, and since the Internet is not localized to a geographic area, territorial cyber space cannot be easily enforced.

Information and communication systems are exemplified by increasing digital content, widespread mobility, and a superior capacity to transform and move data from one place to another. Advances in technology including increased bandwidth and affordability have led to more use of cyber space, which, consequently has increased the possibility of users to cause damage, either intentionally or unintentionally. Episodes of criminal activities in cyber space vary from well-known cyber attacks carried out on a large scale, such as the attempt to shut down the Internet in Estonia in mid-2007, to smaller, less publicized incidents including spamming, pharming, identity theft, and so on. As the magnitude and dimension of criminal activities in cyber space increase, users' trust dips, and entities and countries, especially those on the growth portion of the development curve, will be confronted with growing challenges, as their balance sheets and economies are negatively impacted.

One of the key success factors for cyber security is the development of a consistent cyber culture, with recognized rules of behavior that users adhere to readily. However, such a cyber culture has to be encouraged and cultivated, especially in emerging and developing countries. Practical guidelines in this area are United Nations Resolution 57/239 on the *Creation of a Global Culture of Cybersecurity* (United Nations 2008) and the OECD's *Guidelines for the Security of Information Systems and Networks* (OECD, 2008).

It is the role of the legislative power of states to create legal regimes governing their jurisdictions and for their governments to sign up to international regulatory regimes and ensure security in cyber space. Cyber

security needs the development of a cyber culture reflecting the new reality of cyber space. It is also dependent on standards of appropriate behavior and the means and tools to punish cyber criminals and bring them to justice. The need to deter cyber crime and take legal actions against criminals is global, even for those developing and emerging countries with low Internet diffusion.

Currently, there is only limited authority to impose laws on the borderless environment of the Internet, so improving security is only possible through collective action, and through capacity and awareness building from both the national and international perspectives.

This concluding chapter outlines the flow of research that was undertaken during the study that formed the basis for this book. The purpose of the chapter is, first, to review and restate the research objectives of the study; secondly, to discuss briefly the methods employed in the research; and, thirdly, to summarize the empirical findings and sum up the answers to the research questions outlined in the first chapter. This is to be followed by the major conclusions and implications drawn from the analysis. Finally, a number of recommendations are set forth along with suggestions for future research.

The Internet has led to the revamping of many business processes. Global networking has introduced new methods, generated new channels, and increased the scope and depth of business opportunities. In cyber space the speed of worldwide transactions has improved, leading to disintermediation in some of the business processes, and amplified the competition. Presently, e-commerce accounts for a small percentage of the entire business to business (B2B) and business to customer (B2C) retail markets, worldwide. The two economies that currently have the substantial majority of the present B2B and B2C transactions are the European Union and the United States. Each introduction of new technology generally brings with it new legal questions that have to be tackled by decision makers and governments. However, cyber technology has been developing so speedily that the laws and regulations cannot keep up with these technological advances. Regulating the Internet is thorny because the application of existing law to cyber space is not always possible because of the borderless nature of cyber space. Further, 'commercial codes, criminal codes, court-related rules, and other laws can make the difference' (Jones and Pedigo, 2001). To help developing and emerging countries solve critical economic problems and provide new services by the means of collecting data, turning data into information, and turning information into knowledge quickly enough to reflect its value as a service, governments are investing more and more in electronic commerce technology, but lagging on the legal front. To increase consumers' trust

in cyber space and increase the use of cyber activities, it is essential that countries develop law to tackle problems, challenges, issues, and crimes related to the use of cyber space. This is now a more pressing issue given the fact that cyber criminals are no longer game-minded hackers operating individually but are now structured in profitable conglomerates with considerable technological and financial resources (ITU, 2008). These criminals are progressively developing new software to attack systems and networks.

Although the role and success of cyber space are viewed and perceived differently by different scholars, the fact that it constitutes an integral component of global business is no longer disputable. Practically, many countries have adopted various approaches to and business models around cyber activities. Many of these models are based on using cyber space and cyber activities strategically, creating competitive opportunities, increasing the use of technology more effectively, and enhancing a more enduring connection between information technology investments and strategic goals. Many governments have accepted the notion that electronic commerce can play (and in fact is playing) a strategic role by creating competitive advantage rather than simply displacing cost. The adoption and diffusion of e-commerce have taken place with varying degrees of success among countries, depending on their level of economic development, which has led to what we call the digital divide. Similarly, the maturity of cyber laws in the various countries, especially the differential between developed and developing economies, has led to what we call the cyber legal divide.

The digital divide characterized by highly unequal access and use of information and communication technologies (ICTs), exhibits itself at the international, regional, and national levels and therefore needs to be addressed by national policy makers at the highest governmental levels, as well as the international community. The adoption of ICT by the public and the private sectors requires an environment encouraging open competition, trust and security, and interoperability and standardization, and the availability of the financial resources needed for the development of ICT. This requires the implementation of sustainable measures to improve access to the Internet and telecommunications and increase IT literacy at large, as well as development of local Internet content.

The asymmetrical diffusion of technology and the disparity in access to technologies in developing and emerging economies are apparent in different ways with considerable consequences for social, economic, and political maturity. These end results are mirrored in the reality that anxiety over the digital divide now concentrates on what is referred to as 'digital exclusion'. 'Digital exclusion' broadens the idea of digital divides based on

connectivity and access to highlight ideas of exclusion or lack of participation and representation in more advanced information and communication technologies (FreshMinds, 2008).

The positive impact and significance of technology to economic development have long been acknowledged. This is more pronounced for ICT, which cut across all economic operations and have a wide set of applications. ICT offer the potential for increased availability of information, new means of communication, reorganization of productive processes, and improved efficiency in many different economic activities.

Despite the potential benefits that can be offered by ICT, developing and emerging countries face significant obstacles to ICT connectivity and access. The underlying causes of low levels of penetration of ICT and low level of adoption and diffusion of e-commerce in these countries include: a lack of awareness of what these technologies can offer; insufficient telecommunications infrastructure and Internet connectivity; expensive ICT access; absence of adequate legal and regulatory frameworks; shortage of requisite human capacity; failure to develop local language content; and a lack of entrepreneurship and business culture open to change, transparency, and social equality.

Many of the problems are symbolized by highly disproportionate rates of e-commerce adoption and diffusion across countries. The obvious digital divide between the information/technology-rich and the information/technology-poor countries is of mounting concern. A major challenge for policy makers at the national and international levels, therefore, lies in tackling the problem of the digital divide and digital exclusion: between rich and poor countries, rural and urban areas, men and women, skilled and unskilled citizens, and large and small enterprises.

For any country, moving forward on the e-world map cannot take place without a comprehensive, well-devised strategy at the highest level of government. In developing and emerging economies, one observes a lack of such strategic orientation, in general, and e-strategic inclination, in particular. E-strategies should be better integrated into the overall policy frameworks and strategies of countries. The inflow of foreign investments and international support through development cooperation measures are equally important.

Strategies to improve access to ICT and the Internet, and consequently increase e-commerce adoption and diffusion, include opening up local telecommunications markets to promote competition and creating supportive legal and institutional environments to encourage investment in ICT. The objective should be to decrease the cost of Internet access for private sector entities and individuals. Guaranteeing the availability of a minimum supply of ICT infrastructure and electricity for remote and rural

areas should be considered an important part of those strategies in developing and emerging economies.

The enactment of cyber laws would help and complement what is referred to as Information Security Governance (ISG), both in the private and the public sectors. ISG is an indispensable building block of enterprise governance and involves the leadership, organizational structures, and processes dealing with the protection of informational assets (IT Governance Institute, 2006). In terms of strategic alignment, ISG enables firms to align security with business strategy to support organizational objectives. Firms are also likely to carry out proper measures to decrease risks and possible impacts to a manageable level and incorporate all applicable factors to make certain processes function as planned from end to end (Johnson and Hall, 2009).

In addition, to ensure the success of any initiative, human resources development should be at the center of e-strategies; this necessitates including ICT in the curricula of educational institutions, especially in public ones, and providing training in the workplace to increase IT literacy. To help accomplish some of the objectives of e-strategies, electronic government could be used as a mean, including online services offered by governments and e-business and e-payment operations undertaken through the public procurement process.

UNDERLYING THEORIES

In completing this work, the authors were guided by a number of studies from various disciplines. The IT diffusion literature helped our understanding of the technological, organizational, and institutional factors that affect the diffusion of innovations. In particular, frameworks focusing on country-level Internet diffusion are very strong in including dimensions that are especially pertinent to developing and emerging countries. These include both factors describing the organizational context and factors that specifically reflect a view of technological diffusion. Without a specific focus on institutional factors, it is insufficient for studying the diffusion of cyber activities around the world.

We were also guided by research on IT and Internet diffusion in developing and emerging economies; this line of research considers the many issues that these countries face – factors that are often taken for granted in the developed countries in which most theories of Internet and IT diffusion are set. Travica (2002) provides a good framework that captures many of these issues in dimensions that foster more detailed and focused analysis.

The main theme of this research was to take a step toward understanding the level of maturity of cyber laws, its determinants and its impact on growth and development in developing and emerging countries. In doing so, a framework that is grounded in strong economic theory was developed. The framework used fundamental concepts central to resource-based and technology diffusion literature and provided a decent understanding of cyber space adoption and diffusion processes by public and private sector entities in developing and emerging countries.

So far, little research using a resource-based view framework has examined strategy differences in the social, cultural, and political contexts of developing and emerging economies. As with most resources that create competitive advantage, resources for competitive advantage in developing and emerging countries are intangible. In developing and emerging economies, however, such advantages are difficult to institute without good relationships with national governments.

From a macroeconomic perspective, the resource-based view sees an economy as a bundle of resources and capabilities. Resources are economy-specific assets and competences controlled and used by countries to develop and implement their strategies. Resources can be either tangible (for example, financial assets, technology) or intangible (for example, managerial skills, reputation); they can be heterogeneous across economic sectors, and some resources are valuable yet rare, difficult to imitate, or non-substitutable, giving the economy some distinctive core capabilities. Resources that provide sustainable advantage tend to be causally ambiguous, socially complex, rare, and/or imperfectly imitable. Capabilities are defined to be an economy's abilities to integrate, build, and reconfigure internal and external assets and competences so that it is enabled to perform distinctive activities. The resource-based approach focuses on the characteristics of resources and the strategic factor markets from which they are obtained.

Based on the resource-based theory, economies cannot gain competitive advantage by merely owning and controlling resources. They should be able to acquire, develop, and deploy these resources in a manner that provides distinctive sources of advantage in the marketplace. The traditional conceptualization of the resource-based view has not addressed or examined the process of resource development. In addition, the traditional resource-based view is limited to relatively stable environments, which is not usually the case in developing and emerging markets.

In addition to the resource-based approach, the New Institutional Economics (NIE) theory was also used as a foundation for our work. To date New Institutional supporters seem to focus on transaction cost analysis of property rights, contracts, and organizations. The New

Institutionalism is described as an attempt to extend the range of neoclassical theory by accounting for institutional factors such as governance structures and property rights. The institutional environment is the devised set of constraints that structure political, economic, and social interactions. The philosophical foundation of NIE is classical liberalism; it is dominated currently by scholars who cling to the neoclassical core of the discipline while struggling to broaden its boundaries.

SUMMARY OF THE RESEARCH

This book proposed an empirical/theoretical framework for understanding the level and degree of cyber law maturity in a sample of developing and emerging economies. A framework that is grounded in resource-based and institutional theories was developed. Based on the framework, a set of hypotheses was developed and tested. The analysis used core constructs that appear central to resource-based, institutional economic and technology diffusion literature and provided a fine-grained understanding of cyber space adoption processes by public and private sector entities in developing and emerging countries.

Chapter 1 of this book established the context of the book. It highlighted the importance of the subject at hand and the importance of the digital economy, including the impact of digitization on economic growth and development, and the various impediments and obstacles facing developing economies in the adoption and diffusion phases of cyber activities.

Chapter 2 reviewed the literature on security and trust in cyber space, thought to be the main drivers of conducting cyber activities. The chapter covered the role that consumer trust plays in ensuring success in cyber space; consumers are unlikely to support electronic stores that fall short of creating a perception of trust. Trust can only exist if the consumer believes that the provider has both the capability and the motivation to deliver goods and services of the quality expected by the consumer, and be confident that their cyber activities are safe from hackers and cyber criminals. In this respect, cyber law fulfills two roles; on the one hand, it is perceived as a deterrent to cyber criminals in that they know if they are caught, they will be prosecuted; and on the other hand, it creates a sense of security for consumers knowing they are protected by laws governing cyber activities. The trust concept may be more difficult to establish in cyber space than in the bricks-and-mortar world. In cyber space, providers depend on an impersonal electronic storefront to act on their behalf. Additionally, the Internet lowers the resources required to enter and exit the marketplace. In many developing countries, the Internet is quickly displacing older media

such as television and newspapers as the prime source of important information for young people. It was stated that, compared with developed countries, use of cyber space in developing countries has been relatively slow due to obstacles in the online authorization of credit cards, inadequate marketing strategies, and a small online population. The lack of interest in e-commerce adoption of several consumer groups is also due to unclear price advantages and a poor supply in this shopping mode. Cyber activities in the majority of developing economies are currently afflicted by impediments such as low bandwidth, lack of independent gateways for Internet Service Providers (ISPs), an inadequate telecommunications infrastructure, low rate of PC penetration, and low tele-density, among others. However, the expected higher PC or Internet access device penetration levels, current trend of entry of private ISPs, availability of greater bandwidth, and the coming together of e-commerce infrastructure will lead to an explosive growth in the number of Internet and e-commerce users in developing countries.

Assessing the socioeconomic influences of cyber space is difficult because it requires the use of methods capable of revealing often complex and unpredictable community values. However, the growth of e-commerce and e-government has created enormous influence on services, market structure, competition, and restructuring of industry and markets. These changes are transforming all areas of society, work, business, and government. The use of ICTs for e-commerce deepens and intensifies the socioeconomic divisions among people, businesses, and nations. It is often reported that there is a complicated patchwork of varying levels of ICT access, basic ICT usage, and ICT applications among socioeconomic groups; many disparities are getting even larger. Disparities in the location and quality of Internet infrastructure, even the quality of phone lines, have created gaps in access. Gaps exist in the adoption of digital technologies among different social groups and firms; the former depending on income levels, education, and gender, and the latter, depending on industry structure, business size (large firms versus SMEs), and location. Chapter 2 also covered the threat of cyber crime in the financial industry, considered to be the prime target for cyber criminals. With respect to the state of the regulatory environment, the modus operandi for countries at this point is playing catch-up. Cyber crime law and regulation, especially when it comes to the financial/banking sector, are not moving at the same pace as the technology that has taken place within the past ten years. The chapter also covered the various types of cyber crime, especially that affecting financial institutions.

Chapter 3 covered the resource-based view literature. As an economic theory, the resource-based view focused on the impact of resources at the

micro, firm level; the authors adapted the theory to the macro level of the economy. Simply stated, the resource-based view of the firm is one of the latest strategic management concepts to be enthusiastically embraced by information technology and information management scholars. This book and the empirical analysis carried out maintain that the RBV holds much promise as a framework for understanding strategic information/knowledge economy issues but cautions that, before it is adopted, it needs to be fully understood. Chapter 3 outlined the development of the RBV from its origins in early economic models of imperfect competition, through the work of evolutionary economists to the contributions of strategy economics scholars over the past two decades. The chapter also differentiated between and defined the two categories of resources, firm specific and country specific. In addition, the relationship between resource-based view and institutional theories was covered, along with the few attempts to evaluate the experiences of developing economies from a resource-based perspective. It is apparent that research using resource-based theory and examining macro strategy difference in the social context of developing economies is almost absent. Similar to most resources that create competitive advantage at the micro level, resources for competitive advantage at the macro level in developing economies are mainly intangible. The economics literature has paid attention to the revenue-generating promises of developing economies, and as such, has focused, mainly, on big developing and emerging economies such as China, India, and Russia. Consequently, the authors concluded that it is essential to understand the relationship between economic experiences and the changing nature of the institutional environment.

Coverage of cyber laws in the sample countries was the subject of Chapter 4. It was argued that the battle against cyber attack is principally contingent upon the legal structure of every country. In particular, cyber security is contingent upon every economy having (1) effective laws that criminalize attacks that cause damage to systems and networks, and make certain that law enforcement officials have the authority to look into, and take legal action against, crimes made possible by technology. And, (2) laws and policies that facilitate international collaboration with other parties in the fight against computer- and Internet-related crime. Given the nature of cyber crime, these laws have to be coordinated across borders in order for them to be effective and successful. In order to reach a global harmonization of cyber crime legislation, and a common understanding of cyber security and cyber crime among countries developed, emerging or developing, a global agreement at the United Nations level should be established that incorporates resolutions designed to tackle the global challenges.

The set of hypotheses in the current research addressed the determinants of success of cyber law maturity in developing and emerging economies. These identified the human resources, the financial resources, access, and technical capabilities of an economy, the strength of the rule of law, and the strength of the economic base of a country as measured by the per capita income. The first hypothesis stated that a maturity of cyber law is related to the quantity and quality of human resources available to society; it was stated that a well-educated and trained population will demand better laws to control cyber activities, hence leading to more mature cyber laws. The second hypothesis has to do with the financial resources available to the country. Evidence of a positive relationship between the strength of the financial base of a country and its economic growth has been presented in previous studies; in the Information Age and with more reliance on cyber space, financial investment in Internet-based technologies is positively correlated with economic growth, and this consequently leads to more emphasis on laws to control cyber activities. The third hypothesis dealt with access to Internet-based resources and technical capabilities. Without access to computers and Internet connections at a reasonable cost, citizens in developing and emerging economies will be unable to migrate from traditional markets to electronic markets. Consequently, a more mature technical infrastructure is positively related to more mature cyber regulations. The fourth hypothesis deals with the strength and transparency of the rule of law and the role it plays in facilitating the use of Internet-based technologies in a developing country. Law plays a vital role in the transformation and development of societies. A number of reasons have been advanced in the resource-based literature to highlight the role a strong rule of law plays in affecting transactional integrity in an Internet-based society, and thus investment in such markets. Because of the unique nature of the Internet, its use creates legal issues and questions, especially in areas related to intellectual property rights and cyber crime. Few countries in the emerging/developing world have drafted comprehensive cyber laws; and those which have are still struggling to perfect their implementation. In this book, we argue that the existence of a rule of law leads to a more mature cyber law, and subsequently to economic growth and development. The fifth and last hypothesis set forth in this study had to do with the strength of the economic base of a country as measured by its per capita income. The statistical methods and methodologies were also covered in Chapter 4.

Chapter 5 covered data collection and statistical analysis to test the five hypotheses formulated in the previous chapter. This chapter presented the first systematic study on the maturity of cyber laws in a number of developing and emerging economies. Finally, the concluding portion of

this book is the present chapter, which consists of a summary, research findings, and recommendation for future research.

CONCLUSION AND RECOMMENDATIONS

Based on our research of the sample of emerging and developing countries and their experiences with cyber law and cyber governance, the following main challenges are identified, in addition to the generic challenges cited by economic growth and development authors.

A major issue was found to be the outdated legal system in most of the developing countries. As we have seen from our analysis in Chapter 5, only 26 countries have developed some kind of legislation dealing with cyber issues; many of them have amended their laws in bits and pieces as a reaction to incidents and crimes that have taken place within their borders. Very few have developed comprehensive, mature cyber laws addressing the various challenges raised by the new world. In reality, many of these countries are still at the early stages of drafting and/or implementing cyber laws. In a number of them, the process has taken on more of a political face than an economic/legal face. Take the case of the Philippines for instance; work on developing a cyber law started in the year 2000 in response (reaction) to the so-called 'Love Bug' computer hacker believed to be responsible for disabling millions of the world's computers in May of 2000. The virus is believed to have caused damage of close to US$10 billion due to frozen networks. Even though the Philippines had the criminal and the evidence to convict, the law needed to prosecute did not exist. As we have demonstrated in this book, the Philippines is not alone when it comes to deficient legal structure regarding cyber space. Government prosecutors in the Philippines stated they could not prosecute the hacker due to a lack of cyber legislation. This specific incident has raised questions about the inadequacy of cyber laws in developing and emerging countries.

On another front, cyber law enactment and implementation are a new form of activity in the legal profession, and in many developing and emerging countries the old hands are taking the wheel in drafting these laws or amending existing laws to address cyber issues. It is still debatable whether these countries consider cyber law to be distinctive from other kinds of law, and that it warrants its own specialty. Nonetheless, cyber law is among the hottest new specialties at American law and mass communication schools. Several cyber law texts have been published in the United States during the past few years to meet the explosive teaching and research demands in the booming field of Internet law. The exact content of cyber law is somewhat controversial in what it covers, what it regulates,

and what kind of penalties are levied, in that a number of observers agree that it includes many aspects of intellectual property and technology transfer. It also incorporates the impact of information technology on legal processes, electronic aspects of commercial transaction processing, and most aspects of traditional computer law. Beyond this important core, cyber space is also having significant impact on many traditional areas of law. Given the impact that cyber space is having on law, the idea of a separate legal field called cyber law is becoming a reality in many developed countries and should become a reality in the developing/emerging world.

A number of countries around the world are planning and developing their own information society policies, though operationalized to differing degrees, at different speeds, and in different ways. For cyber technology to make the transition from the potential to the actual requires not just that it is technically feasible but there must also be a desire for it, coupled with the ability to pay for it, and the appropriate institutional mechanisms to facilitate its adoption and diffusion. A number of measures to promote cyber use in developing countries have been identified. These could include establishing a common digital platform to enhance cooperation and knowledge sharing among trading partners across the supply chain, as well as functioning as a route into individual company portals within a sector (Moodley, 2003). They may also require the setting up of support centers or 'incubators' to facilitate suitable country-specific cyber law strategies. However, the path to and into cyber space may be filled with obstacles, particularly when decision makers remain skeptical about its usefulness to overall development and growth. One of the most severe constraints on wider Internet use in low-income developing countries is their limited access to international 'bandwidth', the high-capacity connections needed to transmit the large quantities of digitized information required for full Internet services. Until this bottleneck is removed, e-mail is likely to remain the dominant use of the Internet in those countries, many of them are in the 'black continent', Africa. Developing regions may potentially leapfrog traditional copper- and fiber-based land-lines and go directly to leading-edge wireless technologies that blend voice and data over the same networks.

In recent years, economists have assessed the impact of a technology developed in an industrialized country which is copied by a developing country. They have shown that the rate of growth of the developing country depends on its initial stock of knowledge and the costs of imitation. A country's readiness for cyber activities depends on network infrastructure and technology diffusion. E-commerce growth, it is argued, is fostered by strong growth in infrastructure, including narrow and broadband access, hardware investment, and Internet use; but it depends

also on growth of mobile applications, price reductions, service improvement, speed, and reliability. This theory is not applicable to the legal aspects of cyber space, since Internet activities transcend borders and it should be regulated by harmonized laws and regulations, law developed cooperatively by the various countries.

To facilitate the introduction of the Internet and eventually electronic commerce/services, the necessary and sufficient condition is the creation of the communication infrastructure. This has been demonstrated by the authors in their previous work (Karake-Shalhoub and Al Qasimi (2007). For developing countries, in addition to the absence of the regulatory and institutional environments to govern cyber space, investment is one of the main obstacles since most countries rely on foreign funds. In addition to developing infrastructure there is a need to create a sustainable supply of Internet services including, training marketing, and extension into rural areas, as well as support and training for small to medium sized businesses. To facilitate the diffusion of cyber activities, a necessary condition is the development of e-policies and e-strategies. Telecommunications infrastructure is clearly a necessary but not a sufficient requirement for the development and entry of a developing country into the cyber marketplace. Despite the technology used, the central objective for developing countries is to encourage investment and partnerships with vendors, suppliers, and telecommunications companies outside their borders. This requires a well-developed approach using tools and strategies of an open and fair marketplace; but above all, it requires a mature regulatory environment as represented by the existence of a mature cyber law.

As discussed above, in addition to the hard resources being considered by many developing countries, a host of soft resources has to be emphasized. The first is the establishment of national policies dealing with the information and telecommunications sector. As noted earlier, communications infrastructure is clearly a necessary, but by no means a sufficient condition for successful adoption and diffusion of cyber activities. The second soft factor necessary for successful adoption of cyber space in developing economies is appropriate legal norms and standards; laws dealing with consumer protection, privacy protection, cyber crime, and intellectual property rights are essential for the successful implementation of e-commerce and e-government programs. Additional issues that countries have to consider embrace recognition of digital signatures and electronic documents, and collection of taxes and tariffs. The majority of countries in our sample have not studied or created policies or laws to address the issues originating as a result of cyber space. It is important to state here that the experience of the sample countries in developing a legal system dealing with the digitization of their economies has not

been homogeneous. A number of countries are much more advanced than others in this respect; mainly the Eastern European countries such as Poland, Romania, and the Czech Republic; the Latin American countries such as Argentina, Peru, Mexico, and Brazil; and a number of Asian countries including the UAE, South Korea, and Singapore. Many of these countries have recently established national infrastructures for digital certification. In Peru, for instance, the national telecom operator joined Ecuador as the second Latin American country to develop an infrastructure for digital certificates and allow its consumers to use secure applications for e-services. Customers can now digitally sign and encrypt documents that will build trust in and expand the use of electronic transactions (Tetelman, 2003).

Privacy and information security continue to be one of the most important topics when operating in cyber space. As the number of transactions over the Internet increases, so does the number of security breaches including data theft, vicious file corruption, and even e-commerce site shutdown. Privacy issues would discourage people from using the Internet as a transaction medium, hence reducing telecommunication activities and cyber activities. For many developing countries, the privacy and information security issues are complicated by the lack of security systems, such as trusted third parties, encryption procedures, and secure telecommunications that would provide the protection needed for their e-infrastructure. The ability to realize a high level of e-commerce diffusion, then, will largely depend on the climate of confidence e-businesses are able to create in their relations with consumers. The most important aspect of e-commerce is trust. Most likely, a product will fail if it does not have market trust. Usually the basis of trust is based on risk assessment while confidence is based on familiarity. Society may become reliant on the product when confidence is achieved; however, not all products achieve this level. Establishing trust in the eminently impersonal environment of the Internet is not straightforward. People are unwilling to give their credit card numbers over the Internet. Also, fraud has increased in online transactions and cyber crime is on the rise. Consumers also worry that their private data will not be valued or respected by the company they are dealing with. Karake-Shalhoub (2002) recommends a number of solutions to this problem. First of all the combination of data encryption and legal controls will ensure integrity of data that are transmitted. There has to be certain trust policies to establish trust. If governments try to implement certain policies preventing theft of identity, then fraud can be reduced in cyber transactions. A number of difficulties faced are related to the technical area; trust enhancers were identified by Karake-Shalhoub, including the seal of approval from a trusted third party, the appointment of a chief

information officer, and the development of a comprehensive clear privacy statement. In addition to these tools, the development and implementation of cyber laws seem to be the most important drive in the diffusion of cyber activities.

Since the private sector is the engine of growth in any economy, the involvement of the private sector in cyber space in the form of adopting click-and-click business models should be one of the main objectives of developing and emerging economies because it is the private sector that can create additional jobs and enhanced revenue. Yet many cyber space initiatives in developing and emerging countries are initiated by the public sector and financially supported by the government, as demonstrated by all the e-government initiatives taking place around the world. A number of these programs have been very successful, though. The government of Chile has implemented an e-government model that is rapidly diffusing to the private sector. The government's website began as an information portal to the public but rapidly became a facilitator and instigator of e-commerce. In 2001, the Chilean government began its e-procurement portal where smaller businesses compete for public sector contracts; and both private and public sector entities can conduct transactions over the portal. The portal has since become a meeting place where the government provides, free of charge, a cyber market for buyers and sellers to gather and conduct business. This program has enhanced government services through the upgrading of back office systems and the transparency of its processes. The program has motivated businesses to partake in the Internet's development while increasing their transaction cost efficiency and widening their markets. From our analysis, it is estimated that almost 45 percent of Chile's population are active users of the Internet.

As e-commerce and e-government require technical knowledge and understanding, a lack of education of these technologies is a serious impediment to their adoption. Certain countries lack key elements of education: Internet awareness, understanding of the implications of the Internet, and skilled workers in information technology. Even when people are aware of the Internet, many times the population does not understand how the Internet might improve their lives and they therefore oppose it. The erosion of local culture is a prominent issue when discussing the move to and adoption of cyber space. It is therefore the responsibility of regional governments to foster the development of e-culture and cyber laws to give people the sense that they are protected in cyber space. Culture influences how people perceive certain things, what they value, and how they interpret the graphical images and lines of text they encounter on a website.

Cyber space promises great potential to create and reveal new business opportunities; reduce all types of costs, especially search and transaction

costs; increase business efficiency and effectiveness; and improve the quality of life in adopting countries. Given the enormous benefits cyber space can provide to help the growth and development of any economy, developing and emerging economies should create the necessary conditions to move their economies into the digitized phase; and this includes creating a mature cyber law. Digitization strategies have to be aligned with existing resources in a particular economy, taking into account the different stages of economic development; the heterogeneous regulatory environments; and the diverse social, economic, and cultural frameworks.

It is vital to state here that enhancing capability in cyber space and harmonization of cyber laws among regional economies (such as the Gulf Cooperation Council), through economic and technical cooperation, are needed to enable all developing and emerging economies to reap the benefits of the new world. It is recommended that the private sector plays a primary role in developing the technology, applications, practices, and services. Also, it is advisable that governments promote and facilitate the development and uptake of cyber space by providing a favorable environment and the necessary hard and soft resources, such as the legal and regulatory aspects, which are predictable, transparent and consistent, and creating an environment that promotes trust and confidence among cyber participants. In addition, governments should promote the efficient functioning of cyber space internationally by aiming, wherever possible, to develop domestic frameworks which are compatible with evolving international norms and practices, and becoming leading-edge users in order to catalyze and encourage greater use of electronic means, following the example of the Dubai government.

Cyber activities cannot flourish without the cooperation of business and governments to ensure the development of affordable, accessible communication and information infrastructure. Further, government and private sector businesses should cooperate to develop and instigate technologies and policies that build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy, authentication, and consumer protection.

In order to benefit fully from the cyber revolution, regional developing and emerging economies should strive to work together in developing their cyber laws; this will help build trust and confidence in digital means, and enhance government use. Cooperation will also help intensify community outreach; promote technical cooperation and experience exchange; where appropriate, work toward removing barriers to the adoption of cyber space; and help develop flawless legal, technical, operating, and trading environments to facilitate the growth and development of cyber space adoption.

To accomplish the above, governments in developing and emerging economies should develop programs and action plans aimed at:

1. Developing measures and indicators on level of adoption, use, and flows of cyber activities.
2. Identifying the economic costs that inhibit increased adoption and diffusion of cyber activities, including those imposed by the regulatory and market environment.
3. Considering additional economic and technical cooperation among regional economies to facilitate and encourage cyber activities.

Many developing and emerging countries are deficient in the area of cyber legislation; many have not even amended their existing laws to reflect the new reality of cyber space let alone to develop independent cyber laws. With the exception of a few countries, developing and emerging markets still lack appropriate legislation that deals directly with cyber-related topics. This might be associated with a number of factors, including the underestimation of the magnitude of cyber space and the challenges posed by this new world, and/or the lack of the required judicial expertise in this area.

In those developing and emerging economies where the practice of developing cyber laws has begun, there is an indication that such moves are associated mainly with an increase in foreign investment in the country where such investment has increasingly used electronic means. That has driven those countries to develop laws dealing with e-transactions, e-signatures, cyber crime, and so on (ESCWA, 2007). As mentioned previously, this is an indication of a reactive approach to developing cyber laws as opposed to a proactive one. A key to success in cyber space is to proactively develop and enact cyber regulations which are associated with a country's strategic objectives in terms of economic growth and social development.

On another front, given that cyber space is a global challenge and opportunity at the same time, there is a critical need for international cooperation in the development of laws governing this new world. Cyber space is borderless, and offenders and criminals in one country can commit a crime affecting economic entities in other countries without even leaving their domicile. This borderless nature of cyber space gives rise to cyber attacks independent of time and place, and makes it possible for cyber criminals to abuse 'loopholes of jurisdiction', making it very difficult to prosecute offenders (ITU, 2008).

A number of ways for countries to cooperate in developing cyber laws and fighting cyber crime are proposed here. Regional cooperation tops

the list of our recommendations; coordination covers areas dealing with exchange of information, sharing best practice, and training of legislative personnel and law enforcement officers. A number of economic blocs have already demonstrated their leadership in this area, led by the European Union, the ASEAN countries, and APEC. The countries in the MENA region, as well as the African countries, tread behind. This is a call for those countries to learn from the experience of the avant garde and start their regional initiatives.

On the international level, a number of frameworks have already been developed by the International Telecommunications Union and the European Union. The ITU agenda on cyber security and Europe's Convention on Cyber Crime are exemplary models for developing countries to follow; however, we still do not have a global governance system of cyber space. There is a need for adopting appropriate procedural laws and procedures for bringing cyber criminals to justice. These laws should take into consideration the legal requirements at the national and international levels.

The success of building and implementing cyber law is partly contingent upon creative forms of partnerships of public and private sector entities. Sharing of information, building frameworks, and cooperating in the areas of training and development of personnel would be a good start. Another possibility would be to cooperate in building awareness of citizens, and especially youngsters, of the dangers, both socially and economically, associated with cyber crime. Helping create understanding in this area is essential to developing beneficial policies, strategies, and laws to, possibly not eliminate, but reduce the multifaceted costs of this growing problem.

Building awareness of cyber laws and a cyber law culture is a key success factor in cyber space. An appropriate culture for cyber security should be developed both at the national and global levels, through a global framework for end-users, technologies and content providers, policy makers, and law enforcement officials. This process should be compatible with the different economic, political, social, technical, and legal dimensions of cyber space. This cultural awareness should translate into better training of legal professionals and enforcement personnel; these should undergo training and professional education to cover more technical skills.

A final recommendation has to do with the law itself in terms of content coverage and enforceability. No one can deny the positive role of cyber space in today's world, be it in the political, economic, or social sphere of life. But everything has its pros and cons; cyber criminals are using the technology to their advantage. A number of countries have developed cyber laws which have many advantages as they give legal recognition to electronic records, transactions, authentication and certification of digital

signatures, and the prevention of computer crime. At the same time, however, they have various shortcomings, in terms of lack of coverage of certain crimes and/or the weight and severity of the penalty associated with the crime; the Indian Act 2000, for instance, does not cover the protection of intellectual property rights, domain name, or cyber squatting. Many of these laws lack efficient enforceability mechanisms. A challenge many of these countries face in fighting cyber crime is that most of them lack the expertise and the enforcement agencies to combat crime relating to the Internet. Many of the laws lack teeth to deter cyber criminals from committing cyber crimes; punishment in many instances is ineffective and inefficient. Countries need to enact tougher laws to deal with cyber crimes, especially when those crimes pose a threat to national security or the security of funds, information, or destruction of computer networks.

FUTURE RESEARCH

The growth of the cyber economy has been tremendous, and is expected to reach US$10 trillion by 2010. In many countries, government and business entities have relied on the Internet to, among other things, reduce transaction costs, increase their richness in terms of customer base and depth of services and offerings, reach a wider audience, and improve profitability. Cyber users emerge as the key beneficiaries: they use the Internet as a way to gather information and increase their search efficiency and effectiveness. However, more reliance on the Internet will increase the need and necessity to develop laws to tackle cyber-related attacks and crimes to increase users' trust in this new world. Unfortunately, not many emerging and developing countries have jumped on the bandwagon of developing comprehensive, mature cyber laws, which has led to a widening legislative divide in the digital world.

In general, research on developing and emerging economies faces a number of obstacles. As a starter, theories deducted and/or applied to developed countries may not be suitable to apply in emerging and developing countries. Sampling and data collection are a big problem in addition to difficulties researchers face in developing and applying performance measures. Issues have to be addressed concerning the replication of tests and hypotheses used in developed economies in developing and emerging countries. Developing and emerging economies are dynamic and changes occur at a very fast pace in the institutional environment. As a result, cross-sectional studies may produce misleading results concerning the impact of specific policies. To get around this limitation, there appears to be a need for longitudinal studies.

Another limitation of this study is that at present developing and emerging market economies are not homogeneous, even within the same geographic region. Looking at Middle Eastern countries, one finds clear differences in terms of economic, social, and political dimensions. With respect to the independent republics of the former Soviet Union, they have pursued different development paths to transition and have achieved different degrees of progress. Similarly, in East Asia there are clear differences between China and Vietnam on the one hand and other developing countries such as Korea and Thailand, on the other.

In addition, one limitation of the study is that in the current research the analysis was cross-sectional. Static data were used to test for what are, without doubt, dynamic relationships. Longitudinal analysis would have been beneficial, but unfortunately, given the novelty of the subject at hand, the lack of comprehensive longitudinal data precluded such analysis. Studying economies at different points in time may help identify how changes in the independent variables affect the decisions on both behavioral and non-behavioral constructs.

A profound analysis might be made on an individual country level, when and if data are available. Studies could be conducted at the sector or industry level, such as the banking industry, in some economies; such industry-level studies help in the isolation of industry-specific resources, characteristics, and peculiarities of diffusion of electronic commerce and its impact on growth and development of these industries.

Another recommendation for future research would be to study the relationship between economic structure and level of cyber law maturity and the diffusion of cyber activities in particular countries. Excellent candidates would be countries in Latin America, the Gulf Cooperation Council, and countries in Asia. This recommendation, however, is more difficult to bring to life in the near future because of the less than perfect data collection methodologies and the less than acceptable coverage of existing economies. For any study to be fruitful and professionally acceptable, information and data have to be collected through questionnaires over a long period of time. This is a lengthy and costly process, but it is professionally challenging.

Another proposition explored in this study concerned the impact of the rule of law in a country and its relation to the maturity of cyber law. A country with a strong rule of law is defined as one having a strong court system, well-defined political institutions, and citizens who are willing to accept the established institutions and to make and implement laws and arbitrate disagreements. Many governments and regulatory bodies in developing and emerging countries are starting to recognize the economic potential of cyber space and electronic government and are considering a

number of policy initiatives designed to encourage further development and application of these initiatives. In Singapore, for instance, various amendments to existing legislation and subsidiary legislation have been put in place rationalizing the existing law to cope with moves in various industries toward the electronic framework. The amendments have collectively dealt with computer and electronic evidence, copyright, income tax concessions for cyber trading, electronic dealings in securities and futures, electronic prospectuses, and deregulation of the telecommunications industry. It was suggested that diffusion of cyber activities is positively related to the strength and the level of transparency of the 'rule of law' and the maturity of 'cyber law' in a particular economy. Strong support emerged for this proposition from the findings. If we accept the New Institutional Economics premise that strong institutional and legal foundations would be conducive to diffusion of cyber activities, then we should have found strong support from our statistical analysis. One reason for the lack of support might be the result of less than perfect data. Almost all researchers and practitioners agree that assessing the impact of cyber space will be greatly hindered by the lack of reliable and accessible data. Two problems exist in this respect, which prevent the possibility of multiple studies building on each other. The first is that most of the data are unavailable for analysis by other researchers. The second problem concerns inconsistency across data sources with respect to the data collected. As a matter of fact, deciding what data to collect is much more difficult than collecting the data. In general, the majority of developing and emerging countries have not devised systems to track cyber activities from other areas.

More work is also needed on the interface between relationship development strategy and cyber space strategies. It is the firm conviction of the authors that devising well-articulated e-strategies will lead to a higher rate of diffusion of cyber activities in our sample countries. How are strategies developed in electronic contexts and what is the impact of such contexts on new and existing strategies? Should a country's management strategy be altered under electronic conditions? These are critical questions that have yet to be addressed.

REFERENCES

FreshMinds and UK Online Centres (2008), 'Economic benefits of digital inclusion: Building the evidence', accessed at www.ukonlinecentres.com/corporate/images/stories/downloads/economic per cent20benefits per cent20of per cent20digital per cent20inclusion per cent20- per cent20building per cent20the per cent20evidence.pdf.

Gantz, J.F., D. Reinsel, C. Chute, W. Schlichting, J. McArthur, S. Minton, I. Xhensi, A. Toncheva and A. Manfrediz (2007), *The Expanding Digital Universe: A Forecast of Worldwide Information Growth Through 2010*, IDC White Paper, accessed at http://www.emc.com/about/destination/digital_universe/.

Goodman, S.E. and H.S. Lin (2007), *Toward Safer and More Secure Cyberspace*, report by the Committee on Improving Cybersecurity Research in the United States Computer Science and Telecommunications Board Division on Engineering and Physical Sciences. Congressional Report, Washington, DC: National Academies Press.

International Telecommunication Union (ITU) (2008), *International Telecommunications Union Yearbook*, Geneva: ITU.

IT Governance Institute (2006), 'Information security governance: Guidance for boards of directors and executive management', accessed at www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=24572 (7 July).

Johnston, A. and R. Hale (2009), 'Improving security through information security governance', *Communications of the ACM*, **52**(1): 126–9.

Johnson, L.J. and S. Hall (2009), '9 habits of highly successful CISOs', accessed 2 February at http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1257074,00.html.

Jones, H. and K.L. Pedigo (2001), 'Who's watching the web', *Webtechniques*, **6**(4): 42–6.

Karake-Shalhoub, Z. (2002), *Trust and Loyalty in Electronic Commerce: An Agency Theory Perspective*, New York, NY: Quorum Publishing.

Karake-Shalhoub, Z. and Al Qasimi, L. (2007), *Diffusion of E-commerce in Developing Economies*, Cheltenham, UK, and Northampton, MA, USA: Edward Elgar.

Moodley, S. (2003), 'Whither business-to-business electronic commerce in developing countries? The case of the South African manufacturing sector', *Information Technology for Development*, **10**: 25–40.

Organisation for Economic Co-operation and Development (OECD) (2008), 'OECD Guidelines for the security of information systems and networks', accessed January 29 at www.oecd.org/dataoecd/16/22/15582260.pdf.

Tetelman, M. (2003), *Foundations of Electronic Commerce for Development: A Model for Development Professionals*, Washington, DC: Academy for Educational Development.

Travica, B. (2002), 'Diffusion of electronic commerce in developing countries: the case of Costa Rica', *Journal of Global Information Technology Management*, **5**(1): 4–24.

United Nations (2008), *UN Revolution 57/239 on the Creation of a Global Culture of Cybersecurity*, accessed 7 May at www.itu.int/ITU-D/cyb/cybersecurity/. . ./UN_resolution_57_239.pdf.

United Nations Economic and Social Commission for West Africa (ESCWA) (2007), 'Models for cyber legislations in ECSWA member countries', E/ESCWA/ESEWA/ICTD/200/8, Beirut: ESCWA.

Index