A policy for sending secret information over communications networks, *Charles Cresson Wood.* Here the author proposes one of the fundamental design principles of information security. That is, that information should be consistently protected, and that this principle should apply in all instances. He investigates how policies for sending secret information might be implemented, e.g. by encryption. He concludes that the policy applies to many environments. *Information Management & Computer Security, Vol. 4, No. 3, 1996, pp. 18-19.*

Tales from the crypt, *Douglas Hayward.* Electronic identities are frighteningly easy to assume. A skilled hacker can take control of a genuine user account or pose as a user by creating convincing copies of that person's or organization's account. For electronic commerce to take off in a big way, cyberspace desperately needs a reliable mechanism for checking people's identity, for creating audit trails around transactions, and for authenticating and making sure contracts are honoured over networks. Everyone agrees to carry an electronic 'digital signature' created using encryption technology. They then send a copy of their signature, along with proof of their personal details, to an independent third party organization of their choice. These organizations allow you to check the identity of people you do business with. They also hold a copy of your 'public key' encryption algorithm so that people can send you encrypted messages, and they keep a copy of your 'private key' in case you lose it.

These trusted third parties (TTPs) will be the cornerstone of electronic commerce. TTPs in the UK are expected to be either financial institutions, network providers, or specialist trade and professional bodies. However, major issues remain unresolved. Legal liability is one of the key issues that has to be worked out before a British TTP network can be created. The problem is that TTPs are hopelessly entangled with the politics of encryption. The UK and US governments will only license TTPs if the latter give their national authorities access to customers' encryption keys and digital signatures through escrow agreements. The effect is to extend the state's wire-tapping ability from voice to data networks. The EC is preparing proposals for a European framework for TTPs and the OECD is drawing up guidelines for a common set of international encryption control policies, in conjunction with international business associations and major users. *Computing, August 29, 1996, pp. 16-17.*

Danger! Deadly new computer viruses want to kill your PC, *James Daly.* A computer virus tears up your hard drive and brings down your network faster than the Ebola virus can bring down a man. Don't think you're in danger of becoming a virus victim? Think again. A recent survey by the National Computer Security Association showed that virtually all mid-size and large organizations in North America have had at least one computer virus. And with the arrival of insidious macro viruses and the burgeoning use of the Internet to send and receive software, the odds keep increasing against you. Don't panic. While nothing can protect you 100%, a good virus scanner detects and eradicates nearly all known viruses before they can do any harm to your computer. But although many developers love to flaunt how many viruses their scanners can detect, the real issue is how easy the software is to use. This article looks at four leading scanners for Windows 95 to see which one was not only the most effective, but also the easiest to install and operate. Scanners reviewed are PC-cillin 95, VirusScan 2.0 for Windows 95, Norton AntiVirus 1.0 for Windows 95 and Dr. Solomon's Anti-Virus Toolkit 7.55 for Windows 95. *PC Computing, September 1996, pp. 198-202.*

Testing your plan is more important than the plan itself, *Colin Maslen.* The author states that for business recovery planning to be successful, more than just a recovery plan should be produced. The author proposes that testing and training are just as important as the plan itself. He addresses three key areas: the plan and its importance; what else is needed to manage a disaster; and what is gained by testing and training. He concludes that an extensive programme of testing and training will prepare an organization for almost any contingency. *Information Management & Computer Security, Vol. 4, No. 3, 1996, pp. 26-29.*

Doing business on the Internet: marketing and security aspects, *Karen Forcht and Rolf-Ascan Wex.* This article acknowledges that many prospective business users are wary of the Internet because of existing and potential security loopholes. The authors give an overview of the security problems and solutions and concludes that doing business online involves some risks, like any other business transaction, but, if attention is devoted to installing secure procedures, it is no riskier than other business practices. *Information Management & Computer Security, Vol. 4, No. 4, 1996, pp. 3-9.*