

Data security requirements of UK businesses

Securicor has conducted research into the data security requirements of the UK business community. A questionnaire was sent to IT managers of leading UK organizations. The results are based on the responses of 625 IT managers. The survey looked at 17 000 sites, 70% of which have linked networks. Of the companies surveyed 80% had a mission-critical application running on the PC LAN or Unix network and security issues are of crucial importance to the majority of companies. However, companies are more concerned with their WAN security issues, probably because risks in these environments are more varied.

Over one quarter of organizations experienced serious network problems at least once a month and only 7% of organizations never experience network problems. PC workstations are backed up much less frequently than PC file servers and Unix servers. Approximately 40% of all companies backup workstations on an ad hoc basis and this is done predominantly across the entire organization or by department.

Of the companies involved in the survey, 79% never encrypt their data, whether on-site, off-site or across WANs. Of those that do use encryption, the algorithms used are mainly those built into other software packages.

Over half of the companies had lost data over the last 12 months. Forty-six percent gave the reason for data loss as being due to failure of the backup/restore process, and in 34% of the organizations backup was not carried out. Of the sites with file servers, 34% have experienced data loss from file servers, 22% of data loss occurred at PC sites, 11% at minicomputer sites and 8% at sites with mainframes.

Of the organizations responding, only 55% currently have an IT disaster recovery plan, and 33% expect to have a plan in place within the next year. Smaller companies are placing less importance on disaster recovery plans. Only 25% of businesses with less than 50 PCs have a plan to cover their PC networks. The number of companies with Internet access has dramatically risen over the last year: 49% of organizations have Internet capabilities and 33% are considering connecting to the Internet. Of the companies with Internet access, worryingly, only 10% have firewalls, restricted service access and E-mail virus checking in place.

For further information, contact Securicor on tel: +44 181 770 7000; fax: +44 181 770 1198.

Loss of £1 million from Government departments

In the UK, Government departments lost in excess of £1 million worth of IT equipment during 1996, through theft and mismanagement. *Computing* reveals that the biggest losses came from the Employment Service and the Inland Revenue, which lost £484 000 and £460 00 of equipment respectively. Both of the departments managed to lose bulky servers and file servers. The Customs & Excise department admitted to the loss of IT equipment worth £121 000 and even the MoD police agency suffered the theft of one laptop.

Reports of computer viruses on the increase

According to a story in *The Nikkei Weekly*, the number of viruses reported in Japan in 1996 has risen by 13%. This is based on research carried out by the Information Technology Promotion Agency. The rise was mainly attributed to the spread of macro viruses sent in documents over the Internet. The most prevalent virus found in the wild was the Word Macro virus, which damages the English version of Microsoft's MS Word software. Since 1994 the number of viruses reported had fallen and this is believed to be as a result of better anti-virus software.

“viruses reported in Japan in 1996 has risen by 13%”
