

CORP breach

part 1

Protecting information has never been more important. From inappropriate usage and hi-tech virus attacks to a good old balaclava-led heist, corporate organisations face many risks to their data. **Jon Packman** looks at the threats and solutions for big business security in the first of a three part series.

Security breaches hold a range of implications for large corporations. Commercially-speaking, this could mean the loss of client lists, business and product information. Trust and relationships with staff, suppliers and customers can be compromised, and there's also the prospect of fines and litigation – not to mention the cost of recovering lost data.

Protecting information is vital for business continuity, and for compliance with legal, regulatory and contractual demands. The proliferation of interconnected information systems and networks in recent years has meant that no business can afford to neglect its responsibilities.

“An enormous amount of sensitive information is transferred both within and across large organisations,” says Jill Organ, commercial market manager – Document Communications for Acco. “Customer information in particular has been targeted by fraudsters, leading to a number of instances of naming and shaming in the media of those companies that have failed to provide adequate security.”

Most information types have value. Customers' financial records may be of interest to fraudsters, while marketing plans, research and development and copyright material could benefit competitors. But even personnel records pose a risk if a company is obliged to hold these securely and in confidence. System failures, software attacks, online fraud, laptop and identity thefts present just some of the threats faced by the corporate world today.



The DTI's *Information Security Breaches Survey 2006* highlights the fact that IT systems in general, and the internet in particular, are increasingly important to business operations. As such, the priority attached to information security remains high, but it also finds that many UK businesses are a long way from having a security-aware culture, with security expenditure either being low or not targeted at key risks.

It shows that large businesses are more likely to have security incidents (87%), tend to have more of them (median of 19 per year) and their breaches tend to be more expensive (£90,000 on average for the worst incident). Computer virus infections were the major cause of the breaches, despite the vast majority of companies using anti-virus software. But large organisations are also much more susceptible to theft, being five times more likely to be targeted than smaller companies.

To justify expenditure and spend effectively, says the DTI, businesses need to carry out security risk assessments. However, only 44% of all companies were found to have done this. Another concern is the increasing use of removable media devices, such as USB sticks. Some 55% of firms had taken no steps whatsoever to protect themselves against the threats posed by these new technologies.

Jane Quinn, general manager at Safe International, explains that because most modern data storage is primarily made from plastic based materials, traditional secure storage may not be adequate to prevent destruction in the event of a fire, for example. "Standard fire safes will not protect valuable computer data," she says. "Plastic media has a melting point of approximately 52°C, so a data fire safe is essential to protect precious records held on CDs etc."

No one single set of controls will provide a solution to corporate security breaches. In most cases, a balance of physical, technical and people-based controls usually provides the answer. But if a business is serious about information security, the most important step it can take is to understand the risks faced.


"It's critical that a business is aware of the level of security that it needs to maintain," says Abby Wilson, UK branch manager of shredder manufacturer Martin Yale International. "One way to do this is by contacting professionals in the data security industry for a complimentary data security audit. This can quickly identify areas where greater security levels are required for secure data destruction, for example."

Shredders have become the popular weapon of choice in the battle for information security, but heightened efforts by corporate fraudsters mean there's a constant need to stay one step ahead. Companies are therefore looking to 'trade up' products that protect private data to a higher level of security, says Wilson. "For example, many are now turning towards shredders that can shred paper into cross-cut particles rather than strip-cut. They are also looking for shredders that can cope with various kinds of media – CDs, USB sticks, security tapes, passports, ID badges and computer hard drives."

Because of the variety of potential threats, she advises dealers to approach the task of selling shredding machines by listening closely to a customer's data security requirements. "Find out how many people will be using the shredder, how often they will be shredding, how secure the data destruction needs to be, how many sheets of paper need to be shredded in one pass, and how large the catch-basket needs to be."

Furthermore, adds Acco's Organ, dealers should remember that large organisations are comprised of individual departments with varying security requirements. "Look at these as well as the company as a whole," she says. "Each department will have different needs. HR and accounts, for example, will often require higher levels of security than others."

Understanding the relevant legislation and responsibilities of business, along with knowledge of the products available to help reduce the risk of security breaches is the key to winning customers. Running a 'health check' for your clients is often the best way to get a foot in the door, so make use of manufacturers who are keen to offer their expertise and work alongside dealers to assess their customers' needs. ●



→ "It's critical that a business is aware of the level of security that it needs to maintain"