

Minding your business

Rehman Noormohamed discusses managing the risk of information security breaches.

IT'S DIFFICULT to get exact figures on the cost of information security breaches due to their nature of them, and the reluctance of organisations to openly admit to falling victim, but globally it would be billions of pounds annually. It's estimated that at least two thirds of organisations in the UK are affected by information security breaches, whether it's phishing, spam, emails or viruses. People seem to think these things are simply an annoying part of the electronic world, but technically they are information security breaches and a form of crime. An information security breach is more likely to come from an internal source than externally.

It's estimated that one in five employees have misused the internet and each year one in 500 employees will cause or trigger a major incident. Charities must understand their obligation to comply with the various information security laws, in particular the Data Protection Act. According to the DPA, companies that control the processing of personal data, ie. data controllers, must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data, and accidental loss or destruction of, or damage to, personal data.

It is the second limb of the principle that is particularly relevant to information security breaches. The consequences of non-compliance with the DPA and other information security laws can be wide ranging, for example, imprisonment, fines, damage to brand or reputation, loss of business, breach of confidence and/or even a breach of contract. Just because

you can't see it, don't believe it isn't happening.

Part of the challenge is to increase market awareness of what information security breaches are and what form they can take so that individual organisations can then identify, assess and properly manage relative to their own business the impact of legal, technological and operational risks arising from information security breaches.

As a general rule, organisations should spend approximately 5-10 per cent of their annual IT budget on security. However, typically, UK companies only spend about three per cent on average on IT security, with some spending far less than this. If finances are tight it may be necessary to consider cheaper and more practical ways of dealing with legislation and managing risk, for example, good place to start is putting in place policing and

enforcing policies such as IT/internet usage, data protection, security and control of access to information policies. Even doing simple things like regularly changing passwords and backing up data can significantly reduce the risks.

In the event your organisation is a victim of an information security breach, there are a number of things that can be done. However, delay can be fatal depending on the nature of the incident. Act quickly to minimise the damage and, where appropriate, get experts involved such as IT professionals, lawyers and the police (where appropriate). What can be done from a legal perspective depends on the circumstances, but could include seeking a court order for the preservation of evidence or even serving an injunction on a third party to prevent them releasing confidential information into the public domain. ■

Rehman Noormohamed is head of the technology, media & communications practice at Michelmores LLP

Top tips to mind your business

- 1) Know your organisation and the risks attached to it (legal, operational and technological)
- 2) Always ensure compliance with information security laws
- 3) Review online security measures, check firewalls, password protection, servers and anti-virus software and update them where necessary
- 4) Restrict access to confidential information
- 5) Put in place and periodically test your business continuity and disaster recovery plan and always back-up data regularly
- 6) Strengthen physical and electronic security
- 7) Ensure all remote access connections to your network are secure;
- 8) Set up good practice training and develop, police and enforce policies consistently
- 9) Review your sourcing strategy for managing IT systems and security
- 10) Seek expert advice regarding your business information security strategy