Coping with a major security breach?

What's your contingency plan?

Legal pressures, not to mention your moral obligation to assist unwitting victims, means that you should never delay when disclosing IT security incidents.

In November 2005 a laptop belonging to an employee of the Boeing Corporation was stolen. Among the information on the machine was personal financial data about 161,000 current and former employees of the aerospace giant.

None of the confidential information was encrypted, and therefore the thieves would have been able to read and exploit it easily. Yet this was just one of the two serious failings in Boeing's IT security procedures that this episode highlighted. The second was not to have immediately owned up to the incident. The company still refuses to reveal the precise timings but has admitted that it was 'several days' after the theft before the 161,000 'victims' were officially informed that their personal details were now in the public domain, potentially ready to be used by criminals involved in identity theft.

Companies across the world, have always preferred not to reveal details of IT security breaches. The problem became so bad in the UK that the Metropolitan Police launched a special guarantee under which companies are promised anonymity if they report that their systems have been the target of hackers. Without such a scheme, police were unable to prosecute the hackers because officers were unaware that the incidents had taken place.

It's easy to understand the dilemma of the targeted organisation. A run of the mill incident might cost a typical bank £250,000 in terms of lost productivity, replacement hardware or system downtime. Yet if the attack is reported to the police and the suspects subsequently end up in court the whole episode becomes public knowledge, which results in customers losing trust in the bank concerned. At which point the £250,000 becomes totally insignificant. For if a bank loses the trust of its customers,it will lose those customers and revenue.

The nature of the problems that can be incurred is many and varied, ranging from loss of key information, adverse publicity, loss of trust, legal action by customers, and official censure by regulators. All of which can be avoided with a little forethought and a professional attitude to the use of data encryption.

Where once your key information such as customer account data and profitability figures resided on a few desktop PCs in a private office, now the information is spread far and wide. As well as the master copy on the main system, there are often copies (or at least extracts or summaries) in many other computers. Some of which are laptops, which are incredibly easy to lose or steal.

In addition, unscrupulous staff or dishonest visitors can easily copy information from a bank's main systems to a multitude of external storage devices. These include USB

Companies across the world, have always preferred not to reveal details of IT security breaches

flash drives, digital cameras, MP3 players, mobile phones or even old-fashioned floppy disks. All of which then become vulnerable if subsequently lost, stolen or re-copied.

Although Windows provides some encryption with its Encrypting File System, EFS is difficult to manage and impossible to enforce. Turning it off requires just a couple of mouse clicks, and it doesn't protect areas of the hard disk such as the swap file or other temporary files. Most importantly, if files are copied from a Windows PC to an MP3 player, floppy disk, mobile phone, ftp site or USB drive they invariably lose their encryption, often without the user being aware that this has happened.

An effective encryption policy, therefore, needs to encompass every device onto which employees might wish to copy files. It also needs to be transparent to users, so that it can be centrally controlled without any user action being required. And it should be impossible to disable, except by authorised administrators. Ideally it should also have the selective ability to block files from being copied to external devices at all, or if the target device doesn't support the same level of encryption as that which protects the source data.

Your choice of crypto algorithm is also vital. Choose a proprietary

encryption system and, if anyone discovers the secret mathematical formula behind it, all of the files that you have ever encrypted instantly become public knowledge. Therefore, use a known international standard such as the Advanced Encryption System, or AES, with a key length of at least 256 bits.

What action should be taken?

A management walk through is a great way to assess the impact of a security breach. Simply sit a group of technical and non-technical managers around a table and discuss a series of 'what if?' scenarios. Such an exercise invariably highlights critical weaknesses in existing strategies which can then be corrected before it's too late.

For example, walk through the following scenario. A director of your company attended a conference last week, during which his briefcase was snatched from the back seat of his car. The case contained a laptop computer which held a list of the top 10,000 accounts by revenue. The information was not encrypted. This happened on Friday afternoon but it's now Monday morning and the loss has only just been reported.

Among the topics that you will need to discuss are:

- How will you ensure that those 10,000 affected companies are discreetly informed about the breach as soon as possible?
- Who will brief the regulatory authorities and your company's legal team?
- What will you tell journalists from the national press and broadcast media, once they get hold of the story and want to hear your version of events?
- Who is officially responsible for the security of your company's information, and what will he or she be doing to prevent such an event happening again?
- Who could make use of the stolen information, and how? Can you put systems in place to help detect instances of this taking place?
- What action will the marketing department take to help regain the trust of new customers who have decided to take their accounts elsewhere?
- Which laws and regulations has the organisation broken, and in which countries? For example, the UK's Data Protection Act requires companies to make care of customers' personal information.

Conclusion

The trust of one's customers and investors is among the greatest assets that your organisation owns. Lose it, and you're well on your way to being out of business. But failing to protect key information and data, or to introduce unnecessary delays in making losses public, could make such a situation a reality. Which is why full disc encryption should be mandatory to all organisations no matter what size!

Martin Allen MD.
Pointsec Mobile Technologies.
www.pointsec.com.