

INSIDE

Q&A: Small-ads site Fish4

P20

Managing the **enterprise information** network

The enemy within

Why your biggest security threat may be company insiders



NEWS

Enterprise 2.0:
not just about software **p5**

Nuffield Hospitals
streamline procurement **p6**

Microsoft study provides tips
on corporate blogging **p7**

FAST feasts on Platefood **p7**

CASE STUDY

Young's SPECIAL
e-mail charter **p16**

WORKSHOPS

Modern forms -
processing technology **p26**

Creating killer
web content **p30**

THE LAST WORD

A perfect environment
for projects? **p34**

Published by:

Security

The enemy within

The greatest threat to your company's confidential information may not be hackers or viruses, but a trusted corporate insider with a portable storage device.

Confident that your employees can be trusted with sensitive company data? Think again.

In a November 2006 survey of 1,000 working adults across the UK, conducted by market researchers Tickbox.net, 60 per cent of respondents admitted to taking confidential company documents, customer databases, business contacts and sales leads from their employer. Thirty per cent, meanwhile, said they believed sales leads and business contacts rightfully belonged to them, not their employer.

“Clearly, many employees do not see data theft as stealing and do not apply any moral brakes to these activities,” warns Graeme Pitts-Drake, chief executive of data security specialist Prefix IT, which commissioned the survey. Naïve employers who continue to trust their staff blindly are “just asking for trouble”, he says.

The problem is that, when it comes to data security, most companies have focused primarily on implementing perimeter security technology, such as firewalls, in order to protect corporate networks from external threats, such as hackers, viruses and spam, says Edward Wilding, co-director of computer crime

By Jessica Twentyman

investigators Data Genetics International (DGI) and author of *Information Risk and Security: Preventing and Investigating Workplace Computer Crime*.

In fact, the problem frequently lies far closer to home. “In about 70 per cent of the data theft cases that DGI investigates, the guilty parties are shown to be company insiders,” he says.

At the heart of the problem is the proliferation of portable storage devices, such as memory sticks, handheld computers, digital music players and mobile phones, on to which corporate data can easily and quickly be downloaded. “These seemingly innocent devices offer ever-increasing storage capacity, but at the same time, they are small enough to conceal and unlikely to arouse suspicion,” says Simon Azzopardi, managing director of data security specialists GFI.

Without resorting to spot-checks and physical searches of employees and their possessions, it is extremely difficult to monitor and prevent the misuse of external data storage devices, says Wilding. “Due to their portability, these

“In about 70 per cent of the data theft cases that DGI investigates, the guilty parties are shown to be company insiders.”

Edward Wilding, Data Genetics International.



devices are also easily mislaid or lost, which introduces another risk should the information stored on them be confidential or sensitive,” he says.

At the same time, adds Azzopardi, easy connectivity and high-speed data transfer has become increasingly more widespread. As a result, users can simply plug a device into a PC’s USB port and it’s up and running – no drivers or configuration required. “In practice, this means that a data thief

“A malicious insider could use an iPod to steal potentially millions of financial, consumer or otherwise sensitive corporate records at one go – a practice known as ‘pod slurping’.”

Simon Azzopardi, GFI.

can get away with even more precious data, and a negligent employee can dump more viruses onto the corporate network, even when connecting for only a short time.”

Take, for example, the Apple iPod: “At a glance, it’s an innocent-looking portable audio device. But under the hood it boasts up to 60 gigabytes (GB) of portable storage space – practically large enough to store all the data found in a typical workstation,” says Azzopardi. This means that a malicious insider could use an iPod to steal “potentially millions of financial, consumer or otherwise sensitive

corporate records” at one go – a practice known as ‘pod slurping’.

Forensically, it is possible to determine that USB memory sticks, CD drives or other devices have been attached to a specific PC, says Wilding. The registry of the operating system will record devices that are connected to the computer (see figure one).

“The problem, however, is that there is rarely any indication at all of which files have been copied to (or from) these devices,” he says. The misappropriation of data using memory sticks is therefore “traceless”.

Operating system registry

```
A--> CdRomRICOH_CD-R/RW_MP7083A
      Device Description: CD-ROM Drive
      Hardware ID: IDE\CDRORMRICOH_CD-R/RW_MP7083A
      Class GUID: {4D36E965-E325-11CE-BF1-08002BE10318}
      Service: cdrom
      Driver: {4D36E965-E325-11CE-BF1-08002BE10318}\0001
      Manufacturer: (Standard CD-ROM drives)

I--> Disk&Ven_Generic&Prod_USB_SD_Reader&Rev_2.00
      Device Description: Disk drive
      Hardware ID: USBSTOR\DiskGeneric_USB_SD_Reader_2.00
      Class GUID: {4D36E967-E325-11CE-BF1-08002BE10318}
      Service: disk
      Driver: {4D36E967-E325-11CE-BF1-08002BE10318}\0005
      Manufacturer: (Standard disk drives)

J--> Disk&Ven_SanDisk&Prod_Cruzer_Mini&Rev_0.1
      Device Description: Disk drive
      Hardware ID: USBSTOR\DiskSanDisk_Cruzer_Mini_0.1
      Class GUID: {4D36E967-E325-11CE-BF1-08002BE10318}
      Service: disk
      Driver: {4D36E967-E325-11CE-BF1-08002BE10318}\0007
      Manufacturer: (Standard disk drives)
```

Figure One: Examination of a computer's registry
Source: *Information Risk & Security*, Edward Wilding, 2006



Enough is enough

It's time that company directors made it clear to their employees that this kind of theft will not be tolerated, says Pitts-Drake of Prefix. "While trust in staff is laudable, it's professionally negligent not to protect company assets appropriately through policy and technical means," he says. "Failing to communicate with staff about unacceptable activities is tantamount to endorsing theft."

The first step is to get an acceptable use policy (AUP) in place and to ensure that employees understand it, says Wilding. "It needs to be made clear that company data is company property. An AUP should provide direction on how portable storage devices may be used and which kinds of corporate data may and may not be downloaded onto them," he says.

Making that information clear to staff is simply good business practice, but an AUP can also prove to be vital evidence in tribunal situations, he adds. Indeed, the AUP provides a valuable legal defence in such situations if, for example, a member of staff suggests that they were taking valuable data merely to work from home.

However, relying solely on the compliance of employees to the AUP alone is a risky strategy, says Pitts-Drake. Instead, many companies are exploring ways to technically 'block' the USB (Universal Serial Bus) ports on corporate PCs into which these devices are plugged in order to carry out data transfers.

Some companies simply disable the USB ports on their company PCs – a pretty simple procedure that requires very little technical know-how. But this can be problematic, says Pitts-Drake, as vital peripheral equipment such as mice, printers and keyboards also need to be plugged into these ports in order to work.

Besides, adds Wilding, many employees use portable devices in perfectly legitimate, revenue-enhancing ways and a blanket ban on them would be counter-productive. "Just try it – and see how they squeal," he says.

Instead, other companies are turning to specialist software tools, such as EndPointSecurity from GFI and

DeviceWall from Centennial Software, that generally work in two ways: First, by enabling managers to enforce policies that control the download of corporate data onto portable devices; and second, by keeping an audit trail of authorised downloads.

"DeviceWall knows how to handle devices on your network through a 'master policy' that applies to all devices. This can then be modified with rules for

particular users or groups of users," explains Matt Fisher, vice president of marketing at Centennial Software. In this way, a company's default rule for USB sticks might be that they are blocked for all users, except for the marketing department (for the sole purpose of downloading corporate Microsoft PowerPoint presentations, for example). Hand-held computers, meanwhile, may be blocked for all users, except for sales staff,

Five steps to mitigating the removable device risk

Internal security has been overlooked in many of today's organisations, but it is never too late to take action, says Matt Fisher of Centennial Software. In fact, he suggests, those companies that choose to ignore the threats posed by employee-facing network-access points not only risk the loss of valuable intellectual property, but more importantly, the company's reputation.

He proposes five tactics for closing down this security loophole and ensuring that organisations are adequately protected against the threats posed by removable devices:

1. **Understand the risk**
How many employees use portable media devices at work? How often do they connect those devices to the network? First, you need to determine how removable devices are currently being used within your organisation. Some vendors, such as Centennial Software, offer auditing software on a free-trial basis that can help potential users to determine the risk to your organisation before they define and deploy a security policy.
2. **Review the business requirements**
For a minority of employees, using a hand-held computer to keep track of appointments and contacts or taking a large Microsoft PowerPoint presentation to a sales pitch on a USB drive are efficient ways to conduct business. However, connecting an Apple iPod to the network and downloading music almost certainly is not. The key is to determine what constitutes a legitimate business need by a department or individual employee – whatever activity is not entirely necessary is an operational risk that needs to be addressed.
3. **Create a removable device policy**
Existing 'acceptable use policies' (AUPs) may provide some direction on how employees use portable media devices, but are unlikely to provide detailed or enforceable guidelines. AUPs need to be regularly revised to ensure they are current with the business' attitude towards security. What's more, employees must be aware of the policy through effective internal communication.
4. **Enforce the policy**
If there is no electronic enforcement of these written policies, human nature means that breaches will occur. While complete PC lockdown is a common method for protecting against USB security breaches, companies must be aware that blanket restrictions of a user's access rights will dramatically impact productivity. Key points to bear in mind when assessing possible options for automating removable device management include ensuring protection against the use of WiFi, Bluetooth and Infrared ports.
5. **Educate, review and repeat**
Don't leave staff in the dark. Communicate that security software has been deployed to help enforce the acceptable use policy that has been established. Ideally, your chosen tool should be able to help employees understand the security measures in place and refer them to the appropriate parties if they have further questions. Once deployed, it is important to continue monitoring device connections to spot trends and ensure that the policy is consistent with the current perceived level of threat.

who can plug them in to synchronise their diaries. There may be a blanket ban on MP3 players, but an exception made for the managing director.

“Depending on the device type you’re managing, you get different options for different access types,” Fisher explains. “For example, if you’re working with USB flash drives, you can choose to allow or deny full control, read access or write access. This means you could allow one group to read data from their USB flash drives, but not to write data to them,” he says.

A logging facility in such software, meanwhile, means that a company always has a full record of what’s been downloaded, when and by whom, says Azzopardi of GFI. “With EndPointSecurity, a full list of files accessed to and from a portable storage device is recorded whenever users plug in devices – both successfully and unsuccessfully. We’ve also introduced a reporting package that can be scheduled to automatically generate graphical IT-level and management reports, based on data collected by EndPointSecurity. This gives full details of devices connected to the network, device usage trends and files copied to and from devices, including the actual names of files copies,” he says.

These kinds of tools are proving extremely interesting across all sectors, but among companies in three industries in particular, says Fisher of Centennial Software: “The public sector is hugely interested, because of the implications of the Data Protection and Freedom of Information Acts; the healthcare sector is interested, because it tends to deal with highly confidential personal information; and the financial services sector is interested, because it’s terrified of the regulatory and reputational repercussions of losing customers’ financial information,” he says.

But it isn’t just local government, healthcare organisations and multinational banks that are investing, says Fisher. “Far smaller companies are often heavily reliant on their intellectual property – in fact, their survival may

depend on it,” he says. As a result, users also include small and medium-sized organisations, including specialist design and engineering companies, architectural practices and recruitment consultants.

And for companies of all sizes, securing the network from the security threats posed by portable storage devices need not be expensive, says Azzopardi of GFI. A 10-user licence for

EndPointSecurity, he points out, costs £300, a 25-user licence £400 and a 50-user licence £575.

“Small and medium-sized companies may well need to keep an eye on costs, but when you point out to them that their very survival may depend on them keeping their corporate data private and safe, a few hundred pounds suddenly starts to look like a very shrewd investment,” he says. ■

Case study: New Charter Housing Trust Group

As one of the largest landlords in the UK, New Charter Housing Trust Group takes tenant confidentiality extremely seriously. The housing organisation’s networks play host to vast amounts of sensitive data about tenants, including their financial details, contractual arrangements with the Trust and issues such as anti-social behaviour.

The accidental or malicious disclosure of that kind of information would be a “complete disaster”, according to John Westwood, New Charter’s information systems (IS) infrastructure manager. As a result, data ‘leakage’ is a prime concern for Westwood and his team.

But during a recent security review, Westwood found a worrying loophole in New Charter’s policies and procedures. While external threats were being addressed through the use of firewall protection and anti-virus tools, the threat from portable storage devices had not yet come under the security spotlight.

“The growing popularity of media devices such as iPods, hand-held computers and USB drives posed a real security threat,” says Westwood. “These gadgets help facilitate mobile working, but also mean our employees can carry around large amounts of sensitive information. It’s not that we don’t trust our staff, but more that we can’t afford to lose information through human error,” he says. Not only could confidential information be lost, he adds, but employees could also inadvertently introduce malware onto the network while uploading work from portable devices.

To compound the issue, a blanket ban on portable devices was out of the question. New Charter did not know how many portable media devices were being connected to its network, but it *did* know that certain devices were critical to employees’ day-to-day work.

For example, the organisation has more than 50 digital cameras that are used by inspectors to assess property. What was needed was a system that would enable New Charter to monitor and control what devices were being connected to its network, and by whom.

Westwood therefore tried out Centennial Software’s DeviceWall product, which monitors all device connections and provides flexible enforcement of New Charter’s security policies. In November 2005, the software was deployed on more than 600 PCs and 50 laptops in less than a week.

DeviceWall enabled New Charter to quickly set up groups with their own unique access rights in Active Directory in Microsoft Windows Server. “This means that a group such as housing inspectors can be allowed to connect digital cameras to the network, while staff in the finance department cannot,” says Westwood. DeviceWall’s ‘temporary access’ feature, meanwhile, means that access can be granted for a one-time use, such as if an employee needs to take a large file off-site for an external meeting.

Over time, DeviceWall has enabled the IS team at New Charter to refine security policies as they related to portable storage devices. “Being able to understand what devices were being brought into the office gave us vital insight into where our vulnerabilities lay. This meant that we were able to draw up user policies based on what was actually happening in our own organisation, rather than theoretical information,” says Westwood. Furthermore, by tracking devices usage, the team can spot emerging trends and will be better equipped to identify suspicious behaviour in future, he adds.