

## Press Cutting:

## The Software Bureau Financial Director Online 3<sup>rd</sup> January 2007

**FINANCIAL DIRECTOR**

HOME INTERVIEWS BUSINESS NEWS FEATURES

Financial Director > Features > Companies & Markets

### A winter of disc content

Peter Bartram, Financial Director, 03 Jan 2008

Companies are generating increasing amounts of information, much of it stored on portable electronic devices. But where is that data going and who is seeing it?

**Put aside, for a moment,** the problem of half the UK population's bank details being lost on a couple of disks in a jiffy bag and consider the following: confidential information is found in a skip outside a bank; computer back-up tapes are stolen from a contractor's van; confidential information is ripped off an employee's laptop after a house burglary; payroll and pension details are stolen from three laptops; and mortgage details in documents are stolen from an employee's car. Just some of the other examples of "information leakage" reported in 2007.

In all, an Information Security Forum (ISF) study logged 881 information leakage incidents during 2007. It classed 67 of them as major incidents with many of these "resulting in brand damage". Most, of course, never get reported, so the real number is many times higher.

So is it time for FDs and other members of the board to start taking information security more seriously? A new survey by YouGov suggests that more than one million of Britain's 28 million workforce have either lost or had stolen information on an electronic device, such as a laptop, personal digital assistant, thumb-drive or CD.

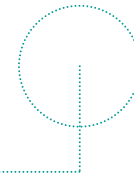
**RELATED CONTENT**

**Similar articles**

- Experts call for public disclosure of information leaks
- IT professionals see need for data breach legislation
- Data loss: yup, it's still going on
- Halifax apologises for mortgage data leak
- Data leakage 'always preventable'
- **More stories**

**White papers**

- Best practices for monitoring and filtering Internet access in the workplace
- Business Travel Specialist Enjoys 100% Protection Against Email-Viruses



Against Email-Viruses.

- The Sarbanes-Oxley Act: A Business Blessing in Disguise

**News centre**

- News
- Analysis
- Comment
- Features
- Special reports
- Email newsletters
- **XML** RSS feeds

**More from Financial Director**

- Bucking the trend
- Investors' chronicles
- Looking forward to 2008?

ADVERTISEMENT

It all adds up to the most comprehensive accountancy coverage



**Safe and sound**

What compounds the problem is that information that was once locked in office filing cabinets can now turn up anywhere. "Nearly five million people now use a laptop from home," says Andrew Durant, managing director in Navigant Consulting's fraud investigation team, which commissioned the survey. "Yet only 25% said their laptops are encrypted to protect the confidential information they contain," says Durant.

Given these figures, it's not surprising that nearly half of British companies don't have a strategy or policy in place on how to handle electronically stored information (ESI), according to a survey from Kroll Ontrack, a division of the Kroll risk consulting company.

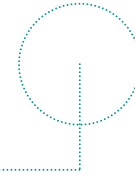
"The explosion of information and the onslaught of new rules, regulations and laws have made it incredibly difficult for companies and counsel to stay on top of everything," says Kristin Nimsger, president of Kroll Ontrack.

What makes it more difficult is that businesses are becoming increasingly "perimeter-less", says Brian Spector, general manager of the content protection group at Workshare, an information security company. "Sensitive customer information, intellectual property and confidential corporate data are constantly sent outside organisations via email, portals, laptops, USB drives and smartphones," he says.

All this means that information leakage is likely to become a growing problem, according to a new report from the ISF. "For large organisations, a certain level of information leakage may be inevitable through unintentional actions rather than malicious intent," says Andy Jones, a senior researcher at the ISF and author of the report. Yet, whether it's intentional or not, when it happens and the news leaks out there are red faces all round. And, as Paul Gray, former chairman of HM Revenue & Customs can confirm, sometimes worse.

Even the companies that are trying to tackle information leakage face a barrage of practical problems. The challenge with data is that it lives where people want to work with it, says Ed Jones, managing director of Thinking Safe, a data back-up and recovery specialist. The job of keeping it secure while ensuring it's readily available "has never been tougher", says Jones.





"Delivering the right message on information leakage is difficult and, all too often, is perceived by staff as 'we don't trust you, therefore we will lock everything up'," says Jones. "A balance should be established between protecting information and sharing it for business benefit. Information leakage is an old familiar problem, but it appears to be enjoying a new lease of life."

One of the reasons that too few companies manage to achieve the balance to which Jones refers is that board members who take strategic decisions don't talk enough to the people who are in charge of information security. A new Ernst & Young survey of 1,300 organisations in 50 countries reveals that one-third of information security chiefs never meet the board. A quarter don't even report to the board on information security compliance or incidents.

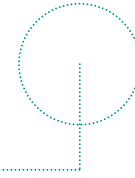
Richard Brown, head of technology security and risk services at Ernst & Young, says: "Data protection and privacy are increasingly big drivers for information security and, with corporate reputations at stake, there needs to be a strong, effective engagement with the business leaders to achieve a holistic approach across the organisation."

### **Security framework**

So what's the solution? "Organisations need to have in place a comprehensive security framework covering governance, people, process and technology," says Mike Maddison, UK head of security and privacy services at Deloitte.

"It only takes one small failing in any one of these areas for an incident on the scale of the HMRC data loss to materialise. For example, it is no good having the governance, process and technology in place if the people are not included in the equation. It is well known that people make mistakes even when fully aware of policies, processes and risks a situation that can be exacerbated if they have lower job satisfaction, variety and motivation."





One problem is that people sometimes don't even realise they're making a mistake. Take those who work on their laptops on trains and in coffee shops making them potential victims of 'shoulder surfing'. "Key executives appear worryingly content to review confidential sales and personnel records on a laptop in a public place, leaving them at the mercy of strangers in the next seat," says Nick Hughes, business development manager at 3M Optical Systems.

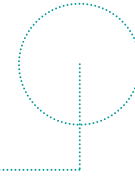
3M's research reveals that 55% of managers have admitted working on a laptop in a public place and 70% said they'd encountered shoulder surfing at some time. As Hughes points out, this sits uneasily with calls from the Information Commissioner's Office for senior executives to take more care with the security of personal information.

The reality is that there are so many types of threats now to information security that FDs and the rest of the board can only hope to gain control by putting a comprehensive management and technical programme in place. The ISF recommends that any holistic policy should be based on six key principles.

These are: educate staff and third parties about information leakage; identify environments that may be susceptible to information leakage; classify information in accordance with its level of confidentiality; ensure general controls include information leakage considerations; consider the deployment of technology solutions for high-value or sensitive information; and be prepared to respond to information leakage incidents.

How these principles are applied will clearly vary from one organisation to another. And part of the grand plan ought to be a rethink about how digital information is managed from a technical perspective. "In response to the threat of local data theft from workstations using portable storage devices, there is a move among security-minded organisations towards centralised network configurations, where sensitive data is processed in one place, rather than being distributed on laptops, desktop PCs and other systems," says Edward Wilding, chief technical officer at Data Genetics International.





### **Restricted access**

The vulnerability of widely distributed information is one of the reasons there is growing interest in "blade technology", which puts the data and processing guts of desktop computers into rack-mounted processors locked inside a central server room. "Blades processor, memory and storage on a card reside in rack-mountable enclosures that supply power, ventilation and other support components. The key security benefit of blade networks is that the user has no access to any local ports or drives through which unauthorised data may be downloaded or uploaded," says Wilding.

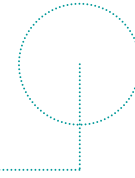
"We have come full circle with blade technology, which resembles the central mainframe and dumb terminal processing environment of old. Among others, the Pentagon and NASA have implemented blade networks, largely in response to the US national infrastructure protection directive."

Boards may also want to ask their CIOs and IT directors to put tougher routines in place to monitor the unauthorised copying or downloading of information. There are several software solutions that can detect USB and FireWire devices, which can be used for unauthorised data downloads over a network. "Administrators of IT systems can disable specific types of storage device such as CD and DVD writers, diskettes, memory sticks, iPods, MP3 players, digital cameras and flash memory, while enabling local USB and FireWire ports for other services," says Wilding.

"A further option is a hardware lockdown of each workstation connected to the network using each computer's on-board BIOS configuration menu," he adds. "Software and source code may be protected using copy-protection mechanisms. I would also recommend that valuable source code be removed from network drives or workstations, and maintained on standalone development computers that are suitably secured physically and logically."

Yet, although arranging the technical side so that it's less vulnerable is important, ultimately stopping information leakage mostly comes down to people. "Human error is, at times, the most common point of failure," says David Murray, sales director at the Software Bureau, which provides data management software.





"These risks can be reduced by ensuring staff are correctly chosen and have gained the necessary competence for the level of asset they are looking after. The training processes of staff handling data should be extensive, with staff being fully aware of the sensitivity of the matter and the reasons why the information must be kept confidential."

All good advice, but past experience suggests even that won't be enough. Just like water, information leaks can occur where they're least expected.

**Box: Culture Club**

BT may not be everybody's favourite telecom company, but at least it hasn't downloaded its customers' details to a disc and put it in the post. As far as we know.

The main reason for this is because of a data quality programme which the company has been running for six years. The programme has created a new culture in which people take more care of the information they generate and use, says Nigel Turner, head of ICT customer management.

BT realised that it was missing business opportunities because it had poor data quality, adds Turner.

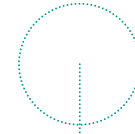
The problems showed up in slow product launches, or missed sales opportunities. Data quality issues have been tackled, in some cases, with the aid of software called TS Discovery from Trillium Software. It enabled data quality owners to help business process owners to prototype potential new business rules quickly.

BT has also nurtured a new information culture. "Errors are much less likely to occur when the organisation behaves in a way that treats its information as a major business asset," says Turner.

Making that happen starts at the top, says Turner. "Senior managers need to realise what their responsibilities are and recognise that they have a leadership role to play."

It also involves looking closely at the business to uncover reasons why data quality might be low then acting on it. For example, BT call centre operators used to be incentivised on the number of calls they handled. Now they're partly incentivised on the accuracy of the information they input.





Similarly, engineers often did not bother to record what they'd done thoroughly. "We spent time educating engineers about the importance of keeping accurate network records."

And if FDs think that this tedious work is not worthy of their attention, they should think again. BT estimates its data quality work has so far saved it more than £600m.

