

Keeping it Classified:

Data Theft Risks & Costs Exposed



Executive Summary

Any business that uses electronic communications is at risk of electronic data theft. Every business has data that should remain confidential.

Theft or loss of customer records, business plans, and even sales presentations can result in legal action, brand damage or a rapidly dwindling customer base.

A quarter of businesses have had IP or confidential proprietary information stolen in the last 12 months¹. The associated costs are astronomical. If every large enterprise in the US suffered one serious data breach, the national bill would exceed USD\$523 billion².

One Australian company reported a total AUD\$40 million loss following a single data breach³. Indeed, theft or breach of confidential data or IP was the greatest cause of financial loss for Australian businesses over the past 12 months⁴.

While the risk of data theft has existed ever since computers were invented, it has skyrocketed in the past five years. Not only are we storing more and more information electronically, but the number of ways data can be stolen or leaked has also climbed.

The explosion of mp3 players, USB keys and mobile phones with portable storage means every employee could be carrying a data theft device. Instant Messaging, Voice-over Internet Protocol and P2P in the office have also created new risks.

Some of the world's best-known organisations – Apple, Yahoo and the US Military – have experienced how damaging data theft can be for their reputation and bottom line.

But just who is stealing data? Surprisingly, insiders are four times more likely than outsiders to be the cause⁵. More often than not, breaches are the result of employee error, with intentional theft by employees the second most likely cause.

Despite the potential risks, many employers are choosing to stick their heads in the sand. Without a comprehensive risk reduction strategy, data theft is just a matter of when. This white paper outlines why companies should take a hard look at their confidential information, including where it is and who has access to it, and how to deploy 360° protection.

¹ 2005 E-Crime Watch Survey, 3 May 2005, p19

² Based on figures in "Lost Customer Information: What does a data breach cost companies," Ponemon Institute PGP Research Report, November 2005, p2

³ Crawford, M., "Rootkits wreak havoc," ARN (ARNnet.com.au), 22 May 2005

⁴ 2006 Australian Computer Crime and Security Survey, May 2006, p26

⁵ Ponemon Institute Data Security Tracking Study 2004, in Ponemon, L., "When Employees Are Risky to Your Business," Darwin (Darwinmag.com), 19 January 2005

The Risks

How vulnerable is your data?

Data theft has never posed a bigger risk. With computers and e-mail now the backbone of business communication, protecting your organisation is no longer a matter of locking the filing cabinet.

Today, 90% of a company's intellectual capital can be found in digital format. At any given time, 45% of those ideas can be found in the e-mail system⁶. In real terms, 90% of a company's sensitive information is vulnerable to electronic data theft.

To add to the risk, this information usually includes material that's highly confidential. Two-thirds of businesses own information assets classified as highly confidential, and for large businesses it's as high as 80%⁷.

A fifth of businesses have no idea how much sensitive information they own. Of those businesses that do know, a quarter has failed to take the next step and classify data according to confidentiality and privacy⁸.

What's at stake?

The amount of confidential information on today's company network and mail servers is only one reason why data theft is so dangerous. Data theft can affect:

- Legal liability
- Compliance with regulations
- Corporate reputation and brand
- Ability to compete in the marketplace

The most common data breach of all, loss of confidential business information⁹, can cripple companies in all of these areas.

For wine giant Southcorp, an e-mail improperly containing earnings information resulted in a federal investigation¹⁰, damaged the company's reputation, and

⁶ SC Magazine, April 2001

⁷ PricewaterhouseCoopers DTI Information Security Breaches Survey 2006, April 2006, p5

⁸ Melek, A & MacKinnon, M., Deloitte Global Security Survey 2005, p28

⁹ Ponemon Institute Data Security Tracking Study 2004, in Ponemon, L., "When Employees Are Risky to Your Business," Darwin (Darwinmag.com), 19 January 2005

¹⁰ Gettler, L., "Watchdogs pounce on Southcorp," Sydney Morning Herald (Smh.com.au), 27 February 2003

contributed to a share price slump. The investigation resulted in a civil penalty fine, despite the court recognising the e-mail was “an honest blunder”¹¹.

The second most common form of data breach – loss of customer information – can cause serious legal liability and compliance issues, and result in customer loss.

One in seven businesses has also reported the theft of intellectual property from their organisation in the last 12 months. A further 12% had experienced theft of other proprietary information¹².

By exposing trade secrets, IP leaks can disrupt product cycles and cause long-term damage to an organisation’s ability to compete. In 2003, Valve Software, the makers of the *Half Life 2* computer game, were forced to delay the planned Christmas release of the game thanks to leaked source code. Valve’s CEO pointed to a hacked e-mail system and key-logging Trojan, and the crime resulted in a number of arrests¹³.

When sensitive information is involved, every single type of data breach has the power to plunge an organisation into the red.

More than a red face – the bottom line

Data theft is one of the most expensive security incidents a business can face. While the 2005 FBI Computer Crime Survey put the average cost of computer security incidents at USD\$24,000¹⁴, data breaches can be significantly more expensive.

In 2005, the average loss caused by theft of proprietary information rose to USD\$355,553, up from USD\$168,529 a year before¹⁵.

In Australia, the average annual losses from electronic attacks, computer crime, and computer access misuse or abuse rose 63% over 12 months, reaching AUD\$241,150 per organisation in 2006¹⁶.

Yet these figures fail to take into account the implicit costs, like lost sales due to negative media coverage. When the Ponemon Institute factored in these costs – including legal services, victim notification costs and increased staffing to handle the initial crisis – their estimate was US\$14 million per single data loss incident¹⁷.

¹¹ Bednall, T., “In the deal,” Issue 10, Allens Arthur Robinson (AAR.com.au), December 2003

¹² 2005 E-Crime Watch Survey, 3 May 2005, p19

¹³ Smith, T., “Code-theft suspects nabbed, claims Half-Life 2 team,” The Register (Theregister.co.uk), 11 June 2004

¹⁴ 2005 FBI Computer Crime Survey Report, p10

¹⁵ Gordon, L.A., Loeb, M.P., Lucyshyn, W. & Richardson, R., CSI/FBI Computer Crime and Security Survey 2005, p15

¹⁶ 2006 Australian Computer Crime and Security Survey, May 2006, p24

¹⁷ “Lost Customer Information: What does a data breach cost companies,” Ponemon Institute PGP Research Report, November 2005, p2

Consider this: if each of the 37,000 large enterprises (those with over 500 employees) experienced just one data breach in a year, it would cost the US over USD\$523 billion.

Theft or breach of confidential data or IP is the greatest cause of financial loss for Australian businesses¹⁸. For one business, the cost of a single data breach totalled AUD\$40 million (USD\$30 million)¹⁹.

If these costs seem difficult to believe, the attitude customers take to data loss puts the figures into perspective. Over a third of US bank customers would take their business elsewhere if they found out about a data breach. The churn increases to 45% if there are two incidents²⁰. When the law is involved, data theft can be even more costly. In the US, ChoicePoint's bottom line took a USD\$15 million battering in fines alone after thousands of customer records were leaked.

ChoicePoint

Data broker ChoicePoint must pay USD\$15 million to settle Federal Trade Commission charges over a data loss incident that affected 163,000 people and resulted in 800 identity theft cases. Lax processes were the cause of the breach²¹. Following the fine, Gartner estimates the direct financial impact of the breach as approximately USD\$79 per exposed customer account²².

Who's most at risk?

While any organisation with sensitive data is at risk of theft, stakes are higher for some:

- Organisations in highly regulated industries like finance and health that manage large volumes of personal customer data.
- Firms with a large investment in intellectual property, such as technology companies. Theft of R&D data is on average the most expensive per incident (USD\$404,000), followed by financial information (USD\$356,000)²³.
- Large organisations, no matter what the industry, are more likely to experience security incidents than smaller enterprises. The incidents are also likely to be more expensive²⁴.

¹⁸ 2006 Australian Computer Crime and Security Survey, May 2006, p4

¹⁹ *ibid.*, p26

²⁰ Ponemon Institute Privacy Trust Study for Retail Banking 2006 in "Ponemon Institute Names Most Trusted Retail Banks," media release, Ponemon Institute (Ponemon.org), 26 January 2006

²¹ Kawamoto, D., "ChoicePoint to pay \$15 million over data leak," CNet News (Cnet.com), 13 February 2006

²² "Management Update: Data Protection is Less Costly than Data Breaches," Gartner, 16 September 2005

²³ PricewaterhouseCoopers Trends in Proprietary Information Loss Survey Report, September 2002, p1

²⁴ PricewaterhouseCoopers DTI Information Security Breaches Survey 2006, April 2006, p2

Know your enemy

Businesses rate hackers as the biggest IT security worry (37%), over current employees (18%) and terrorists (2%)²⁵, but data theft statistics tell a different story. The number one cause of data breaches is employee error. Coupled with deliberate data theft, insiders are four times more likely than outsiders to cause data breaches.

Insiders are often know the value and location of key data, and are twice as likely to steal intellectual property than outsiders, while outsiders are more likely to commit identity theft²⁶.

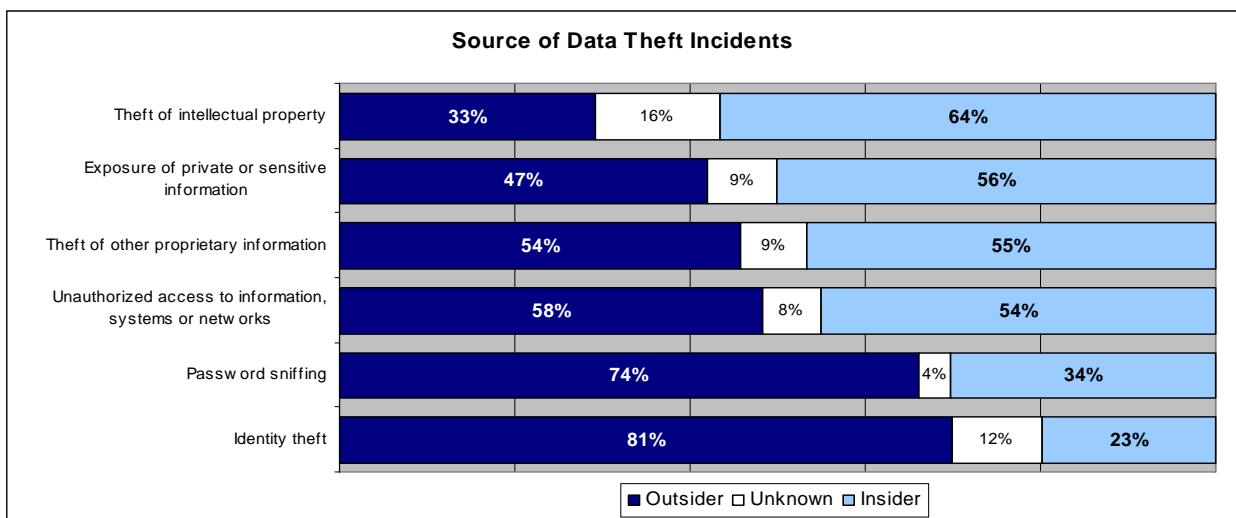


Chart: 2005 E-Crime Watch Survey

Worryingly, one in six data loss incidents are never solved²⁷.

The insider threat

Even the best employees can leave organisations exposed by accident. Poorly trained or disgruntled workers are a particularly high risk.

While good management can reduce the risk of employee error, intentional data theft is less easily controlled, and is far more prevalent than employers would like to think.

An Ibas survey of 400 UK business professionals found 70% had stolen corporate IP from their employer when they left a job. The thieves felt they owned this information

²⁵ 2005 E-Crime Watch Survey, 3 May 2005, p19

²⁶ *ibid.*

²⁷ Ponemon Institute Data Security Tracking Study 2004, in Ponemon, L., "When Employees Are Risky to Your Business," Darwin (Darwinmag.com), 19 January 2005

and were entitled to take it with them²⁸. The survey noted the most commonly stolen forms of IP were e-mail address books (54%), sales proposals (33%), and customer databases or contact information (30%)²⁹.

One web designer stole a customer database by e-mailing it to his partner, used the information to attempt to poach customers, and deleted over 100 important files in an act of sabotage³⁰.

In 2006, a case publicised by PricewaterhouseCoopers' forensic investigation services showed that three employees had used e-mail to smuggle IP out of the organisation before they defected to a rival³¹.

With notebooks now outselling PCs³², workers are taking confidential data with them when they leave the office. Boeing and Fidelity Investments both ran into problems when employee laptops were stolen³³. In addition, data can be compromised by employees connecting laptops to less secure networks when out of the office.

Now that e-mail is the most common data theft tool for insiders, it's essential that corporate security strategies cover outbound electronic communications.

The outsider attack

Unknown outsiders and ex-employees are also a serious threat, responsible for over one in six breaches³⁴. At ACIL Tasman, an ex-employee used his knowledge of the company's e-mail system to steal commercial-in-confidence data for his new employer.

ACIL Tasman

A data theft attack on a rival consultancy destroyed the careers of two senior executives and forced ACIL Tasman to appear in court on charges of breaching the Corporations Act. The attack saw a part-time ACIL Tasman employee hack into the e-mail system of a former employer, Access Economics, to steal confidential information including tenders for policy reviews and draft proposals. An ACIL Tasman whistleblower notified the Australian Federal Police and the company was taken to court. The chief executive and another senior executive admitted to receiving the stolen information³⁵. Both executives stepped down over the scandal³⁶. The findings of the court case have not yet been released.

²⁸ "UK businesses lose £billions in Intellectual Property (IP) theft," media release, Ibas UK (Ibasuk.co.uk), 11 May 2004

²⁹ *ibid.*

³⁰ Henzell, J., "NZ man denies cyber-sabotage," Sydney Morning Herald (Smh.com.au), 29 July 2005

³¹ Head, B., "Preserving the chain of evidence," Sydney Morning Herald, 11 April 2006, p29

³² Dean, T., "What's Hot in 2006," PCAuthority (PCAuthority.com.au), 23 January 2006

³³ "Security holds up in laptop theft," The Australian (AustralianIT.com.au), 28 March 2006

³⁴ Ponemon Institute Data Security Tracking Study 2004, in Ponemon, L., "When Employees Are Risky to Your Business," Darwin (Darwinmag.com), 19 January 2005

³⁵ Robinson, N. & Uren, D., "Bosses face court over 'hacking'," The Australian, 28 October 2005

³⁶ "Latest News," ACIL Tasman (Aciltasman.com.au), February 2006

Attractive targets for cyber criminals are customer databases, which can be plundered to commit identity fraud, as well as network and internet banking passwords.

What puts your business at risk?

Unsecured e-mail

While unsecured e-mail can be intentionally exploited to steal data, unwitting accidents can also lead to serious breaches. With e-mail now more widely used than ever before, accidents are shockingly common.

In a 2003 Australian study, almost 30% of employees said they had received an e-mail not intended for them. E-mail accidents can range from careless 'reply-all' mistakes to poor document control, particularly when confidential files are incorrectly attached and distributed. The speed of e-mail also means that disclosures can be made without proper forethought or clearance from supervising staff.

Corporate e-mail

More than 25% of employees in an Australian University of Western Sydney study admitted to sending an e-mail to the wrong person. For one in five, their accidental e-mail contained confidential information³⁷. Yet only one in 10 companies scans their outgoing e-mails for confidential information.

Corporate e-mail has led to embarrassing scandals and financial damage. For Westpac, it was a work-related e-mail with the wrong attachment.

Westpac

For Westpac, an incorrect e-mail attachment halted trading and sparked an investigation from the Australian Securities and Investment Commission. The accident revealed the bank's full year profit results before they could finalised and lodged with the Australian Stock Exchange. 37 analysts received the spreadsheet, which required some manipulation before the financial results could be viewed. The e-mail gaffe was widely publicised, leading the embarrassed chief executive to say, "the buck stops with me. The accountability is absolutely mine."³⁸ The new figures were embedded in a template of last year's results and were accessible with minor manipulation of the spreadsheet³⁹.

³⁷ University of Western Sydney/SurfControl Internet & E-mail in the Workplace Survey 2003

³⁸ Ferguson, I., "Hit send...and regret it," ZDNet (ZDNet.com.au), 4 November 2005

³⁹ Knight, A., "Westpac jumps the gun on profit," Sydney Morning Herald (Smh.com.au), 3 November 2005

Sun Life Financial in Canada was forced to announce a quarterly profit report one day early after the results were inadvertently e-mailed to analysts. The results were not immediately obvious but, again, could be revealed with some manipulation⁴⁰.

Webmail

Using a personal email account is now the commonest way of stealing intellectual property from an organisation⁴¹. Webmail accounts, Hotmail and Gmail can be more dangerous than company e-mail because:

- Outgoing e-mails can't be traced in standard network logs
- High storage capacities (ie: 2GB) mean large amounts of data can be leaked
- The sender can be anonymous to hide the source of the leak from recipients

Data slurping

Data slurping is fast becoming one of the biggest data theft threats. The low price and widespread popularity of portable storage devices, like USB keys and portable media players, mean every employee can own one.

Portable storage devices have never been easier or cheaper to own. Today, 1GB costs less than USD\$100. In addition, almost all models offer data storage capabilities. The most popular device, the Apple iPod, currently boasts a worldwide circulation of over 40 million. In fact, most mobile phones double as portable storage too.

While CDs and floppy disks can be used in a similar way, they have never posed the same risks. Floppy disks have a limited 1.44MB capacity. Successfully smuggling data out on a CD can be more conspicuous than using a USB device because it requires time at a CD burner.

Today, standard portable storage devices offer 2GB – enough to store lengthy documents, customer databases, financial spreadsheets or confidential presentations. The US Military discovered this for themselves when portable storage devices containing confidential data were smuggled out of a base in Afghanistan.

US Military

The US Military is battling an embarrassing scandal after USB keys containing secret military information were found for sale in an Afghan bazaar. A reporter obtained several drives at the bazaar and found documents that were potentially embarrassing to Pakistan, a US ally, presentations that named suspected militants targeted for "kill or capture" and discussions of US efforts to "remove" or "marginalise" Afghan government officials whom the military considered "problem makers." The drives also included deployment rosters and other

⁴⁰ "Sun Life Q4 profit up to \$478M from \$438M; reports a day early to prevent leak," Yahoo! Canada Finance (ca.Finance.Yahoo.com), 8 February 2006

⁴¹ "UK businesses lose £billions in Intellectual Property (IP) theft," media release, Ibas UK (Ibasuk.co.uk), 11 May 2004

documents that identified nearly 700 US service members and their social security numbers, information that identity thieves could use to open credit card accounts in soldiers' names. Soldiers are suspected of smuggling the USB keys out of a nearby military base to sell them⁴².

Alongside the risk of intentional misuse, employees who take work home using a portable storage device could inadvertently compromise confidential data by transferring it to a poorly protected personal computer.

Despite the risks, companies are surprisingly lax about portable storage devices. The top two management methods in the UK are nothing (55%) and banning them (33%)⁴³. In Ernst & Young's Global Information Security Survey 2005, even though half of business rated removable media devices as a significant security concern, 57% had no immediate plans to address the risk⁴⁴.

Instant messaging (IM)

The rise of instant messaging (IM) applications like Microsoft's Windows Messenger and ICQ are also opening up new areas of data theft risk. Fifty-seven percent of workers have used IM at work for personal reasons.⁴⁵

Without the right security approach, IM is impossible to monitor. Much like e-mail, IM programs can be used to smuggle files and information out of an organisation, yet conversation threads can't be logged without dedicated software.

Developed as a social chat tool, IM is now surfacing as a handy e-mail alternative to the in-box overflow facing many employees. It's readily available: Windows Messenger is standard with Windows XP, and other applications can be downloaded in a minute.

Yet despite its growing popularity in corporate environments, IM continues to be left out of many enterprise security strategies and policies. Two-fifths of UK companies that allow IM admit to having no controls in place, and only 10% logged messages⁴⁶. Yahoo, the developer of one IM program, became a victim itself in early 2006.

Yahoo

Yahoo has launched a lawsuit against seven former engineers and business development staffers, who are alleged to have confidential business and technical data when they left the company. Archived instant messaging conversations provide the bulk of Yahoo's evidence for the theft of financial forecasts, business strategy documents and even source code. Yahoo

⁴² Watson, P., "U.S. Military Secrets for Sale at Afghan Bazaar", Los Angeles Times (Latimes.com), 10 April 2006

⁴³ PricewaterhouseCoopers DTI Information Security Breaches Survey 2006, April 2006, p20

⁴⁴ Ernst & Young Global Information Security Survey 2005, p14

⁴⁵ Gonsalves, A., "Meta Group: Clamp down on instant messaging," Techweb (Techweb.com), 11 November 2004

⁴⁶ PricewaterhouseCoopers DTI Information Security Breaches Survey 2006, April 2006, p20

claims the employees often switched IM programs to avoid detection. Reggie Davis, Yahoo associate general counsel, said the handful of employees had, "abused our trust."⁴⁷ Yahoo's experience fits with the findings of the PWC DTI Information Security Breaches Survey 2006, which found that technology companies had the most confidentiality breaches, in fact four times as high as the overall level which represents a serious risk because of the importance of intellectual property to the business⁴⁸.

Peer-to-peer (P2P) filesharing

Unregulated use of peer-to-peer (P2P) software can also lead to theft of confidential information. Kazaa, BitTorrent and Limewire all allow users to join file sharing networks where files are downloaded from the user's computer, rather than a central server.

While many employers are aware P2P can be used to download music and other unwanted material onto a corporate network, few know company data can also be made available to other file sharers on the network.

This is most likely to occur when users unwittingly include confidential company files in the list of materials they have agreed to share. For Apple in 2004, P2P became a serious threat when trade secrets were stolen and leaked onto BitTorrent, and the data instantly became available worldwide. Apple's only recourse was to sue for damages.

Apple

Apple is seeking unspecified monetary damages from three men it accuses of leaking a pre-release version of Mac OS X onto the Internet using the P2P network BitTorrent. As a technology company with a high investment in intellectual property, the loss of the information was sorely felt, according to a statement made in the lawsuit. Apple said the tracker on one of the BitTorrent sites indicated that more than 2,500 copies of one version were downloaded⁴⁹.

To complicate matters, many P2P applications come secretly bundled with spyware, or malware. Some of these can record key-strokes to steal information, such as computer passwords, permitting the theft of even more confidential data (see 3.6)

P2P users have also become the target of viruses specifically designed to compromise confidential data. For example, the Antinny virus targets users of the Winny P2P file-sharing application, particularly popular in Japan. It's dangerous as it finds random files on the user's PC and makes them available to other members of the P2P network⁵⁰.

Many enterprises have now taken the step of banning P2P applications through their internet usage policy. However, without the right tools, companies can only police this by regularly scanning and uninstalling P2P applications.

⁴⁷ Borland, J., "Yahoo claims start-up stole trade secrets," ZDnet (ZDnet.com.au), 28 February 2006

⁴⁸ PricewaterhouseCoopers DTI Information Security Breaches Survey 2006, April 2006, p25

⁴⁹ Fried, I., "Apple sues over loose Tiger", CNet News (Cenet.com), 21 December 2004

⁵⁰ "Computer virus highlights problems of Internet security, safety for Japan," Sydney Morning Herald (Smh.com.au), 13 June 2006

Voice-over Internet Protocol (VoIP)

Voice-over Internet Protocol (VoIP) applications are P2P networks that offer telephone services over the internet. Like the P2P networks used to share music and files, they rely on a network of computers to provide resources, including bandwidth, storage space, and computing power. Just like traditional P2P programs, they expose users to the data theft and spyware risks.

In the case of one of the most popular VoIP applications, Skype, VoIP streams are heavily encrypted. In fact, all information above the IP level is rendered unreadable, making filesharing effectively undetectable. This greatly increases the ease with which confidential information and intellectual property can be removed from an organisation.

Nevertheless, VoIP is booming. In the financial services sector, over a fifth of businesses worldwide have already deployed VoIP. A further 17% are currently piloting the technology while 15% are considering doing so over the coming 18 months⁵¹.

Despite, or perhaps because of, the potential telecommunications cost-savings for businesses, its danger goes largely unnoticed. In Ernst & Young's Global Information Security Survey 2005, 21% of businesses identified VoIP as a significant security concern, yet two thirds had no immediate plans to address the risks⁵². Only half of UK companies that have implemented VoIP evaluated the security risks prior⁵³.

Malware and spyware

Often unwittingly downloaded, malware (an umbrella term for malicious software) and spyware, the most concerning form of malware, spy on users, whether by tracking online activity or recording every key stroke.

One of the most paralysing data losses of recent years was the exposure of over 40 million Mastercard customer credit card records, executed through malicious code.

MasterCard International Inc.

More than 40 million credit card details were accessed by a computer hacker, potentially exposing customer to identity fraud. Malicious code caused the massive breach at a CardSystems processing centre in Tucson, USA⁵⁴. It was later revealed CardSystems was not meant to be in possession of the data, and had inappropriately retained it for "research purposes"⁵⁵.

⁵¹ Melek, A & MacKinnon, M., Deloitte Global Security Survey 2005, p31

⁵² Ernst & Young Global Information Security Survey 2005, p14

⁵³ PricewaterhouseCoopers DTI Information Security Breaches Survey 2006, April 2006, p20

⁵⁴ Krim, J. & Barbaro, M., "40 Million Credit Card Numbers Hacked," Washington Post (Washingtonpost.com), 18 June 2005

⁵⁵ Leyden, J., "Unauthorised research opened door to MasterCard breach," The Register (TheRegister.co.uk), 21 June 2005

Key-logging Trojans can also capture highly confidential data, giving cyber-criminals the 'front door key' to your organisation's network and finances, or exposing your company to a legal grey area if an employee's own bank account is hacked after conducting Internet banking at work.

Rootkits can be used to gain access to networks and cover up breaches. Government organisations are more likely to have a problem, with 60% finding a rootkit on their system⁵⁶, while one in five enterprises has reported such a discovery.

Despite high awareness of malware and spyware risks, a quarter of businesses remain unprotected⁵⁷.

Attacks are occurring at a rapid rate. According to the 2005 E-Crime Watch Survey, over 60% of businesses have experienced some form of spyware attack in the last 12 months alone, 85% of those by outsiders. These external attacks reinforce the need to protect the network perimeter.

Combating data theft

Despite the obvious and pressing dangers, only two-fifths of businesses worldwide rate data theft as a threat in the coming 12 months⁵⁸.

Yet if an organisation has left any of their vulnerability points unprotected, they are at serious risk. A 360° approach is vital to preventing data theft.

The basis of any data theft strategy should be a thorough assessment of your organisation's vulnerability points, coupled with an Acceptable Usage Policy that covers handling of confidential information. While these steps can minimise the risk, they can't prevent data theft from happening.

Stopping confidential information from leaving the organisation requires technology solutions at each and every vulnerability point. Yet data theft prevention doesn't have to be a tangle of different security products.

SurfControl believes the only effective approach to reducing the risks of data theft is multi-layered protection that covers all electronic communications, including e-mail, internet traffic, desktop application use, and access to confidential documents.

⁵⁶ Crawford, M., "Rootkits wreak havoc," ARN (ARNnet.com.au), 22 May 2005

⁵⁷ PricewaterhouseCoopers DTI Information Security Breaches Survey 2006, April 2006, p3

⁵⁸ Melek, A & MacKinnon, M., Deloitte Global Security Survey 2005, p27

Best practice

Who's responsible?

Data theft is a risk that cuts across all business divisions and functions. It can be perpetrated by any member of staff, and, as the cases in this white paper show, its consequences can affect the careers of executives at the very top.

More than two-fifths of organisations believe general IT security is a matter for the IT department. Only 15% believe it's the responsibility of business owners⁵⁹.

Most companies believe data theft breaches are the responsibility of the CIO or head of IT, but the same survey showed many businesses simply don't know. 'Unknown' was the third most popular response⁶⁰.

Employees themselves have a responsibility to be aware of confidentiality sensitivities, and to behave appropriately. Business owners and managers are, in turn, responsible for educating staff and ensuring an effective risk reduction strategy is in place.

As an IT security risk however, SurfControl believes it's the IT department's responsibility to ensure business owners and managers are fully aware of the risks and the need for a proper management strategy.

Acceptable Usage Policies

The most effective way of ensuring employees are aware of their obligations when handling sensitive or confidential data is to include these responsibilities in an Acceptable Usage Policy (AUP).

With most data theft breaches the result of staff activity, either accidental or intentional, internal security management and policies are critical.

SurfControl has always promoted AUPs as effective ways to manage staff use of electronic corporate assets, such as desktop and notebook computers and the internet. Good AUPs not only clarify expectations and responsibilities, but they also shield organisations from potential legal liability.

Every AUP should include clear policies about the handling of sensitive and highly confidential information. In 2006, Progressive Casualty Insurance in the US was forced

⁵⁹ Melek, A & MacKinnon, M., Deloitte Global Security Survey 2005, p20

⁶⁰ Ponemon Institute Data Security Tracking Study 2004, in Ponemon, L., "When Employees Are Risky to Your Business," Darwin (Darwinmag.com), 19 January 2005

to let a staff member go after she wrongfully accessed confidential information about foreclosed properties for personal gain. Organisations must be clear about which data is confidential, and who has access to it⁶¹.

To be effective, employers need to ensure staff is aware of, and understand, these policies. Yet despite the obvious advantages of communicating confidentiality expectations to staff, one in eight organisations continues to do nothing to educate employees about their security responsibilities⁶².

360° Protection

The sheer number of data theft vulnerability points, coupled with threats which originate from both inside and outside of an organisation, can only be countered with a viable 360° protection technology solution to prevent data theft

A 360° solution will prevent malware and spyware entering the network, stop outbound leaks at the network perimeter and desktop, and improve ability to manage confidential information internally.

SurfControl's Enterprise Protection Suite is the only offering of its kind to provide simultaneous protection against data theft and other security threats from the Internet—ensuring both inbound and outbound protection; spam; spyware, phishing and keylogging attacks; IM; P2P; gaming and malicious content; artificial intelligence tools, heuristics, custom data signatures and dictionaries to recognize when your sensitive data is about to be communicated.

The suite integrates best-in-class Web, e-mail, and endpoint security solutions. The Adaptive Threat Intelligence Service provides continuous updates and allows for the sharing of threat signatures between all suite components.

SurfControl's 60 Global Threat Experts located in more than 20 countries continuously monitor Internet threats, offering multilingual and multicultural understanding to address the increasingly global nature of attacks.

Extensive human review of signatures and updates avoids miscategorisation or 'false positives' in SurfControl's messaging and web security solutions.

SurfControl has eight multilingual databases, plus an additional layer of protection from the integration of the databases to target blended threats that propagate over multiple entry points (e.g., web, e-mail, IM, P2P).

⁶¹ Vijayan, J., "Data breach at Progressive highlights insider threat," Computerworld (Computerworld.com), 6 April 2006

⁶² PricewaterhouseCoopers DTI Information Security Breaches Survey 2006, April 2006, p3

Customers gain access to the only reporting tool that provides authenticated log-in and access control, with delegated levels of reporting access for users.

SurfControl offers policy-based administration, including automatic enforcement of end user time and bandwidth thresholds, through a graphical interface with drag and drop, real time monitoring of messages, policies and remote access.

About SurfControl

SurfControl plc is the leading provider of enterprise threat protection that shields organizations from known and emerging Internet dangers through Layered Threat ProtectionSM. The Company has redefined traditional "filtering" into a unified set of Web, e-mail and messaging security solutions that continuously filter inbound and outbound Internet traffic to eliminate spam, spyware, phishing and Web and e-mail abuse.

SurfControl provides Adaptive Threat IntelligenceSM from its Global Threat ExpertsSM to respond quickly with automatic, proactive security updates to protect customers. Customers avoid significant business downtime that impacts productivity and the bottom line while limiting legal liability and enforcing regulatory compliance and confidentiality.

SurfControl has more than 20,000 customers worldwide, and employs more than 500 people in offices across the United States, Europe and Asia/Pacific. For further information and news on SurfControl, please visit: www.surfcontrol.com.