

Workshare Global Security Threat Report

January - April 2007

WORKSHARE

THE LEADER IN SECURE CONTENT COMPLIANCE

Contents

Contents	1
Overview	2
Privacy: Threat Activity	3
Intellectual Property: Threat Activity	6
Mobile Workforce: Threat Activity	7
Corporate Compliance: Threat Activity	8
General	9
Security Events	10
Conclusion	10

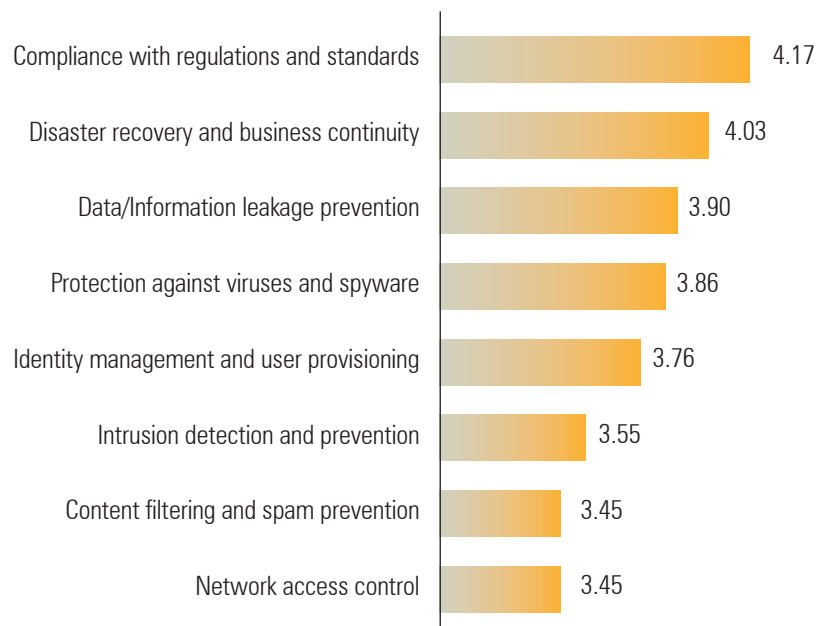
OVERVIEW

Today's businesses are more security conscious than ever before. With exploding amounts of data in circulation the risk of information security breaches, leaks or loss has never been higher than in today's digital world. However, while most organizations and industry commentators have focused their attention on viruses, hackers and malicious information leaks, most have ignored the real threats which are emerging within the four key areas of privacy, Intellectual Property, the mobile workforce and corporate compliance.

The volume of information, web 2.0, and mobility have created a new cause for organizational concern that, while not as troubling for the masses, is the greatest risk to the loss of business information. The risk to organizations in terms of customer loyalty, financial, legal and brand reputation have never been more acute.

The Workshare Global Security Threat Report seeks to highlight the impact that security breaches have on businesses and indeed, on the public. In a world where consumer loyalty is no longer a given, where customer experience can account for 38 per cent of margins, 40 per cent of revenue growth and 38 per cent of shareholder value (Accenture research), then why are organizations failing to take the appropriate measures when it comes to privacy and corporate compliance, and severely lacking adequate protection of their Intellectual Property and mobile workforce? Unless organizations quickly address these key concerns, they will feel the impact when they hear the sound of customer footsteps walking out of the door.

“Please rank how critical these security issues are to you on a scale of 1 (not at all concerned) to 5 (extremely concerned)”



Base: 30 delegates to Forrester's Security Forum EMEA 2007

Source: Forrester Research, Inc.

PRIVACY: THREAT ACTIVITY

SUMMARY

We recently saw a security breach at TJX which security experts are billing as the biggest privacy breach of all time, indicating that the threat to customer and corporate data is now higher than ever before.



KEY EVENTS AND NEWS

GLOBAL

- TJX, parent company to the TJ Maxx brand, revealed that at least 45.7 million credit and debit card numbers were stolen by hackers who accessed their computer systems at the TJX headquarters in Framingham and in the United Kingdom over a period of several years. TJX, which runs more than 2,500 stores worldwide, is facing an investigation by the Federal Trade Commission and numerous lawsuits from individuals and banks. The security breach has already cost the retailer \$5 million for the investigation and new computer security, among other efforts, but TJX said it cannot yet estimate total losses – March 07

EU

- Datamonitor announced the results of a survey of 1400 large enterprises across the US, UK, Australia, France and Germany. The findings show that only 6 per cent of companies can say with confidence that they have not experienced data leakage problems in the past two years. The research quantifies the cost of a data breach and states “the average cost of a data breach was estimated to be \$1.86m”. In addition, “states such as California now require companies to inform their customers when a data leak has taken place, and companies estimated that this notification process alone costs on average \$268,000.” – April 07

- 84 per cent of UK residents want to be informed if their personal data is lost or stolen after a corporate security breach, the latest E-Communications Household Survey from the European Commission (EC) has revealed. The study of 27,000 households across Europe highlights that people in the UK are more concerned about obtaining data breach details than other Europeans (85 vs. 75 %). The results could provide further evidence of the need for US-style data breach notification rules to be rolled out in the UK and across Europe – April 07
- The German Finance Office started investigations of bank customers from Julius Bär. A former employee from Julius Bär wanted to take revenge on the bank for personal reasons. He was burning a CD with delicate facts about customers when he was employed. Later he sent it to the German Finance Office. The customers now have to face a penalty for committing tax evasion – April 2007

APAC

- A review of the Privacy Act has resulted in a push for tougher data protection standards. Federal privacy commissioner, Karen Curtis, has called for tougher standards in Australia to force organizations to notify customers of a security breach that exposes customer information. Curtis said forcing organizations to notify customers of a breach is a “strong market incentive” that will encourage organizations to adequately secure databases and increase customer trust – March 07
- Fraudsters defrauded 49 Jaccs Co. credit card holders of a total of 6.67 million yen in a personal data leak case involving 150,000 of its customers. The data, which included names, addresses, telephone and card numbers, were used to purchase personal computers and other merchandise via the Internet. The 150,000 cardholders were from a wide area ranging from Hokkaido and the north eastern region of Tohoku to the Kanto area surrounding the Tokyo metropolitan area. The leaked data had been put in the custody of Dai Nippon Printing Co. for direct mail printing. The data was then duplicated by a former employee of a software house to which Dai Nippon had outsourced data input work. The person subsequently sold part of the duplicated data to a group of fraudsters. The Metropolitan Police Department arrested the person as well as three members of the group in connection with the data leakage – February 07

- Identity theft costs Australia an estimated \$3.5 billion annually. Michael Coomer, of Westpac, said that “identity fraud and theft is the greatest challenge facing financial institutions over the next decade.” Business and government leaders around the world are concerned about identity fraud not merely from a financial point of view, but also for because it may undermine trust between corporations and governments and clientele and citizens. The rise of internet banking and the development of a national access card (smartcards) have increased fears of infringements of privacy – February 07

US

- The US Government Accountability Office (GAO) has issued a 78 page report called Privacy: Lessons Learned About Data Breach Notification. The report primarily addresses notification – when to notify and offer credit monitoring services. Key implications are increased focus on incident management, including PR, notification and risk management; and increased impetus in the federal government space to buy products that handle breach incident reporting, risk management and process. This type of focus will often flow out into other countries and sectors – April 07
- JP Morgan Chase has alerted thousands of its Chicago-area millionaire clients, as well as some of its own employees, that it can not locate a computer tape containing their account information and Social Security numbers. The tape, which was in a locked container, was being transported from a bank location to an off-site facility last month when it went astray, a JP Morgan spokesman said. It is not clear if the tape arrived at its destination or was lost along the way. The tape contained data from JP Morgan’s private-client services business, which provides financial services to clients who have a net worth of between \$1m (€733,135) and \$25m, the spokesman said. The tape also included data belonging to JP Morgan employees. Some 47,000 accounts were affected – May 2007
- Computer equipment containing files with sensitive information of nearly 160,000 current and former employees of the Neiman Marcus Group has been stolen. The files were in the possession of a pension consultant and included each person’s name, address, Social Security number, date of birth, period of employment and salary information. There is no evidence that the personal data was the target of the theft, however Neiman

Marcus has contacted all affected individuals and has paid for credit monitoring services for all involved for at least one year – April 07

- Caterpillar Inc. has announced that a laptop computer containing personal data on employees was stolen from a benefits consultant that works with the company. Although it is not confirmed how many employees were affected, the majority are based in the U.S. and letters have been sent to notify them. In addition a call centre has been set up and increased security measures are being put in place – April 07

- The social security numbers of 63,000 people who received Agriculture Department grants have been posted on a government website since 1996, but have only just been spotted and removed. Free credit monitoring has been offered to those affected at an estimated taxpayer cost of \$4m, and the case has raised the question as to whether those states (including Washington, where the incident occurred) without legislation to ensure individuals are notified in the event of a breach, should implement it – April 07

DEVELOPMENTS TO WATCH

EU

- Consumers are demanding data breach disclosure. A recent UK survey showed that 82% expected institutions that suffered a breach to notify those affected automatically – April 07
- Lord Alec Broers, from the UK’s House of Lords select committee on internet security, recently stated that the introduction of a law forcing disclosure of serious data breaches, similar to that operated in the US, was likely. “Of all the possible recommendations, we are likely to recommend strongly that a breach law be introduced,” he said. However, Lord Broers also conceded that by the third or fourth disclosure, the public might begin to lose interest in the reports – April 07

APAC

- Laws designed to combat the multi-billion dollar problem of identity fraud in Australia were up for public consultation by the Minister for Justice and Customs, Senator David Johnston. “This discussion paper highlights a serious social problem and I would

- encourage comments from all interested members of the public, community organizations and business groups on these proposed reforms,” Mr Johnston said – April 2007
- As a part of its ‘Trusted Sourcing’ initiative, Nasscom announced the appointment of Shyamal Ghosh as the chairman of the proposed independent self-regulatory organization (SRO) to make India a better outsourcing destination. The SRO initiative came in the wake of allegations in the US and the UK that the country’s call centre workers have stolen and sold data processed by local outsourcing/BPO firms. Its objective is to raise the bar in data security and data privacy by including the best practices currently stipulated by certifications such as ISO17799 for information security by the International Organization for Standardisation in Geneva, as well as data privacy and data protection laws worldwide – April 07
 - Karen Curtis has recommended to the Australian Law Reform Commission (ALRC) that changes to the Privacy Act may be necessary to reflect technological developments. One of the proposals suggests that “... organizations should be required to notify customers of a security breach...” – March 07
 - Data leaks equal 8 per cent drop in revenue – one in five companies hit. The IT Policy Compliance Group released research showing 20 per cent of enterprises suffer from more than 22 sensitive data losses per year. The most sensitive losses include customer, financial, corporate, employee, and IT security data, which is either stolen, leaked, or destroyed, according to the research report entitled “Taking action to protect sensitive data.” – March 07

INTELLECTUAL PROPERTY: THREAT ACTIVITY

SUMMARY

Intellectual Property and privacy rights are truly a global issue. As the amount of data in the world continues to grow, businesses and organizations are discovering they must take precautions in order to protect the information which they are creating.



KEY EVENTS AND NEWS

EU

- With counterfeit DVDs and luxury goods widely available on the streets in China, the country's position on intellectual property rights is increasingly becoming a source of tension with its trading partners. Weeks after the US made a formal complaint, EU trade chief Peter Mandelson has threatened WTO action against Beijing – April 07
- A UK report from the Enterprise Strategy Group demonstrated that fear of intellectual property theft has become such a priority that 90 per cent of companies plan to deploy new technologies to secure their information in the next 12 months – March 07
- Two former Ferrari engineers accused of stealing trade secrets have been convicted of industrial espionage. Sensitive data stolen from Ferrari – including engineering documents, test data and other undisclosed documents – was allegedly used to develop the 2002 and 2003 edition of rival Toyota's car. Security firms were quick to highlight the case as an example of the dangers of uncontrolled use of removable storage devices in facilitating data theft – April 07

- A Chinese delegate visiting a German company was found under a desk connecting a USB stick to one of the company's computers; though in this instance the German company did not file charges. 80 per cent of German firms have said that they have been victims of cyber crime, though only 11 per cent reported it, as firms do not believe that the police would be successful in finding the delinquents. In Germany there is a growing, reported fear of spies who steal information and of plagiarism – April 07
- Germany now also has to face a general trend of hackers from China attacking companies with the purpose to gain information for economical and commercial use, says Hans Elmar Remberg, vice president of the Federal Office for the Protection of the Constitution. Furthermore, there is increasing coverage of this topic in the German media – February 2007

APAC

- Police stated that they will join with the Self-Defence Forces in investigating a case in which a Maritime Self-Defence Force petty officer secretly came into possession of confidential data on the high-tech Aegis defence system – April 07

US

- Cingular Wireless' latest Palm Treo 750 was posted on the web one week before the planned announcement date through a sales presentation leaked to website Engadget Mobile – April 07

DEVELOPMENTS TO WATCH

EU

- General availability of Apple iPhone in Europe later this year. These devices can store up to 8GB of data and could potentially trigger a rise in 'podslurping' – when the mass storage devices are used to steal corporate information

MOBILE WORKFORCE: THREAT ACTIVITY

SUMMARY

High-profile cases of lost or stolen laptops, and data leaks due to an increasingly mobile workforce, continued to hit the headlines this year. Companies and organizations affected included Nationwide, HSBC and the NHS.



KEY EVENTS AND NEWS

EU

- In the UK, financial institution Nationwide was fined almost £1m after a laptop was stolen from employee who took the equipment out of the office in order to work from home – February 07
- UK building society Halifax was forced to apologize to customers when a briefcase containing details relating to some 13,000 mortgage owners was stolen from an employee's car – March 07
- According to PriceWaterhouseCoopers, 50 per cent of misuse and theft of data is caused by employees. They are often unsatisfied with their job or think they are underpaid. These circumstances cause them to act in a way which damages the firm – April 2007
- German companies are frequently noting that others are committing industrial espionage by sending interns to work within their firms. These people, often coming from Russia or China, misuse their access to the companies to steal formulae, construction plans or other data – April 2007

APAC

- HSBC Australia exposed more than 100 customers banking details and other personal financial information. Later on, HSBC customers expressed outrage at the bank's handling of the security breach. It was felt that commercial interests were favoured over privacy – April 07

US

- Defence contractor Lockheed Martin Corp. has announced that a "concerned citizen" found one of its computer memory sticks at a filling station in Azle, Texas. The stick contained information about the Joint Strike Fighter, the nation's most expensive weapons program. A Lockheed employee "inadvertently dropped" the device, the company said. It said the stick contained no classified information and the employee was authorised to have it, however the incident has provoked investigations by both the US Air Force and the FBI – April 07

DEVELOPMENTS TO WATCH

EU

- New entries into the mobile working space. In April BT launched Office Anywhere, a combination of data services and mobile applications aimed at workers who spend a lot of time on the road. The more information employees are sharing on the go, the greater the risk of a mobile data breach.
- The German association BITKOM is warning that devices like smartphones and PDAs will be increasingly become targets for criminals. Compared to laptops, these devices are less secure. BITKOM is offering a brochure with a checklist for the safe handling of such devices – April 2007

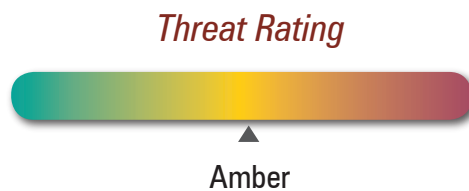
APAC

- IDC: global mobile device forecast

CORPORATE COMPLIANCE: THREAT ACTIVITY

SUMMARY

Changes in the US and increasing calls for legislation around data storage and data breaches means the compliance arena is certainly starting to heat up when it comes to information laws.



KEY EVENTS AND NEWS

EU

- Recent changes to the Federal Rules of Civil Procedure (FRCP) require all US companies to know where electronic documents are stored and to be prepared to make corporate email available to the court in case of a lawsuit. Subsidiary companies based in the UK may also be affected by these new regulations – March 07

APAC

- A university has extended its messaging platform to public Instant Messaging. It stated that third-party access is key for collaborative research – April 07
- Macquarie meets new global security standard – ISO 27001 replaces Australian certification. Bill Trussell, managing director of TIP's security sector, said it is a trend that cuts across industry and corresponds with growing concerns about the consequences stemming from data breaches – April 07
- IDC has said that IT departments must convince executives of security's business value. Microsoft Australia's chief security officer Peter Watson said security is now being considered as an enabler of technology, specifically with mobile devices, rather than "an expensive means of peace-of-mind". IDC's senior analyst Patrick Bihammar said it is unlikely that Australian IT security regulations will mirror those in the US despite the country's condensed, wealthy IT

industry being an "easy target". "Australia is a big target for identity and data theft because we have a small, rich industry that often has [lax] security measures," Bihammar said. "Local compliance is driven more so by Europe than the US, but we tend to take a best-practice and common-sense approach to avoid the risk of legal problems and [red tape]." – April 07

"Does your organization have a policy for notifying customers when their private data may be at risk?"



Surprisingly, 48% of organizations still don't have a policy for notifying customers when their private data may be at risk, as shown above.

Source: IDC Security Survey 2006

DEVELOPMENTS TO WATCH

EU

- Currently UK organizations that lose sensitive customer or employee data, or expose it to others, do not have to disclose details of the breach, even to those affected. Now, in the wake of recent data losses, security experts have called on UK legislators to bring laws in line with US law SB 1386, which was introduced in California in 2003 and has spread to 34 states, requiring full disclosure.

GENERAL

EU

- In April, thousands of IT security specialists gathered in London for the annual Infosecurity show. Top of the discussion agenda was identity management, both in the private and public sectors. Further education for the general public and within businesses was also discussed, especially regarding its role to play in combating online crime – April 2007
- At CeBIT 2007 (leading business event for the digital world), one major topic regarding IT security was system software. There are new solutions which combine different protection measures with a central configuration and administration. The new products mainly focus on small and medium-sized enterprises. Participants also discussed the enforcement of security guidelines for clients (work stations, mobile devices etc.) logging onto a firm's network. Other trends were proactive protection as well as protection against root kits and similar threats – March 2007
- The ASW (Arbeitsgemeinschaft für Sicherheit der Wirtschaft: working group for security in the German economy) announced the results of a survey where German companies were asked about their biggest worries. Internet attacks against their IT security systems were top of the list. 79 per cent of the companies expect a growing risk caused by hackers infiltrating their computer networks. 77 per cent are afraid of viruses from the internet. 87 per cent of the companies anticipate growing expenses for data security – April 2007
- The European Union is planning a project called "European Information Sharing and Alert System (EISAS) which aims to warn small and medium-sized companies against security leaks. There will be a web-based security portal using an RSS feed and SMS to warn the enterprises against threats. The European Agency for Net and Information Security has also started to conduct a survey to find out how security leaks in European companies can be identified and how companies can be provided with advice to fight those threats – April 2007
- During CeBIT 2007, Heinz-Paul Bonn, vice president of the association BITKOM, announced that small and medium-sized enterprises will focus on systems for mobile communication as well as solutions to improve their IT security in the future – March 2007

APAC

- Australian IT security professionals set to embark on huge spending spree – security software developed in-house faces extinction. IDC's security system management analyst, Patrik Bihammar, said the local security market will increase from \$850 million to \$1.3 billion in less than three years – April 07

SECURITY EVENTS

- **DC Security and Continuity Conference – May 07**
<http://www.idc.com.sg/Security2007/default.asp>
- **AusCERT2007 Conference - Internet Security for CFOs – May 07**
<http://conference.auscert.org.au/conf2007/cfp2007.html>
- **Security 2007 – July 07**
http://www.securityexpo.com.au/page/seminars__events.html
- **Gartner: Business Continuity Planning, Critical Infrastructure Protection, Customer Security and Privacy, Managed Security Services, Securing the Workplace, Security Software, Security Strategies – August 07**
<http://www.gartner.com/EventsCal>
- **BKA (Bundeskriminalamt: Federal Criminal Police Office) / ASW (Arbeitsgemeinschaft für Sicherheit der Wirtschaft: working group for security in the German economy): economic conference – May 2007**
<http://www.asw-online.de/veranstaltungen/2007/07-05-07-BKA-ASW-Wirtschaftskonferenz-2007.php>

CONCLUSION

Today, organizations are at risk of breaching security every time an email is sent, a document written, a file downloaded onto a laptop or USB stick, or material printed off and put in a briefcase. While this threat can never be fully prevented, organizations can no longer place the responsibility for information protection solely on their employees. While nearly every employee is focused on their job, the amount of information and Intellectual Property in circulation, the mobility of workers, and the volume of information being shared means that processes and systems need to be put in place to enable users of the data to carry out their work, safe in the knowledge that what they handle is secure.

Whether securing information means cleansing documents

of confidential data, preventing employees downloading documents from the central server onto their laptop, or indeed only allowing authorised personnel to see a document sent via email, organizations must embrace and adopt information leak prevention solutions. The next few years will see the rise of inadvertent information leaks, now is the time to take action before they hit your organization.