

Deloitte.

Technology, Media & Telecommunications

Protecting the digital assets.

The 2006 Technology, Media &
Telecommunications Security Survey

Audit. Tax. Consulting. Financial Advisory.

Foreword

Digital information and digital technology have become the lifeblood of the technology, media and telecommunications (TMT) industry. This fundamental shift is creating tremendous opportunities and, for savvy companies, considerable value. But the move to digital also presents significant new challenges and risks, including security threats such as computer viruses and intellectual property theft that can disrupt or even disable a business.

In the aftermath of the dot-com bubble, TMT companies have generally had their hands full dealing with major challenges such as uncertain economic conditions, rapid technology advances and digital convergence – and, as a result, may have overlooked security. But many are now realizing that security is simply an integral part of conducting their business and thus too important to ignore.

Against this backdrop, the Deloitte Touche Tohmatsu (DTT) TMT Industry Group, made up of DTT member firms' TMT practices, conducted an in-depth survey of security practices at TMT organizations around the world, primarily through face-to-face interviews with senior security executives.

The survey of 150 TMT organizations shows that although TMT businesses are making significant strides to improve their security, they still have much to do. This report examines the industry's security issues in greater detail, and provides a number of specific insights to help companies protect their information and digital services.

Igal Brightman.

Igal Brightman
Global Managing Partner
DTT Technology, Media & Telecommunications Industry Group



Executive Summary

Security has long been neglected in the TMT industry and the problem continues today – despite the TMT industry’s growing reliance on digital information and technology. This inadequate response has left many TMT companies critically vulnerable to attacks.

Over half of the TMT companies surveyed suffered a security breach in the preceding 12 months. Some companies surveyed reported breaches causing millions of dollars’ worth of damage. And both the frequency and sophistication of the attacks are growing. Yet many companies continue to underestimate the need for security.

Common shortcomings include:

- Inadequate resources and funding
- Ineffective actions that do not address the latest threats
- Lack of awareness and management support
- Insufficient attention to internal risks
- Failure to plan for serious attacks and business disruption.

Part of the challenge is that many companies do not appreciate the full magnitude of the problem. Although companies that have been the victim of security breaches are able to appreciate the direct impact and financial losses that ensue, they often overlook indirect and intangible factors such as brand damage, customer dissatisfaction, market erosion and lost productivity.

The survey suggests that companies that have developed strategies, policies and procedures are much less likely to experience security breaches or financial losses. Yet most TMT companies surveyed are not investing enough time, money and resources to protect themselves adequately. In fact, many TMT executives surveyed believe their companies are “falling behind” – or at best “catching up.”

Carefully structured and managed security may not be a substantial source of sustainable competitive advantage, but it is certainly a critical part of any mature and well managed business in the 21st Century. Customers instill a great deal of trust in contemporary TMT companies, and may increasingly migrate towards those which are able to demonstrate a comprehensive and credible approach to securing all of their digital assets, processes and transactions.

Introduction

Information security is commonly considered to revolve around three fundamental principles: confidentiality, integrity and availability. In most businesses, that translates into protecting the company from unauthorized access to property and information, preventing fraud and embezzlement and avoiding business interruption. But in the TMT industry, security also relates to the protection of digital media, content, intellectual property and services.

Security incidents are in the news every day, and the overall risks are growing¹. TMT companies are particularly vulnerable because their businesses increasingly revolve around digital information and technology. For example:

- Technology companies are increasingly using offshore resources to accelerate product development cycles. While this approach saves time, it may increase vulnerability to intellectual property theft².
- Media companies are increasingly creating their content in all-digital form, and distributing it online. While this has created a market for digital music downloads that is already worth in excess of \$1 billion, it has also created multiple opportunities for theft, data corruption and large-scale piracy.
- Telecommunications companies are increasing the launching of Voice-over-Internet Protocol (VoIP)-based services, which exposes phones to the risk of viruses.

The list of external threats includes everything from viruses, spyware, worms and trojans to denial of service attacks, wireless network breaches and social engineering (that is, tricking people into divulging confidential information in order to impersonate them). And while TMT companies are gradually expanding their focus on security to combat these threats, DTT's 2006 TMT Security Survey indicates that hackers appear to be consistently a step or two ahead.

More than half of the companies surveyed said their systems were breached over the last 12 months. Even worse, both the magnitude and complexity of the attacks are increasing. Roughly a third of the breaches reportedly resulted in a significant financial loss of up to several million dollars³. And that is even without considering the indirect and intangible losses – such as damage to the company's reputation and brand, system down time and lost revenue – which can add up quickly. Even by conservative estimates, the indirect cost in terms of lost revenue alone can easily exceed \$12,000 per employee⁴, for each virus-infected PC.

TMT companies face a bewildering and growing list of digital threats, which derive both from the digitization of their own commercial operations to the increasing number and diversity of malicious and criminal digital activities.

DTT's 2006 TMT Security Survey looked at what TMT companies around the world are doing to secure their businesses and protect them from attack. Most of the data was gathered through structured, face-to-face discussions with security executives and security management of TMT clients of DTT member firms around the world. In total, TMT companies from more than 30 countries participated.

The survey identified the types of security threats that are of the greatest concern to TMT companies and the level of resources being used to address them. It also examined which technologies are being implemented to improve security and the value TMT companies are deriving from their security investments.

About the survey

DTT member firms' TMT practices undertook a survey to help TMT companies benchmark their security activity investments and efficacy as compared to their peers around the world. Data was gathered through structured, mostly face-to-face discussions between TMT security specialists of DTT member firms and TMT companies. Respondents were typically: Chief Information Security Officers (CISO), Chief Security Officers (CSO) or security management teams. 34 percent of responses were from the technology sector; 24 percent from the media sector and 42 percent from the telecommunications sector. Responses were from all regions: Europe, Middle East and Africa (60 percent), the Americas (24 percent) and Asia Pacific (16 percent). All submissions were anonymous.

The survey identified the types of security threats giving greatest concern and the level of resources being used to address them. It also examined which technologies are being implemented to improve security and the value TMT companies are deriving from their security investments. Specific interview topics included:

- Governance
- Investment in security
- Value
- Risk
- Responsiveness
- Use of security technologies
- Quality of operations
- Security of Intellectual Property, Digital Media, Data Piracy.

The global survey included 150 technology, media and telecommunication companies from more than 30 countries, covering every major region.

Threats outpace investment

TMT companies struggle to stay abreast of growing threats

Despite their ever increasing reliance on information technology and digital media, most TMT companies still appear to lack a sense of urgency around security. Although 73 percent of companies surveyed expect to spend more time and money on security in 2006, the average budget increase is expected to be just nine percent. And only one in 12 expects to increase its security budget by at least 20 percent. In general, DTT TMT Industry Group's view is that this increase is not enough to keep pace with the growing list of challenges, which include increasingly sophisticated attacks, emerging technologies, and concerns about privacy and piracy.

The majority of TMT companies surveyed consider themselves "reactive" when it comes to investing in information security. 54 percent of Chief Security Officers (CSOs) believe their companies' security investments are "falling behind" the threats – or at best "catching up". Few companies (only four percent) believe they are doing enough to address the problem.

Given recent trends in corporate governance, accountability and privacy, it might seem that senior executives would be strong proponents of security. Yet more than half of the companies in the survey specifically cite budget constraints and lack of management support as the main challenges to achieving their security goals.

Bottom line

TMT companies must recognize just how important an issue security is. The TMT industry stands to gain handsomely from digitization. Yet it is also now one of the industries most exposed to the risks of digital disruption and crime. And the level of exposure is growing daily.

Everything from voice telephony to prime time television is now created and transmitted as a series of zeros and ones – making it vulnerable to infection, attack and theft. Moreover, TMT companies must recognize that they represent an increasingly attractive target. Media companies' content represents the basis of a global market in illegal downloads and counterfeit goods; telecommunications operators increasingly represent the gateway into the digital home and office.

More often than not, digital security attracts management interest only after disaster has struck. But this approach is not tenable for companies whose livelihoods increasingly depend on the capacity to communicate, produce, distribute and transact in digital form. Reactivity is becoming an increasingly inappropriate approach: proactivity is now becoming an imperative. Indeed, security has to be seen as an investment in business continuity, and as such companies must recognize that continuous and growing investment is required in order to keep step with the evolving techniques and strategies of the criminal fraternity.

It is likely that digital crime will increasingly be committed by organized gangs, rather than individual opportunists. Though these gangs can be large and well resourced, they are minnows by comparison to the titans of TMT. In other words, if TMT companies act now – individually and in concert – they have the strength, the resource and the reach to have a very substantial impact. They may never stop criminals altogether, but they can certainly put up a formidable fight – and win many battles.

Top Five emerging security threats⁵

- **Instant Messaging (IM) spreads viruses and worms:** the growing popularity of instant messaging as a form of corporate communication is extending the risk of infection. IM is often used by employees without the approval or knowledge of the IT department. Viruses, worms and other malicious code can easily be embedded into the messages received by employees, and can make their way into corporate networks with relative ease.
- **Phishing fraud becomes more prevalent and sophisticated:** At present, phishing scams are primarily focused on the financial services industry. But as the number and variety of online transactions grows, and consumers give out sensitive personal data more frequently, it is likely that phishing operations will target a wider range of sectors, corporations, and individuals.
- **Viruses attack cell phones and PDAs:** Last year, the number of viruses and worms that affected cell phones and PDAs increased dramatically. Antivirus software is not yet widely used in mobile phones, and they therefore represent an easy target. And as increasingly sophisticated phones synchronize with corporate networks, the risk of infection extends way beyond the mobile device - into corporate IT infrastructure.
- **Hackers target online brokerage accounts:** The practice of using malicious code to crack passwords and obtain sensitive personal data is likely to extend beyond online brokerages. Indeed, the TMT sector is a prime target, with a growing number of consumers paying for services and content online. This trend has the potential to disrupt growing consumer confidence in e-commerce and the growing range of online services.
- **Internet crimes go unreported:** Although the number of reported Internet crimes rose in the past 12 months, comparatively few victims filed a report or notified the police. As a result, the true extent of digital crime is probably being underestimated. Not only does this situation make catching criminals more difficult, but it also makes the process of protecting against new types of criminal activity less effective.

Source: Department of Homeland Security and National Cyber Security Alliance, 2006

Open to attack

TMT companies remain vulnerable to a variety of threats

Effective security responses require clear strategies, clear procedures and clear responsibilities and accountability. The survey results suggest that companies with a formal security strategy are much less likely to experience security breaches or financial losses. Moreover, many of the companies surveyed that experienced a breach do not have a formal information security policy.

According to the survey, only 63 percent of TMT companies have a dedicated, senior-level security officer (or are in the process of appointing one). Surveys show that this figure is lower than for other industries that are less reliant on digital information and technology. Even among technology companies, which some might argue should know better, the proportion with a dedicated security officer is only 53 percent.

Most security activities undertaken by TMT companies limit their security policy to the basics, such as firewalls, anti-virus applications, spam-filtering and virtual private networks. Yet more advanced threats are not being adequately addressed. For example, phishing is considered to be a major threat to TMT companies, yet only 18 percent have currently implemented anti-phishing technologies, and only seven percent are currently piloting technologies in this area.

Moreover, the effectiveness of security activities in TMT appears relatively low. According to the survey, 24 percent of TMT companies do not believe the security tools they have deployed are being used effectively and 26 percent have not implemented a security incident management solution to help identify and track security issues.

Bottom line

TMT companies can no longer afford to have an opaque or ad-hoc approach. A formal policy on security, and a dedicated individual (or team) in charge of every aspect of corporate data security and integrity are no longer optional extras – they are absolute essentials. Deploying, managing and optimizing security is a full-time job, and one that requires very specific skills and competencies. All TMT companies should move to establish a formal security office, with clear systems, policies and procedures, as soon as possible.

Moreover, companies should recognize that the security of enterprise systems and data is a moving target, requiring constant revision, reassessment and scrutiny. This recognition has to come from the top – and senior executives need to lead the drive for tighter security across the board. There must be a continuous internal dialog, informed by the need to raise the effectiveness and sophistication of all security activities, to ensure that the company strives to protect itself and its assets from every possible angle of attack.

Doing so is likely to be increasingly important to customers. Customers confer a huge amount of trust – and personal data – in TMT companies; particularly those whose primary route to market is the Internet. As the public at large becomes more aware of the myriad of security threats and risks, they will likely migrate towards TMT companies that demonstrate the greatest commitment to optimizing security – not only of their own assets and data – but also those of their customers. In this respect, therefore, investment in security can be seen as a considerable strategic opportunity.

The impact of regulation

Developments in corporate governance and privacy regulations are fueling the security activities at many TMT companies. According to the survey, 74 percent expect to spend more time in the coming year on information security due to governance and privacy regulations. Only six percent believe they are ahead of the requirements.

National regulations put greater emphasis on privacy and accountability at all levels of the organization. For example:

- In the European Union's member states, companies are required to implement technical and organizational measures to ensure adequate security and confidentiality⁶.
- In the United States, many states require that companies formally disclose security breaches. To date, at least 21 states have finalized or proposed breach notification laws similar to those in California, which state "any agency that owns or licenses computerized data that include personal information shall disclose any breach of the security of the system following discovery or notification of the breach in security of the data"⁷.
- In Japan, the **Act on the Protection of Personal Information**, which took effect in April 2005, protects the rights and interests of individuals by regulating how personal information is handled⁸.

Everybody's problem

Security requires awareness and education at every level

Although recent trends in corporate governance and privacy legislation have made security a higher priority than ever, the survey shows most TMT companies (52 percent) still treat security as an IT issue: only one in three considers security a C-suite level responsibility. And only one in five considers its board "very well informed" on security topics. That probably should not be a surprise, however, given that only 26 percent of TMT security executives surveyed report directly to the board.

Lack of awareness at lower levels of the organization is also a major problem. Every worker at every level needs to understand the company-wide impact of lax security. Although 76 percent of respondents believe their employees accept responsibility for protecting corporate information, systems and facilities, the vast majority do not provide regular and up-to-date training.

Only 37 percent of respondents had provided security training to their employees in the last 12 months. Moreover, only 33 percent use classroom training, which some argue is preferable to e-learning for teaching complex issues, such as security⁹.

Monitoring employee activity on systems and networks can help validate the training; however, only 59 percent of respondents currently have such tracking mechanisms in place. And only a third have implemented a self assessment or awareness program to facilitate compliance with security regulations and procedures. More than 30 percent of the companies surveyed believe their employees below the management level are not well informed.

Bottom line

The role of managing security is not just a matter of knowing which technology, software and policies to put in place; it is also an issue of monitoring the activity of employees, contractors and others. The easiest way for a criminal to get hold of a user name and password is to ask for them – and the larger the company, the easier it is for a criminal to pretend to be a diligent network administrator or similar role. Periodic communication and relevant training are therefore also critical, so that all employees and partners know who and what to look out for, and when to raise the alarm.

Every employee has a role to play in maintaining and monitoring security; a company's security is only as strong as its weakest link. As a result, companies must seek to ensure that employees at every level, in every function, are adequately trained and aware. Individual and departmental effectiveness should be monitored and assessed on a regular basis to ensure widespread understanding of the seriousness of the issue.

Companies should also consider informing their customers of the security measures taken. Making customers aware of the lengths that a company goes to in order to protect their privacy, security and integrity has the potential to be received positively, and contribute to brand equity. Doing so not only helps customers to become more security aware, but also has the potential to increase their confidence in using a wider array of digital services.

The enemy within

External threats get most of the attention, but internal threats may be a similarly significant risk

External security threats such as phishing, pharming, viruses and worms get most of the attention, as well as the lion's share of resources. Yet the risks from internal threats such as fraud, employee misconduct and human error may be just as great. Among TMT companies whose security had been reportedly breached in the preceding 12 months, half were attacked from outside the company, and half from within.

That might explain why many TMT companies lack confidence in the security of their internal IT infrastructure. According to the survey, most companies feel they are better protected from outside threats than inside threats. Only 47 percent of respondents are "very confident" that their infrastructure is properly protected against internal attacks, as opposed to 63 percent for external attacks. And 83 percent are concerned about employee misconduct involving information systems.

In the preceding year, the two biggest internal threats were "insider fraud" and "leakage of customer data", cited by 25 percent and 22 percent of respondents respectively. Looking forward, the internal threats TMT companies are most worried about include: employees sending out confidential information via email to unauthorized parties (67 percent), employee misconduct (57 percent), and theft of intellectual property (52 percent).

The 2006 TMT Security Survey also showed that while most TMT companies use advanced systems to filter email content, the vast majority only filter incoming messages in order to mitigate external threats such as viruses, worms and spam.

Portable media devices such as memory cards, MP3/MP4 players and writable CDs also pose a significant threat: the largest memory sticks can now hold 64 gigabytes of information¹⁰, sufficient to store volumes of confidential data. While most corporate networks are relatively secure, critical business information stored on portable devices remains extremely vulnerable to theft and losses. One way to effectively address this problem is to use only portable storage devices with strong encryption, making it extremely difficult for unauthorized individuals to read the data.

Bottom line

The threat posed by companies' own employees is becoming as immediate and insidious as external threats. For example, of the tens of thousands of movies illegally posted on file-sharing websites, it is estimated that well over 70 percent were 'leaked' by studio employees¹¹, rather than directly stolen by criminals. This one example is costing the TMT industry potentially tens of millions of dollars in lost revenues.

Though many companies shy away from monitoring employees for potential malpractice, doing so is now essential. For all companies, email filtering should be used to encompass outgoing as well as incoming mail, so that messages containing restricted data can be blocked (and other action taken where appropriate). Portable computers, Personal Digital Assistants (PDAs), smart phones and other devices that can be taken away from company premises should be strictly monitored – and should only be issued to employees with a business-critical need. Where appropriate, restrictions should also be placed on the use of personal data devices in the workplace.

Additionally, employees' use of portable digital storage devices should be carefully monitored – and in some cases, prohibited altogether. For example, a number of movie studios and production companies have already instituted clean-room conditions, such that employees may not enter or leave carrying anything other than the clothes they are wearing. Severe though this may appear, it has proven an effective means of protecting valuable files.

Staying in business

Security attacks are more than a nuisance – they can disrupt a business

Security-related business disruptions are a major concern now that TMT companies have become so reliant on digital information and technology. Businesses such as digital television and radio, online music sales, and VoIP telephony systems can be completely shut down by security attacks. The same goes for web advertising and digital media distribution. In these TMT businesses, service disruption translates directly into loss of customers and revenue.

Moreover, in today's technology-reliant business environment, many companies depend on the Internet and other technologies for critical services such as communication, supply chain management and procurement. This means that even traditional businesses are vulnerable to disruption and attack.

Despite the widespread threat of business disruption, the survey shows that only 48 percent of TMT companies have an enterprise-wide program to manage business continuity. This is well below the average in other industries. For example, in a recent survey across multiple industries in the United States¹², 83 percent of respondents had formal business continuity plans.

Bottom line

Security breaches are capable of bringing entire companies to their knees – sometimes for days, rather than just hours. There are countless examples of viruses, worms, hackers and other malicious activities costing companies dearly, as everything from reservation systems to decision support systems are taken down.

No company is entirely impervious, no matter how seriously they invest money and management time in bolstering security. As a result, knowing how to respond to a breach is as important as having multiple lines of defense in place.

Planning sits at the heart of business continuity – knowing who should do what, where, when and how – can make the difference between inconvenience and catastrophe. Clearly, companies should have redundant systems ready – but only if employees know how to use them. Practice and training are therefore important – so that when a real incident happens, employees know how to react, and how to keep the business running as smoothly as possible.

Companies must remember that the threat to security extends way beyond the desktop computers and company servers. IP telephones and exchanges, call centers, mobile phones, PDAs, point of sale devices and even automated production lines are all potentially vulnerable – and all must be included in disaster recovery planning.

Investment in business continuity and disaster recovery is about more than just security – it is good business practice for any company whose business relies heavily on technology. There is a huge amount of accumulated expertise and experience from other sectors, and the TMT industry has the opportunity to leverage that body of knowledge and take a short-cut to best practice.

Sector by sector

Each TMT sector faces different security challenges

Looking beyond the general TMT security trends, the individual sectors – technology, media and telecommunications – face their own unique challenges and boast varying levels of maturity.

Technology

Technology companies spend huge sums on research and development (R&D)¹³, which is the lifeblood of their business. Their biggest security challenge is protecting the intellectual property that results from their massive R&D efforts. Yet only 20 percent of technology companies surveyed are “confident” that their patents and other intellectual property are properly protected. Another 49 percent are only “somewhat confident”. Roughly 24 percent of the companies surveyed are “concerned” or “very concerned” about intellectual property protection.

Most technology companies focus on network security and firewalls to protect their R&D activities from external attack. However, as in other TMT sectors, the biggest threat is actually from within. For example, 59 percent of the surveyed technology companies identify “email messages to unauthorized persons containing confidential information and/or intellectual property” as a high risk area. To keep their secrets to themselves, technology companies should focus more attention on access control, on email (encryption, scanning and filtering – especially for outgoing email), and on strong authentication (for example, smart cards and token-based authentication mechanisms).

Media

The benefits of digitizing media production are compelling¹⁴. However, media companies should give careful consideration to specific details such as timing, digital security and process change. They should also protect themselves against new risks such as increased vulnerability to hackers and intellectual property theft. For example, moving to network-based storage provides a company with greatly improved access to its content assets, but also exposes those assets to viruses and pirates – neither of which was a critical issue when content was held on tape in a store room.

One of the biggest challenges for a media company is to remain in control without sacrificing flexibility, creativity and the entrepreneurial spirit¹⁵. Of media companies surveyed, 53 percent are “somewhat confident” or “very confident” that their intellectual property, from video games to digital music, is adequately protected during the design and development phases. This is surprisingly high and could be seen as good news. Yet only a third perform a security risk assessment on a regular basis (quarterly, six-monthly or annually).

To be on the safe side, every media company's board should be asking itself tough questions such as: what happens if our network gets infected by a virus, or a hacker starts corrupting files? What if a worm with a destructive payload starts wiping the archive? In the absence of airtight security, digital media content is a hacker's dream – and an investor's nightmare.

Telecommunications

The telecommunications world is rapidly shifting from analog and physical networks to digital and virtual networks. In connection with this shift, the ubiquity and usefulness of communication technology are growing by leaps and bounds. Telecommunications is increasingly critical to the way people all over the world live and work, which brings issues of security and reliability to the fore.

For instance, the survey shows most telecommunications companies see security risks in the future development of WiFi networks, VoIP, WiMAX and 3G networks¹⁶. Yet half of the surveyed TMT companies that have adopted these technologies – or are considering them – do not feel confident they are protected by existing security measures.

In response, more and more telecommunications companies are using security and reliability as a way to strengthen and differentiate their brands. In some cases, security and reliability are even proving to be the difference between success and failure. For example, in the market for VoIP services, two distinct types of services are taking shape. Managed VoIP operates on a managed network and features high levels of quality, reliability and security. Ad hoc VoIP uses the open Internet as the service platform and is therefore less secure and less reliable. Although both offerings use the same underlying technology, ad hoc VoIP continues to struggle for mass market acceptance while the more secure and reliable managed VoIP offering is rapidly increasing its share of the voice market¹⁷.

Conclusion

Companies in the technology, media and telecommunications industry have tended to treat security as a relatively minor issue. This is in part because of the rapid pace of change in the TMT industry. The digital age has come upon us in under two decades, and few corners of the industry remain unaffected. As a result, security – as it pertains to digital assets, processes and transactions – is a relatively new phenomenon. But the time has come for the TMT industry to recognize that substantial action is necessary.

The volume, sophistication and potential damage of security attacks continue to grow. More than half of the companies in DTT's 2006 TMT Security Survey had their systems breached in the last 12 months – and roughly a third of those breaches resulted in significant financial losses of up to several million dollars. Factor in the indirect and intangible losses, and the impact is even higher.

What can TMT companies do to address this increasingly critical problem?

- Establish formal security strategies, policies and procedures. Stay abreast of the latest challenges and threats.
- Improve security awareness and training at all levels of the organization – starting at the top.

- Focus more resources on internal security threats.
- Allocate sufficient budget and resources to get ahead of security threats. Playing catch-up is not good enough.
- Develop and maintain a formal contingency plan for business continuity.

Although different TMT sectors face their own unique challenges, one thing they have in common is increasing vulnerability to attack. Security is no longer a minor operating detail, or a problem best left to the IT department. Today, security is a fundamental business requirement – and a strategic imperative.

Acknowledgments

The 2006 TMT Security Survey was conducted by TMT professionals of DTT member firms in over 30 countries on five continents. Data was primarily collected through face-to-face interviews with 150 TMT organizations' security officers or their equivalent. In some cases, respondents submitted their data online. All interview results were submitted and processed in DeloitteDEX, an online benchmarking tool¹⁸.

DTT TMT Industry Group is grateful to everyone who responded to the survey, and also thanks everyone involved in preparing and executing the survey, collecting and analyzing the data and writing this report.

Notes

- 1 For example, see: Bank theft technology sold on Internet, Financial Times, 10 May 2006; Movie Industries Target Theft on Internal Campus Networks, Collegiate Presswire, 27 April 2006. ICT-gevaar van binnenuit vele malen groter, Vooral overheid zwaar getroffen door gerommel met bestanden en diefstal, Security.nl, 19 May 2006; Defensie raakt geheime gegevens kwijt; RTL, 20 January 2006; La seguridad informática preocupa a las empresas; Computerworld España, 17 March 2006.
- 2 For example, see: <http://www.csoonline.com/read/110103/outsourcing.html>.
- 3 In the UK alone, cyber-attacks are estimated to be costing businesses £10bn a year. A recent survey by the US Federal Bureau of Investigation estimated that cybercrime costs US businesses \$62bn (£33bn) a year; Sleuths on the cybercrime trail, Financial Times, 5 May 2006.
- 4 **Financial Damage Caused by Viruses, F-Secure.** See: <http://www.f-secure.com/news/newsletter/protected/archives/prot-3-2002/page1.shtml>.
- 5 Emerging Internet Threat List, Department of Homeland Security and NCSA 2006, <http://www.staysafeonline.info/basics/2006threatlist.html>.
- 6 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
- 7 California SB1386: An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information. Approved on 25 September 2002. More information is available on: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.
- 8 Law No.57, 2003. Enforced on 30 May 2003 except for Chapter 4 to 6 and Article 2 to 6 of Supplementary Provisions. Completely enforced on 1 April 2005.
- 9 For more discussion on the efficacy of e-rooms, see: E-learning: effective but awkward, Management Issues, 17 May 2004.
- 10 For more information see <http://www.buslink.com>.
- 11 Analysis of Security Vulnerabilities in the Movie Production and Distribution Process, AT&T Labs Research, 13 September 2003. For full transcript, see: <http://lorrie.cranor.org/pubs/drm03-tr.pdf>.
- 12 Managing business continuity risk: Continuing the Journey; 6th Annual Business Continuity Survey from Deloitte & Touche LLP and CPM Group, Deloitte Development LLC and The CPM Group, 2006.
- 13 For more discussion on the rising costs of research and development and the implications of this for TMT companies, see "Imperatives for TMT CEOs, 2005-2010", Deloitte Touche Tohmatsu, 2005 and also "TMT Trends: Technology Predictions 2006", Deloitte Touche Tohmatsu, 2006.
- 14 A variety of media companies around the world are gradually digitizing their archives, both to preserve archived material and also to enable commercial exploitation of back catalogues. For more information, see: http://creativearchive.bbc.co.uk/archives/what_is_the_creative_archive/index.html; http://portal.unesco.org/ci/en/ev.php-URL_ID=19998&URL_DO=DO_TOPIC&URL_SECTION=201.html.
- 15 Sustaining Compliance; Leveraging investments in compliance to generate business value and improvements. Report from Deloitte Accountants B.V. the Netherlands on the TMT Roundtable held in January 2006. Copyright, Deloitte Accountants B.V. Netherlands, February 2006.
- 16 For more discussion on security issues resulting from VoIP deployments see: VoIP Security a Moving Target, Network World, 17 January 2005.
- 17 For further discussion on the risks related to deployment of VoIP see: Getting off the Ground – Why the move to VoIP is a decision for all CXOs, Deloitte Touche Tohmatsu, 2004.
- 18 DeloitteDEX is a DTT suite of proprietary products and processes for diagnostic benchmarking applications.

Contacts at Deloitte Touche Tohmatsu and its member firms

Igal Brightman
Israel
Global Managing Partner
Technology, Media & Telecommunications
+972 3 608 55 00
ibrighman@deloitte.co.il

Americas

Alberto Lopez Carnabucci
Argentina
+54 11 4320 2700
alopezcarnabucci@deloitte.com

Elsa Victoria Mena Cardona
Colombia
+571 546 1815
emenacardona@deloitte.com

José Luis Rey
Uruguay
+598 2 916 0756
jrey@deloitte.com

Marco Antonio Brandao Simurro
Brazil
+55 11 5186 1232
mbrandao@deloitte.com.br

Xavier Ribadeneira
Ecuador
+593 2 2251 319
xribadeneira@deloitte.com

Christopher Lee
USA, Deloitte & Touche LLP
+1 408 704 4314
chrislee@deloitte.com

Adel Melek
Canada
+1 416 601 6524
amelek@deloitte.ca

Francisco Silva
Mexico
+52 55 5080 6310
fsilva@dtmx.com

Carlos Brown
Venezuela
+58 212 206 8653
carlbrown@deloitte.com

Arturo Platt
Chile
+56 2 2703 361
aplatt@deloitte.com

Fernando Parodi
Peru
+51 1 211 8585
fparodi@deloitte.com

Europe/Middle East/Africa

Gerhard Feuchtmueller
Austria
+43 1 537 00 4800
gfeuchtmueller@deloitte.at

Kim Gerner
Denmark
+45 36 10 32 81
kgerner@deloitte.dk

Tom Cassin
Ireland
+353 1 417 2210
tcassin@deloitte.ie

Jack Hakimian
Middle East
+965 243 8060
jhakimian@deloitte.com

Mike White
South Africa
+27 11 806 5899
mikwhite@deloitte.co.za

Mike Maddison
United Kingdom
+44 20 7303 0017
mmaddison@deloitte.co.uk

Andre Claes
Belgium
+32 2 600 6670
aclaes@deloitte.com

Tuomo Salmi
Finland
+358 40 716 9728
tuomo.salmi@deloitte.fi

Eyal Hendler
Israel
+972 608 5522
ehendler@deloitte.co.il

Jacques Buith
Netherlands
+31 20 4547066
jbuith@deloitte.nl

Eduardo Sanz
Spain
+34 91 514 5000
edsanz@deloitte.es

Jiri Polak
Central Europe
+420 22 489 5322
jipolak@deloitteCE.com

Eric Morgain
France
+33 1 5561 2798
emorgain@deloitte.fr

Alberto Donato
Italy
+39 064 780 5595
adonato@deloitte.it

Jorn Borchgrevink
Norway
+47 2327 9210
jborchgrevink@deloitte.no

Tommy Maartensson
Sweden
+46 8 506 711 30
tommy.maartensson@deloitte.se

Gennady Kamyshnikov
CIS & Russia
+7 495 787 0600
gkamyshnikov@deloitte.ru

Andreas Gentner
Germany
+49 711 1655 47302
agentner@deloitte.de

Dan Arendt
Luxembourg
+352 451 452621
darendt@deloitte.lu

Carlos Freire
Portugal
+351 21 042 7511
cfreire@deloitte.pt

Oktay Aktolun
Turkey
+90 212 339 8524
oaktolun@deloitte.com

Asia Pacific

Ian Thatcher
Australia
+61 2 9322 7640
ithatcher@deloitte.com.au

John Bell
New Zealand
+64 9 303 0853
jobell@deloitte.co.nz

Charles Yen
China
+86 10 8520 7000
chyen@deloitte.com.cn

Shariq Barmaky
Singapore
+65 6530 5508
shbarmaky@deloitte.com

N. Venkatram
India
+91 22 6667 9125
nvenkatram@deloitte.com

Hyun Chul Jun
South Korea
+82 2 6676 1307
hjun@deloitte.com

Yoshitaka Asaeda
Japan
+81 3 6213 3488
yoshitaka.asaeda@tohmatsu.co.jp

Clark C. Chen
Taiwan
+886 2 2545 9988 x3065
clarkchen@deloitte.com.tw

About TMT

The Deloitte Touche Tohmatsu (DTT) Technology, Media & Telecommunications (TMT) Industry Group consists of the TMT practices organized in the various member firms of DTT and includes more than 5,000 member firms' partners, directors and senior managers supported by thousands of other professionals dedicated to helping their clients evaluate complex issues, develop fresh approaches to problems and implement practical solutions.

There are dedicated TMT member firms' practices in 45 countries and centers of excellence in the Americas, EMEA and Asia Pacific. DTT's member firms serve nearly 85 percent of the TMT companies in the Fortune Global 500. Clients of Deloitte's member firms' TMT practices include some of the world's top software companies, computer manufacturers, wireless operators, satellite broadcasters, advertising agencies and semiconductor foundries – as well as leaders in publishing, telecommunications and peripheral equipment manufacturing.

About Global ERS Security & Privacy Group

Deloitte member firm ERS Security & Privacy practices help their clients manage information securely.

The global Security & Privacy Services Group, made up of Deloitte member firm ERS Security & Privacy practices, assists member firm clients in addressing and managing risks in an increasingly complex network environment, including risk of security breach, the regulatory environment (e.g. e-privacy), and labor shortage issues. Deloitte member firm enterprise-wide services include:

- Application security/integrity
- Business continuity management
- Identity and access management
- Infrastructure and operations security
- Privacy and data protection
- Security management
- Vulnerability management.

Deloitte member firms offer knowledge and experience combined with national coverage and global reach. Member firm resources include over 600 Certified Information Systems Security Professionals (CISSP) globally, presence in more than 80 cities, access to 18 global technology centres, and access to technology solution sets developed through long standing vendor alliances.

Recent DTT thought leadership

"Eye to the future: How TMT advances could change the way we live in 2010", Deloitte Touche Tohmatsu

"Flying high: 2006 Global Survey of CEOs in the Deloitte Technology Fast 500", Deloitte Touche Tohmatsu

"Strategic Flexibility in media and entertainment: Scenarios, options, action!", Deloitte Touche Tohmatsu

"TMT Trends: Predictions, 2006 – A focus on the technology sector", Deloitte Touche Tohmatsu

"TMT Trends: Predictions, 2006 – A focus on the media sector", Deloitte Touche Tohmatsu

"TMT Trends: Predictions, 2006 – A focus on the telecommunications sector", Deloitte Touche Tohmatsu

"Be prepared: Imperatives for TMT executives, 2005-2010", Deloitte Touche Tohmatsu

"The trillion dollar challenge: Principles for profitable convergence", Deloitte Touche Tohmatsu

"Knowledge is power: Technology, Media & Telecommunications Global Industry Group", Deloitte Touche Tohmatsu

"The hundred year storm: Wireless disruption in telecommunications", Deloitte Touche Tohmatsu

"Television networks in the 21st century: Growing critical mass in a fragmenting world", Deloitte Touche Tohmatsu

"Rational exuberance: 2005 Global Survey of CEOs in the Deloitte Technology Fast 500", Deloitte Touche Tohmatsu

"Reconnected to Growth: Global Telecommunications Industry Index 2005", Deloitte Touche Tohmatsu

"Getting off the Ground: Why the move to VoIP is a decision for all CXOs"

"Changing China: Will China's technology standards reshape your industry?", Deloitte Touche Tohmatsu

"Moore's Law and electronic games: How technology advances will take electronic games everywhere", Deloitte Touche Tohmatsu

"Making the offshore call: The road map for communications operators", Deloitte Touche Tohmatsu

For more information, please contact

Noel J. Spiegel

United States
Deloitte & Touche LLP
Partner in Charge of Global TMT Marketing
+1 212 492 4135
nspiegel@deloitte.com

Amanda Goldstein

United States
Deloitte & Touche USA LLP
Director of Global TMT Marketing
+1 212 436 5203
agoldstein@deloitte.com

Hiro Notaney

United States
Deloitte Services LP
Director of North America TMT Marketing
+1 408 704 2464
hnotaney@deloitte.com

Craig Fowler

United Kingdom
Director of EMEA TMT Marketing
+44 20 7303 5293
crfowler@deloitte.co.uk

Steven Dow

China
Director of Asia Pacific TMT Marketing
+852 2852 5638
sdow@deloitte.com.hk

Disclaimer

These materials and the information contained herein are provided by Deloitte Touche Tohmatsu and are intended to provide general information on a particular subject or subjects and are not an exhaustive treatment of such subject(s).

Accordingly, the information in these materials is not intended to constitute accounting, tax, legal, investment, consulting, or other professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

These materials and the information contained therein are provided as is, and Deloitte Touche Tohmatsu makes no express or implied representations or warranties regarding these materials or the information contained therein. Without limiting the foregoing, Deloitte Touche Tohmatsu does not warrant that the materials or information contained therein will be error-free or will meet any particular criteria of performance or quality. Deloitte Touche Tohmatsu expressly disclaims all implied warranties, including, without limitation, warranties of merchantability, title, fitness for a particular purpose, noninfringement, compatibility, security, and accuracy.

Your use of these materials and information contained therein is at your own risk, and you assume full responsibility and risk of loss resulting from the use thereof. Deloitte Touche Tohmatsu will not be liable for any special, indirect, incidental, consequential, or punitive damages or any other damages whatsoever, whether in an action of contract, statute, tort (including, without limitation, negligence), or otherwise, relating to the use of these materials or the information contained therein.

If any of the foregoing is not fully enforceable for any reason, the remainder shall nonetheless continue to apply.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 150 countries. With access to the deep intellectual capital of 120,000 people worldwide, Deloitte delivers services in four professional areas—audit, tax, consulting, and financial advisory services—and serves more than one-half of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names.

© 2006 Deloitte Touche Tohmatsu. All rights reserved.

Designed and produced by The Creative Studio at Deloitte & Touche LLP, London.