THE NEW BUSINESS CHALLENGE

Next Generation Security

IT'S HOW
WE CONNECT

EXECUTIVE SUMMARY

RECENT ADVANCES IN INFORMATION TECHNOLOGY HAVE DELIVERED HUGE BENEFITS TO PUBLIC AND PRIVATE-SECTOR ORGANISATIONS, BUT THEY HAVE ALSO BROUGHT SOME SIGNIFICANT CHALLENGES.

Major trends such as cloud computing, mobility, online commerce and social networking are causing sweeping changes to ICT infrastructures. Together, these trends have the potential to dramatically improve efficiency and boost productivity.

However, counter balancing these advantages is the growing challenge of security. As organisations find themselves more reliant on ICT systems and services, ensuring these systems remain resilient, functional and trusted becomes critical.

Seemingly every day, reports surface of information security breaches, hacktivism and data loss. Examples range from credit fraud and identity theft to industrial espionage and targeted online attacks. For organisations, the results can range from disruption to key services to severe financial loss and even ruin.

Organisations are now trying to find a balance between embracing the advantages technology can deliver and the task of providing vital systems and data remain secure. It's a balance not easy to achieve and maintain in an ever-changing threat environment.

The security challenge covers a range of areas which must be considered. These include:

- **The people challenge:** Humans remain the weakest link in any security chain
- **The process challenge:** Devising an effective and flexible security framework
- **The technology challenge:** The different types of attacks and methods used.

By having a comprehensive security framework and fully tested security controls senior managers can be more confident their organisation will be able to withstand such threats. The first step is to understand the nature of the risks in the context of your organisation.

1. THE ESCALATING THREAT ENVIRONMENT

AROUND THE WORLD, CEOS ARE TAKING ADVANTAGE OF DEVELOPMENTS IN ICT SYSTEMS AND SERVICES TO RESHAPE THE WAY THEIR ORGANISATIONS FUNCTION.

Internal processes, customer interactions and supply chains are being re-architected to improve levels of service and reduce operational costs.

As a result, ICT infrastructures are becoming more porous. Staff demand access to centrally held systems and data from external locations and on a variety of devices. Suppliers and partners are increasingly being linked into core applications to allow orders to be taken, stock levels to be checked and payments to be made.

For senior executives, the situation is full of both opportunities and threats. Indeed, almost eight out of ten CEOs recently surveyed saw business complexity, uncertainty and volatility as a significant challenge. Yet the gap between expected change and the ability to manage it has widened significantly.[1]

The challenge is highlighted by a spate of recent high-profile attacks on organisations around the world (refer to timeline below).

A key motivation behind many such attacks is to cause disruption and/or gain financial benefit. Customer records and sensitive corporate information can be sold on the black market or used to gain a competitive advantage.

Organisations can also suffer from simple mistakes or accidents by the use of microsites (web interfaces, forms or websites) and inadvertently expose important company information.

There are also other drivers at work. Activities of organisations such as LulzSec and Anonymous, together with recent Middle-Eastern political uprisings, reinforce the threat of a phenomenon known as 'hacktivism'. Rather than seeking commercial gain, the objective of such organisations is to protest against what they see as injustices or bad decisions by large corporations.

Their targets can find themselves under sustained attack from a group of hackers with no central control point. Rather, the groups rally support from around the world and mount focused attacks against chosen targets.

The result for an organisation is that, even if it is not the direct target of an attack, it can suffer collateral damage if another organisation on which it relies falls victim. This could be anyone from a hosting company or networking provider to a supplier or bank. In some cases, as seen in the exercise of Cyberstorm 3, the whole internet in Australia was impacted and taken down for a period of time. Your private IP networks must continue to function in this type of scenario.

EXAMPLES INCLUDE:

June 2010

Security experts discover the Stuxnet worm designed to cause severe disruption to industrial SCADA systems and critical infrastructure networks.

March 2011

A hacking incident potentially compromised millions of RSA security tokens.

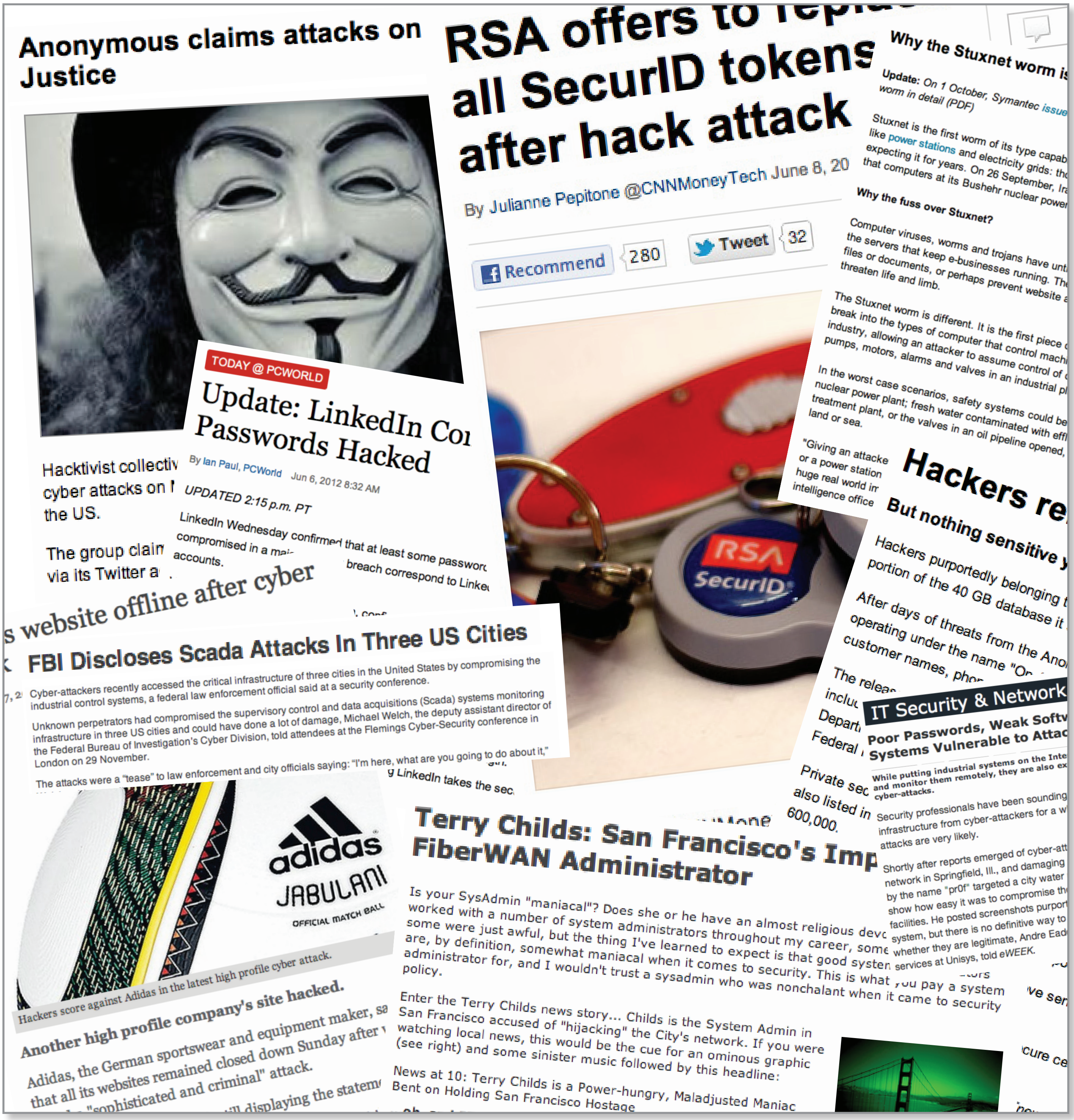
April 2011

An attack on Sony by hacking group LulzSec compromises 77 million user accounts on the PlayStation Network. Each account contained verified names, addresses and credit card numbers. This was directly followed by a DDoS attack launch by Anonymous.

June 2011

More than 4800 Australian websites are lost after an attack on hosting company Distribute.IT.

[1] IBM Global CEO study: Capitalising on Complexity 2010. A study based on face-to-face conversations with more than 1500 CEOs worldwide.



Anonymous claims attacks on Justice

Hacktivist collectiv cyber attacks on t the US.

The group claim via its Twitter a

TODAY @ PCWORLD

Update: LinkedIn Co Passwords Hacked

By Ian Paul, PCWorld Jun 6, 2012 8:32 AM

UPDATED 2:15 p.m. PT

LinkedIn Wednesday confirmed that at least some passwor compromised in a mai breach correspond to Linke accounts.

s website offline after cyber

FBI Discloses Scada Attacks In Three US Cities

Cyber-attackers recently accessed the critical infrastructure of three cities in the United States by compromising the industrial control systems, a federal law enforcement official said at a security conference.

Unknown perpetrators had compromised the supervisory control and data acquisitions (Scada) systems monitoring infrastructure in three US cities and could have done a lot of damage, Michael Welch, the deputy assistant director of the Federal Bureau of Investigation's Cyber Division, told attendees at the Flemings Cyber-Security conference in London on 29 November.

The attacks were a "tease" to law enforcement and city officials saying: "I'm here, what are you going to do about it,"

g LinkedIn takes the sec

RSA offers to repla all SecurID tokens after hack attack

By Julianne Pepitone @CNNMoneyTech June 8, 20

Recommend 280 Tweet 32

Why the Stuxnet worm is

Update: On 1 October, Symantec issue worm in detail (PDF)

Stuxnet is the first worm of its type capab like power stations and electricity grids: th expecting it for years. On 26 September, Ira that computers at its Bushehr nuclear power

Why the fuss over Stuxnet?

Computer viruses, worms and trojans have unti the servers that keep e-businesses running. Th files or documents, or perhaps prevent website a threaten life and limb.

The Stuxnet worm is different. It is the first piece o break into the types of computer that control machi industry, allowing an attacker to assume control of c pumps, motors, alarms and valves in an industrial pl

In the worst case scenarios, safety systems could be nuclear power plant; fresh water contaminated with effl treatment plant, or the valves in an oil pipeline opened, land or sea.

"Giving an attacke or a power station huge real world im intelligence office

Hackers re

But nothing sensitive y

Hackers purportedly belonging t portion of the 40 GB database it

After days of threats from the Ano operating under the name "Op customer names, phon

The releas inclu Depart Federal

Private sec also listed in 600,000.

IT Security & Network

Poor Passwords, Weak Softw Systems Vulnerable to Attac

While putting industrial systems on the Inte and monitor them remotely, they are also ex cyber-attacks.

Security professionals have been sounding infrastructure from cyber-attackers for a w attacks are very likely.

Shortly after reports emerged of cyber-att network in Springfield, Ill., and damaging by the name "pr0f" targeted a city water show how easy it was to compromise th facilities. He posted screenshots purport system, but there is no definitive way to whether they are legitimate, Andre Ead services at Unisys, told eWEEK.

Hackers score against Adidas in the latest high profile cyber attack.

Another high profile company's site hacked.

Adidas, the German sportswear and equipment maker, sa that all its websites remained closed down Sunday after "sophisticated and criminal" attack. displaying the statem

Terry Childs: San Francisco's Imp FiberWAN Administrator

Is your SysAdmin "maniacal"? Does she or he have an almost religious devo worked with a number of system administrators throughout my career, some some were just awful, but the thing I've learned to expect is that good systen are, by definition, somewhat maniacal when it comes to security. This is what you pay a system administrator for, and I wouldn't trust a sysadmin who was nonchalant when it came to security policy.

Enter the Terry Childs news story... Childs is the System Admin in San Francisco accused of "hijacking" the City's network. If you were watching local news, this would be the cue for an ominous graphic (see right) and some sinister music followed by this headline:

News at 10: Terry Childs is a Power-hungry, Maladjusted Maniac Bent on Holding San Francisco Hostage

November 2011

The main Adidas website was taken offline for three days following a security breach.

April 2012

Websites of CIA, MI6 and the US Department of Justice are taken off the air by DDoS attacks launched by the ‘hacktivist’ collective known as Anonymous in protest of the proposed Cyber Intelligence Sharing and Protection Act (CISPA).

June 2012

A file containing 6,458,020 unencrypted passwords from LinkedIn.com is posted on the Internet.

July 2012

As part of a protest against online censorship, hacking group Anonymous conducted an attack on AAPT and published thousands of business customer records online including some of Australia’s most high profile organisations.

2. THE IMPORTANCE OF SECURITY

AROUND THE WORLD CEOS FACE AN INCREASING CHALLENGE. WITH ICT SYSTEMS NOW UNDERPINNING VIRTUALLY EVERY FACET OF OPERATIONS, ENSURING THOSE SYSTEMS REMAIN SECURE AND OPERATIONAL HAS BECOME A PRIORITY.

For this to be achieved, a coordinated approach to security is necessary. It must address everything from the behaviours of an organisation's people, the processes they follow, core hardware and software to networks and client devices. Any areas not covered become a potential weakness for the organisation and, as new technologies and services emerge, security tools and frameworks must evolve to match them.

Of those included in a recent survey, 60% said they perceived a change in their risk environment as a result of new technologies.[2] Most are becoming aware of the importance of having a comprehensive security system in place.

The key reasons organisations are investing in ICT security include:

01

Reputation protection
An organisation's brand and trusted reputation takes years to develop, yet can be severely damaged through a single incident. According to a recent survey, 82 per cent of senior executives saw ICT security as important in protecting the reputation and brand of their organisation.[3]

02

Technological security failures
ICT security failures can have a significant impact on an organisation's ability to function. Disruption to manufacturing or service provision capabilities will result in an immediate hit to the bottom line.

03

Financial loss
Losses can come directly from disruption to critical systems, hindering an organisation's ability to function. They can be the result of the theft of commercially sensitive data which impinges on competitive advantage. In addition there are the long-term intangible costs associated with loss of trust and potential litigation from affected parties.

04

Intellectual property
Loss of competitive advantage in the event of company secrets or potential patents being stolen.

[2] Ibid

[3] Ernst & Young's 2010 Global Information Security Survey. Nearly 1600 organisations from 56 countries and across all major industries participated.

“60% SAID THEY PERCEIVED A CHANGE IN THEIR RISK ENVIRONMENT AS A RESULT OF NEW TECHNOLOGIES”

3. THE PEOPLE CHALLENGE

IN MANY ORGANISATIONS, ONE OF THE BIGGEST SECURITY RISKS IS NOT TECHNOLOGY – BUT PEOPLE.

Through ignorance of risks, process non-compliance, technical naivety or intent of malice, an organisation's employees can cause significant disruption and damage to critical data and applications.

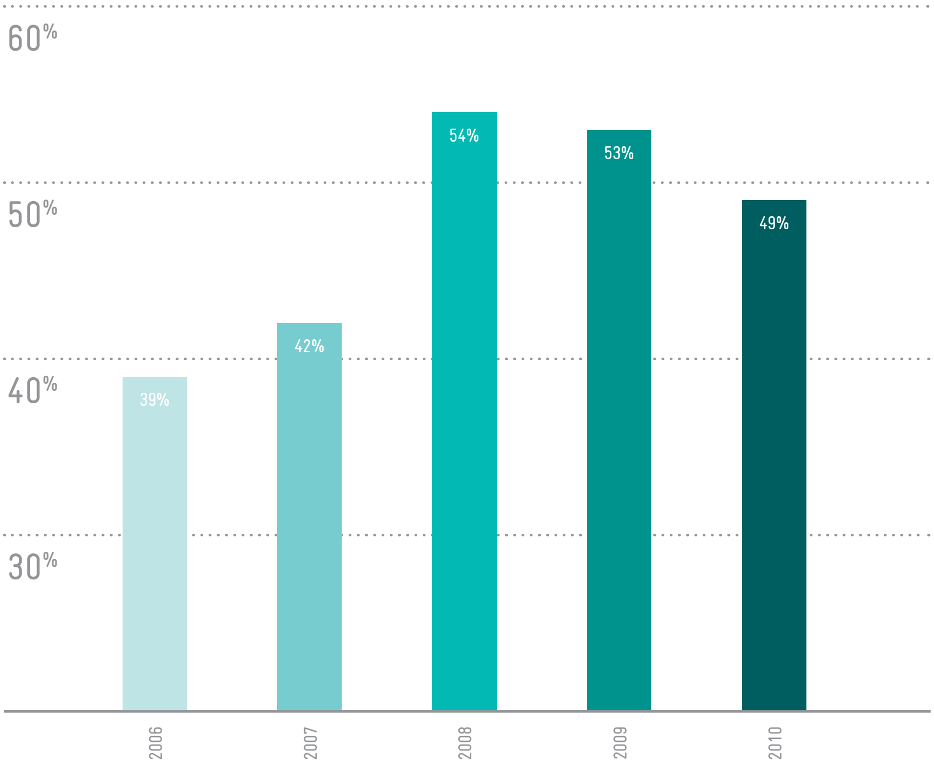
Typical scenarios include the use of weak access passwords (names of children, spouses or simple number sequences etc), the loss of portable computing devices and insecure remote access of centralised ICT resources. Failure to understand the potential ramifications of their actions makes employees a very real security problem. Those who don't follow policies and procedures introduce additional risk by bypassing controls that have been put in place. This can be as simple as clicking on an email attachment directed at a staff member via a spear phishing email, similar to what happened to RSA (refer to page 6).

Yet despite this risk, less than half (49 per cent) of organisations recently surveyed by PricewaterhouseCoopers confirmed that they conduct employee security awareness programs. This figure has dropped from 54 per cent in two years.[4]

Of similar concern was the finding that, despite the rapid take-up of social networks, blogs and wikis within organisations, 60 per cent of those surveyed were yet to implement corresponding security technologies.[5]

Further research has found human error is a contributing factor in nearly all data breaches. Poor decisions, omissions, and process breakdowns have been shown to occur somewhere in the chain of events that lead up to a data loss incident.[6]

Figure 1: Organisations who conduct security awareness programs:



PricewaterhouseCoopers 2011 Global State of Information Security Survey. A worldwide security survey based on online responses from more than 12,840 CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 135 countries.

[4] PricewaterhouseCoopers 2011 Global State of Information Security Survey. A worldwide security survey based on online responses from more than 12,840 CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 135 countries.

[5] Ibid

[6] Verizon 2010 Data Breach Investigations Report. A study conducted by the Verizon Risk Team in co-operation with the United States Secret Service.

THE INSIDER THREAT

While it's a common perception that security threats come from outside an organisation's boundaries, the reality is that many actually originate from within.

Current or former employees, contractors or trusted business partners with access to internal systems all have the power to cause system disruption or data loss. According to research, in 2010, 21 per cent of all security attacks were caused by insiders.[7]

While such a number is concerning, it may not be painting the entire picture as many incidents go unreported outside the affected organisation. It has been estimated by CERT.org that 70 per cent of insider security incidents are handled internally without legal action.[8]

However while it may be difficult to get an accurate picture of the number of incidents, there is no doubt that the impact they have on organisations is significant. According to a CERT survey, a third of all respondents viewed insider attacks as being more costly than those coming from outside an organisation.

According to CERT's Insider Threat database, 86 per cent of the insiders who commit ICT sabotage held technical positions within the organisation they targeted and used sophisticated methods to conduct their attacks. Of the organisations that fell victim to attacks, 75 per cent reported their operations had been disrupted and 28 per cent experienced reputation damage.[9]

One example of the problems an insider can create was seen in the case of convicted computer expert Terry Childs. When working as a network administrator for the City of San Francisco in 2008, Childs was arrested after refusing to hand over passwords that gave access to the city's wide-area network. The action caused disruption to city services and Childs was eventually found guilty of a felony charge of denying computer access.

[7] Insider Threat Deep Dive: IT Sabotage: www.cert.org/blogs/insider_threat/2010/09/insider_threat_deep_dive_it_sabotage.html

[8] http://www.cert.org/blogs/insider_threat/2010/10/interesting_insider_threat_statistics.html

[9] http://www.cert.org/insider_threat/

THE CHALLENGE OF SOCIAL NETWORKING

While the majority of the security threats facing organisations have been understood for some years, the rise of social networking has brought with it a range of new challenges.

The use of popular social networks, such as Facebook and Twitter, break through the traditional communication channels that exist within organisations. As well as facilitating direct communication between individuals, they allow the exchange of photos, files and other information.

As such social networks are often accessed using corporate systems, they provide an enticing conduit for hackers and malware attacks. Already a number of malware applications for Android and Windows Mobile 7 have been detected that are designed to open a back door into corporate networks.

Social networking sites also provide a rich source of information about people within organisations. This information can be used to tailor messages that trick individuals into downloading malicious software or providing their log-in or password details.

Other social networking techniques used by attackers include embedding malicious code within advertisements, pictures and third-party applications. According to Kaspersky Labs, malware spread by social networking sites is ten times more effective than malware spread by email.[10]

The URL shortening services, made popular by sites such as Twitter, also allow the rapid spread of rogue code as the original source of the URL is not immediately apparent to users.

Recent examples of social network-based attacks include an online security consultant who used a simple code to collect user data from Facebook and publish it on the worlds' largest file sharing website Pirate Bay.

The UK Ministry of Defence has identified 16 security breaches which are directly attributable to social networking sites, while a Twitter employee's administrative account was compromised, allowing hackers to change the passwords on other accounts and gain control of them.

[10] http://www.kaspersky.com/about/news/press/2009/kaspersky - Lab offers free guide to staying safe online in the wake of the latest Facebook phishing attack.

4. THE PROCESS CHALLENGE

FOR SECURITY INITIATIVES TO SUCCEED, A STRUCTURED FRAMEWORK IS REQUIRED TO ENSURE ALL CHALLENGES ARE FACED AND POTENTIAL WEAKNESSES COVERED.

Such a framework will assist in allowing critical systems and data to remain secure and available to an organisation's employees, suppliers and partners.

However, because organisations and their ICT infrastructures are in a constant state of flux, the framework must be able to cope with changes while still maintaining required security standards.

BUILDING A FRAMEWORK

To achieve this, a security framework should be supported by an end-to-end Governance, Risk and Compliance (GRC) program. A GRC program involves careful assessment of all risks faced by an organisation and the suitability of any security components put in place.

While a successful security framework relies equally on people, process and technology-based controls, there must also be a solid strategy and supporting process to assist in ensuring desired security outcomes are met.

The outcome of such a process will be an Information Security Management System (ISMS) which encompasses and defines an organisation's security structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.[11]

[11] Reference: AS/NZS ISO/IEC 27001:2006

5. THE TECHNOLOGY CHALLENGE

THE SECURITY THREATS FACING ORGANISATIONS COME IN A VARIETY OF FORMS. THESE RANGE FROM NETWORK-BASED CYBER ATTACKS, VIRUSES AND WORMS TO SOCIAL ENGINEERING EXPLOITS THAT TARGET EMPLOYEE BEHAVIOUR.

The challenge for senior managers is to help ensure their defences are capable of dealing with them all.

The task is made more difficult by the complex nature of ICT infrastructures within large organisations. A mix of hardware and software from different vendors means each infrastructure is unique. Add the extra layer of outsourced resources and the job gets even harder.

CEOs and senior managers must also constantly weigh up the seemingly conflicting priorities of the availability and usability of critical systems versus their security. It's only through an understanding of the challenges being faced that this can be achieved.

The major security challenges facing organisations include:

HACKER ATTACKS

Of all the security threats currently faced by public and private-sector organisations, the most high profile is the hacker attack. Varying in nature from simple intrusions to sophisticated data thefts by organised criminal groups and sovereign governments, hacker attacks can cause widespread disruption and significant financial loss.

Often exploiting vulnerabilities found in computer software systems and network infrastructures, the attacks can come in a variety of forms. Further compounding the situation, the rise of the internet as a business tool means attacks can be mounted from anywhere in the world. Hackers are not hindered by national or international boundaries and use these to their advantage.

More recently attacks have even occurred on systems that are not connected to the internet, such as seen with the Stuxnet worm. Even organisations which do not use SCADA systems (the target of Stuxnet) can fall victim when such attacks target highly-secure departments (so-called 'air gapped') such as treasury.

MALWARE

Constantly changing in form and intent, viruses and worms represent a significant threat for any organisation. While anti-virus tools provide solid protection, awareness of this threat is still needed to determine how attacks are prevented.

Virus writers are continually changing their creations to circumvent detection and removal of applications installed on an organisation's ICT systems. In what has become a cat and mouse competition with security companies, viruses regularly alter their signatures to avoid detection.

Typical attack vectors include email attachments and the hiding of code within certain web sites. In these instances, all a user has to do is visit the site to have their browser, and potentially an organisation's computer system, compromised. Known as 'drive-by downloads' these attacks can occur without a user being aware that anything has gone wrong.[12]

Other virus and worm attacks target vulnerabilities in popular software applications such as Microsoft Office and Adobe Acrobat. PDF exploitation continues to be favoured by attackers as they represent a relatively easy way to gain access to an organisation.[13]

ADVANCED PERSISTENT THREAT (APT)

APTs are sophisticated long term attacks which use a range of attack vectors targeted at obtaining valuable information from a specific target system. The attacks can be used for espionage or as a cyber attack against specific critical systems, processes or infrastructure. One example was the use of Stuxnet to target Iranian nuclear centrifuges.

DENIAL OF SERVICE ATTACKS

Another form of cyber attack known as Distributed Denial of Service (DDoS) is also growing in popularity. DDoS attacks involve a network of compromised computers, known as a botnet, configured to launch a co-ordinated attack on a specific victim organisation. Such attacks can take down that organisation's web site or cause disruption to vital ICT systems and services.

Because of their potential to cause such disruptions, DDoS attacks have become a high-profile issue for many organisations. In a survey conducted during 2010, 47 per cent of respondents indicated they experienced between 1 and 10 DDoS attacks per month. A further 47 per cent said they experienced between 10 and 500 such attacks each month.[14]

[12] Cisco 2008 and 2010 Annual Security Reports, providing an overview of the combined security intelligence of the entire Cisco organisation.
[13] IBM X-Force 2010 Mid-Year Trend and Risk Report
[14] Arbor Networks Worldwide Infrastructure Security Report Volume VI, 2010

PHONE HACKING

Organisations are also under threat from a variety of attacks aimed at their telecommunications systems. If not stopped, they can result in significant financial costs and have an impact on employee productivity.

Some network-based attacks target an organisation's central PABX. If successful they can lead to hackers being able to make cheap long-distance and international calls using an organisation's phone system, resulting in significant costs.

Such techniques have also been used to organise criminal and terrorist activities in an attempt to thwart lawful interception activities of law enforcement and security agencies. The first a victim (if they ever do) becomes aware they have been hacked is when the bill arrives or they receive a search warrant from authorities. Techniques include:

- **Direct Inward System Access (DISA):** A facility available on most PABXs and some key systems to allow calls to be made to a destination but charged to the PABX owner.
- **Unsecured remote access modems:** PABXs and larger key systems are often equipped with a dial-up modem to allow remote maintenance and diagnostics of the device. Hackers can log in and reprogram the PABX at will.
- **Voicemail hacking:** Highlighted by the controversy surrounding the now defunct News Of The World newspaper, this technique involves illegally accessing mobile voice mail accounts to obtain personal or sensitive information.

MOBILE DEVICES

Security challenges are also being posed by the growing usage of mobile devices within organisations. Smartphones, tablets and notebook PCs provide significant productivity benefits but also create new avenues for potential attacks.

Thanks to a trend dubbed the 'consumerisation of IT', employees are increasingly looking to make use of personal mobile devices in the workplace. Rather than opting for company-supplied equipment, they are pushing to connect their own tablet and smartphone devices and other 'BYO' equipment to corporate networks. This requires policies to be developed for when staff with their own devices leave your organisation. How do you ensure your sensitive data is removed from the device without compromising the owners' personal data?

SMARTPHONES, TABLETS AND NOTEBOOK PCS PROVIDE SIGNIFICANT PRODUCTIVITY BENEFITS BUT ALSO CREATE NEW AVENUES FOR POTENTIAL ATTACKS.

For CEOs and senior ICT managers, this poses the challenge of ensuring security of systems and corporate data, regardless of the type of mobile device being used as an access point.

At the same time company-supplied devices must also be kept secure. Ranging from notebook PCs and tablets to mobile handsets, steps need to be taken to help ensure they remain impervious to external attacks.

Challenges also arise from the methods used by mobile devices to connect to corporate resources. These connections range from cellular mobile networks to Wi-Fi hotspots in locations such as cafes, airports and hotels.

Many of these networks are open, meaning that data travelling across them is susceptible to interception by unauthorised parties. CEOs and their senior ICT managers must ensure security tools are in place on devices and users are made aware of the potential threats they face, including:

- **Email:** A hacker sends an unsolicited email, mobile contact or ring tone to a victim with an enticing message. Opening the message causes the device to be compromised
- **Brute force attacks:** An attacker attempts to discover a device's MAC or unique hardware address through constant polling of the device over the network. Such a compromise can give access to contact lists, text messages, emails and private photos or videos
- **Hijacking:** A hacker uses a number of sophisticated techniques to gain control of victim's mobile device, potentially forwarding calls from the victim's mobile to the attacker's own device. In addition, this technique can be used to remotely activate a mobile phone and turn it into a listening device without your knowledge.

6. OVERCOMING THE SECURITY CHALLENGE

COMBATING THE MANY AND VARIED SECURITY THREATS FACED BY AN ORGANISATION REQUIRES A COMPREHENSIVE AND MULTI-PRONGED APPROACH.

The types of potential threats must be understood and tools and processes put in place to combat them. Ongoing monitoring can then help ensure these measures remain effective. Critical components of a robust security plan include:

SECURITY GOVERNANCE

Information security governance involves establishing and upholding a culture of security within an organisation. This helps to ensure that all security management functions are designed, implemented and operating effectively. It also provides assurance that business objectives and stakeholder requirements for the protection of key information are being met.

Information security governance must begin at the top of an organisation, with the CEO and CIO, who are responsible for fostering a culture of compliance and accountability. This culture must then permeate every facet of the organisation, ensuring the required tools and approaches are put in place.[15]

Around the world, about 60 per cent of organisations admit they do not have an accurate inventory of where personal data for employees and customers is stored.[16] Introduction of a proper information security governance program would help to address this failing.

To assist in the process, there are a range of internationally recognised information security governance standards including ISO/IEC 27002 Information technology - Security techniques - code of practice for information security management, and ISO/IEC TR 13335 Information technology - guidelines for the management of ICT security.[17]

ORGANISATIONAL SECURITY POLICIES

To complement information security governance procedures, organisations must also have organisational policies that cover how employees use and access ICT resources. Such policies must be communicated to all staff, reminding them that it sometimes only takes 'one click' for sensitive systems to be compromised and vital information lost.

Policies should cover a range of areas including:

- **Social networking:** who can access these sites and from where, and what can be said when acting as an employee of the company
- **Mobile devices:** what devices can connect to the network and under what circumstances, expected conduct while using mobile devices, and policies for what happens to data on devices when employees leave the company
- **Desktop device policy:** what devices can connect to the network, what level of patching is required, what anti-virus tools should they have installed and expected conduct when using the device
- **Physical security policy:** who is allowed access to buildings and when, whether certain areas are restricted, are certain documents restricted and how are they stored and shared.

COMPLIANCE

While central to assisting the effective operation of an organisation's own ICT systems, proper adherence to security procedures is also important when it comes to compliance.

Organisations involved in dealing with personal records or financial transactions must be able to show they have put in place suitable security processes and tools to maintain the integrity of that information.

Also, if an organisation wants to do business with other large companies or government departments, adherence to a range of recognised compliance standards will be necessary.

Examples of such compliance standards include:

- **ISO 27001:** International security standard for security management, compliance may be required by end customers or business partners.
- **PCI DSS:** A requirement for companies that accept credit card payments. Failure to comply will result in fines and full exposure to any financial losses resulting from a security breach.
- **ASCI 33:** The Australian Government security standard, often a prerequisite when working on sensitive government projects.
- **Basel II:** Compliance is required when providing banking services in countries that are signatories to the agreement.
- **FISMA** (Federal Information Security Management Act of 2002): Compliance is required when dealing with agencies of the US Federal Government.
- **SANS-FBI:** Security guidelines developed by the SANS Institute which is regarded as one of the largest security research groups in the world.
- **Sarbanes-Oxley:** Compliance is required if listed or operating the US.

NETWORK SECURITY

To allow protection against external attacks, it is important to have robust network links. While some organisations rely on the public internet for connectivity, far better security is afforded through the use of a private IP network sourced from a telecommunications provider.

By separating public internet traffic from private IP networks, some carriers can provide for a distributed denial of service attack (DDoS) will not have a detrimental impact on customers using the core private IP network.

MAKING USE OF SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTIONS

Many organisations have limited knowledge of exactly what is happening within their IT systems and network infrastructure. A lack of monitoring tools means they are unable to detect signs of external security threats or evidence of inappropriate insider activity.

In a survey conducted by PricewaterhouseCoopers, 23 per cent of respondents admitted they were unsure about how many security incidents had occurred within their organisation. When asked what types of threats posed the greatest risk, 33 per cent did not know. Asked to nominate the source of attacks, 34 per cent of respondents were unable to answer.[18]

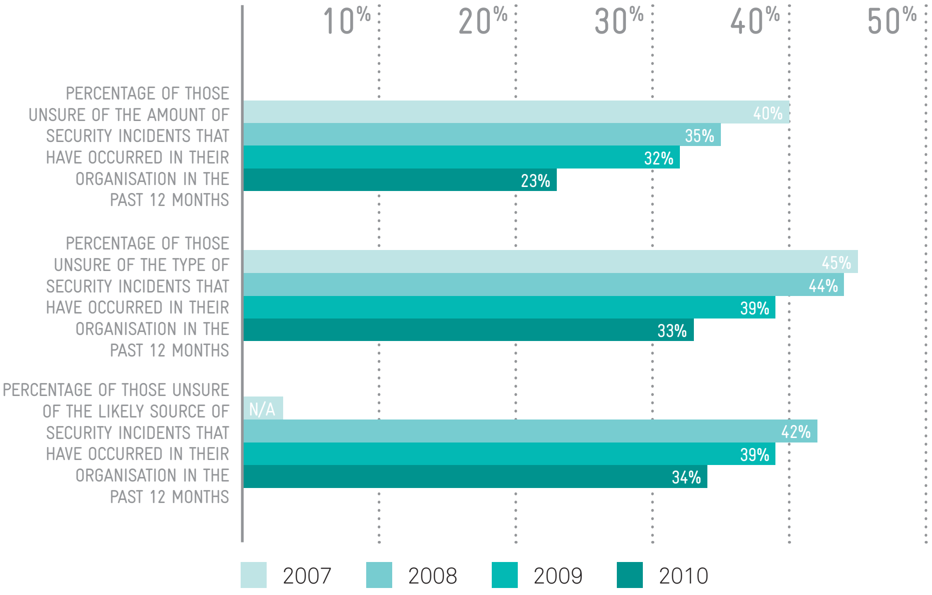
These numbers are particularly troubling when it is realised that evidence of events leading up to 96 per cent of data breaches is available to organisations prior to an actual compromise. However in most cases such evidence goes unnoticed.[19]

For this reason, real-time monitoring of networks and critical systems is vital. SIEM solutions can be used to collect, analyse and log details of activity from which evidence of security threats can be obtained.

SIEM can be particularly effective in spotting evidence of insider security threats. A large proportion of insiders undertaking attacks will perform technical precursors including downloading hacker tools, failing to undertake backups or inappropriately accessing data and systems. Such activities can be flagged by SIEM tools for further examination.

In order to build a comprehensive system to log and analyse data in real time, and determine anomalous events over time, SIEM tools should be complimented by additional forensic tools.

Figure 2: Percentage of survey respondents who report the following information with respect to negative security-related events impacting their organisation.



PricewaterhouseCoopers 2011 Global State of Information Security Survey.

An example of these tools in action can be seen within the sophisticated TSOC (Telstra Security Operations Centre). The Canberra-based T4 certified centre provides 24-hour, 7-day monitoring across Telstra's entire infrastructure providing end-to-end visibility of all circuits carrying customer traffic.

SEEKING PROFESSIONAL HELP

As the complexity of ICT systems continues to grow, keeping them secure becomes an increasingly complex task. Techniques, policies and tools that have worked in the past will struggle to meet the challenges raised by trends such as mobility, cloud computing and social networking.

To help ensure an effective security infrastructure is designed, implemented and managed, growing numbers of organisations are turning to external trusted parties for assistance. It is important that these parties are able to not just act as consultants but also act as partners in providing an in-depth approach to security defence. More importantly, these partners must have the network and technology to provide an in-depth defence approach for your organisation.

This should be complimented by an ability to monitor changes in the threat landscape to help ensure your organisation is prepared for new threats as they emerge.

[15] Leading Practices and Guidelines for Enterprise Security Governance, Trusted Information Sharing Network, Commonwealth of Australian 2006.
[16] PricewaterhouseCoopers 2011 Global State of Information Security Survey.
[17] www.iso.org
[18] PricewaterhouseCoopers 2011 Global State of Information Security Survey.
[19] Verizon 2010 Data Breach Investigations Report.

7. CONCLUSION

The security threat landscape continues to evolve at an alarmingly rapid rate. Each day, fresh threats emerge with the potential to cause significant disruption and loss to organisations of all sizes.

Threats range in type from hacking and viral attacks to nefarious activities undertaken by insiders. Maintaining effective protection against these threats is not an easy task.

Ensuring an organisation has the appropriate security processes and tools in place requires direction from the top. Board and senior executives must instill a culture of security within their organisation and allow it to be communicated clearly to all employees.

Organisations must also recognise that it is increasingly difficult, if not impossible, to have all the required security skills in house. Effective use of external experts and resources is a key component in a security plan.

HOW TELSTRA CAN HELP

Telstra has significant experience and expertise in providing end-to-end security services that cover:

- **Assessment:** Careful review of specific customer requirements and potential security risks
- **Governance:** Assessment of requirements and the organisation's ability to meet them
- **Compliance:** Review of relevant legislation and recommendations for adherence
- **Technology:** Implementation of tailored tools and services to secure infrastructure
- **Management:** Provision of network and infrastructure security management services

TELSTRA CONSULTING

Telstra's teams of security experts have been involved in the design, build and management of some of the largest and most complex networks in the country. This real-world experience means they understand the challenges faced by organisations and are well placed to provide advice and guidance on all security-related issues.

Telstra Consulting works with organisations across multiple sectors including government, finance, utilities, transport and manufacturing. Each has different security needs, and Telstra Consulting experts are well placed to deliver the type and extent of support that is required.

Telstra Consulting services include:

- **Security Certification and Compliance**
- **Risk Management**
- **Security Architecture and Implementation**
- **Policy Development**
- **Business Continuity and Disaster Recovery**
- **Security Framework and Strategy**
- **Security Vulnerability Assessments, Ethical Hacking, PC Forensics and Auditing**

NETWORK-ENABLED SECURITY

Rather than bolting on security as an additional component, Telstra has integrated advanced security capability and features into the heart of its networks. This capability includes network-based unified threat management, intrusion prevention systems, anti-virus tools and data encryption.

The result is a network infrastructure with increased resilience to security attacks and flexibility to respond to new threats as they emerge.

MANAGED SECURITY SERVICES

As more security technologies are deployed within organisations, their monitoring and management becomes increasingly complex. To assist with this, Telstra can provide a suite of Managed Security Services that can supplement an organisation's internal capabilities.

An integral part of this offering is the Telstra Security Operations Centre (TSOC), a dedicated monitoring facility that operates 24 hours a day, 365 days a year to detect malicious activity and help ensure ICT resources are not compromised.

The TSOC, a government classified (T4) facility, provides an integrated approach to security for customers. Monitoring activities are fully integrated with Telstra's Global Operations Centre (GOC) which provides service monitoring across the Telstra core networks, and the Managed Network Operations Centre (MNOC) for customer network environments.

By providing security monitoring across both customer and Telstra's core networks, the Security Response Centre team is able to pre-empt threats and escalate major issues Telstra's Computer Emergency Response Team (T-CERT) as required.

We can assist your organisation to meet your increasingly sophisticated security requirements. For more information contact your Telstra Account Executive.

CALL 1300 TELSTRA
CONTACT YOUR TELSTRA ACCOUNT EXECUTIVE
telstra.com/enterprise

IT'S HOW
WE CONNECT