Deloitte.

Cyber security
Empowering the CIO

From the Deloitte Cyber Risk Services Team

The ability to operate in our digital world is dependent on the capability we have to maintain an environment that is secure and trusted. Security has to be considered as the foundation on which we can build a business. Gone are the days when we can build a perimeter, sit back and feel secure. In today's environment we partner with others, we outsource, we have alliances, we let our customers into our systems and as we extend our networks so the once solid perimeter becomes more porous. This increases our digital footprint and reliance on others significantly.

Our approach to security and how we protect what we do has to take cognisance of these changes. Our security strategies need to align with the changes in the way we do business and the resulting structural environments. We need to be vigilant and extend our security programs to monitoring and understanding what is happening in and to our environment. We need to work on the basis of already been attacked and being prepared. We need to get the business to understand that the way they behave impacts the security of our environment. We need the business to be invested in security. Ultimately security is a symbiotic relationship between the business and IT. Business can't operate without security and the support of IT and IT cannot operate without the direction, correct behaviour and funding of business.

Deloitte is focussed on helping strengthen the security relationship between business and IT and ultimately helping improve the trust we can place in operating in our digital world.

Tommy Viljoen
Lead Partner
Deloitte Cyber Risk Services

Contents

Introduction

Thanks to the internet and mobile devices, your organisation has an ever-expanding online footprint. Your technology is online. Your employees work online. Your customers and suppliers do business with you online. And your reputation can be made or broken online.

This means cyber security is no longer an issue that can be resolved simply with more investment in software and equipment. Today's cyber attacks are increasingly sophisticated and complex, driven by elaborate and resilient professional organisations that innovate faster than their targets.

The motivations for cyber attacks have also become more complex. Hackers are more diverse and no longer just after customers' credit card details – they're interested in any information that can be monetised or used to support their objectives. Some want to make money. Others want to damage your brand. Some are just having fun at your expense.

These trends mean cyber security can't be confined to the IT department. A cyber attack can damage a business in many different ways. Recent high-level incidents have shown that a single breach can cause a domino effect, culminating in loss of revenue and goodwill, regulatory scrutiny and fines, and even share price plunges.

The first key consideration for an organisation assessing its cyber security is whether its measures are capable of preventing, detecting and adequately responding to attacks, rather than just complying with industry best practices. Compliance does not equal protection, and organisations with a mature approach to cyber security must go further.

The second crucial point to consider is whether protection against cyber incidents is accepted and managed as a whole-of-business responsibility with the appropriate level of commitment from senior stakeholders. The CIO cannot and should not accept full responsibility for managing cyber security – it must be shared with key executives and include every person with access to the organisation's facilities.

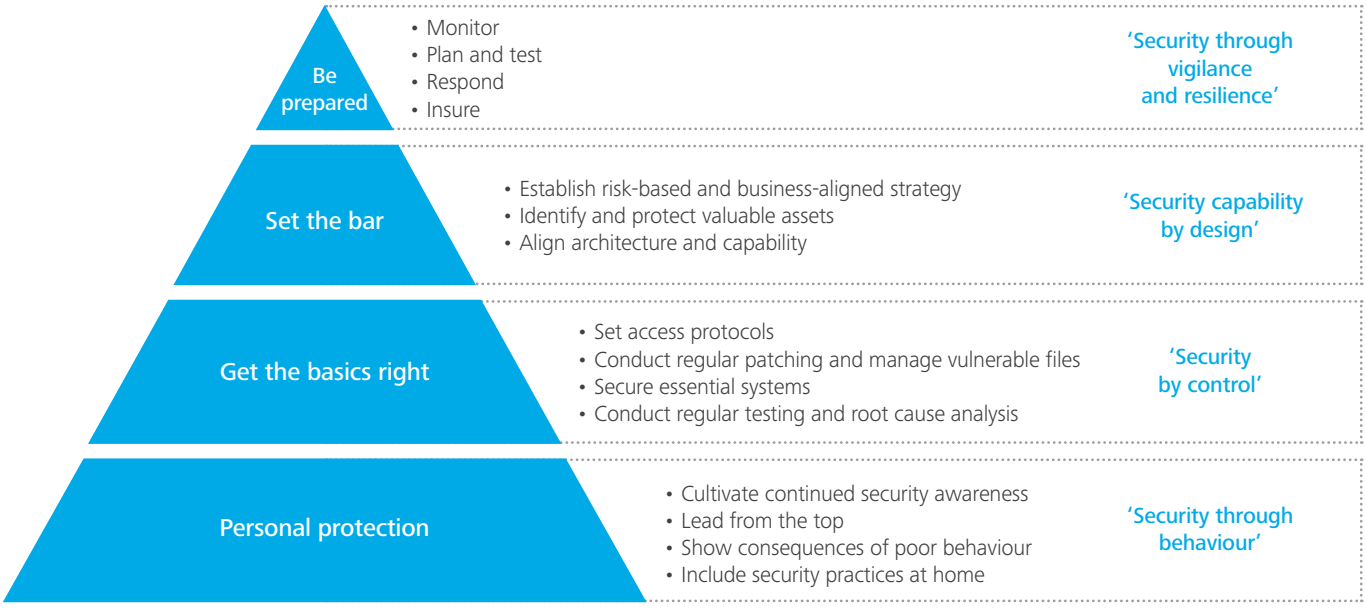
Against this backdrop, Deloitte has developed this handbook as a high-level guide to thinking about and dealing with today's cyber threats. The handbook poses many questions and provides practical insights into the evolving role of a Chief Information Officer (CIO) in relation to cyber security. It also offers advice on how to transform redundant cyber security approaches into effective ongoing security solutions.

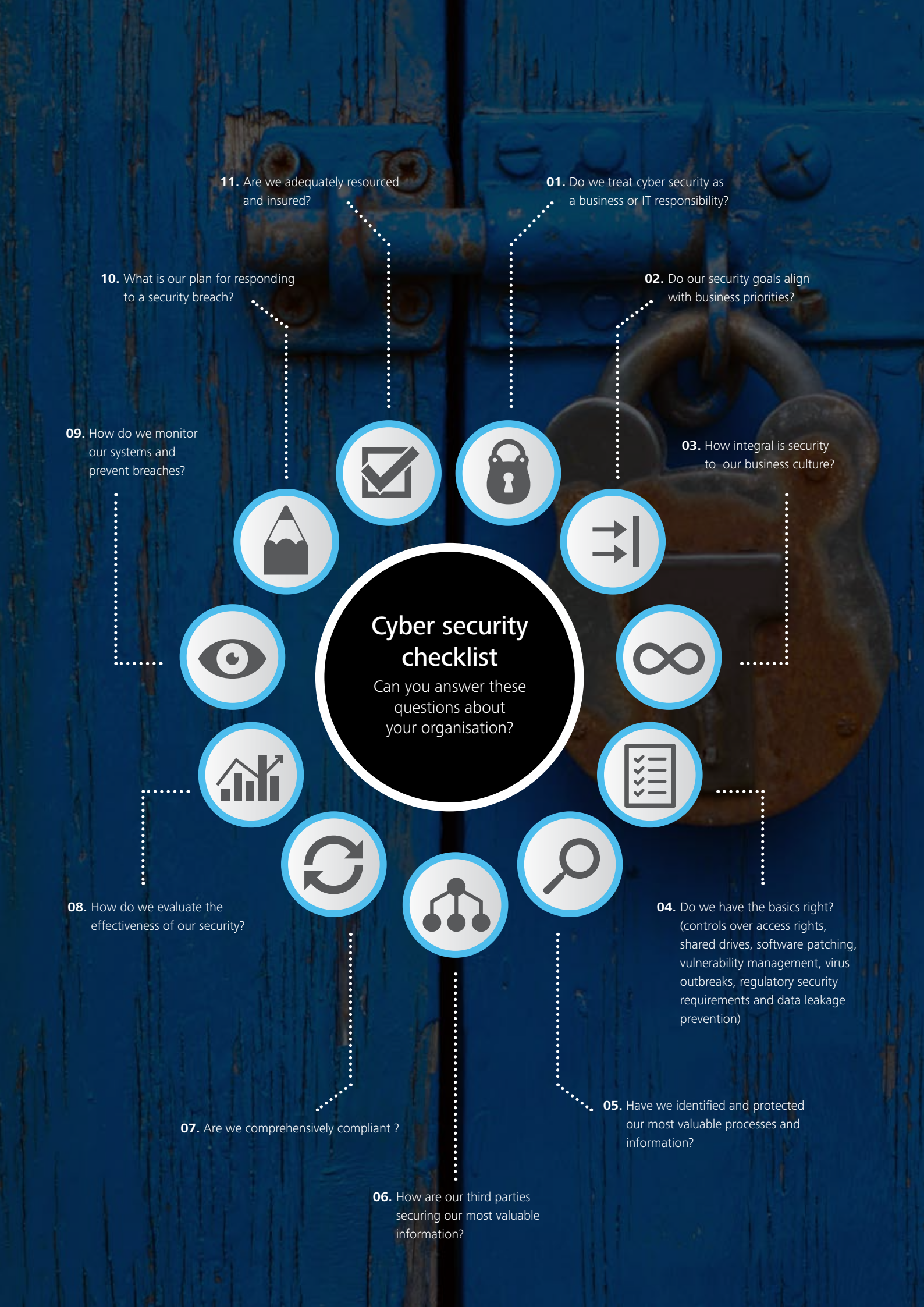
How to use this handbook

This handbook is based on the premise that an organisation's executives and board members should have 'skin in the game' when it comes to cyber security, as they are every bit as responsible to their stakeholders as the CIO. For this reason, we present a series of questions executives and the board should be asking about cyber security along with answers CIOs should be prepared to give.

The CIO should become the lynchpin in this conversation – the visionary, the facilitator, the conduit for information and the challenger of the business. The complexity of the role is a reflection of the complexity of cyber security. To assist in this process and simplify the conversation we have developed the following four steps to cyber security.

Figure 1: The four steps to cyber security




Cyber security checklist
Can you answer these questions about your organisation?
01. Do we treat cyber security as a business or IT responsibility?
02. Do our security goals align with business priorities?
03. How integral is security to our business culture?
04. Do we have the basics right? (controls over access rights, shared drives, software patching, vulnerability management, virus outbreaks, regulatory security requirements and data leakage prevention)
05. Have we identified and protected our most valuable processes and information?
06. How are our third parties securing our most valuable information?
07. Are we comprehensively compliant ?
08. How do we evaluate the effectiveness of our security?
09. How do we monitor our systems and prevent breaches?
10. What is our plan for responding to a security breach?
11. Are we adequately resourced and insured?

Know your enemy

Knowing how the threat landscape has changed is only the first step in understanding the enormous importance of cyber security. When educating stakeholders and business leaders, it helps to paint a picture of those behind the threats.

Your adversary

The organisation behind a cyber threat is well resourced – it may even be sponsored by a nation state – and is likely to run rigorous, multi-layered and long-term campaigns.

It is also highly organised, professional and capable of innovating faster than you can. For example, a cyber-crime cartel might target your network to sell the access keys to another organisation that specialises in penetrating the next layer.

Their tactics

Cyber attackers no longer use the 'smash and grab' approach. Many maintain presences inside the target organisation for years and often operate well below the security radar of their target's organisations.

Traditional security controls such as firewalls, antivirus and intrusion detection systems have become increasingly ineffective as attackers develop innovative new techniques to evade them.

Their goal

Attackers are no longer simply after credit cards data or website defacement. Instead, they're looking for whatever has value finding and prosecuting offenders and makes you competitive as an organisation: your research and development information, customer data, intellectual property (IP) and marketing strategies.

Their motivation

The motivations behind cyber-crime are varied but often fall into one of three broad categories, defined by those responsible for the threat.

1. States

State-sponsored espionage has become more common strategy for nations seeking to stay a step ahead of competitors, with numerous recent public disclosures about the extent of governmental intervention. State-level cyber threats are often characterised by extremely advanced technologies and methods, which makes them expensive and difficult to evade.

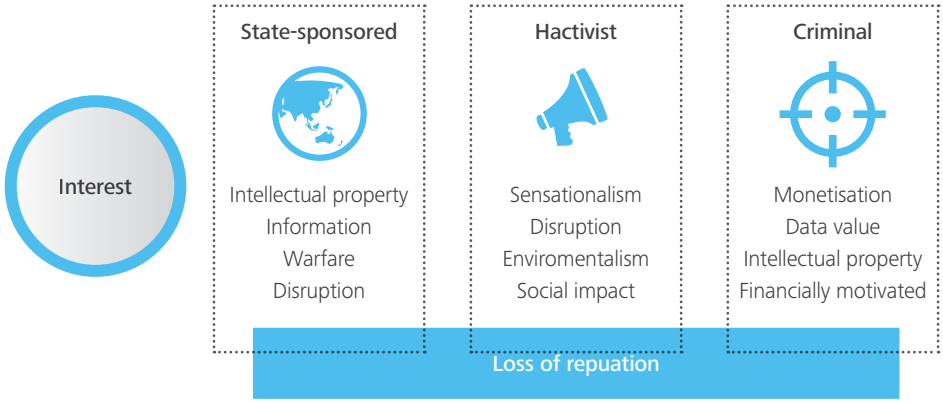
2. Hacktivists

Hacktivists are organised groups of politically motivated individuals who voice their cause publicly by targeting the reputation of organisations that do not yield to their demands. Hacktivists often launch attacks to gain publicity. Accordingly, they present more of a risk to an organisation's brand and reputation than its funds or IP.

3. Cyber criminals

The goal for cyber criminals is to monetise elements that organisations or individuals value. Cyber criminals often use sophisticated methods and tools to tailor attacks to specific organisations. This type of cyber crime is a growing source of major risk for organisations, and is exacerbated by the difficulty many have.

Figure 2: Organisations behind cyber security threats



Tip: Accidental data loss or system glitches exacerbate the effects of the three main threat sources and accounted for 54 per cent of data breaches in Australia in 2014.[1]

[1] Ponemon Institute, 2014 Cost of Data Breach Study: Australia, www14.software.ibm.com/webapp/iwm/web/signup.do?source=gts-LITS-bus-conn-NA&S_PKG=ov23509.

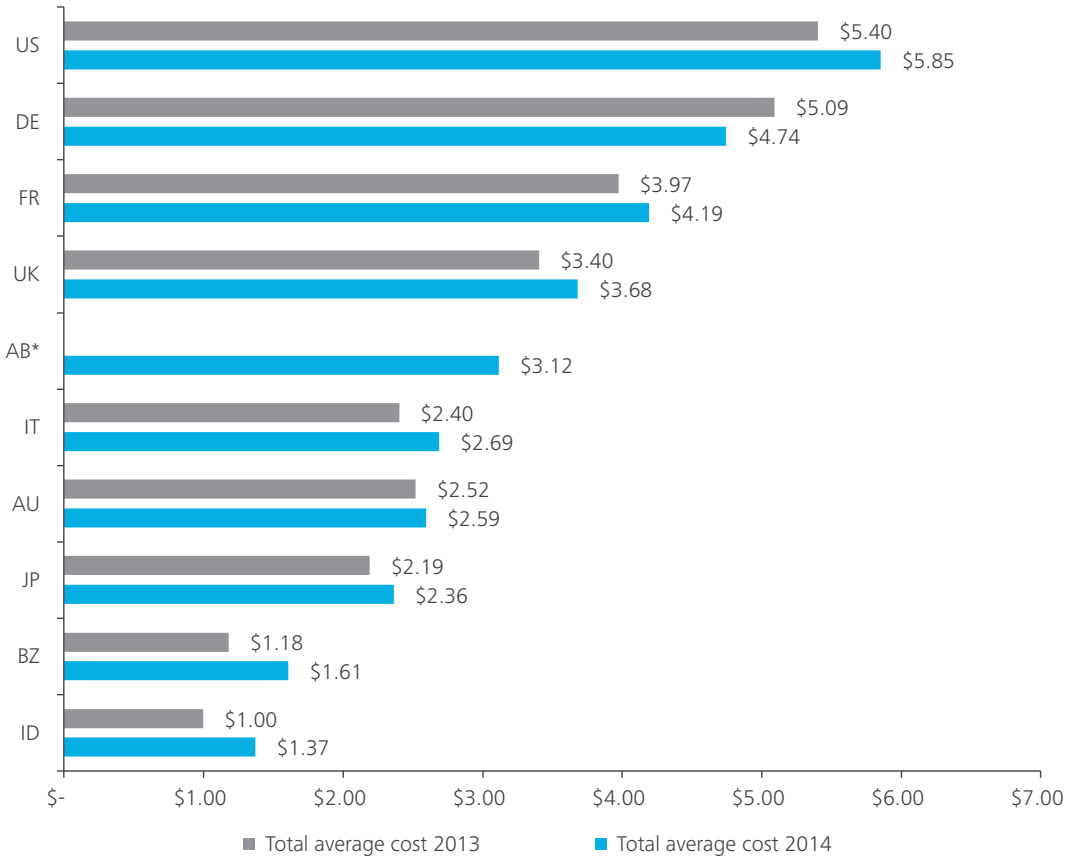
The impact of a cyber security breach

Activists, nation states, cyber terrorists and cyber criminals are just three of the potential groups actively seeking to exploit your system's vulnerabilities. However, other threats – such as human error – are less malicious but can be just as dangerous.

The consequences of cyber breach range from embarrassing to life-threatening. The fallout can extend from brand damage and loss of revenue to lower share prices and greater regulatory scrutiny. The costs of investigation, remediation, fraud, litigation and the associated penalties are also typically high.

Figures 3 to 5, sourced from the Ponemon Institute's 2014 Cost of Data Breach Study: Global Analysis, demonstrate the potential impact of cyber security breaches [2] and the average cost per record of data breaches in Australia over the five years to 2014.

Figure 3: The average global cost of data breach per organisation, in US$



* Data not available for FY 2013

[2] Ponemon Institute, '2014 Cost of Data Breach Study: Global Analysis', May 2014, http://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf.

Figure 4: The global average number of breached records, in US$ per market

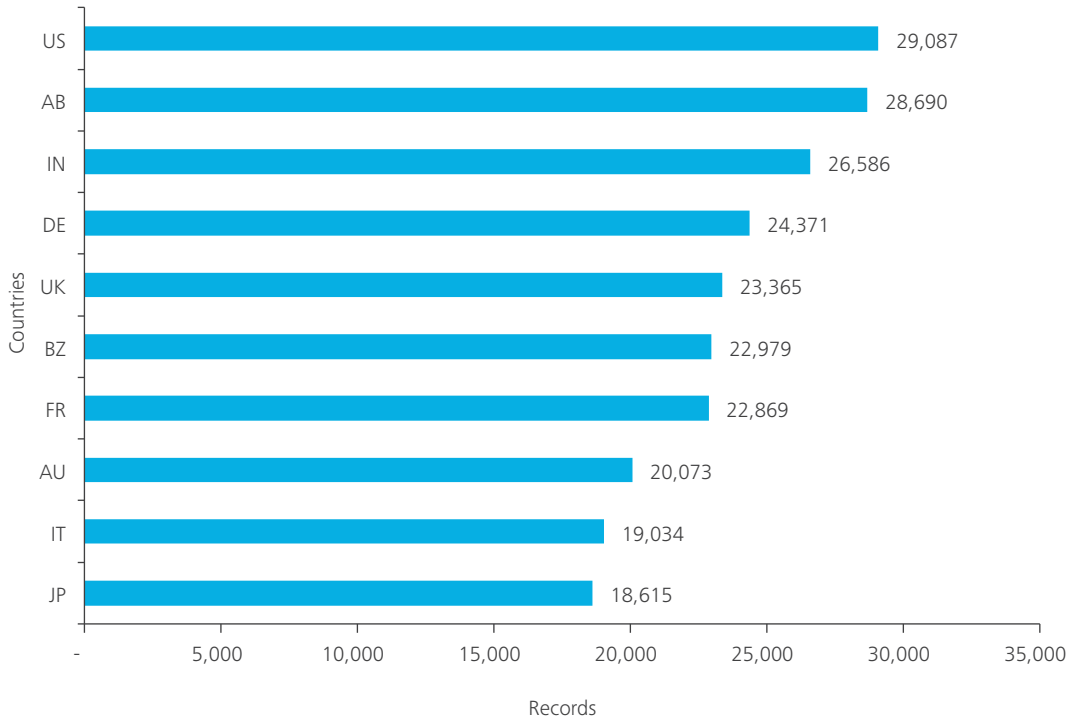
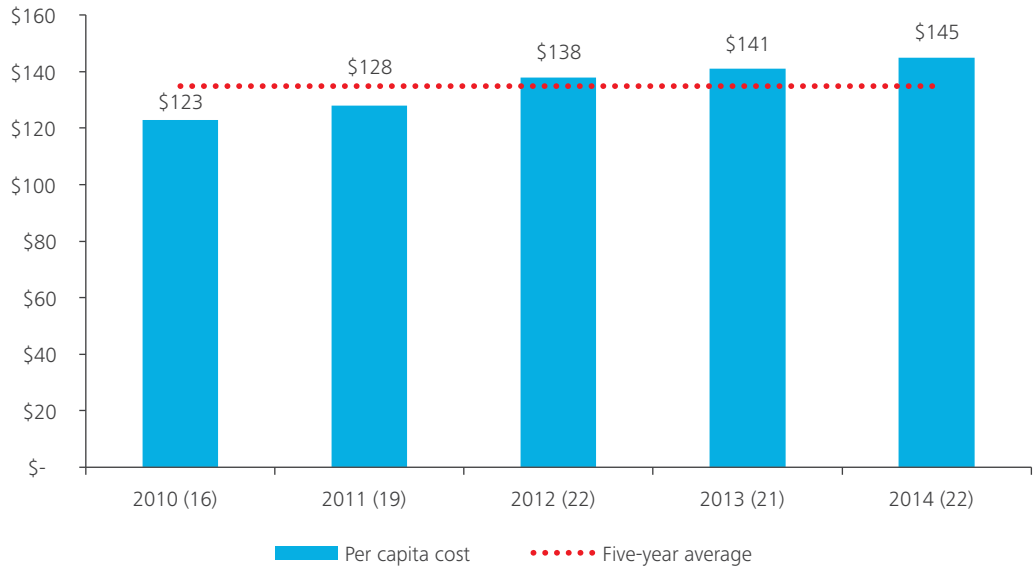


Figure 5: The average cost per capita of data breaches in Australia over five years in US$ (the bracketed numbers indicate benchmark sample sizes)



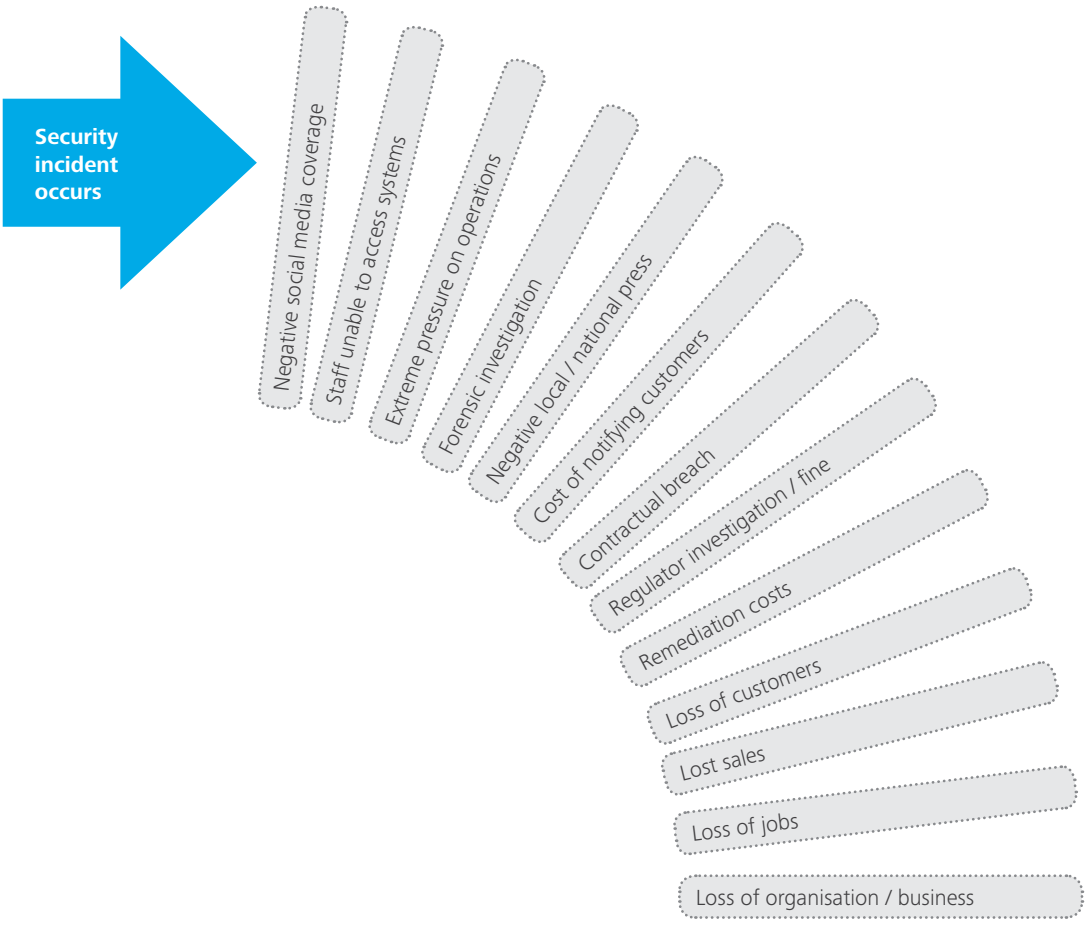
The domino effect

Recent large-scale security incidents have shown that security breaches can have a range of adverse consequences. In 2013, global retailer Target was hit with a cyber attack that cost millions of dollars and drastically affected its share price. Although the retailer had invested over US$100 million in cyber security measures, it had failed to establish end-to-end monitoring and response capabilities, and could not respond quickly enough when hackers targeted its point of sale (PoS) system during an intensely busy period.

The breach exposed 40 million customer payment card details and precipitated a domino effect that caused difficulties across the entire business, including repayments to cardholders, regulatory fines, loss of share value and significant legal action. Rather than focusing on regulatory compliance to drive security scope. Target should have considered the broader set of vulnerabilities and processes.

The other lesson is that effective cyber security has as much to do with good practice and common sense as it does with technology tools. Focusing too closely on IT alone prevents the business from seeing the bigger picture and can result in unauthorised data loss or exposure.

Figure 6: The domino effect following a security breach



Case study: Distribute.IT, when a hacker destroys your business

Snapshot:

- Distribute.IT was founded in 2002 by brothers Carl and Alex Woerndle as a start-up Internet-related business
- The pair launched the business after receiving a Domain Registrar licence from auDA, the regulator created to administer Australian internet domain names.
- The business adopted a channel sales strategy, appointing resellers to on-sell its services. Over the next nine years, the firm branched into cloud-based web server hosting, distributing SSL certificates and SMS services.
- By 2011, Distribute.IT had secured 10 per cent of the market for Australian domain names, held multiple international domain accreditations and had 30,000 hosting clients through 3,000 active resellers
- Later that year the business suffered a severe cyber attack, just as it was growing at 4 per cent a month and had recently expanded into Asia.

The initial breach – week 1

The events that unfolded from Friday 3 June 2011 would forever change Distribute.IT and the lives of its owners. At 5pm that day, Carl received a call from his CIO alerting him to a breach in the company's network.

"We had about 30,000 clients and a minimum of two per day were targeted on our network, so we were used to managing security," says Carl Woerndle.

DOS attacks and single targeted sites on servers are fairly common for hosting providers, but this attack was different. The hacker had managed to bypass the company's entire security protocol, get behind its firewall and gain access to its master user access information.

This event was the catalyst for a three-week nightmare ride for all involved with the business and its clients. While Distribute.IT was proactive in its response and compliance obligations, and re-built most of its network over the next week, these measures would not be enough to save the business. "We put in two back-to-back, 72-hour shifts during the week so it was a massive effort by all," Woerndle adds.

First-week incident response

Initial planning meeting – response considerations

- Investigate the extent of the intrusion and entry points
- Conduct breach reporting in accordance with compliance obligations
- Acknowledge potential data theft
- Prepare for client fallout from the response
- Anticipate potential hacker re-entry to network.
- Speed of response; given the access level, we could have been locked out, so a quick response was warranted.

Response

- Take the network down and lock down firewall access completely. This essentially created a network blackout for 48 hours
- Re-build large sections of the network with new hardware, password resets and network segregation
- Produce hourly updates on recovery but not disclose full breach details to clients
- Report breach to regulators, which required password resets.

Fallout

- Domain resellers down for approximately six days, resulting in loss of revenue for the business and resellers
- Firewall access carefully re-established, which slowed productivity for clients
- Client fallout largely mitigated to complaints, minor client loss.

The destructive attack – week 2

Although the company felt it had mitigated its issues in the first week, it proved that the work completed during that time was for nothing. At 4:30pm on Saturday 11 June, Distribute.IT's network monitoring system went crazy. The IT team watched servers go offline every few seconds, as the hacker had regained access to the company's network. This time around, the event escalated into an extremely malicious attack.

"The first thing they did was replace our primary website with a blank page with comments from the hacker/s about the company being under attack. The hackers then targeted and destroyed servers inside Distribute.IT's network, including back-ups," says Woerndle. "They then locked the IT team out of its own network, meaning the only way to get control was to 'pull the plug' at the data centre."

This attack targeted Distribute.IT's primary trading and hosting systems, shared web servers and backup systems, removing its ability to trade. The company had to rebuild its entire infrastructure from the ground up … again.

"We were into our third 72-hour block [working on the problem] and by this time, we were completely and utterly exhausted," says Carl Woerndle.

The network was switched on again on the evening of Monday 13 June. But with its primary websites and VoIP systems down and client databases compromised, Distribute.IT had no easy way of communicating with its clients.

The company was also facing client backlash, regulator issues and a major crisis that would grow to become a very public story. With core trading systems down for an extended period, the recovery process was going to be lengthy.

By Tuesday 14 June, Distribute.IT started to lose clients as people came to the company's data centres to pick up their equipment. The trust and brand equity that had been built up over nine years was starting to erode, and the increasing pressure of the situation began to affect all involved, mentally and physically.

"The game changed again for the company on the 16th [Thursday] because it was the first day we made the mainstream press," reports Woerndle. "The customer churn during this period was starting to accelerate … there was a lot of pressure and misinformation running around the place."

The media coverage hit its peak on 18 and 19 June – journalists were camped outside Distribute IT's door.

"Every time you wanted to go out for a break, they would stick a microphone in your face for an interview," says Woerndle. "The company sat behind the scenes as a wholesale provider so was not used to nor equipped to deal with the media pressure."

Knowledge of the hack became so widespread that the company had an email from hacking group Anonymous saying 'it wasn't us'.

"We had phone calls from every major bank in Australia concerned about credit card leakage, PCI compliance," says Woerndle. "We had the privacy commissioner on the phone – people we hadn't even heard of wanted to get a piece of the action, so to speak."

By Monday June 20, with mounting pressure and a still lengthy recovery process ahead, time had run out. With resellers possibly losing their livelihoods and many websites unrecoverable, the company had no choice but to seek a quick alternative solution.

"My brother and I knew at this point that our business was gone," he says.

They contacted Netregistry, a competitor that had expressed interest in buying the business before the disaster, and negotiated a sale of assets. The next day Netregistry assumed control of the business. The company shell also had to go through liquidation in the months ahead.

The aftermath

So, how have the brothers recovered personally and professionally from this incident?

"It was a perfect storm of events because we had plans to open up in China and were preparing for an acquisition," says Carl Woerndle. "So after nine years, early 2011 was the first time we put our homes up against our business. The single hardest thing to this day was me going back home a day after the end of it – I hadn't seen my family in three weeks – and telling them we had lost everything."

The two spent nine years on the business, working seven days a week, and taking only four weeks of holiday during that whole period.

"We put our heart and soul into it. It took Alex and I six to 12 months to be ready to move on," adds Woerndle. "To my brother's credit, it was he who came along one day and said, 'You know what? Nobody ever talks about this stuff. There are a lot of lessons there for

other people; maybe we should talk about it' … I remember looking at him thinking, 'Are you mad?'".

Since then Carl Woerndle has joined Deloitte's Cyber Security team taking the messages learned from his experiences to clients. He's now presenting across Australia in association with the CIO Executive Council and working with Deloitte's clients to help them better protect themselves from similar events.

The perpetrator and access points

The hacker was almost certainly an Australian resident. The main suspect (although never formally charged) was not connected to the company in any way and the motivations seem to be completely random and malicious in nature.

The main entry point was carefully targeted towards a company employee who was deemed vulnerable. The hacker was able to save key logging malware onto the staff member's laptop (malware checks did not detect the application). The malware built up a password database and used the laptop's secure VPN connection to access the network.

Key takeaways

The game is changing rapidly. Cyber security is no longer just a concern for the CIO and IT. This is a whole-of-business issue and requires a whole-of-business approach.

Educate your employees both in terms of business IT security and IT use and personal security – the crossover between the two is too large to ignore personal security behaviour.

Get the basics right. In today's world, systemic security failures are hard to justify when defending against negligence.

Protect what matters. Redirect spending and capability to information and systems that really matter and isolate these from the rest where possible. You cannot protect everything.

Know when you are being attacked. Invest in monitoring and detection, not just protection.

Be prepared to deal with a successful hack. It can be difficult to make sound decisions in a state of panic. Test the effectiveness of your response plan and use what you learn to improve it.

Have a communications plan in place to respond to and manage media attention.

Understand how your insurance treats cyber security. Review your insurance policies with regards to IT risks, especially cyber-related claims and data loss, as many older polices may not cover these. Also review against crisis costs – many policies will cover companies from expenses related to an incident recovery (see insurance discussion, page 35).

Get help. Don't be afraid to engage external parties in the planning process. Having third party organisations challenge your processes can add great value to your security capability.

Start forensics early. The way you respond to an incident initially can dictate how it is resolved in the long-term. Engaging forensics early in the process can help you isolate entry points, capture key information and carefully plan a response. Jumping too quickly and aggressively into the response process can tip the hackers off and create a much larger issue. Forensics is critical to ensure a considered and effective response process.

Don't entrust key information to a single employee. Fatigue can become an issue in lengthy outages following an attack. Sharing the load and responsibilities among a handful of trusted staff makes it easier to manage fatigue and help the business recover successfully.

Cyber security myths

Organisations commonly mistake the following 10 assertions as evidence of adequate security.

1. We conduct penetration tests

A penetration test is worthless unless the organisation can manage and remediate the vulnerabilities it discovers. It is also important to consider the scope of the test; does it cover your whole infrastructure and simulate the most likely type of attack and does remediation also focus on root cause?

2. We have invested in a high-end security tool

Security tools are only fully effective if they are correctly configured and appropriately monitored, maintained and integrated with overall security operations.

3. We comply with industry regulations and best practices

Compliance often requires only the bare minimum of security measures. Consider whether the compliance requirement is enough and the scope covers all your important systems and information. For example, PCI compliance focuses on payment card information often to the exclusion of other valuable information.

4. A third-party provider manages our security

Regardless of the provider's capabilities and credentials, it is critical you understand the threats to your organisation and how they are dealt with. Make sure your security provider is formally obliged to keep you informed of its security roles, responsibilities, control effectiveness and any breaches.

5. We only need to protect our internet-facing applications

Protecting the internet-facing perimeter of an organisation is important, but should not be your only focus. You also need to have controls against malicious and accidental insider threats.

6. We have never been attacked, so our security is good enough

Security threats are constantly growing in complexity and sophistication and perpetuators can be dormant for considerable periods.

7. Security is well-managed by the IT department

IT should not be solely responsible for managing cyber security. A security incident can have significant and long-lasting effects for the entire business. This is why it's important for business leaders and the IT department to manage cyber security together.

8. We have invested in strong security controls

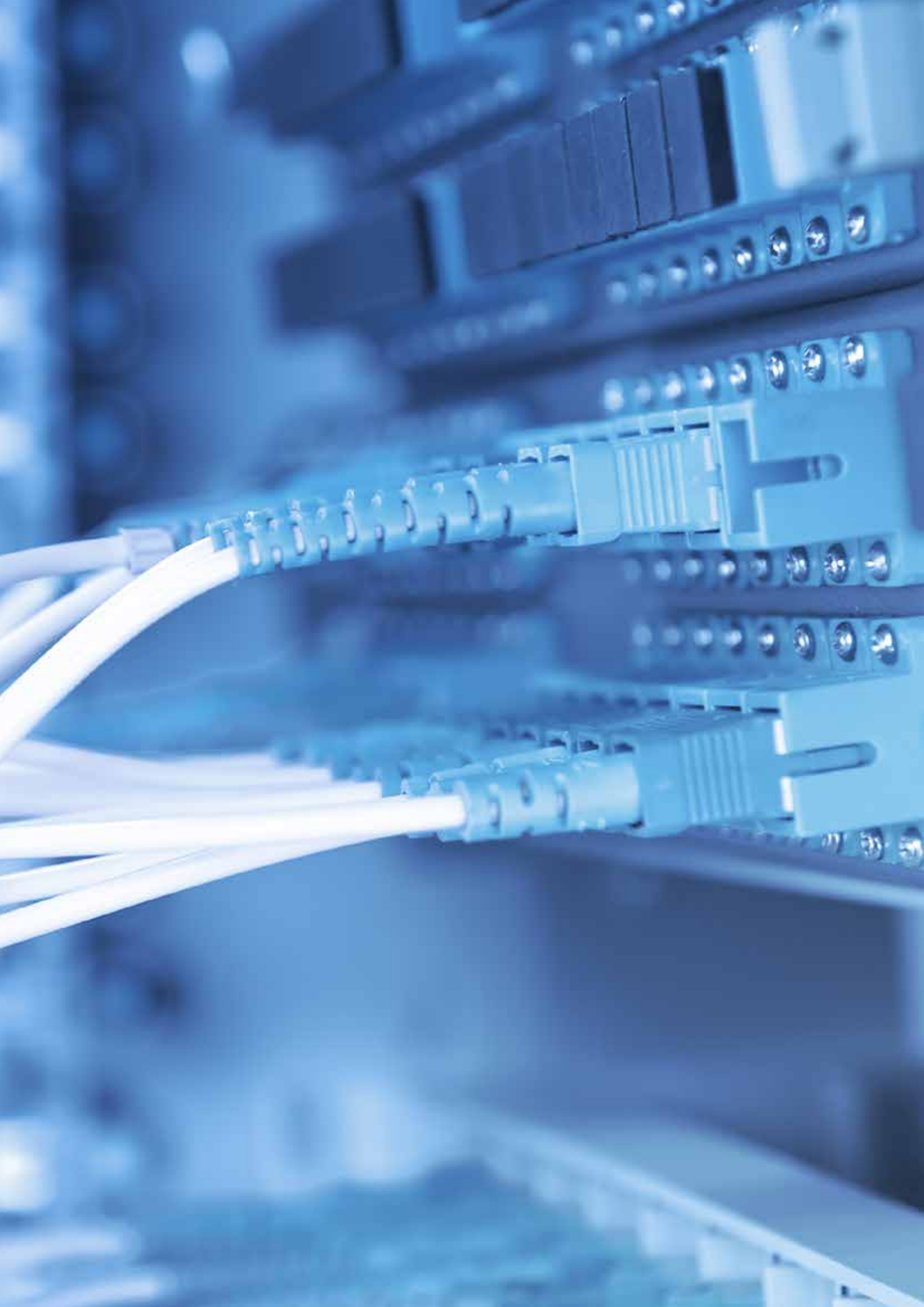
It is not enough to focus on traditional IT security controls driven and prioritised by the IT team. To be effective, security investment needs to align with and secure critical business elements such as point-of-sale devices, medical equipment and engineering systems.

9. We are statistically unlikely to experience a security breach

It is actually highly likely you will suffer a breach at some stage, so be prepared. Every organisation needs to be ready to quickly respond to breaches and have a plan for communicating the situation to customers and third parties so business can return to normal as quickly as possible.

10. We have completed our security project

Security is an ongoing process rather than an outcome. It is also something that should not be confined to a specific team or department. You need to embed cyber security measures into your organisation's key processes and invest in ongoing updates and monitoring to protect against newer, more elaborate attacks.



The 11 questions leaders should be asking the CIO

Over the past few years, we have encountered a number of questions that savvy boards and executives commonly ask when assessing the level of their organisation's cyber security. We have built on these to give you a list of 11 questions the board and executives should be asking CIOs. To accompany each of these, we have also listed questions the CIO should be asking about the business to assist with effective cyber security.

The 11 key cyber security questions

1. Do we treat cyber security as a business or IT responsibility?
2. Do our security goals align with business priorities?
3. Have we identified and protected our most valuable processes and information?
4. Does our business culture support a secure cyber environment?
5. Do we have the basics right?
   (For example, access rights, software patching, vulnerability management and data leakage prevention.)
6. Do we focus on security compliance or security capability?
7. Are we certain our third-party partners are securing our most valuable information?
8. Do we regularly evaluate the effectiveness of our security?
9. Are we vigilant and do we monitor our systems and can we prevent breaches?
10. Do we have an organised plan for responding to a security breach?
11. Are we adequately resourced and insured?

It is the leader of the business who ultimately is responsible for managing cyber security risks. It is critical that business leaders ask the hard questions about cyber security, and are sufficiently informed on the state of cyber security within the organisation to be able to assess those risks and their potential impact to the business.

Is cyber security a business risk management issue?

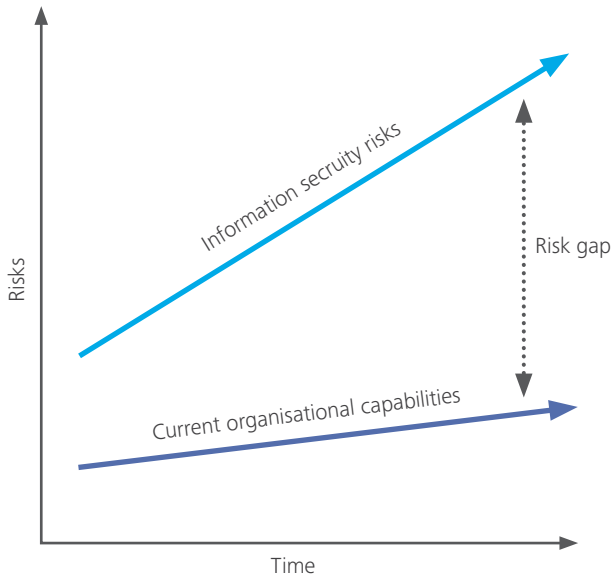
(Considerations for questions 1-3)

Organisations should only conduct business over the internet if they have applied the appropriate security.

As the internet becomes increasingly central to operations, organisations become more vulnerable to cyber security threats such as hacking, denial of service and data theft (see Figure 7). The always-on nature of the internet means these threats are ever-present and constantly evolving.

Most organisations treat cyber security as an IT issue – they purchase and deploy security software, complete the ISO27000 spreadsheet and cross cyber security off the 'to do' list. However, as CIOs know, the growing complexity and constant presence of online threats means cyber security is a strategic risk management issue that demands constant attention and ongoing investment.

Figure 7: The growing 'risk gap' between cybersecurity capabilities and potential risks.



In the digital economy, effective cyber security can mean the difference between a business's success and its failure. The most successful businesses will be those that are:

- **Secure** and protect their critical assets against known and emerging threats
- **Vigilant** in detecting unforeseen threats and reducing detection time
- **Resilient** so they can properly respond to critical incidents.

Questions for the CIO to ask of IT and the business

1. How often are executives and the board informed of the organisation's cyber capability and any attacks?
2. What level of interest do the executives take in setting the level of cyber capability and cyber security budget?
3. Do the executives and board treat security as the foundation that provides the right to conduct internet-based business?
4. Is the business embarking on any major digital, big data, cloud, mobility, outsourcing or third-party ventures in the next three years?
5. Is the cyber strategy for the next three years aligned to the business strategy?
6. Has the business specifically identified the most important information collected and held by the business and the level of protection expected for that information?

Does your business culture support a secure cyber environment?

(Considerations for question 4)

A strong security culture can in some ways make up for poor controls by helping staff do the right thing despite the environment. On the other hand, a poor culture will often override adequate controls. This is why it's important to have the right cyber security culture in place across the business.

Without a convincing reason to behave in a secure way, employees often follow cues from their peers, which can increase the risk of a security breach.

In contrast, organisations that promote a culture of security – by building security-by-design into systems, establishing decision-making processes for staff and creating a security-minded workforce – are more likely to successfully defend against social engineering, insider attacks and other security threats.

Questions for the CIO to ask of IT and the business

1. Does the executive actively support a secure online environment?
2. Do we tolerate minor infringements?
3. Does functionality trump security?
4. Do we provide ongoing security awareness training to all staff?
5. Does awareness training extend to personal and home-based security?

Case study: Johnson & Johnson, WWIS Enterprise ISO Leadership

Pablo Diez Del Corral,
Global Director,
Enterprise Security & Risk Management

A highly competent and experienced executive in the healthcare, consumer goods and services markets with significant achievements in leading IT and developing relationships at CXX and Senior Government levels. Pablo accumulates 23 years of global leadership experience (Americas, Europe and Asia Pacific) in multinational companies with full P&L responsibilities, including seventeen years in senior management of information technologies and communications, and eight in retail operations. He is characterised by his exceptional ability to achieve outcomes through high-level motivation, influencing and negotiation skills that have allowed him to successfully lead organisations through periods of substantial change in company culture, operations and organisational models. Security and Operations have been the hallmark of his professional career and the constant focus of his professional development.

Angela Coble,
Director Information Technology
(Former: Global Manager,
Enterprise Security & Risk Management)

An internationally published author with experience in Health, Utilities and Finance sectors - enthusiasm and personal energy has supported Ange's eclectic experience. Ange has enjoyed senior roles in ICT; operations; consumer strategy; strategic development; organisation transformation; information management and information security programs; and risk management. Ange's ongoing success is due to her strong leadership and proven ability in implementing effective strategies to achieve successful business outcomes to create operational advantage. Ange is also passionate about supporting and mentoring young women through life choices and into IT careers.

NOTE: Since the writing of this article Angela has moved into the role of Director Information Technology at Johnson and Johnson.

Highly recommended:

- SANS Top 20 Critical Security Controls Report
- 2012 Unified Communications and Collaboration Study Unified Communications and Collaboration

> When I took over this role, first thing I asked is 'what's the strategy that we've been following?

The security triangle of people, processes and technologies can be found in every security framework. Technology is always taken care of by technologists; processes are frequently reviewed and updated, but the third element – people – is often forgotten.

A more rigorous focus on people and culture acknowledges that having the latest technology is not a foolproof solution to information security. After all, what's the point of the tools and processes if someone still uses the password "password"? With breaches fuelled by ignorance almost as frequently as malice, a tech-agnostic strategy is also needed.

Johnson & Johnson are working to create awareness, teach the appropriate skills, while providing the platforms for collaboration and communication that have led to a more connected and highly secure corporate environment. This is their journey.

Identifying the issue

"When I took over this role, first thing I asked is 'what's the strategy that we've been following?'" says Pablo Diez del Corral, Global Director, Enterprise Security & Risk Management at Johnson & Johnson.

"I got great documentation and presentations saying we're implementing an IDPS system and deploying web filtering appliances, and we're doing this and that, so I asked – are we only dealing with machines? The security function was properly staffed in all other aspects except this one," he says.

"For me it was a matter of following a rigorous approach. At the time, the people piece was almost an afterthought. Somebody was looking after it, but they just followed pre-written instructions and didn't question it. Unless you create the conversation around it, you're still going to see the problems."

Creating a strategy

Diez del Corral, coupled with his colleague Angela Coble, Global Manager, Enterprise Security & Risk Management, set to work on creating an initial gruelling 90-day plan to kickstart their three-year strategy complete with roadmaps, major and minor initiatives across four different quadrants.

A long-term vision and mission were crucial to help guide and empower all stakeholders, while branding helped to tie ideas back to the strategy. But most importantly, it had to be dynamic and ongoing - not dependent on Coble and Diez del Corral, their team or where security sits in the organisation.

"No matter what the changes in my organisation and structure, no matter who is sitting in my chair in the future, this strategy is not going to be affected; there's no need to change it. It's got to survive three years; then we need to review it and start looking at the following three years," says Diez del Corral.

Four roadmaps, three years, 12 quarters

Johnson & Johnson's people and culture strategy contains four different functional focus areas in which to plot key initiatives with a planned quarterly outcome, and an annualised event project plan.

Each functional area has a roadmap that covers:

- Preliminary investigations
- Analysis of business activity
- Assessment of existing systems
- Identification of unique functional strategies and interdependencies
- Design and roadmap of functional stream (including priorities)
- Processes and controls
- Education and awareness (internal & external)
- Global, regional & local external environment
- Implementation
- Post-implementation review

The functional areas of Johnson & Johnson's strategy include:

Education and Awareness

"At the beginning all we had was a monthly call with our Information Security Officers (ISOs) and Information Security Groups (ISGs), and we asked people what they were getting out of them to ensure they were always helpful," says Diez del Corral. "We didn't provide the option of cancelling them, just improving them."

"We have to do different forums for different groups," adds Coble. "Nothing is too small, even if you start with just this monthly call, planting the awareness, that's enough. We're seeing that flow-on as people pro-actively invite us to take part in those types of conversations."

The education and awareness factor extends from information security officers and information security generalist, throughout the business and even to external partners. The initial education program, which covers technical skills as well as people skills, was carried out

in the first year. This is being followed by a business succession program, which will ultimately become a mentoring program.

"A lot of these guys have plenty of experience, it's not that we're teaching them the first letters of the security alphabet. But it is that relationship that puts them in an alert state, it creates a community or a family, and you don't want to let your family down."

The education of J&J professionals will eventually be measured on an annual recertification process, with the potential for all preferred qualifications to be available in-house, along with a process to measure progress. Coble says semantics are important when approaching highly qualified individuals.

"It's a development opportunity, but you have to be careful how you approach it, because there's nothing worse than going up to a highly qualified person and saying 'hey, we're going to measure your skills and then give you some training'," she says.

"Some of them can really run circles around us in specific technical areas, so you need to be very careful," adds Diez del Corral. But they recognise that their people skills aren't that great, and for someone high up to recognise that within our organisation in under 12 months is great."

While some companies worry that investing in the training and development of staff might mean they will leave the company to seek different opportunities with competitors, Coble and Diez del Corral say it's still vital to invest in your people.

"When people see that you are investing in them, their loyalty increases. Yeah, you might lose some, but you might win a lot more, so we want to be able to give people the training that they need to make us the best we can be," says Diez del Corral.

Collaboration and Communication

Knowledge shared is knowledge used, so Coble and Diez del Corral also set about enhancing the communication and collaboration capabilities of their staff.

This involved creating an omni-channel support platform for sharing information, asking questions and connecting with other professionals with up to 30 different channels that looked simple and easy to use, but which took a huge amount of effort to plan.

"The message was: Be aware, not alarmed," says Coble. "Like a duck, our legs can be really paddling under the surface, but our exterior is calm. So we deliver the message in a way that creates awareness, not panic, and gives our partners confidence that we are the paranoid ones so they can go about their normal business."

The strategy is intended to expand from providing support in the form of blogging and sharing platforms, to becoming a system for real-time updates and response, which should lead to increased productivity and business expansion. Coble says she was inspired to take on the omni-channel project after seeing the results of a 2012 IDG Enterprise survey on the primary drivers for unified communications, which found 61% of respondents saw increases in productivity after implementing UC.

"Any commercial business needs to be thinking that way, so why can't we use it in security? It's not like I'm reinventing the wheel, I'm just using it for a different purpose with my audience," says Coble.

The company currently has a branded data protection site that is visible to all J&J employees, while Coble also records presentations and distributes them among staff members to play back on-demand as a means of consistently drip-feeding information.

The two are currently in the planning stages of developing a new security hub where practitioners can find all their existing updates and documentation, while allowing them to seek additional information from other sources and connect to the broader community, including subject matter experts, security operation centres, and global service desks.

"There's so much work behind the scenes, but for our security family and business partners it should appear effortless. When in reality, it is a well orchestrated strategy with drip-fed initiatives, delivering vested outcomes for J&J. That's how we want it to look, like something that's just happening through natural osmosis," says Coble. "Yet behind the scenes there's this full omni-channel strategy happening, which encompasses not only collaboration but the multi-channel and diverse channel piece so we're delivering consistent, trusted, unified communication at every step."

In addition to security teams around the globe, Coble and Diez Del Corral are also working to create a connection between the ISOs and their security governance and operating teams, in order to build relationships at every tier of the organisation.

"We work in the middle giving them visibility to our ISOs and vice versa," says Coble. "It was recognized in our initial voice of customer surveys that a better connection was required with the ISOs. Which as the governance team we believed was quite remiss – this extended team has lot to offer and their doors are always open."

Diez del Corral asserts that it's not a matter of everyone holding hands and singing kumbaya, because that's not how security works. Instead, it's emphasising the importance of making security the responsibility of everyone, as increased awareness and support throughout the organisation will ultimately lead to greater productivity.

Roles and responsibilities

In order to have that company-wide awareness, the responsibility has to start with the security professionals. J&J's three year strategy involves invigorating and committing to creating a more people-based security landscape, which should lead to an expansion of that commitment throughout the business that can be maintained and continually assessed.

"There's about 40 ISOs globally, and sitting beneath them is a series of ISGs who these security officers are mentoring to see if they want a career in security," says Coble.

Starting with new recruits, Diez del Corral and Coble have set up a seven-step induction program for new information security officers.

"During the course of that program, we have conversations about their experience, their education, as well as their interest in security overall, and then you understand who they are as well as their motivations," Coble adds.

J&J uses a four block model that allows them to place potential new ISOs under a category based on a combination of experience and education, connecting them to the ISO community, alongside both their colleagues and their leadership team.

"We don't want our ISO's in the red, where they have no experience and no education, but I'm happy for most of them to be playing in the amber, with high experience but no education or vice versa. Then you want a couple, a small percentage that sit in the green area, who have both experience and education, and they can be team mentors," Coble explains.

You can use any model to marry people to quadrants, so long as it's reflecting what's important to your company, she says.

"For us, education and experience are important, but for others it could be something completely different, which rephrases how they approach the measurement of those quadrants. This is very much a people and culture driven strategy so I'm not as concerned with education because that something you can achieve as you go."

The next step, according to Diez del Corral, is to show your staff that you trust them by not micro-managing a project.

"If I give someone something to do, I know that he or she will be running on this. They often come back to you and say 'oh you're not checking on this' and I say 'of course not, it's your responsibility and I know you're doing it' and they really can't believe it," he says.

"They're professionals that have been in the field for years and they still think you're giving them too much freedom. Now they feel proud of their job, and they're doing it better. I don't use it as a technique to get more out of them but it does seem to just work that way."

Maturity and metrics

To gather metrics, the monitoring and review of J&J's people and culture must be completed at a strategy level, and be incorporated within each of the specific functional areas as part of the post implementation review. Items to be covered will include a general maturity model against strategy, an ongoing audit/review program, as well as frequent metrics reporting.

"When we started on this journey, we had no metrics to measure the people side of security. But as an engineer, for me, being able to measure something is key," says Diez del Corral. "We want to have metrics that are meaningful. I don't want to measure anything that nobody is going to be looking at."

Coble says it's good to pulse check your audience for good news, bad news and ideas, then revisit your strategy twice a year. J&J will also apply pressure tests to the strategy to see what has changed, while revisiting their roadmaps each month. Coble says that doing this will ensure they remain aligned and have not deviated from the roadmaps.

From getting feedback about the earlier monthly call sessions with ISOs, to annual in-house surveys on simple housekeeping logistics, metrics were collected and answers were delivered to governance teams.

"You just need to ask the questions of the people working with you, and then without filtering those, give the answers to your management, without any painkillers. So you are going to see them and take them on the chin," says Diez del Corral.

Coble explains that a survey was carried out at the very beginning of the initial 90-day plan to kick off the strategy, and then again one year later. The results were quite positive, with a number of people feeling more secure and satisfied.

"It was validation for us, because we were personally committed to delivering this strategy," she says. "We asked simple things, like do you like the monthly forum? Then slowly stretched it to say, would you be interested in using

social media and other collaboration tools? We gained valuable insights into our community and their needs..”

Metrics and feedback regarding the usefulness of tools and platforms should be gathered continually in a bid to remain productive and relevant, says Diez del Corral, as well as trimming unhelpful expenditure.

“For the first survey, there were no tools being used for communication, but there were other tools for different aspects of their functions to evaluate risks, to analyse our business, to do all the renewals, etc. So we wanted to know - are these tools really a help in your daily life, or are they a burden?” says Diez del Corral.

Security is no different to any other part of the business, says Coble, so the first thing you want to do is to get rid of waste.

Stakeholder management

In the first 90 days of developing their strategy, stakeholder engagement was heavily featured, with over 50 hours of meetings, getting feedback, and listening to the voice of that consumer, says Coble. Now, down the track, regular stakeholder meetings are a must, with a recommended 10 hours per week set aside to discuss global strategy.

Leadership buy-in

“It is critical of course to have senior management buy-in, because they are going to make the final calls,” says Diez del Corral.

Both the Corporate CISO and the VP of Education for the J&J corporate IT area took interest in the messages being sent in this space. Now that they’ve hit the ground running, Coble and Diez del Corral have had to commence stakeholder engagement at a whole new level.

While stakeholder management should be covered in each of the functional areas, a broader engagement in change and communications on the ISOs framework is important. Having walked in the shoes of ISOs and ISGs they now work with, both Diez del Corral and Coble were able to identify the issues and rely on their understanding of the roles and the landscape to create the right relationships.

Building relationships

“We were successful because we had two things. First, we had trust on all sides, not only management but the people that were working with us. And secondly, we asked the right questions because we have been there before,” says Diez del Corral.

Though many companies would opt to work with HR, Coble explains how, despite coming into the role from a sales and marketing, communication background, with little technical security experience, she could have that different level of conversation with staff because of her background.

“It wasn’t by chance that we were put into these roles, there was consideration of our experience but also that we had already formed those relationships, so for us it was just a natural progression,” she says. “We were already trusted as being part of the team, and when we stepped across the line into the governance team, we were still the same people.”

Whether it is via email, call, Skype or face to face, your time is always valued, says Diez del Corral, who found there’s great success in giving first and asking second.

“If we go out to them with something fairly critical that we need an answer on immediately, they know we only ask when we need it, and they respond without hesitation - and that costs you nothing but your time,” he says.

In the end, the focus on people and culture as a security strategy means recognising that you can’t do anything without taking the people on the journey with you.

“If the board is looking to appoint someone in a role, they have a specific skillset they’re after, but the board has to decide what’s the right fit - which could actually be an unusual appointment – based on historical roles and its not an easy thing to determine,” says Coble. “When an organisation is willing to put resources behind an initiative like this, actually understanding their networks is really important. The effort you put into people and networks really pays dividends in a people and culture piece.”

Conclusion

The success of J&J’s strategy, while crucial for IT and the information security team, can also be tied back to the organisation’s credo.

“What are we trying to achieve? It’s not just all these applications and hardware. Whatever it is, it translates into what our company does,” says Diez del Corral. “We are not isolated, or put into silos, you are not only the technical people but a part of a company that is touching millions of people one at a time, so it puts it all into perspective.”

Lastly, Diez del Corral and Coble say that it’s important for all companies looking to take on a strategy in people and culture to ensure they are being realistic and taking into account the resources available to you.

Angela Coble's simple steps to develop your people & culture security program:

Pulse check your audience
- Good news
- Bad news
- Ideas

Build your strategy
- 3 years
- Dynamic – not dependent on you, your team or where security sits in the organisation
- Maximum 5 functional focus areas

Create your brand
- Need a visual to tie your ideas back to your strategy

Operationalise your strategy
- Build your roadmaps for the 3 years
- Cascade to major initiative level for each year

Sell your story
- Create the communication plan
- Needs to look simple externally but huge effort to plan

Revisit your strategy twice a year
- Pulse check your audience
- Pressure test your strategy – has anything changed

Revisit your roadmaps each month
- You need to make sure you're aligned and have not deviated
- Teams need to work autonomously with clear direction

Set up regular stakeholder meetings
- Example: 10 hours of meetings for global strategy per week is average

Create a delivery channel for your efforts
- How to get the outcomes to your audience

Do you have the basics right?

(Considerations for question 5)

Deloitte conducts extensive vulnerability testing, penetration testing and social engineering work for clients. Based on our experience, we have found that the 80:20 principle applies to cyber hacking – in 80 per cent of cases, we can penetrate security systems because the client has not vigorously applied the basics of security controls.

The Australian Signals Directorate issued a list of the top 35 strategies for mitigating the threat of cyber attacks on ICT systems. It rates four of these as essential for security effectiveness:

- application white-listing
- patching applications
- patching operating systems
- minimising administrative access and privileges.

In the past, lower threat levels and plentiful paper trails made it easier for the entire organisation – from the shop floor to the boardroom – to understand and observe security controls. In today's environment, that visibility is lost and the importance is not always understood.

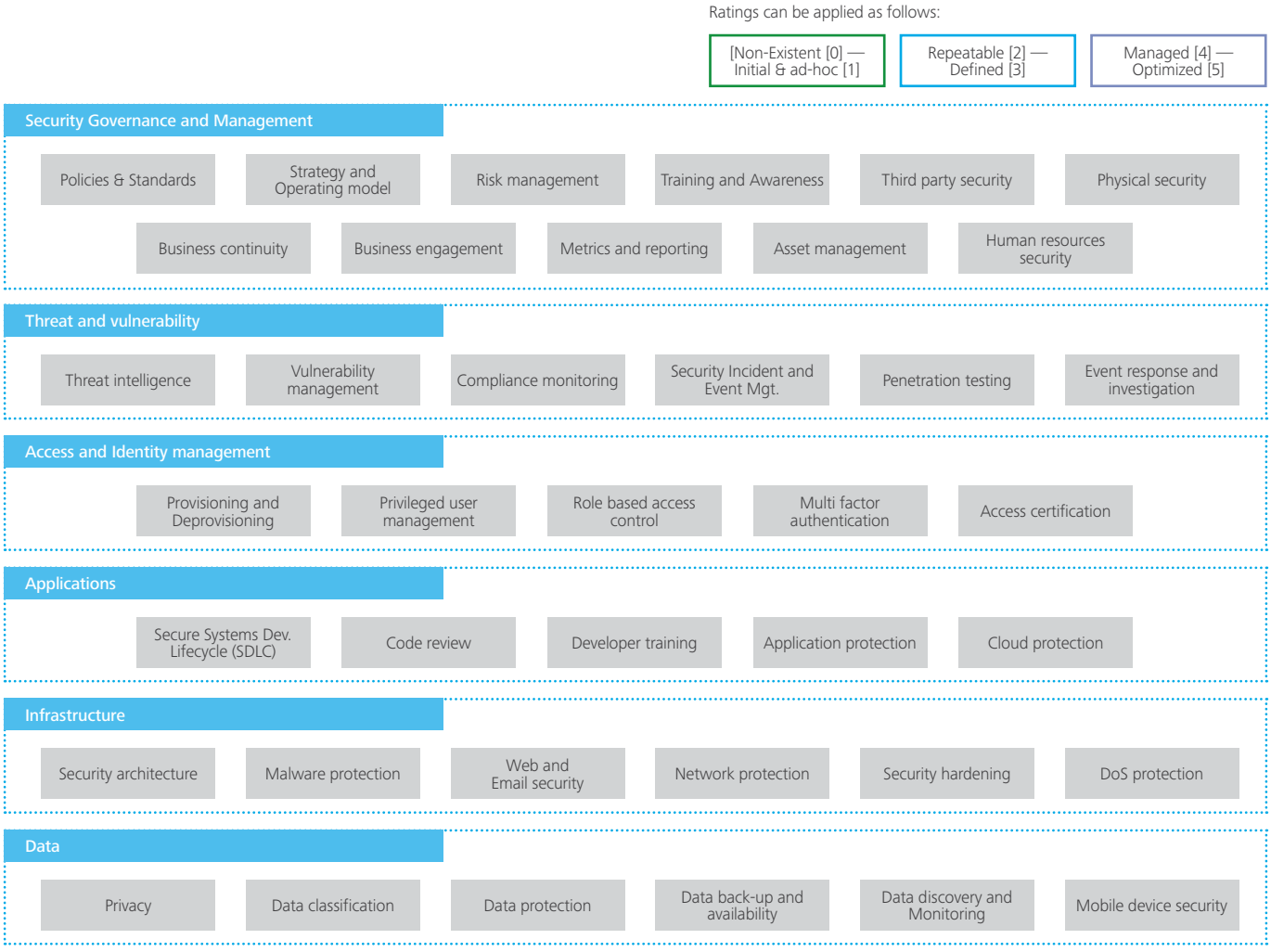
Although application white-listing is a challenge for many, we believe it is vital that organisations rigorously observe the remaining four essential strategies listed above.

The first step in establishing the basics of cyber security is to consider the capabilities the business needs, given the nature of the organisation and the threats it faces.

Rather than employing checklists, Deloitte uses frameworks that focus on capability and services required as well as the value of the information and how staff acquire and use it.

Figure 8 is an example of a model that shows the capability and specific services of each layer within an organisation.

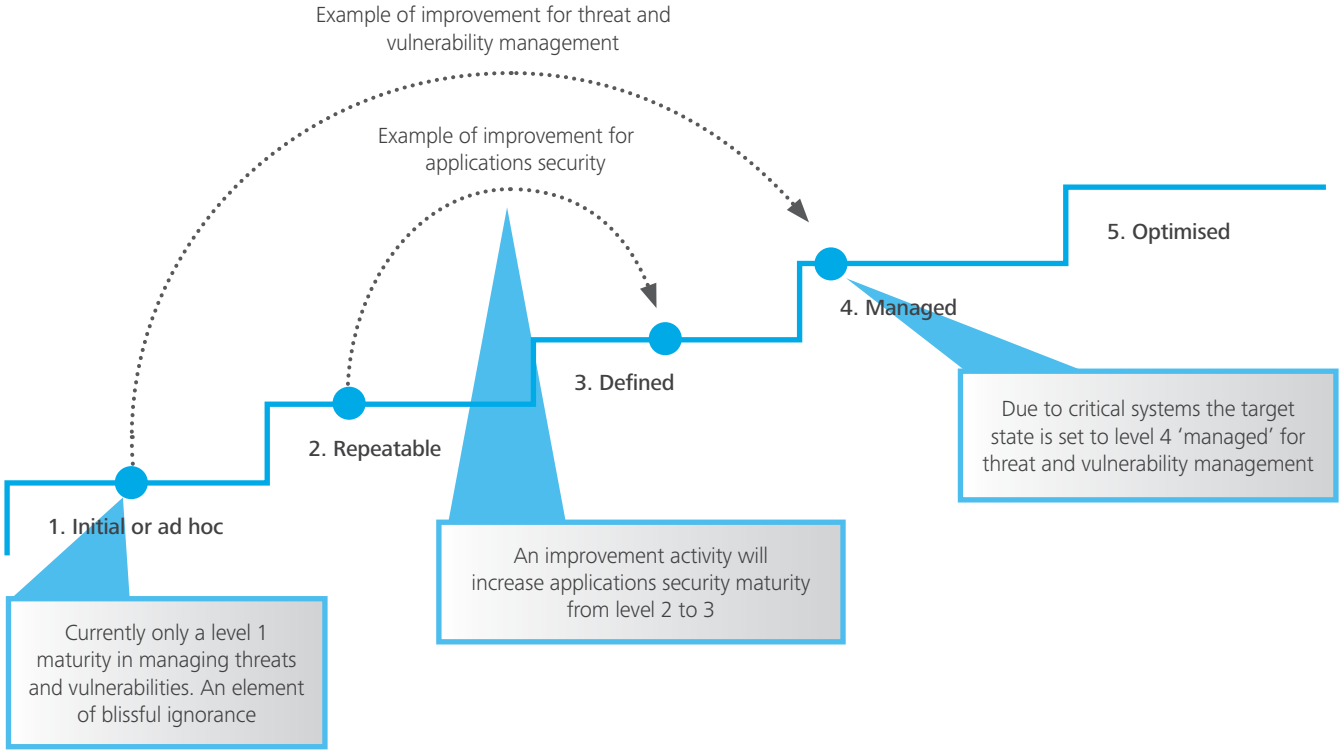
Figure 8: An example of a security capability framework



Assessing your maturity

The next step is to rate your level of maturity within each framework layer according to the five levels of cyber security maturity outlined in Figure 9. Identify which best describes your business and then choose a target state that reflects your intended level of risk management, based on your risk appetite.

Figure 9: Using the COB IT maturity model ratings to demonstrate the five levels of cyber security maturity.



Level 1: Initial or ad hoc security

- Insufficient skilled personnel with no roles and responsibilities assigned
- Processes are undefined and are performed in an ad hoc manner
- Lack of or ineffective tools necessary to perform the required duties

Level 2: Repeatable

- High degree of dependence on individual specialists
- Roles and responsibilities are vaguely defined
- Processes and policies are not defined, but are consistently applied
- Tools may be used, but are not standardised

Level 3: Defined

- Defined roles and responsibilities
- No mandatory training
- Policies and processes are defined and executed consistently
- Tools are defined and used consistently
- Capability known

Level 4: Managed

- Training is mandatory and approved by management
- Policies and processes are defined and approved by management
- Tools are properly maintained and there is a set level of automation
- Capability assessed and monitored according to a plan

Level 5: Optimised

- Effectiveness of skills is measured so they can be improved or adjusted
- Security practices are continually reviewed and tested to influence process redesign
- Innovative and effective tools are employed with a high degree of automation

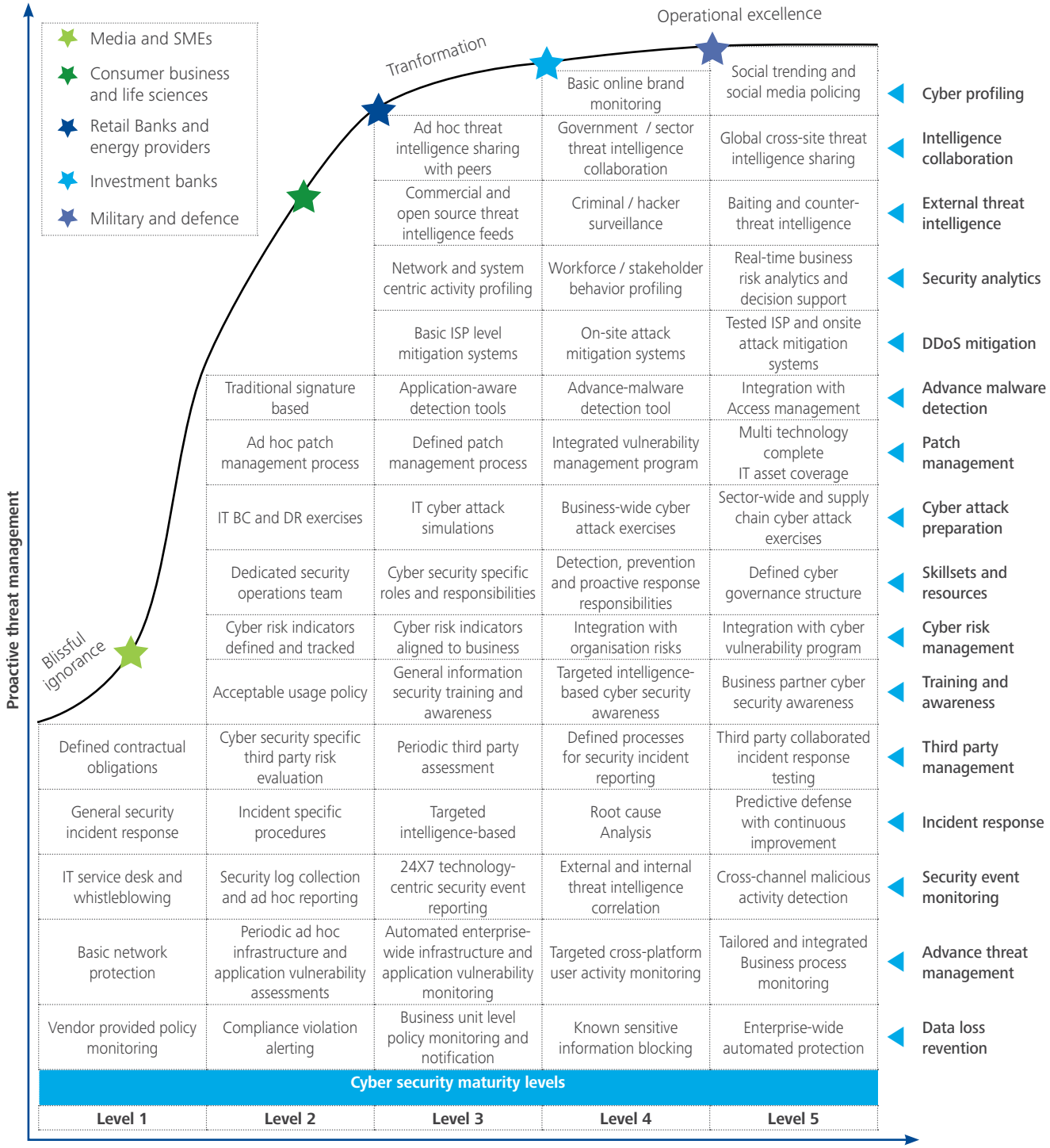
Tip: An example of more mature organisations

If you identify issues while reviewing penetration test results, consider how the issue is a symptom of a larger systemic problem or an isolated incident. In our experience it is often the former.

Assessing your positioning against others in the industry

Figure 10 displays the capabilities and services organisations need to consider at an industry level. For example, investment banking involves higher-value transactions. The transactions touch many parties and can be extremely confidential and time sensitive, requiring a greater level of maturity than, for example, a retail outlet.

Figure 10: The capabilities required for cyber security maturity



Are you compliant and capable?

(Considerations for question 6)

Recent high-profile security incidents resulting in data loss or system unavailability have raised awareness of the need for strong cyber security capabilities.

The key for CIOs is to emphasise that cyber security is not about complying with regulation and investing in technology – it is about protecting the business and securing its intellectual property and sensitive information. Compliance should be part of information security, not the other way around.

Organisations should start by considering the systems and information they value the most. These may include web-facing applications, personal data or core network and storage components. Having invested in the technology to guard those assets, organisations should confirm that technology is rigorously configured, monitored and maintained.

Doing the bare minimum to pass compliance requirements is a common approach to cyber security, but fails to address the key risks and doesn't provide organisations with the core capabilities necessary to protect valuable systems and information. Today's cyber attackers pay no heed to compliance frameworks – you need to confirm your organisation's security measures are actually capable of withstanding an attack.

Questions for the CIO to ask of IT and the business

1. Do we talk about security compliance or capability?
2. Do we assess our security capabilities formally beyond the periodic internal or external audit reviews?
3. Do we know what level of maturity we need to attain for each capability?
4. Have we tested our capabilities in a simulated real-life situation?
5. Do we look beyond the checklists at real operational technology and process capabilities?

Do third parties handle your valuable information?

(Considerations for question 7)

The move to outsourcing, third-party joint ventures, cloud-based solutions and collaborative initiatives have compromised the boundaries of many organisations and caused them to reconsider the definition of a secure perimeter.

This new landscape has prompted some organisations to outsource security measures to a third party, creating the dangerous misconception of security through transfer of responsibility. Remember, whoever owns the customer is always in the firing line when there is a cyber security issue. Risk management cannot be outsourced.

Questions for the CIO to ask of IT and the business

1. How much of our organisation's valuable information is managed by third parties?
2. Which third parties do we rely on to manage valuable information?
3. To what extent are cyber security controls enforced by us on our third parties?
4. How much visibility do we have over third-party controls?
5. Can we validate third party controls on an ongoing basis?
6. Does our insurance cover third parties cyber breaches?

Do you evaluate the effectiveness of cyber security?

(Considerations for question 8)

Accepting that cyber security is an ongoing process rather than a one-off achievement is the first step in ensuring your business is comprehensively secure. Once you have established the necessary capabilities and maturity levels, it is important to consider how to maintain them over the long term.

Organisations need to continually evaluate and improve the effectiveness of their cyber security measures. Every incident or failure to adhere to set requirements should be treated as an opportunity to evaluate the root cause of the issue and to improve your capability.

Testing and evaluation should be broad and regular. Avoid falling into the common trap of feeling secure because one aspect of testing gives you a good result.

Questions for the CIO to ask of IT and the business

1. Do we treat cyber security as an ongoing process?
2. Do we continually evaluate the effectiveness of our cyber security measures?
3. Do we act on these evaluations to improve our cyber security measures?

Monitoring and reporting (vigilance)

(Considerations for question 9)

To date, most Australian organisations have focused on implementing preventative controls such as firewalls, perimeter security, vulnerability testing and intrusion prevention. However, the increasing sophistication of cyber attacks means these measures are no longer enough and organisations should expect to experience a breach sooner or later.

This is why the organisation needs to invest in the ability to monitor data systems and processes for breaches, and analyse and act on cyber threat intelligence and integrate cyber credential response processes.

Tip:

The multitude of threat information published daily is of little value unless it is relevant to and actionable by the organisation. The organisation should focus on gathering actionable intelligence.

Questions for the CIO to ask of IT and the business

1. Do we receive and act on actionable intelligence?
2. Can we tell if a breach has occurred?
3. Does the intelligence we action cover our most valuable information assets?
4. What cyber-security reporting is appropriate for IT and the business?

Do you have an effective way to respond to cyber incidents?

(Considerations for question 10)

In worst-case scenarios, a cyber attack can result in a business replacing its key executives, experiencing serious financial loss enduring extensive litigation or shutting down completely.

This is why it is essential to create an incident response plan that details technical and business measures to limit the potential impact of a cyber attack on your business. Having a clearly defined incident response plan helps minimise the impact of a breach, improves visibility of the attack and confirms that the response is measured and appropriate. The ability to respond appropriately to a cyber incident or breach can mean the difference between a business's success and failure.

Knee-jerk reactions can taint a security incident. For example, turning power off in the event of a breach could erase any trace of the incident held in the operating memory of the system and the temporary files, making recovery and forensic analysis difficult. A comprehensive and considered incident response plan may instead have involved disconnecting the server from the network and contacting a technical emergency response team.

Below are four steps that will help reduce the impact of a breach.

Step 1: Plan

Create an intelligent response plan that:

- outlines the scenarios you could face and their potential impact on the business
- identifies the critical systems you need to keep online, as well as your obligations to customers, third parties, stakeholders and regulators
- establishes the decisions you would need to make and who would need to make or approve those decisions
- accounts for the dependencies you have on other entities
- explains how you would legally preserve evidence in the event of the attack
- details the resources you would need and the processes you would use to respond to a successful attack.

Where you may need to call on additional capability from external vendors, ensure you have appropriate contracts and response-time terms in place.

Step 2: Communicate

Ensure you have a considered communication plan with consistent internal and external messaging. Have a single spokesperson and prepare an unambiguous script that provides answers to likely technical questions. Determine in advance which stakeholders, third parties and customers you should contact in the event of a breach, as well as the escalation process for response to a cyber attack and potential liabilities that can be mitigated.

Step 3: Maintain logs and evidence

Make sure the organisation stores, secures and retains all system logs in their original form to ensure they are admissible as evidence. Only copies of the logs should be distributed to incident responders and IT teams. Engage a forensic agency to professionally review the affected systems if you do not have the internal capability.

Step 4: Practice and simulate

Conduct frequent small-scale table-top exercises and annual full scenario run-throughs to prove your crisis management and incident response plans work. Highlight any shortcomings and update the operational documentation. Doing this will familiarise the operational teams and managers with the process, decreasing your incident response time and assisting in scenario planning being taken seriously.

Tip:

"Failing to plan is planning to fail" – Benjamin Franklin


Login
Password

Are you adequately insured against cyber risks?

(Considerations for question 11)

Having the right insurance cover can reduce potential financial loss. The underwriting pressure can offer a focus for the organisation and trigger a proactive assessment of cyber-security regulation.

Every cyber or data loss incident is different in nature. Incidents that pose the potential of serious risk or harm through lost or compromised data can have a very real impact on an organisation, including significant financial implications and damage to brand and market reputation.

Having adequate insurance in place that provides at least partial cover for cyber security incidents could be a major factor in recovering successfully from a cyber-related incident.

Understanding your existing cover will enable you to make informed decisions about risk transfer and determine which cyber liability insurance product best suits your organisation's risk profile and needs. For example, your organisation's existing insurance policies may provide some protection from cyber risks or data loss but how much?

It is also essential to understand how your individual policies interact with each other, as in the event of a claim you are required to advise your insurer of other policies that may provide cover.

Here are some points to consider when reviewing your main existing insurance policies.

1. Business insurance policies (business property)

Standard business insurance policies only cover tangible assets, such as building and contents. Electronic data is not generally considered a tangible asset under standard business insurance policy definitions. Some policies may include an extension to cover some 'loss of data', but generally also apply sub-limits that are typically too low to properly compensate for the loss or pay for the restoration of data.

2. Public and products liability insurance policies (sometimes referred to as general liability)

This type of insurance may form part of a business insurance policy (including covering buildings and contents), or could be a stand-alone policy. Unless specifically endorsed, this policy will generally exclude personal injury or property damage arising from your online operations, and property damage to electronic data, computer programs or storage media.

3. Professional indemnity

Professional indemnity policies may offer some cover, but this will depend on the specific policy wording, definitions and exclusions. Note that some professional indemnity policies exclude cyber crime.

Cover will generally only relate to third-party losses, such as claims for compensation and damages. These third-party losses may be limited to exclude certain events, such as transmission of a virus through your computer system to a third party.

It's unlikely your professional indemnity policy will cover first-party losses to your business, such as data rectification costs, breach notification costs to your clients and customers, breach of an employee's data, loss of revenue, forensic investigation costs, and public relations expenses.

However, your professional indemnity policy may cover legal defence costs, punitive fines and penalties, and court attendance costs.

4. Management liability (including directors and officers)

As with professional indemnity, management liability insurance may include some cover for cyber attacks. The nature of the cover available will depend on the specific policy wording, extensions, definitions and exclusions. Some management liability policies will exclude cyber crime, while other policies offer the option to add cyber cover as an extension.

Management liability cover will generally relate to third-party losses and may be subject to specific exclusions and sub-limits. Again, this type of insurance may only offer limited cover for first-party losses.

Deloitte is grateful to Paul Waite from CyberPlus for his contribution to the insurance discussion.

Essential points to consider when purchasing cyber insurance

Once you have a comprehensive picture of the cover available under your existing insurance policies, you'll be in a better position to purchase the type of cyber liability insurance that best suits your organisation's risk profile and needs. The following are additional points to consider when topping up your existing cover or purchasing additional cover.

1. Identify your real unique risks

The first step in purchasing cyber liability insurance is understanding the nature and extent of the risks facing your organisation. Every organisation has a different risk profile based on the information that it manages and stores. For many banks and retailers, the primary concern is the loss of bank account details and personal identifiable information. In contrast, a utility or energy organisation might face the risk of disruption of critical business or physical operations through attacks on networks. It is very important for organisations to tailor their cyber liability coverage to the most likely risks they face.

2. Purchase what you need

It is possible to design a policy and cover to suit your risk profile, and that only covers you for the items you need. If an insurer is not willing to remove an objectionable exclusion or limitation from its policy, obtain quotes from an insurance carrier that will offer the coverage without the limitation.

3. Secure appropriate limits and sub-limits

Compare the anticipated costs associated with a data breach (or security event) with the policy's liability limit options and the related costs. The costs of responding to a data breach can be substantial. Estimates vary, but in 2014 the average cost of a breach in Australia was $2.8 million overall, which translated to a cost per lost electronic record of $145.

Most cyber liability insurance policies impose sub-limits on some cover, such as for crisis management expenses, notification costs and regulatory investigations. These sub-limits are often inadequate, but many insurers are willing to negotiate the size of the sub-limit, often without increasing the premium.

4. Beware of exclusions

Often, cover for a loss or claim depends on the policy exclusion wording as opposed to the wording in the grant of cover. As cyber liability insurance is a relatively new product, the policy wording is not standardised. Check that your policy does not contain irrelevant exclusions taken from other types of insurance forms.

5. Get retroactive coverage

Cyber liability policies sometimes restrict coverage to breaches or losses that occur after a specific date, such as the inception date of the policy. This means that there would be no coverage for breaches that occurred before the start of the policy. As breaches may go undetected for some period of time, it is important to purchase coverage with the earliest possible retroactive date.

6. Consider coverage for acts and omissions by third parties

Many organisations outsource business processes. IT, data processing or storage to a third-party provider. It is important that your cyber liability insurance policy provides cover for claims arising from data cyber breach of security, or after cyber-security issues at one of your providers.

7. Evaluate coverage for data restoration costs

Many cyber liability insurance policies do not provide cover for the costs to replace, upgrade or maintain a computer system that has been breached. Data restoration costs are potentially prohibitive. Any organisation that faces the risk of a data breach should take steps to ensure that its insurance policies cover the costs of putting the organisation back in the position it was in before the breach.

8. Dovetail cyber insurance with indemnity agreements

It is important that your organisation's indemnity agreements work hand-in-hand with your cyber liability insurance. For example, many cyber liability insurance policies have retentions that must be satisfied by the insured. Insurers may interpret this to mean you pay the retention out of your own pocket and that a payment by a third party under an indemnity agreement would not satisfy the retention. This is a subject for negotiation with the insurer during the underwriting process.

9. Understand what activates cover

It is important to understand what activates cover under a cyber liability insurance policy. Some policies offer cover from the date the loss occurs, while others are triggered on the date a claim is made against the insured. To provide proper notice to your insurer, you need to understand how coverage applies under each policy you purchase.

10. Consider coverage for loss of information on unencrypted devices

Professionals today often work on computers, smartphones and tablets outside the office. While organisations commonly encrypt company-owned laptops, many neglect to do the same with employees' personal computers and storage devices. This is why it is important for organisations to buy cyber liability insurance that covers loss of data through personal computers.

11. Consider coverage for regulatory actions

In addition to information loss, data breaches can result in regulatory actions against your organisation. Federal agencies have become more active in responding to data and privacy breaches. You should consider whether your organisation's cyber liability insurance policy provides cover for a regulatory investigation or action arising from a cyber or data loss incident.

Cyber liability insurance doesn't replace the need for sound corporate controls, robust technology security systems or vigilant security processes. Regardless, it should be considered as an important component of any organisational cyber risk management strategy in today's networked and cloud-connected environment.

Tip:

Know what your policies cover. For example, many business interruption policies cover the cost of engaging forensic specialists in the event of a breach.

Elevating the conversation

Modernising your approach to cyber security may require enterprise-wide changes to strategy, people, processes and technology. Cyber security is not just the IT department's challenge – the broader C-suite must be involved before the entire organisation can become more secure.

Anecdotal evidence indicates that the most effective cyber security programs exist where the CIO has the full support, cooperation and involvement of the organisation's executives and board. The most successful CIOs drive this outcome using business rationale, executive and board education, informed and risk-based decision making, and a continual flow of relevant cyber security information.

Keeping sponsors, executives and the board engaged on cyber security in the long term requires continual commitment and communication reinforced by the CIO. We recommend the CIO delivers ongoing updates to the executives and the board that provide insights into the organisation's cyber security maturity, capability, improvements, incidents, responses and emerging topics.

Deloitte understands that communicating the scale and importance of cyber security to business leaders can be challenging. We recommend CIOs use the following four steps to position cyber security as an ongoing conversation within the organisation, and to gauge the effectiveness of existing cyber security measures.

Step 1: Culture of security

Improve the organisation's security culture by lifting awareness of potential risks at home and at work.

Step 2: Get the basics right

It's important to address all security gaps across the business. Most breaches arise from a failure to cover the basics.

Step 3: Set the bar

Protect what matters most in terms of confidentiality, integrity and availability, and focus spend in these areas.

Step 4: Be vigilant and prepared

Monitor, but accept that you will be hacked and be prepared for that eventuality.

Tips for driving continued executive engagement:

Dashboards

Interactive dashboards are useful in helping executives take ownership of an organisation's cyber security. Configured correctly, a dashboard can present key information in an intuitive and visual way that makes cyber security more approachable for the C-suite.

Dialogue

Monthly reporting and regular board briefings can elevate the cyber conversation and embed it into the organisation's management framework. Briefings can cover areas such as current maturity levels, unsuccessful breach attempts, response activity to breaches and emerging threats. Where possible, it's important to highlight what has been prevented and illustrate the potential consequences if breaches had not been detected.

Commitment

Regular demonstrations of executive and board commitment to cyber security can help the rest of the organisation follow suit. Instigate cyber security discussion at management meetings, and encourage senior management to communicate with staff when issues arise. It can also be helpful to engender a business-led program of ongoing cyber security awareness, and include key performance indicators relating to security in performance evaluations. Ideally, your organisation will also have methods for responding to behaviour that breaches cyber security protocols and controls.

Contact us:

Sydney
Tommy Viljoen
Partner, Risk Services
tfviljoen@deloitte.com.au
+61 2 9322 7713

Adelaide
David Hobbis
Partner, Risk Services
dhobbis@deloitte.com.au
Tel: +61 8 8407 7283

Perth
Richard Thomas
Partner, Risk Services
richathomas@deloitte.com.au
Tel: +61 8 9365 7024

Melbourne
George Stathos
Partner, Risk Services
gstathos@deloitte.com.au
Tel: +61 3 9671 6853

Brisbane
Ian Blatchford
Partner, Risk Services
iblatchford@deloitte.com.au
Tel: +61 7 3308 7171

Canberra
Sid Maharaj
Partner, Risk Services
sidmaharaj@deloitte.com.au
Tel: +61 2 6263 7160

MCBD_SYD_11/14_050330