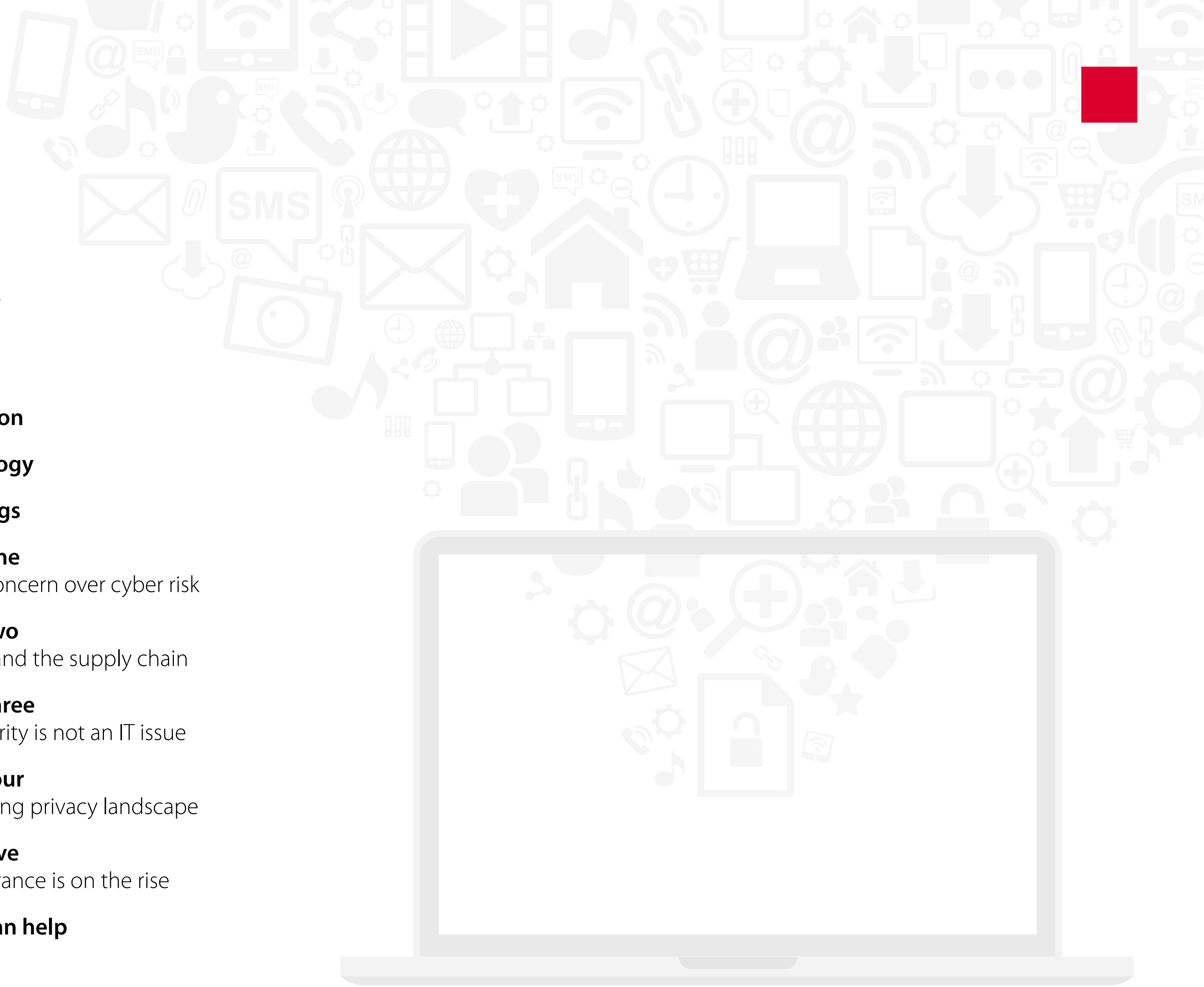
PERSPECTIVES ON CYBER RISK 2017

MinterEllison

> Most people are starting to realize that there are only two different types of companies in the world: those that have been breached and know it and those that have been breached and don't know it.

Ted Schlein, Venture Capitalist at Kleiner Perkins Caufield & Byers

Contents



Introduction

The 12 months since the publication of our last *Perspectives on Cyber Risk* report have seen some of the most devastating cyber incidents yet. Every kind of organisation – government, state owned enterprises, public and private companies and not-for-profits – has been affected. In every industry – from finance, retail, hospitality and healthcare, to mining and resources, utilities, professional services and education, it's clear that everyone is fair game in cyberspace.

High profile incidents occurring during 2016 include:

- Allegations that Russia was involved in hacking activities relating to the US election, including hacks on the Democratic National Convention and consequent email leaks.
- A US$81 million cyber heist involving an attack against global financial messaging system SWIFT.
- Large data thefts from social media networks, including Tumblr (65 million accounts), LinkedIn (117 million accounts), AdultFriendFinder.com (339 million accounts), Myspace (427 million accounts) and Yahoo (500 million accounts).
- The attack against Panamanian law firm Mossack Fonseca, which resulted in the theft of more than 11 million documents, the subsequent resignation of Iceland's Prime Minister, and ongoing investigations into numerous organisations and individuals (including a number of world leaders).
- Distributed denial of service (DDoS) attacks against security researcher Brian Krebs, French media company OVH, the Rio Olympics online presence, the Australian Bureau of Statistics eCensus website, and domain name server company Dyn. The attack against Dyn was particularly devastating, disrupting internet connectivity for around 70 companies, including giants like Twitter, Spotify, Paypal, Airbnb and Reddit.

By 2021, cyber crime could cost the world in excess of

$6
trillion

ANNUALLY

Introduction continued

- The accidental exposure of the personal information of around 550,000 blood donors by the Australian Red Cross.
- The potential compromise of hundreds of point-of-sale systems, enabling hackers to remotely administer POS devices located in retail outlets around the world.

Cyber security can no longer legitimately be considered the domain of IT alone. Cyber attacks can entirely shut down businesses, causing significant (and sometimes irreparable) damage to corporate and government reputations, relationships and systems; adversely impacting other businesses in the supply chain; compromising the privacy of millions of individuals and threatening economic wellbeing and national security. By 2021, it is estimated that cyber crime will cost the world in excess of $6 trillion annually.[1]

In this increasingly fraught climate, in late 2016 we conducted our second annual cyber security survey, to assess changes in Australian organisations' cyber resilience over the past 12 months.

The survey was targeted at legal counsel, risk managers, Board members and senior executives. Respondents to the survey came from both public and private sector organisations, across a wide range of industries.

We found that, although incremental progress has been made during the past 12 months, organisations' issues and concerns, far from abating, have intensified. This is being driven by the growing volume, scale and sophistication of the cyber security threat; an increasingly onerous Australian and global regulatory landscape; and an increase in organisational interconnection and interdependence as a result of the rapid adoption of cloud-based technologies.

Cyber security has transcended the realm of the technical – it is now a business, economic and national security priority, which requires that a culture of cyber resilience be woven into the fabric of public and private sector organisations' overall risk management approach.

Our survey indicates that most organisations still have a long way to go to achieve this.

We have revised the terminology used in this year's report in line with evolving industry practice:

cyber attack A deliberate act that seriously compromises national security, stability or prosperity by manipulating, denying access to, degrading or destroying information systems or the information resident on them [2]

cyber incident An occurrence that actually or potentially results in adverse effects on information systems or the information resident on them [3]

cyber security The safeguards and actions that can be used to protect against cyber incidents [4]

cyber risk Operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information systems or the information resident on them [5]

cyber resilience An organisation's ability to prepare for, respond to and recover from a cyber incident (including its ability to operate during, and adapt to and recover from, a cyber incident) [6]

data breach A situation where information (usually including personal information) is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference, often as a result of a cyber incident [7]

Methodology

MinterEllison's online survey was completed by more than 100 legal counsel, CIOs, COOs, Board members, IT specialists and risk managers of ASX200 and private companies, government and not-for-profit organisations. Depending on their role within the organisation, they responded to either the CIO survey or Board survey.

Participants responded to questions about cyber security roles, responsibilities and attitudes within their organisations.

The survey was conducted between September and November 2016. This report reflects the quantitative results of the survey questions and the respondents' qualitative comments.

All information provided by the participants is confidential and reported primarily in aggregate form.

Where appropriate, MinterEllison has used interviewee quotes to support the report's findings and opinions. The views expressed in this report do not necessarily reflect the views of the individual respondents unless otherwise stated.

We make no representation or warranty about the accuracy of the information, or about how closely the information gathered will reflect actual organisational performance or effectiveness.

Due to rounding, responses to the questions covered in this report may not add up to 100 per cent.

Key findings

one

Awareness of cyber risk has increased as the problem grows – but concrete actions have not changed

two

Despite concerns about the increasing cyber threat, organisations remain complacent about reviewing and testing their own cyber resilience (and the cyber resilience of their suppliers)

three

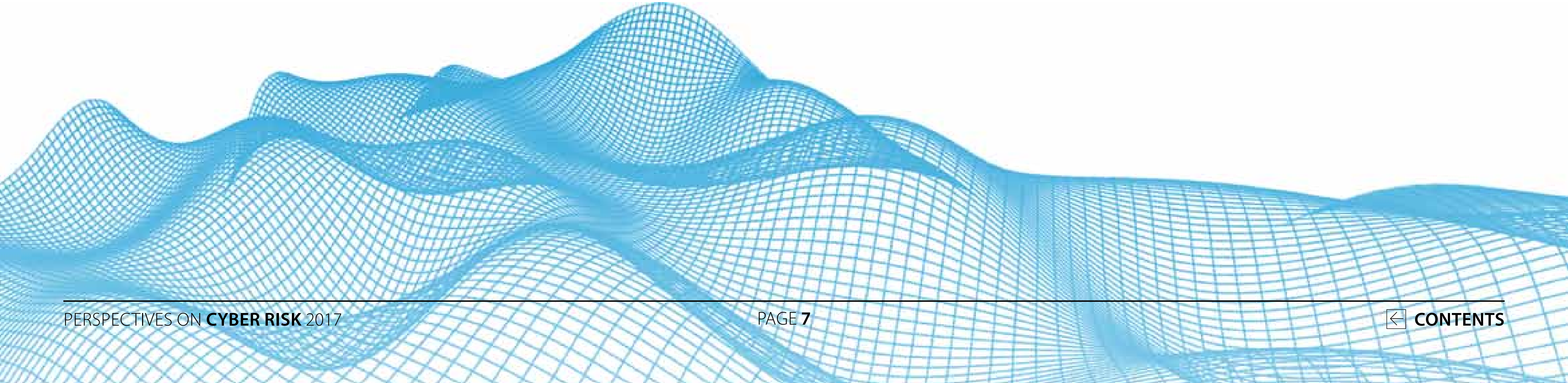
Cyber security is still (wrongly) seen as being primarily an IT issue

four

The privacy landscape is changing – both in Australia and overseas

five

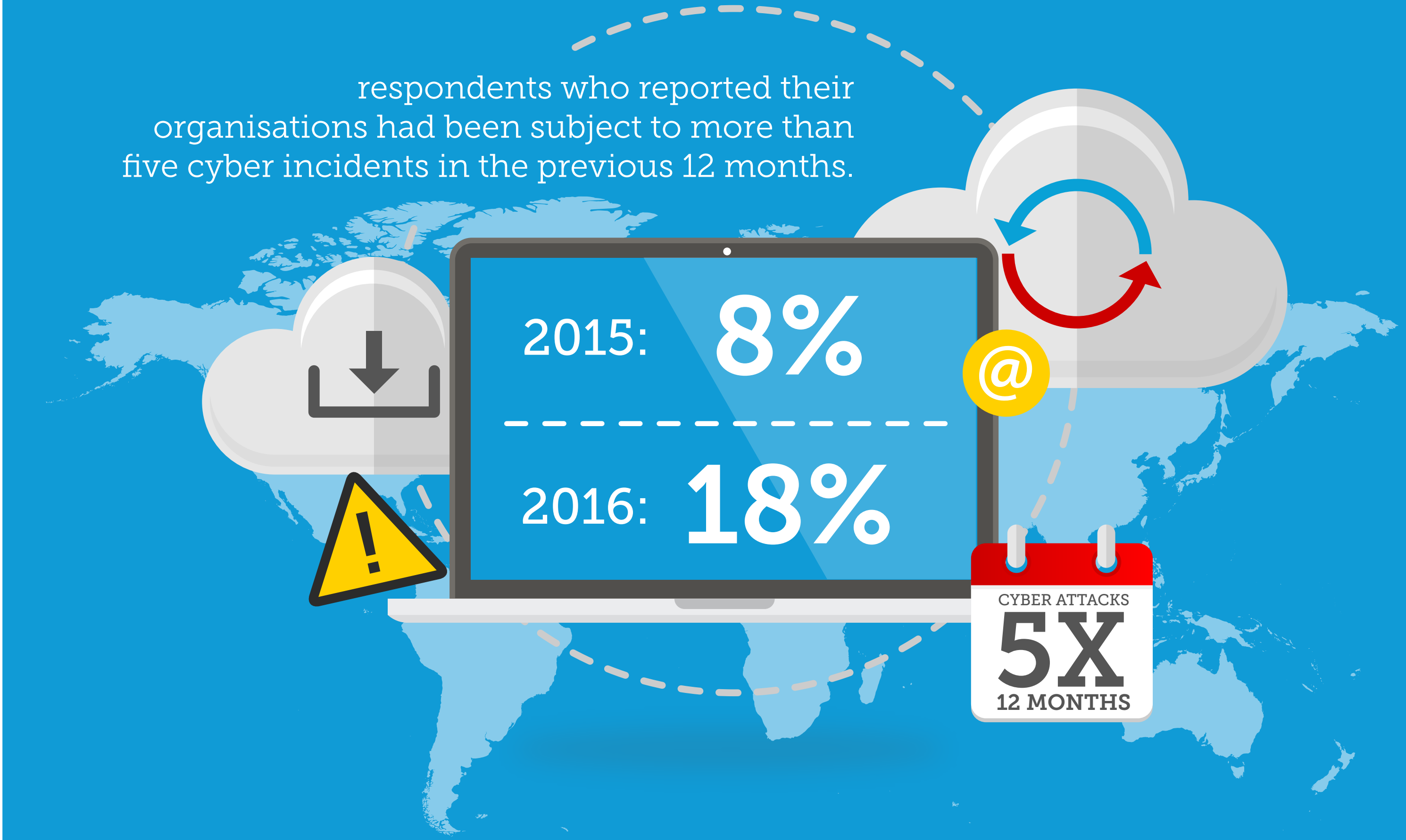
The increasing uptake of cyber insurance indicates some willingness to act on managing cyber risk



one

Awareness of cyber risk has increased as the problem worsens – but concrete actions have not changed

respondents who reported their organisations had been subject to more than five cyber incidents in the previous 12 months.



2016 saw a year-on-year increase in the number of reported cyber incidents, including many high profile incidents.[8] 2016 was also the year of ransomware, with the number of daily ransomware attacks increasing by 300% over 2015.[9]

Our survey results reflect this increase in the number of cyber incidents occurring.

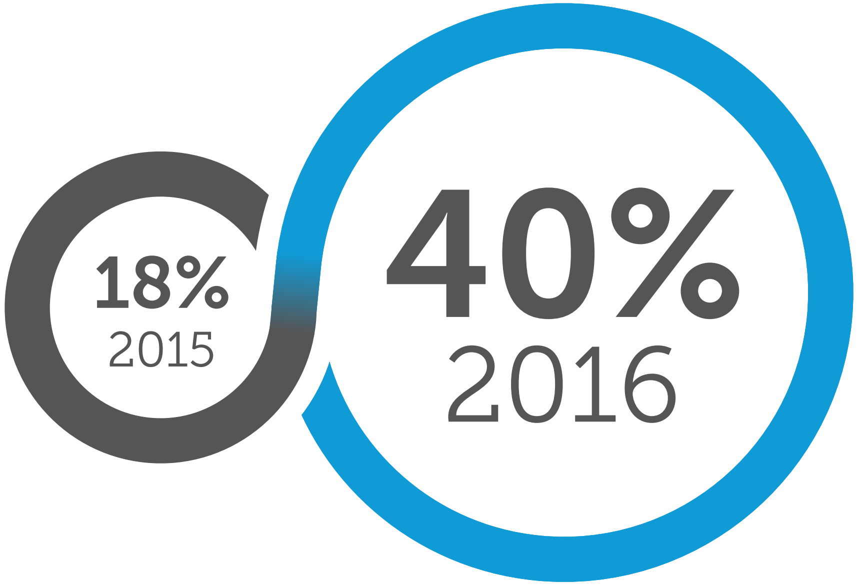
In 2015, just 8% of respondents reported that their organisations had been subject to more than five cyber incidents in the previous 12 months that had compromised their systems or data. In 2016, this percentage more than doubled, to 18%.

With the increase in the number of cyber incidents, it is little surprise that survey respondents expressed increased concern in relation to their organisations' ability to prevent such incidents. In our CIO survey, the percentage of respondents who indicated that they were either somewhat or very dissatisfied with their organisation's capability to prevent cyber incidents doubled, from 18% in 2015 to more than 40% in 2016.

Similarly, at the Board level, 65% of respondents indicated that they considered cyber risk to be more of a risk than 12 months ago, while 35% of Board respondents indicated that cyber risk ranked as a top 5 risk (up from 29% in 2011).

We're seeing greater awareness, but also less understanding, and not enough action

Perhaps because of the increased awareness and the increasing scale and complexity of cyber risk, our survey results indicate organisations perceive that they understand less about the extent of their own exposure to cyber incidents than they did 12 months ago.



Percentage of respondents dissatisfied with their organisation's capability to prevent cyber incidents

Our survey results show that, although organisations are aware of the ever increasing cyber security threat, many are still not taking appropriate steps to properly understand the extent of their exposure, and to implement necessary practical measures to mitigate cyber risk and improve their cyber resilience.

In 2015, just over 40% of our CIO survey respondents considered they had a very good understanding of their organisations' exposure to cyber incidents. However, in 2016, only 10% indicated they had a very good understanding, while more than 20% considered they had a poor understanding.

Our results also indicate there has been little change in the practical actions that organisations are taking in order to address cyber risk.

42%

DO NOT HAVE A DATA BREACH RESPONSE PLAN (UP FROM 27% IN 2015)

In our Board survey, 44% of organisations responded that the Board is only briefed on cyber security issues annually or on an ad hoc basis, while 13% of organisations said that the Board received no briefings at all.[10]

In our CIO survey:

- Just over half of respondents indicated their organisations had increased their expenditure on IT security over the previous 12 months (similar to 2015).
- Less than 20% indicated they regularly assess their customers' cyber risk profile (largely unchanged from 2015).
- About 47% indicated that they do not regularly audit their suppliers' IT security practices (largely unchanged from 2015).
- Over 40% indicated their organisation does not have a data breach response plan (up from 27% in 2015).
- Only 8% of respondents conduct regular internal staff training on IT security issues more frequently than annually (only marginally improved from 2015).

And for those organisations that do have a data breach response plan, nearly 44% reported they do not regularly test that plan (at least annually).

> "*[We need to]* audit third party **suppliers' security practices** *[and provide]* greater **awareness raising** for staff."
>
> *CIO survey participant*

Embedding cyber resilience within an organisation involves more than just keeping the Board regularly informed of cyber risk issues.

EMBEDDING CYBER RESILIENCE

Identify the extent of the organisation's exposure to cyber risk.

- Identify the information and other assets that are essential to the organisation (including intellectual property, infrastructure, personnel and financial information).
- Identify and prioritise threats and vulnerabilities faced by the organisation (and not just technical threats, but also vulnerabilities relating to personnel and processes).
- Ensure that the organisation has sufficient resources to deal with a cyber incident.
- Assess the level of awareness of cyber risk within the organisation.
- Assess the extent to which the organisation is exposed to supply chain risk by its reliance on third party suppliers and key customers (which may require reviewing the cyber resilience of those third parties).
- Assess the extent to which cyber risks are integrated into the organisation's general risk management procedures (including into periodic organisational risk assessments and business continuity planning).

Develop and implement procedures to protect the organisation.

- Implement and continually assess and update the organisation's security-related policies and procedures (including its monitoring and detection policies and processes and its data breach response plan).
- Recognise that cyber security is about people, not just technology, and ensure that all of the organisation's personnel (beyond just those charged with dealing with cyber incidents) are properly educated and trained. This may involve:
    - Raising awareness of cyber security issues and concerns in a wider context to engage personnel (for example, how individuals can better protect their families and personal finances).
    - 'Gamification' of cyber security issues, to increase the level of engagement and interest in the organisation's cyber security program.
    - Enlisting other departments within the organisation to assist the IT security department, so that others within the organisation can be the eyes, ears and voice of the cyber security program.

Deploy the resources (both human and technical) required to identify a cyber breach in a timely manner.

- Implement and continually improve monitoring processes and procedures.
- Collaborate with peer organisations and government agencies to share and improve the organisation's cyber intelligence.

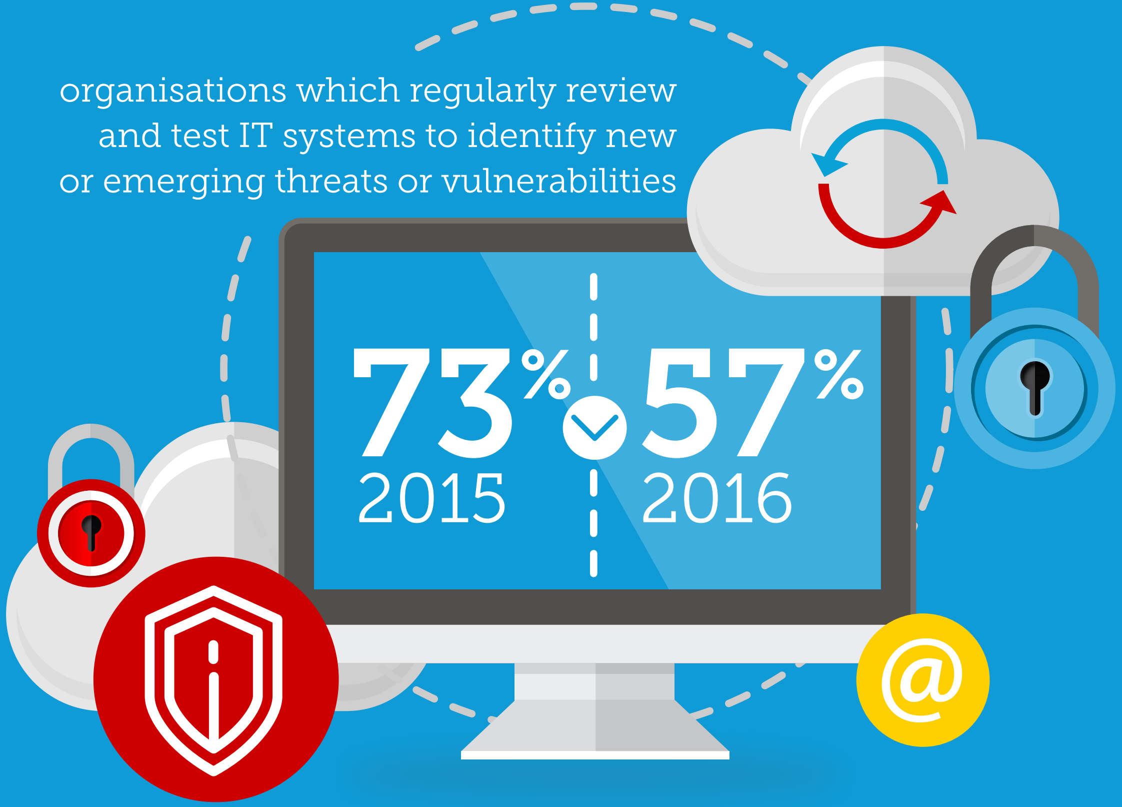
Have procedures in place to respond to, and recover from, a cyber breach.

- Implement and regularly test a data breach response plan (see page 23).
- Implement and regularly test business continuity and disaster recovery plans (which should include a regular backup plan for all data stored in the cloud).

two

Despite concerns about the increasing cyber threat, organisations remain complacent about reviewing and testing their own cyber resilience (and the cyber resilience of their suppliers)

organisations which regularly review and test IT systems to identify new or emerging threats or vulnerabilities



According to our CIO survey only 57% of organisations regularly review and test their key IT systems to identify new or emerging threats or vulnerabilities (down from 73% in 2015).

At the same time, only 33% of organisations regularly audit their suppliers' IT security practices (largely unchanged from 2015).

This is despite a significant number of high profile attacks over the last three years which have involved external actors attacking IT systems through vulnerabilities in the systems or practices of third party suppliers. There is also an overwhelming perception of those surveyed (nearly 80%) that external actors – including nation states, terrorists, organised crime syndicates and hacktivists – constitute the most significant cyber security threat to their organisations.[11]

Target US's 2014 data breach is a dramatic example of what can go wrong when a third party supplier opens the door to malicious external actors. In that case, 40 million credit card numbers, as well as the personal information of 70 million individuals, were stolen through malware installed within Target's point-of-sale system.

The subsequent investigation determined that hackers had accessed Target's network through credentials stolen from a company that supplied Target with refrigeration and HVAC services.

The fallout from the Target data breach included:

- Significant reputational damage, which may have explained, at least in part, a 46% year-on-year reduction in profits.
- The resignation of Target's CIO, followed a few months later by the resignation of its CEO, President and Chairman of the Board.
- The layoff of 475 employees at Target's head office.
- Institutional Shareholder Services' (ultimately unsuccessful) attempt to remove all of the members of Target's audit and corporate responsibility committee (comprising 7 of Target's 10 directors).
- More than US$160 million in costs booked by Target across 2013 and 2014 relating to the data breach.
- More than US$200 million in estimated costs on the part of banks and credit unions having to re-issue 21.8 million credit cards.
- More than 140 class action and other law suits launched against Target (including by banks and consumers).

More recently, in the October 2016 data breach affecting the Australian Red Cross, a file containing the personal information (including sensitive medical information) of more than 550,000 blood donors was inadvertently published on a publicly exposed server by the third party contractor charged with maintaining the Red Cross' website.

> "*[We need]* **independent review** of **cyber protection** for adequacy."
>
> *Board survey participant*

Other examples of data breaches occurring because of third party suppliers include:

- Cogent Healthcare's 2013 data breach, where a medical transcription vendor's security lapse resulted in the data of 32,000 patients being inadvertently published on a publicly exposed server.
- US Home Depot's 2014 data breach, where hackers used credentials stolen from a third party vendor to gain access to point of sale data and steal the details of 56 million payment card accounts.
- Vulnerabilities in the web-based platform of photo service vendor PNI Media, resulting in the theft, during 2014 and 2015, of the personal information of many thousands of Costco and CVS customers.

Yet, according to our CIO survey, only a third of organisations regularly audit their suppliers' IT security practices, while more than 90% plan to deliver one or more of their IT functions via the cloud over the next 12 months.

Risk of legal and regulatory action

In addition to potentially significant financial and reputational consequences, organisations may face legal and regulatory action for failing to properly consider and manage supply chain risk. For example, under the accountability provisions in the Australian *Privacy Act 1988*, organisations that disclose personal information overseas are deemed to be responsible for the acts and practices of their overseas vendors in relation to that information (unless an exception applies).

Other legal and regulatory consequences, including breach of the *Corporations Act 2001* (Cth) (Corporations Act), and under 'long arm' overseas legislation (such as the EU General Data Protection Regulation) are considered in Findings 3 and 4 of this report.

More than

90%

plan to deliver one or more of their IT functions via the cloud over the next 12 months.

Organisations must improve their own cyber resilience by taking proactive steps to identify and mitigate supply chain risk.

ADDRESSING SUPPLY CHAIN RISK

- Conduct thorough due diligence on the cyber resilience of suppliers and key customers (including by considering the technical, personnel and process issues raised in Finding 1 from the standpoint of those organisations).
- Identify the data (including personal information) that will be handled by suppliers, including where it will be held, where it will be transferred to, and how it will be accessed and stored.
- Impose rigorous contractual obligations on suppliers in relation to cyber security and the protection of data:
  - Mandate compliance with specific security and data protection, storage, backup and recovery requirements and standards (and require that those obligations be imposed on the supplier's subcontractors).
  - Mandate compliance with applicable privacy and data protection laws
  - Where applicable, require the supplier to comply with privacy and other specific regulatory requirements that apply to the organisation (but may otherwise not apply to the supplier), including flowing down any specific audit rights imposed by regulators.
  - In light of the enactment of Australia's mandatory data breach notification law:
    - Require the supplier to notify the organisation should it suffer a data breach (whether or not affecting the organisation's data).
    - Where the breach does affect the organisation's data, mandate that the organisation will control the process for notifying regulators and other parties in relation to the data breach.
  - Confirm the organisation's ownership of its data, and require prompt access to the organisation's data in the custody of the supplier (in an open industry standard or other pre-agreed format).
  - Provide for appropriate disengagement rights and obligations.
  - Appropriately allocate risk between the organisation and the supplier:
    - Scrutinise the impact of limitations and exclusions on the supplier's liability in the context of a cyber incident.
    - Incorporate indemnities that shift risk to the supplier in circumstances where they have failed to adequately prevent or mitigate a cyber incident.
    - Require the service provider to take out insurance (including, where appropriate, cyber insurance).
  - Apply restrictions and controls on subcontracting, so that the organisation maintains transparency and control of the end-to-end supply chain.
  - Impose business continuity and disaster recovery obligations, including requiring the supplier to have, and to regularly test and update, a data breach response plan.

Finding

three

Cyber security is still (wrongly) seen as being primarily an IT issue

Board respondents who said IT departments remain principally responsible for cyber risk management, compliance and review activities

Australian and other corporate regulators understand the growing nature of cyber risk, and the systemic, enterprise-wide – and potentially economy-wide – effects of a serious cyber incident. Their views are supported by empirical data.

The 2016 *Ponemon Institute Cost of Data Breach Study* found that the total cost of a data breach has now increased to US$4 million *per breach* (up from US$3.79 million in 2015). Juniper Research estimates that the rapid digitisation of consumer and enterprise records will increase the global cost of data breaches to US$2.1 trillion by 2019 – four times the 2015 estimate.

The cyber incidents referenced (pages 4 and 5) that occurred in 2016 (including the eBay, LinkedIn, Target, Mossack Fonseca, SWIFT and Red Cross data breaches), as well as numerous other high profile cyber incidents over the last 24 months (including the 2014 Sony Pictures data breach, the 2015 Ashley Madison breach, and the 2015 Anthem Health data breach), exemplify not only the increasing sophistication of the cyber security threat, but also the severe financial, reputational and legal consequences that cyber incidents may have on affected organisations. It is the potential scale and severity of damage to organisations that elevates cyber risk beyond the realm of IT risk alone, transforming it into an enterprise-wide risk, and one requiring appropriate Board oversight. According to ASIC: [14]

> *"The dynamic nature of the cyber threat landscape means that a comprehensive and long-term commitment to cyber resilience must be embedded within organisations' culture. As we pointed out in Report 429: Cyber Resilience - Health Check (Report 429), the obligations on company directors and officers to discharge their duties with care and diligence extend to cyber security. However, many boards are still leaving it to their technology leaders to manage this threat. "*

The SEC has expressed equivalent views:[15]

> *"… boards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. Boards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk – and there can be little doubt that cyber-risk also must be considered as part of board's overall risk oversight. "*

Unfortunately, our Board survey results do not reflect Australian and overseas corporate regulators' perspectives on how Boards should approach cyber risk. More specifically:

- Just over half of our Board survey respondents told us that their IT departments remain principally responsible for cyber risk management, compliance and review activities (largely unchanged from last year).
- About 44% of Board survey respondents told us their Boards are only briefed on cyber security issues annually or on an ad hoc basis while 13% told us that their Boards received no briefings at all.

Percentage of Boards briefed annually, on an ad hoc basis or not at all

Potential for legal exposure if directors don't take appropriate action

In addition to the reputational harm to the organisation that may result from a cyber incident, there is the potential for substantial legal exposure (including personal liability on the part of directors and employees). This may include:

- Personal liability for directors for breach of their obligations under section 180 of the Corporations Act. This section requires directors to exercise their powers and discharge their duties with reasonable care and diligence. Given the widespread coverage of cyber incidents, particularly over the last five years, and public statements of Australian and overseas corporate regulators as to the proper approach to cyber risk, it seems apparent that directors must now consider cyber risk as part of their risk management activities, and implement appropriate strategies to mitigate it.
- Where the organisation has raised capital from investors through a public offer, personal liability for directors if cyber risk is not adequately disclosed in the relevant prospectus. If cyber risk is a significant factor for the organisation such that it would form part of the information that investors and their professional advisers would reasonably require to make an informed assessment of the organisation's offer, the directors of that organisation may be personally liable (under section 729 of the Corporations Act) for loss or damage suffered by investors as a consequence of cyber security issues materialising, if cyber risk was inadequately disclosed.
- Derivative shareholder actions against directors where such an action can be shown (to the Federal Court) to be in the best interests of the company (under Part 2F.1 of the Corporations Act). No such action has, as yet, been brought in Australia in relation to a cyber incident. However, with the increase in shareholder activism and litigation-funder driven class actions against companies and directors (both in Australia and overseas), and the ever increasing volume and sensitivity of data being handled by organisations, a derivate action stemming from a large-scale data breach may only be a matter of time.
- Where the organisation is an ASX-listed entity, liability for breach of the continuous disclosure rules, which require an organisation to disclose matters that a reasonable person would expect to have a material effect on the price or value of the organisation's shares.[16] Although the vast majority of data breaches are unlikely to reach this standard, it is conceivable that a particularly serious data breach (of the scale and severity of the Target or Sony Pictures breaches) would invoke these continuous reporting obligations.
- Liability of the organisation (and potentially its officers or employees) for claims of misleading or deceptive conduct under the *Competition and Consumer Act 2010* (Cth), for example, as a result of failing to act in accordance with the organisation's privacy policy. Although no such action has yet been brought in Australia, the US Federal Trade Commission has launched over 50 enforcement actions against organisations relating to cyber security under equivalent provisions of the US *Federal Trade Commission Act*.[17]
- Liability for breach of contract claims from suppliers or customers, for breach of specific obligations imposed on the organisation in relation to data security, the protection of personal information, and obligations of confidence (which may, in some cases, permit the termination of the contract by the affected customer or supplier).
- Responsibility for breaching APRA's prudential standards relating to outsourcing for organisations regulated by APRA (banks, insurance companies and most members of the superannuation industry).

> A cyber-attack can affect us all. It can undermine businesses and impact our economy. It may also erode investor and financial consumer trust and confidence in the financial system and wider economy.
>
> THE AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION (**ASIC**)[6]

> Effective board oversight of management's efforts to address [cyber security] issues is critical to preventing and effectively responding to successful cyber-attacks and, ultimately, to protecting companies and their consumers, as well as protecting investors and the integrity of the capital markets.
>
> LUIS AGUILAR, COMMISSIONER, US SECURITIES AND EXCHANGE COMMISSION (**SEC**)[7]

EDUCATING BOARDS ABOUT CYBER RISK

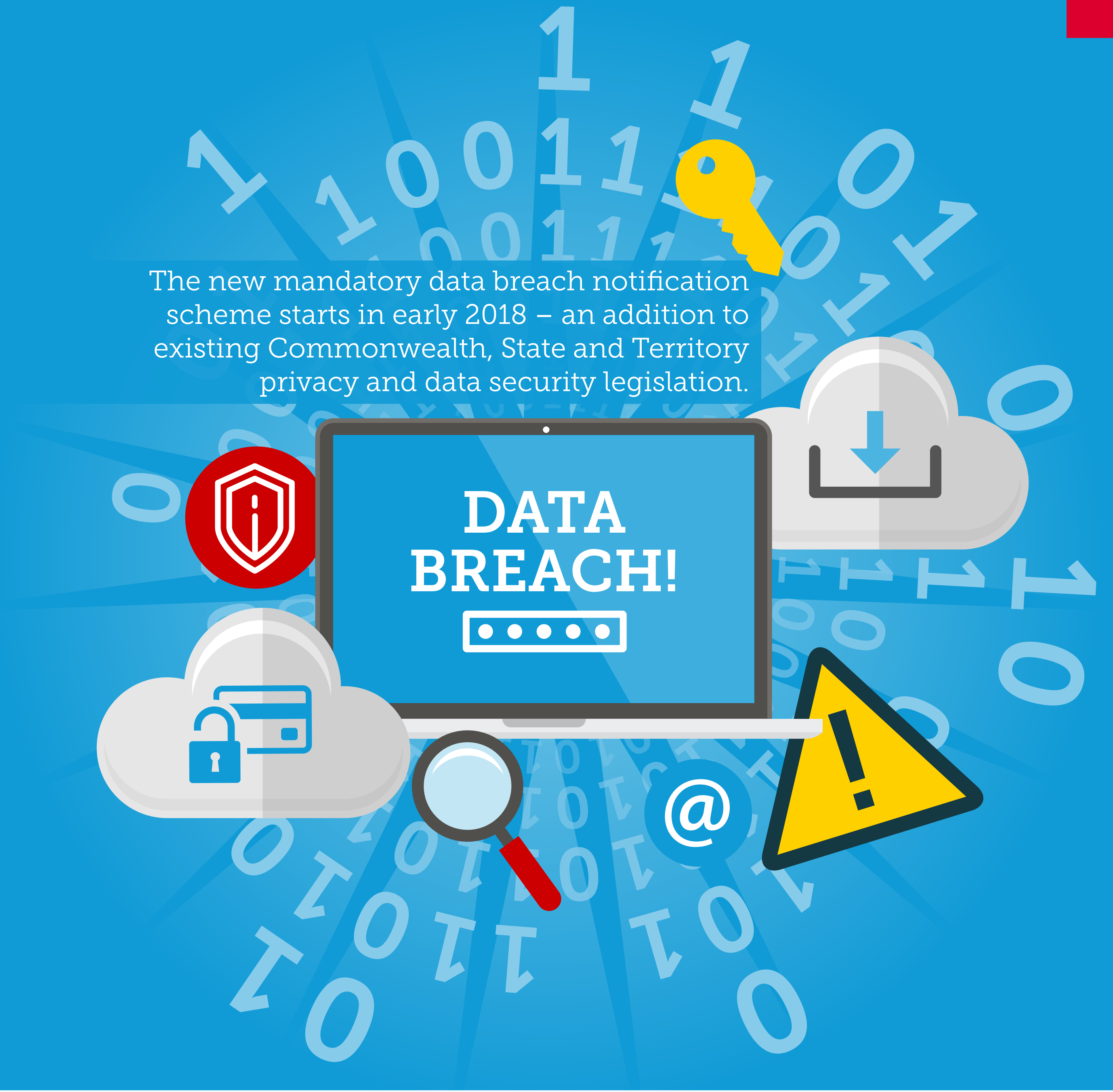
Boards must be cyber risk aware, and there are a number of steps they can take.

- Adopt written cyber security policies, procedures and internal controls, including:
  - Clearly setting out who in management has primary oversight of cyber security issues.
  - Adopting and regularly reviewing the company's data breach response plan.
  - Maintaining a responsive approach to new threats or elevated threats against an agreed risk appetite.
  - Receiving and reviewing regular reports on cyber security incidents.
  - Supporting cyber awareness and training across the organisation.
- Appoint a Board member who has cyber security expertise, or alternatively, appoint an independent expert who can present to the Board on cyber security issues.
- Adopt a cyber 'value-at-risk' model that not only quantifies cyber risk in financial terms, but enables the Board to formulate strategies and controls in relation to cyber risk, to treat cyber resilience as a potential differentiator, and to track the organisation's cyber maturity across time.
- If the organisation is a listed company, comply with continuous disclosure obligations in relation to cyber incidents that may reasonably be expected to materially affect the price or value of the organisation's shares.
- If the organisation is seeking to raise capital from retail investors, clearly and concisely outline the cyber risks faced by the organisation in any prospectus or public offer document that is issued.
- Review annual budgets for IT security and data protection expenditure (including for cyber insurance).

> "*[We need to]* continue to **educate our people** that cyber security is an **organisation wide issue**, not an IT issue."
>
> *CIO survey participant*

Finding four

The privacy landscape is changing, both in Australia and overseas



The new mandatory data breach notification scheme starts in early 2018 – an addition to existing Commonwealth, State and Territory privacy and data security legislation.

More than half of CIO survey respondents agreed that mandatory data breach notification requirements should be introduced into Australian law (largely unchanged from 2015). This will now happen.

Mandatory data breach notification in Australia

The *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* has passed both houses of Federal Parliament with little objection and no amendments. The new mandatory data breach notification scheme will therefore be inserted into the *Privacy Act 1988* (Cth) as new Part IIIC, and will commence in February 2018.

The scheme imposes new obligations on organisations that are subject to the Privacy Act to:

- Carry out a reasonable and expeditious assessment if they have *reasonable grounds* to suspect that there may have been an eligible data breach (and to take reasonable steps to complete that assessment within 30 days).
- Unless an exemption applies, make the prescribed notifications to the OAIC (and, if practicable, to affected individuals) as soon as they are aware that there are reasonable grounds to believe that there has been an eligible data breach.

Other Australian privacy and data security requirements

The scheme will be in addition to all of the existing privacy and data security requirements imposed by Australian Commonwealth, State and Territory legislation, as well as requirements that may be imposed on organisations under contract. These include:

- The Australian Privacy Principles (**APPs**): most notably, APP11, which requires organisations to take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification and disclosure, and to permanently destroy or de-identify the information when it is no longer required for any purpose permitted by the APPs.
- The additional obligations imposed on credit providers and credit reporting bodies under Part IIIA of the *Privacy Act* and the registered Credit Reporting Code in relation to the security of credit and credit eligibility information.
- The data security requirements imposed by the *Privacy (Tax File Number) Rule 2015.*
- Requirements imposed on telecommunications carriers and internet service providers under the *Telecommunications (Interception and Access Act) 1979* (Cth) to maintain the confidentiality of the metadata that they are required to retain under that Act.
- Legislative requirements imposed on Commonwealth, State and Territory government agencies in relation to the protection of personal and other information, such as the *Commonwealth Government's Protective Security Policy Framework.*
- Requirements imposed on public sector organisations under State and Territory privacy legislation, and which require the implementation of additional procedures and policies for dealing with data security breaches (these obligations may also be imposed on private sector organisations through outsourcing contracts with public sector entities).
- Additional requirements imposed on public and private sector organisations under State and Territory health records laws.
- Contractual requirements imposed on organisations that collect and handle payment card information under the Payment Card Industry Data Security Standards **(PCI DSS)**, which set out obligations to maintain the security of card information and respond when data breaches involve payment cards or cardholder data.
- Mandatory data breach notification requirements imposed on healthcare provider organisations, registered contracted service providers as well as registered repository and portal operators under the *My Health Records Act 2012* (Cth).

In Finding 3 we discussed other legal risks to an organisation that may result from a cyber incident, including liability arising under Australian corporations and consumer protection legislation.

Overseas privacy and data security laws

In addition to Australian laws, organisations must be aware of overseas privacy and data protection laws that may apply to them, either because they do business in one or more overseas jurisdictions, or because 'long arm' overseas regulation may apply to their activities.

This includes mandatory data breach notification requirements in:

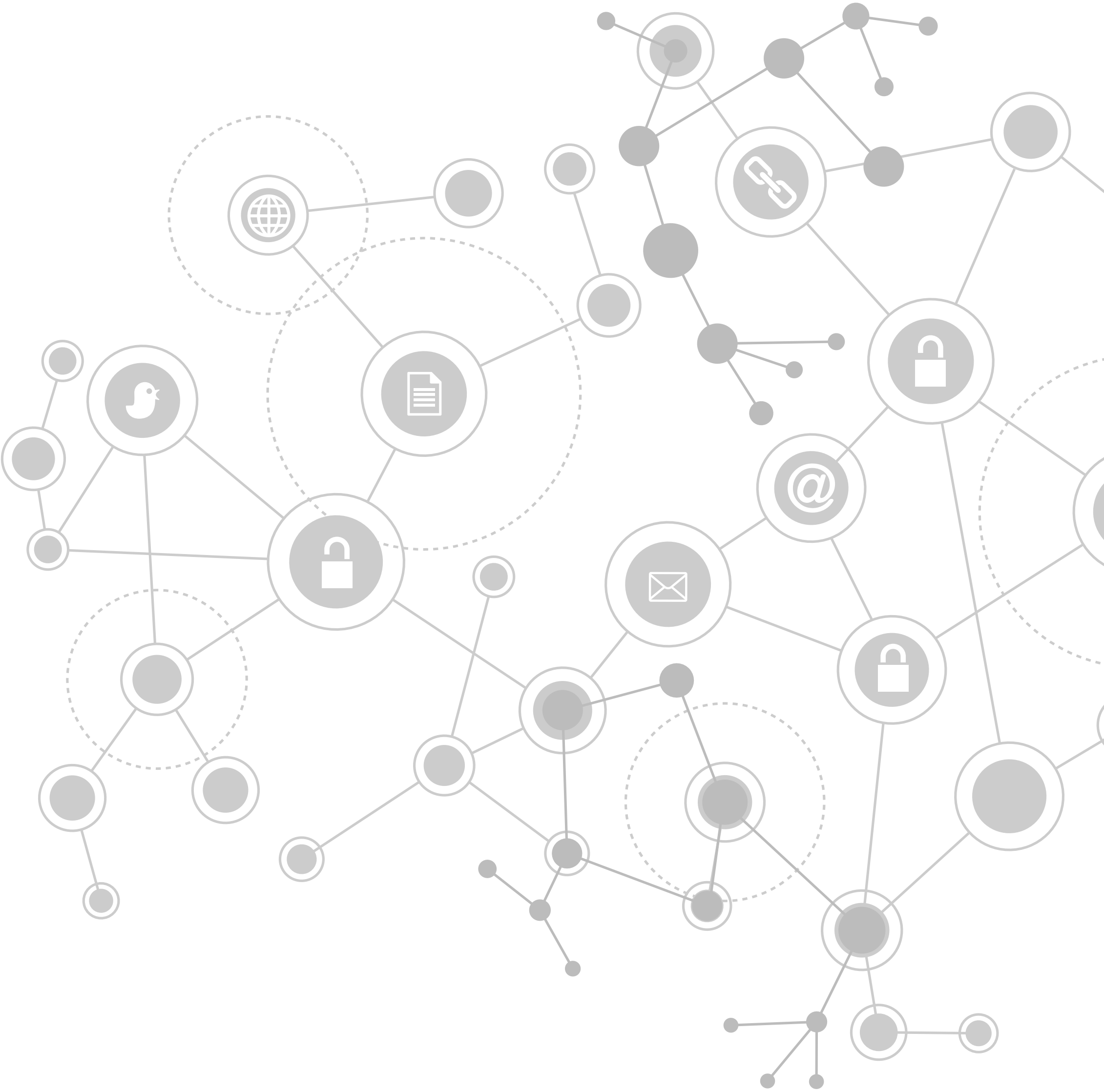
- 47 US States
- Alberta, Canada (with the whole of Canada expected to be subject to a mandatory Federal notification scheme by 2018)
- South Africa and South Korea.

Moreover, from April 2018, the European Union's General Data Protection Regulation (**GDPR**) will come into effect. The GDPR:

- Mandates stringent data security and privacy protection standards.
- Operates extraterritorially in requiring non-EU organisations that offer goods or services online to data subjects in the EU, or who monitor the behaviour of EU data subjects that takes place in the EU, to adhere to those standards.
- Provides for the imposition of penalties for breaching the GDPR of up to €20 million or 4% of annual worldwide revenue, whichever is higher.
- Requires organisations (whether or not based in the EU) to provide EU data subjects with the ability to have their data deleted or modified, to request reasons for decisions, to object to automated decisions or profiling and to request manual intervention.
- Provides for mandatory data breach notification.

This GDPR has significant implications for organisational process change requirements, and is likely to impact many Australian organisations that hold the data of EU data subjects or that do business in the EU.

Some US commentators have expressed concern that the effect of mandatory data breach notification is increased class actions, triggered by harm caused by the breach. This may ultimately occur in Australia as notifications increase. Breach prevention, and failing that, swift and effective containment and notification to mitigate and redress harm, will be critical.



Australian organisations must prepare for mandatory data notification.

PREPARING FOR MANDATORY DATA BREACH NOTIFICATION

Implement an effective data breach response plan, which at minimum should set out:

- The members of the response team (which will usually include senior IT, risk, legal, HR and media/communications representatives), including who in the organisation 'owns' the response plan.
- The circumstances in which actual or suspected breach should be escalated to the response team.
- The actions and escalations to be taken by the response team, including:
  - delegations of authority
  - reporting lines (including when and how reporting to the Board will occur)
  - when and how third parties will be engaged (such as forensic IT, lawyers and PR advisors), including the identities of those third parties
  - when and how insurers will be notified (including to ensure that delays in notification do not adversely affect the insurance policy)
  - when and how law enforcement agencies will be engaged.
- The specific legislative obligations arising from a data breach (including under Australian and applicable overseas mandatory data breach notification legislation, and where applicable, continuous reporting requirements) and the processes for complying with those obligations (including having near 'ready to go' template notices).
- Specific contractual requirements arising from a data breach such as an obligation to notify customers of a suspected or actual breach and provide assistance on request to respond to and investigate the breach, and the processes for complying with those requirements.
- The process for capturing 'lessons learnt' from the breach.

The data breach response plan should be regularly 'battle tested' and rehearsed. This may involve conducting 'red teaming' exercises – simulated adversarial attempts to breach the organisation's cyber and data defences.

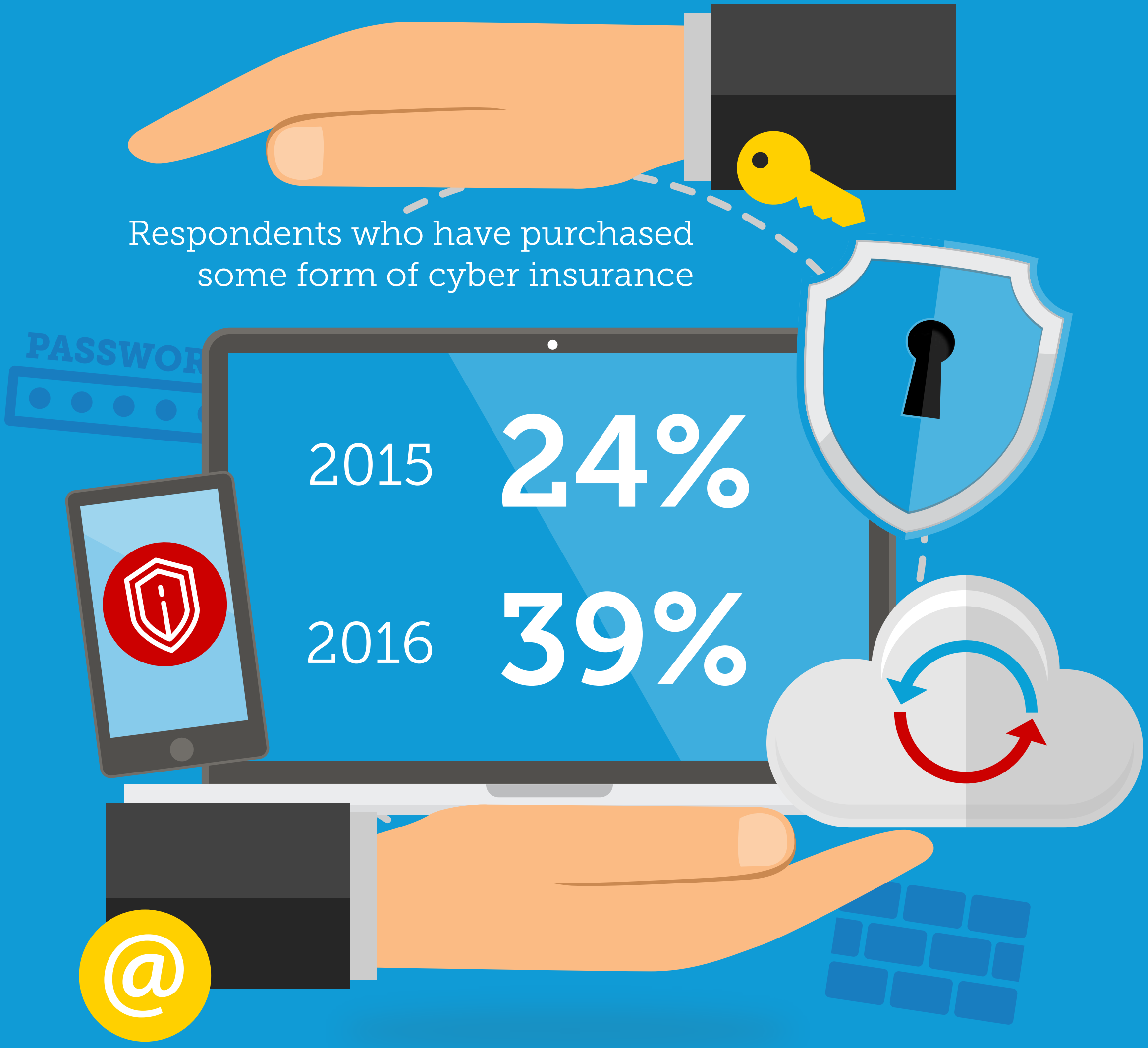
It should also be regularly updated based on the outcome of testing, as well as to reflect changes to the organisation's business, strategies, policies, processes, legal and regulatory obligations and cyber risk profile.

All staff should receive regular training in data security and identification and escalation of suspected or actual breaches.

Finding

five

The increasing uptake of cyber insurance indicates some willingness to act on managing cyber risk



Respondents who have purchased some form of cyber insurance

2015 24%

2016 39%

Our CIO survey results show that a rising proportion of organisations are electing to purchase specialist cyber insurance to help manage the risks associated with a cyber incident.

While five years ago cyber insurance was a niche product offered by only a small handful of insurers in the Australian market, most blue-chip Australian insurers now offer tailored policies covering cyber risk, privacy and data security losses.

In the past 12 months we have seen the continued evolution of cyber insurance offerings, from traditional policies focused on liability to third parties, to comprehensive hybrid products covering additional losses such as breach response costs, regulatory expenses and business interruption. In recognition that cyber resilience is a collaborative process, insurers are increasingly partnering with IT professionals, forensic accountants, public relations professionals and regulatory lawyers to provide a holistic response to cyber incidents. Traditional claims management protocols are commonly set aside in favour of insured organisations accessing urgent 'breach coaching' services from these teams of professionals through telephone hotlines, websites or monitored email addresses.

Cyber risk insurers are providing value-add services to assist organisations in becoming more cyber resilient. Common value-adds for insured organisations include cyber risk assessments by specialist IT professionals, credit monitoring services and data breach response training.

With the passage through Federal Parliament of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*, the uptake of specialist cyber insurance is likely to continue rising in the coming year.

Organisations seeking to secure cyber risk insurance, or to renew an existing policy, need to consider some critical factors.

CONSIDERATIONS WHEN PURCHASING CYBER RISK INSURANCE

- Whether the policy provides cover for the new assessment and notification obligations under the mandatory data breach reporting scheme set out in the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*.
- Whether the insurer offers urgent breach coaching or cyber incident response services (providing access for insured organisations to IT professionals, forensic accountants, public relations professionals and lawyers).
- Any limitations on an organisation's preferred response to a cyber incident (for example, does the insurer require an insured organisation to obtain written permission prior to paying a ransom?).
- The availability of value-add services, such as credit monitoring, to assist organisations in establishing and maintaining goodwill with customers following a data breach.
- Policy exclusions for liability assumed under contract. As there is no basis under Australian common law to sue for breach of privacy, third party liability claims may be advanced against insured organisations in contract. Organisations should therefore take care to identify potential exclusions in the policy that may apply to such contractual claims.

> "*[We need to]* provide **additional resources** and budgets to **strengthen** our cyber security."
>
> *Board survey participant*

MinterEllison's cyber security team can help you address and mitigate cyber risk.

Conduct independent cyber risk reviews and Board-level cyber risk assessments.

Review third-party supplier contracts

to ensure that they appropriately address privacy and data protection issues, and do not inappropriately transfer cyber-related risks to your organisation.

Develop, review and update data breach response plans

as well as related policies and procedures, such as privacy and document retention policies.

Advise on privacy, data protection and cyber-related legal and commercial issues.

Develop and deliver cyber risk and privacy compliance tools

through face-to-face and online training (including via our award winning Safetrac online compliance system).

Conduct privacy audits and impact assessments

including in relation to cloud-based products and services.

Plan for, respond to and rebuild from, a data breach or cyber incident,

including breach coach services (where MinterEllison leads the data breach response process).

Advise on cyber insurance issues

including assisting with cyber risk advice coverage issues, and strategic management of notifications and claims arising from cyber risk losses.

Contacts

Paul Kallenbach
Partner
T +61 3 8608 2622
M +61 412 277 134

Anthony Lloyd
Partner
T +61 2 9921 8648
M +61 411 275 811

Anthony Borgese
Partner
T +61 2 9921 4250
M +61 400 552 665

Amanda Story
Partner
T + 61 2 6225 3756
M +61 423 439 659

Cameron Oxley
Partner
T +61 3 8608 2605
M +61 417 103 287

Veronica Scott
Special Counsel
T +61 3 8608 2126
M +61 411 206 248

Leah Mooney
Special Counsel
T +61 7 3119 6230
M +61 421 587 950

John Fairbairn
Partner
T +61 2 9921 4590
M +61 410 475 965

Endnotes

[1] Cybersecurity Ventures, 2016 Cybercrime Report, available at http://bit.ly/2bHNaBz.

[2] Australian Government, *Australia's Cyber Security Strategy*, April 2016 at 15, available at http://bit.ly/1r6MNr0

[3] US National Initiative for Cybersecurity Careers and Studies Glossary, available at http://bit.ly/2jrROaX

[4] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (2013), available at http://bit.ly/1Gp5CbC

[5] J J Cebula and L R Young, 'A Taxonomy of Operational Cyber Security Risks' (2010) Technical Note CMU/SEI-2010-TN-028, CERT Carnegie Mellon University, available at http://bit.ly/1NEBcTU

[6] ASIC, *Cyber resilience: Health check* (March 2015), available at http://bit.ly/1HyFGJC

[7] Office of the Australian Information Commissioner, *Data breach notification – a guide to handling personal information security breaches* (August 2014), available at http://bit.ly/1XVFk9h

[8] 2016 Cyber Attack Statistics, www.hackmagedon.com.

[9] US Department of Justice, *How to Protect Your Networks from Ransomware* (2016), available at http://bit.ly/2jRV2nD.

[10] These results are consistent with the New York Stock Exchange's 2015 *Cybersecurity in the Boardroom* survey (available at http://bit.ly/1P4v5yX), which found that 42% of surveyed Boards only discussed cyber security issues 'occasionally'.

[11] Interesting, Intel Security's 2015 *Grand Theft Data* report (available at http://intel.ly/2kFXBMP) found that external actors were responsible for only 57% of data breaches, while 43% of data breaches were caused by the actions (whether negligent or malicious) of trusted insiders.

[12] Australian Securities and Investments Commission, *Cyber Security and Directors* (May 2016), available at http://bit.ly/2lEHf8o.

[13] Speech by SEC Commissioner Luis Aguilar, *Cyber Risks and the Boardroom* (June 2014), available at http://bit.ly/2kFtG8M.

[14] Speech by ASIC Chairman Greg Medcraft, *Building Resilience: The Challenge of Cyber Risk* (December 2016), available at http://bit.ly/2m1B7Y7.

[15] Speech by SEC Commissioner Luis Aguilar, *Cyber Risks and the Boardroom* (June 2014), available at http://bit.ly/2kFtG8M.

[16] ASX Listing Rules, Rules 3.1, 3.1A and 3.1B.

[17] Paul Ferrillo and Christophe Veltsos, *Take Back Control of your Cybersecurity Now* Advisen, 2017.

www.minterellison.com

MinterEllison