Report:

Perspectives on cyber risk

January 2016

MinterEllison

Introduction

Although an issue for many years, cyber security has risen to particular prominence in the news media over the past 24 months. Cyber attacks against Sony, Target, Ashley Madison, eBay, Microsoft, Las Vegas Sands, Anthem Insurance, Home Depot and many others have shown what can occur when high profile organisations experience the downside of our global and digitally integrated economy. As recently as October 2015, significant and sustained cyber attacks have impacted Australian retailers David Jones and Kmart; telcos T-Mobile (UK) and TalkTalk (US); US web hosting provider 000webhost.com; and US online broker Scottrade.

The Ponemon Institute's 2015 data breach study[1] found that the total cost of a data breach has increased by 23% since 2013. During this period, the frequency of cyber attacks has also increased, with cyber attacks identified as being the root cause of data breaches in 47% of cases in 2015 (up from 37% in 2013). And according to security firm Gemalto, one billion data records were compromised in 2014.

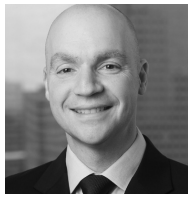
For almost all modern organisations, the opportunities afforded by the digital economy far outweigh the risks of participating in it; however, those risks must nevertheless be understood, assessed and appropriately addressed.

Vigilance and preparedness across the whole organisation, from Board members to individual employees, is particularly important in driving an organisation's cyber resilience strategy.

With the expected introduction of mandatory data breach legislation in Australia in 2016, the potential for Board members to incur personal liability as a result of a data breach, and the significant reputational consequences, both for individuals and organisations, that may flow from a cyber attack, it's never been more important for all levels of an organisation to turn their attention to cyber risk and how their organisation might be vulnerable.

We hope that this report provides a useful tool for organisations to benchmark their current cyber resilience capability, and asses whether further action is required to improve it.

MinterEllison Cyber Security Team



Paul Kallenbach
Partner

Anthony Lloyd
Partner

—

'Instead of being treated as a technical problem that calls for technical solutions, digital risk should be approached as an economic risk; it should therefore be an integral part of an organisation's overall risk management and decision making processes. The notion that digital security risk merits a response fundamentally different in nature from other categories of risk needs to be countered.'

OECD, Digital Security Risk Management for Economic and Social Prosperity[2]

—

About this survey

MinterEllison conducted the 2015 cyber security survey in order to provide a view of Australian organisations':

- risk posture in relation to cyber attacks
- cyber resilience capability, and
- current and future intentions in adopting services that may give rise to additional cyber risk (such as cloud-based services).

We distributed two different surveys: one directed at chairmen, directors and CEOs (*Board Survey*), and another directed at CIOs, CISOs, general counsel, and other risk-related managers (*CIO Survey*).

The surveys were distributed to a diverse range of organisation types (including top 100 ASX companies, non ASX-listed entities, State and Federal government departments and not-for-profit organisations). Surveyed organisations operate in a diverse range of industries (including agriculture, forestry and fishing; education; energy, mining and resources; entertainment and leisure; finance and insurance; government; health and aging; manufacturing; professional services; property and construction; retail; technology, media and telecommunications; and transport and logistics). We received and evaluated a total of 159 responses across all of these organisation types and industries (81 responses to the Board Survey and 78 responses to the CIO Survey).

Glossary of terms used in this report

cyber attack	any offensive activity designed to obtain unauthorised access to, or degrade, damage, disrupt or destroy, one or more information systems[3]
cyber security	the safeguards and actions that can be used to protect against cyber attacks[4]
cyber risk	operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of data or information systems[5]
cyber resilience	an organisation's ability to prepare for, respond to and recover from a cyber attack (including its ability to operate during, and adapt to and recover from, a cyber attack[6]
data breach	a situation where data (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 attack[7]

1 Cyber risk is front of mind for Australian organisations

The World Economic Forum ranks cyber attacks as a top 5 risk in terms of combined likelihood and impact (along with interstate conflict; water crises; failure of climate change adaptation; and underemployment/unemployment).[8]

Our survey shows that there is significant awareness of, and a growing concern about, cyber risk among survey respondents.

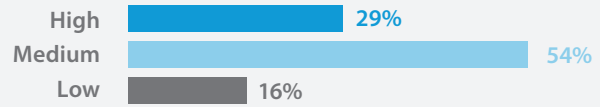
Among Board Survey respondents, 60% perceived cyber risk as being more of a risk than it was 12 months ago. A similar percentage of Board Survey respondents (54%) ranked cyber risk as a **medium risk** to their organisations (that is, outside the top 5 risks), with a further 29% of respondents ranking it as a **high risk**.

At the operational level, nearly 40% of CIO Survey respondents reported a cyber attack compromising their organisation's systems or data in the past 12 months, with a further 8% reporting more than 5 attacks. Cyber attacks reported by our respondents were not limited to particular organisation types or industries, with attacks reported by all organisation types, and in almost all of the industries surveyed.

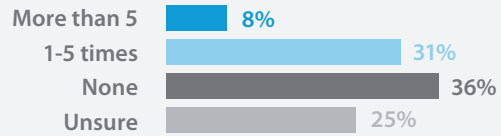
A majority (58%) also indicated that their organisations are spending more on IT security than they were 12 months ago.

A majority of respondents to both the Board Survey and CIO Survey considered that their organisations had an adequate or detailed understanding of their exposure to the risk of cyber attacks, while 58% of CIO Survey respondents reported being 'somewhat satisfied' or 'very satisfied' with their organisation's current capability to prevent and respond to cyber attacks.

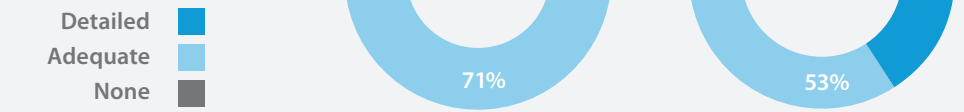
Where does cyber risk rank on your organisation's corporate risk register? (Board Survey)



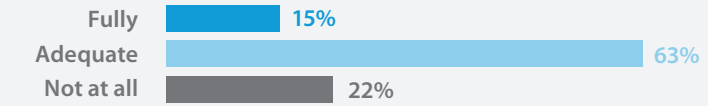
How many times has your organisation been subject to a cyber attack in the past 12 months that has compromised your systems or data? (CIO Survey)



What level of understanding does your organisation have of its exposure to the risk of cyber attack? (CIO Survey)



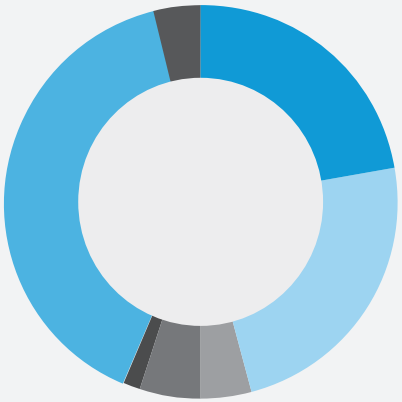
To what extent do you consider that the Board is adequately informed of, and kept appraised of, cyber risk issues? (Board Survey)



1 Cyber risk is front of mind for Australian organisations

Considering the consequences of a cyber attack, 'reputational risk' was perceived by 40% of respondents to the CIO Survey as being their organisations' greatest exposure resulting from a cyber attack, followed by data loss (24%) and business interruption (22%).

What do you perceive as the greatest exposure to your organisation resulting from a cyber attack?
(CIO Survey)



- **Business Interruption** 22%
- **Data loss** 24%
- **Fraud** 4%
- **Loss of customer contracts** 5%
- **Other** 1%
- **Reputational damage** 40%
- **Regulatory action (eg Privacy Commissioner)** 4%

Interestingly, just 4% of respondents considered regulatory action to be the greatest exposure resulting from a cyber attack. This was surprisingly low, given the significant regulatory requirements that apply to many Australian businesses in relation to the protection of data held by them or their third party service providers – as well as onerous penalties and other sanctions should they fail to comply with those requirements.

For example:

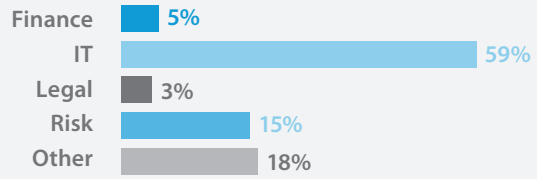
- organisations that are regulated by the Australian Prudential Regulatory Authority (APRA) – which includes banks, insurance companies and most members of the superannuation industry – must comply with APRA's Prudential Standards, which include specific requirements for privacy and data security[9]
- Guideline 6.1 of the statutory tax file number (TFN) guidelines requires TFN recipients to protect TFN information by such security safeguards as are reasonable in the circumstances
- credit providers and credit reporting bodies are subject to additional obligations under Part IIIA of the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Credit Reporting Code in relation to the security of credit reporting and credit eligibility information
- carriers and internet service providers are subject to specific requirements in relation to maintaining the confidentiality of the metadata they are required to retain under recent amendments to the *Telecommunications (Interception and Access Act) 1979* (Cth), and
- many public sector organisations are subject to agency-specific legislative requirements that add further protection for personal information, and to government data protection requirements that apply generally (such as the Australian Government's Protective Security Policy Framework).

2 Managing cyber risk is increasingly recognised as an enterprise-wide challenge

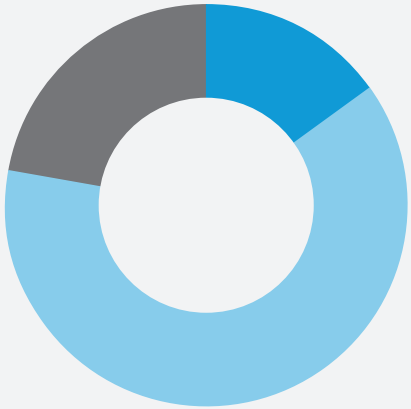
While the IT department is viewed as having principal responsibility for cyber risk management, compliance and review activities by 59% of respondents to our Board Survey, there is evidence in the qualitative responses to the CIO Survey that organisations are increasingly treating cyber risk as an enterprise-wide challenge.

In addition, 78% of respondents to the Board Survey indicated that they considered their Boards to be adequately or fully informed of cyber risk issues. This is a positive result, given recent studies which have shown that Board involvement in particular can significantly reduce the organisation's financial loss flowing from a data breach.[10]

Who in your organisation is principally responsible for its cyber risk management, compliance and review activities?



To what extent do you consider that the Board is adequately informed of, and kept appraised of, cyber risk issues? (Board Survey)



Fully	15%
Adequate	63%
Not at all	22%

—

'This is a continual and growing process. We need to keep doing more. But as we do more, the hackers do more, and the size of the challenge grows.'

Respondent feedback, Board Survey

'[We need to] raise the profile of cyber security across the broader business. Cyber security is not simply an IT issue.'

Respondent feedback, CIO Survey

'We need to consider cyber security as part of our risk profile and strategy.'

Respondent feedback, Board Survey

—

2 Managing cyber risk is increasingly recognised as an enterprise-wide challenge

Embedding cyber resilience

Embedding cyber resilience within an organisation involves more than just keeping the Board abreast of cyber risk issues. It also involves:[11]

Cyber security governance (which includes raising awareness of cyber risk across the whole organisation and assessing the organisation's cyber resilience against objective frameworks).[12]

Determining the organisation's level of exposure to cyber risk, including by identifying:

- the business assets (including information assets) that are critical to the organisation
- the extent to which the organisation is exposed to supply chain risk by its reliance on third party suppliers (for example, outsourced IT providers and other contractors) or particular customers
- how well informed the organisation's personnel are in relation to cyber risk and cyber risk management
- whether the organisation has sufficient resources to deal with a cyber attack.

Continually assessing (and updating where necessary) the organisation's policies and procedures relating to cyber risk and cyber resilience, including by:

- implementing and testing a data breach response plan (discussed further in section 4 below)
- reviewing and testing the organisation's information security policies and procedures (including the organisation's business continuity and disaster response plans)
- reviewing and testing the organisation's cyber attack monitoring and detection processes
- properly training employees and contractors.

Reviewing the organisation's insurance policies and coverage to ensure that risks are appropriately covered by insurance (including cyber risk insurance, where this is considered appropriate).

'I think we are on top of it from an awareness viewpoint but still have some way to go from a preventative viewpoint'

'There needs to be more information for staff and discussion about IT security including cyber security'

'Put more emphasis on 'could happen', be more proactive rather than reactive'

'Regular briefings to the Board on the security environment would be useful'

Respondent feedback

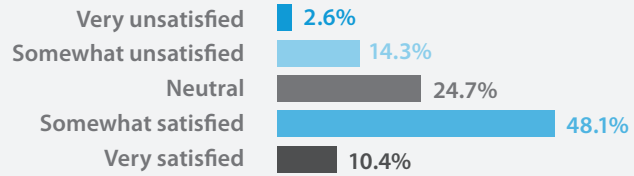
3 Organisations can do more to improve their cyber resilience capabilities

Our survey results indicated that 39% of Board Survey respondents and 58% of CIO Survey respondents were somewhat or very satisfied with their organisations' capacity to respond to cyber attacks, with only 15% and 17% respectively expressing dissatisfaction in relation to this. These results suggest, overall, a moderate to high level of satisfaction among respondents as to their organisations' cyber resilience capabilities.

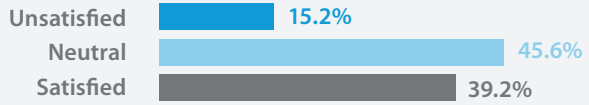
However:

- over half (58%) of respondents to the CIO Survey were either unsure as to whether, or were not satisfied that, their organisation's systems or data were appropriately segmented to mitigate the risk of a cyber attack. (Segmentation involves dividing one large network into smaller functional networks, to reduce the extent to which an attacker can move across the network, and is a key cyber risk mitigation strategy)[13]
- a significant number of respondents to the CIO Survey (27%) reported that their organisation did not have a data breach response plan in place. Preparing (and, where necessary, implementing), and regularly testing, a data breach response plan should be a key element of every organisation's cyber resilience planning (see section 4 below)
- 56% of respondents reported that they conducted IT security training of their personnel on an ad hoc basis only. Conducting regular security training of personnel (in particular, training of those personnel most likely to be targeted by hackers) is another key cyber risk mitigation strategy)[14]

How satisfied are you with your organisation's current capability to prevent and respond to cyber attacks?
(CIO Survey)



How satisfied are you with your organisation's current capability to prevent and respond to cyber attacks?
(Board Survey)



- only 25% of respondents to the CIO Survey had cyber risk insurance in place, with a further 32% unsure about their insurance arrangements (see section 5 below).

These results suggest that there may be a disconnect between respondents' perceptions of their level of cyber preparedness, and the practical measures that respondent organisations have implemented in order to address cyber risk.

4 Every organisation should have a data breach response plan

The view of the Office of the Australian Information Commissioner (OAIC)[15] is that all organisations governed by the Privacy Act should have a data breach response plan,[16] as doing so will assist an organisation to meet their obligations under Australian Privacy Principle (APP) 11 (which requires the organisation to take 'reasonable steps' to protect the personal information it holds – and 'reasonable steps' may include having a data breach response plan).

A data breach response plan should set out the organisation's framework for managing a data breach.[17] The plan should be regularly tested and amended as necessary.

If the organisation has insurance, the data breach response plan should also set out the steps that must be followed in relation to that insurance cover, which may (for example) include that the insurer be promptly notified, so as not to adversely impact the organisation's entitlement to coverage under the insurance policy.

The delayed involvement of insurers – who will generally provide value-add services such as IT recovery, forensic accounting and public relations assistance – may also lead to an increase in the losses an organisation ultimately sustains as the result of the data breach. The availability of cover for regulatory expenses (including fines and penalties) is another good reason not to delay notification to the organisation's insurers.

Of course, subject to the terms of the insurance policy, notification to the organisation's insurers should be effected in a co-ordinated way, so that reputational risks are also properly managed.

Features of an effective data breach response plan

A data breach response plan should set out:

- the members of the response team (which will often include senior IT, risk, legal, HR and media/communications representatives)
- when a breach (or suspected breach) should be escalated to the response team
- the actions and escalations to be taken by the response team if a data breach has occurred (including involvement of third parties, such as forensic IT, lawyers and PR advisors, where required) and specific legislative obligations arising from a data breach
- specific contractual requirements arising from a data breach (for example, a contract with a customer may contain an obligation to notify that customer of the breach)
- key internal and external contacts
- procedures for determining whether to notify affected individuals and regulators (including the OAIC)
- reporting requirements to other key stakeholders (including regular reporting to the Board)
- process for capturing 'lessons learnt' from the breach.

5 Cyber insurance has not yet been widely embraced

Only 25% of respondents confirmed their organisation held specialist cyber risk insurance. A further 32% were unsure of whether cyber risk was addressed in their existing insurance arrangements.

Does your organisation have cyber risk insurance?

Specialist cyber risk (or security and privacy) insurance is a relatively new product in the Australian market, but most blue-chip insurers have been offering these products in other markets for a number of years.

Organisations should exercise caution in seeking to rely on traditional insurance policies as these are unlikely to offer protection in the event of a cyber attack. For example, references to the theft of property in fidelity or crime policies are generally references to tangible physical property and these policies are therefore unlikely to provide cover in the event of a data breach.

Most of the specialist cyber risk insurance policies in the market are hybrid policies covering first party losses (such as the cost of hiring technical experts to identify and address the cause of the breach or engaging public relations specialists for the purposes of reputational repair) and regulatory costs (such as fines or penalties, and notification and monitoring expenses), in addition to third party cover for any claims arising from a data breach.

We expect to see an increase in take up levels of specialist cyber risk policies in the next 12 months, particularly with the imminent introduction of mandatory data breach notification laws. In the interim, readers of this report may wish to consider the following factors when evaluating cyber security insurance policies for their own organisations:

- the insurer's knowledge of the organisation's industry and regulatory requirements and restrictions
- any applicable deductibles, retentions and limits of liability, having regard to the organisation's appetite for risk. In some cases a time retention may apply in place of the monetary equivalent
- whether a standalone comprehensive cyber risk policy should be obtained in place of an extension to an existing traditional policy
- ongoing audit requirements imposed on the organisation
- jurisdictional and territorial issues around where claims against the organisation arise, and
- the potentially applicable exclusions under the policy.

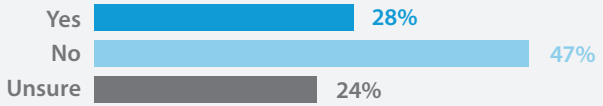
6 Many organisations are not adequately considering supply chain risk

Only 28% of respondents to the CIO Survey reported that they regularly audited their suppliers' IT security practices.

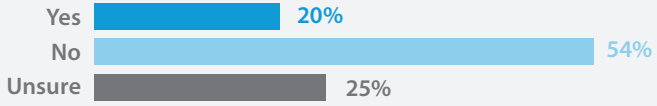
Similarly, only 20% of respondents indicated that they regularly audited their customers' IT security practices.

This suggests that respondents were not, in general, adequately taking account of supply chain risk as part of their cyber risk mitigation activities. This is of particular concern given the high proportion of respondents who are using, or are planning to use, cloud-based services (see section 7).

Does your organisation regularly audit your suppliers' IT security practices (at least annually)? (CIO Survey)



Does your organisation regularly assess your customers' cyber risk profile (at least annually)? (CIO Survey)



Organisations should take steps to mitigate supply chain risk, including:[18]

- identifying and evaluating cyber risk throughout the organisation's supply chain (including subcontractors of their key suppliers)
- conducting thorough due diligence on new suppliers and key customers (including their cyber security competence), which, for cloud-based services, should consider issues like:
  - the particular data that will be stored in the cloud (including its sensitivity)
  - where the data will be held (and will travel to or through)
  - whether the data will be logically separated from other customers' data
  - the service provider's business continuity and disaster recovery arrangements.
- incorporating provisions in contracts:
  - confirming the organisation's ownership of its data
  - mandating compliance with specific security and data protection, storage, backup and recovery requirements (including flow-down of those requirements to subcontractors)
  - mandating compliance with applicable privacy and data protection laws and relevant policies and procedures of the organisation
  - requiring the counterparty to notify the organisation should it suffer a data breach (whether or not affecting the organisation's data)
  - allowing for prompt access to the organisation's data in the custody of its suppliers (in a pre-agreed format)
  - providing for appropriate transition and disengagement rights and obligations.

Supply chain risk may arise from:

collateral damage to an organisation, resulting from:

- the interruption, degradation or cessation of supply (of goods or services, including cloud-based services) from a key supplier due to a cyber attack on that supplier, or
- solvency issues experienced by a key customer due to a cyber attack on that customer.

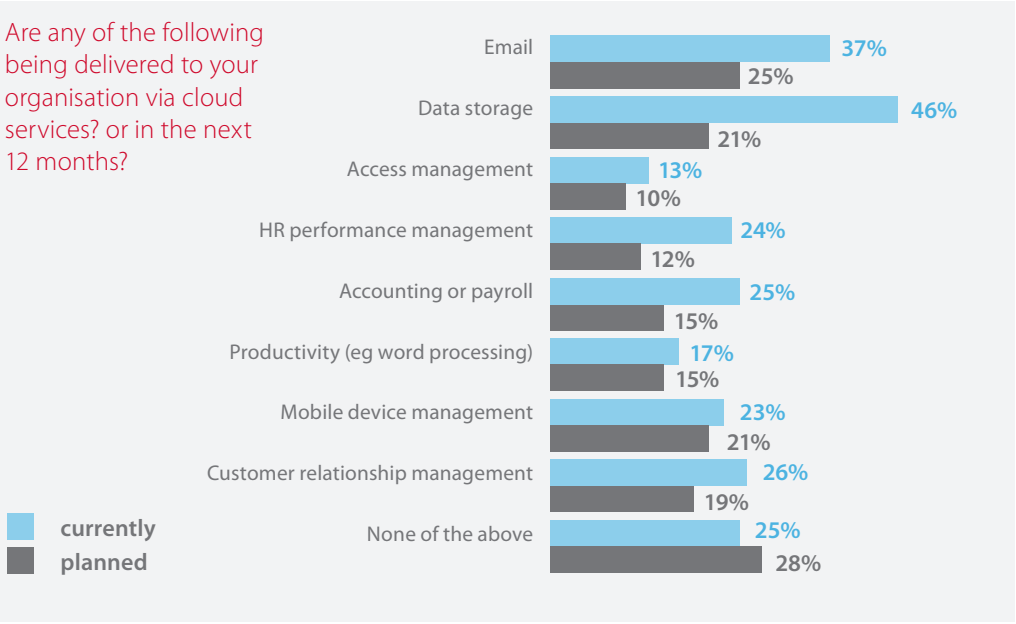
deliberate targeting of an organisation's ICT systems, using vulnerabilities identified within the ICT systems of other participants in the supply chain – a determined aggressor will try to identify the organisation with the weakest cyber security in the supply chain to effect this.[19]

7 Adoption of cloud services could increase cyber risk exposure

We asked respondents to the CIO Survey whether they were currently using cloud services, or were planning on doing so within the next 12 months.

46% of respondents reported currently using a cloud data storage service within their organisation. A further 21% of respondents indicated that they were planning to move to cloud data storage services within the next 12 months. This means that in 12 months time, as many as two-thirds of respondent's organisations could be storing data in the cloud. Only around 25% of our respondents reported not utilising any commonly used cloud services.

Interestingly, 48% of respondents also reported that their organisation did not permit personal information of their personnel, customers or suppliers to be transferred, accessed or stored outside of Australia.



In our experience, many organisations underestimate the ease by which personal information can be transferred offshore by providers.

In particular, many standard form agreements for enterprise-grade IT services expressly permit the service provider to transfer the customer's data offshore. Organisations may also not be aware that an overseas 'disclosure' of personal information (from a Privacy Act perspective) may occur when the overseas-based personnel of an IT service provider (such as their support personnel) view personal information on their computer screens from an offshore location. This will be the case notwithstanding that the data remains hosted on Australian servers and may be viewed by the overseas service provider via a secure and dedicated connection.

From a Privacy Act perspective, an important risk consideration in relation to the adoption of cloud services is section 16C of the Privacy Act (introduced in March 2014). This section provides that, in certain circumstances, conduct engaged in by an overseas recipient which would constitute a breach of the Australian Privacy Principles (had the overseas recipient been bound by the APPs) will be deemed to have been engaged in by the disclosing organisation.

When this deemed liability under section 16C is taken together with the enhanced suite of enforcement powers available to the Australian Privacy Commissioner (which includes the imposition of civil penalties of up to A$1.7 million for companies and A$340,000 for individuals per breach of the Act), it is more important than ever for organisations to turn their attention to the issue of supply chain risk as it relates to the adoption of cloud services.

8 Outsourcing IT security to a third party doesn't transfer cyber risk

A number of respondents to the Board Survey and CIO Survey reported that responsibility for cyber risk management, compliance and review activities had been outsourced to an IT service provider.

It is important for all organisations to understand that outsourcing their IT security function will not transfer responsibility for a cyber attack to the third party service provider even though they may be tasked with fixing or preventing these attacks.

There are a number of heads of liability that may be implicated in the case of a cyber attack, including:

- liability under the Privacy Act, particularly where personal information is disclosed outside of Australia in circumstances where the organisation has failed to take reasonable steps to protect the information from unauthorised access, modification or disclosure
- personal liability for directors under the *Corporations Act 2001* (Cth), including for breach of their obligation under section 180 to exercise their powers and discharge their duties with reasonable care and diligence. This is an objective standard of care. As the risk of cyber attacks have now received widespread coverage, it is arguable that an objective standard of care would require directors to have considered this issue, including the implementation of appropriate cyber risk mitigation strategies
- liability of the organisation for breach of the ASX Listing Rules dealing with continuous and periodic disclosure (where the organisation is an ASX listed entity)
- 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
- liability for claims of breach of contract with 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
- for organisations regulated by APRA (banks, insurance companies and most members of the superannuation industry), liability for breach of APRA's prudential standards relating to outsourcing.

Beyond purely legal risk, outsourcing of IT security will not transfer reputational risk – perceived by 40% of respondents to the CIO Survey as being their organisation's greatest exposure resulting from a cyber attack. Even if the service provider's systems were the subject of a cyber attack, media reports will not usually distinguish between the organisation's systems and those of its service provider.

In order to address key legal risks, organisations should ensure that relevant outsourcing contracts:

- impose detailed IT security requirements on service providers (which may mandate compliance with objective security standards, such as the ISO 27000 series of standards)
- appropriately allocate risk as between the organisation and the service provider, including by incorporating indemnities that shift risk to the service provider in circumstances where they have failed to adequately prevent or mitigate a cyber attack, and by requiring the service provider to take out insurance (including, where appropriate, cyber insurance)
- contain restrictions on subcontracting, so the organisation maintains transparency and control of the service provider's supply chain
- contain appropriate obligations of the service provider's use, storage and disclosure of, and the organisation's access to, the organisation's data
- sets out business continuity and disaster recovery obligations, including requiring the service provider to have, and to regularly test and update, a data breach response plan, and
- appropriately flow through any regulatory requirements to which the organisation is subject, such as the Privacy Act or other applicable data protection laws, and any specific audit requirements imposed by regulators.

9 There is majority support for mandatory data breach notification

A majority of respondents to the CIO Survey supported the introduction in Australia of mandatory data breach notification laws.

This may reflect our experience that, overall, organisations consider the benefits of having a more transparent view of data breaches across their supply chain outweigh their own potential cost of compliance. It may also mean that respondents, while generally satisfied with their own organisation's cyber preparedness, are less confident about the preparedness of their suppliers and customers.

The OAIC received 110 voluntary data breach notifications in 2014-15 (64% up on the previous year).[20] This is in contrast to the 'thousands' of unreported privacy breaches that are considered to be occurring in Australia each year.[21]

Organisations subject to APP 11 (under the Privacy Act) must take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. The OAIC's view is that following the voluntary data breach notification guide[22], and responding appropriately to a data breach (which may include notifying the OAIC and affected individuals), will assist organisations to meet the 'reasonable steps' requirement under APP 11.

Under step 3 of the OAIC's voluntary data breach notification guide, notification should be considered if there is a 'real risk of serious harm' to an individual, and this harm could be mitigated by notifying the individual.

Our survey response to this question may reflect that the majority of respondent organisations view mandatory data breach notification as largely consistent with current privacy and disclosure practices.

Following a number of Bills and the announcement in March 2015 that it planned to introduce mandatory data breach notification laws, the Federal Government released a draft exposure Bill and Discussion paper on 3 December[23] for industry consultation by March 2016. The Privacy Act will likely be amended by the end of 2016 to include such a scheme.

The exposure Bill would require agencies and private sector organisations subject to the APPs, credit reporting bodies and credit providers who hold credit reporting and credit eligibility information, and tax file number recipients, unless otherwise exempt, to notify affected individuals and the Privacy Commissioner if there will be a 'real risk of serious harm' to any individual from:

- an unauthorised access to or disclosure of any of their personal or other information, or
- the loss of any of their personal or other information in circumstances where unauthorised access or disclosure is likely to occur.

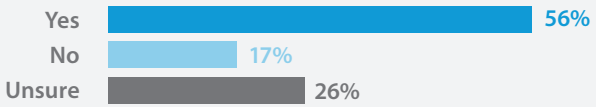
The scheme will also apply to organisations who disclose personal information overseas under APP 8.1. This means that organisations may be required to provide notification of serious data breaches suffered by overseas organisations (such as their cloud service providers) to whom they have disclosed personal information.

The draft exposure Bill defines a 'real risk' as one that is not remote, and sets out a range of factors by which a real risk may be determined. 'Harm' is defined broadly (beyond just financial harm) to include physical, psychological, emotional and reputational harm.

The proposed scheme reflects many of the considerations contained in the OAIC voluntary data breach notification guide and only mandates notification of data breaches that reach a threshold level of seriousness.

Until the scheme becomes law, the OAIC will continue to maintain that, in certain circumstances, notification of a data breach is nevertheless required as an incident of an organisation's current obligations under the Privacy Act – which means that organisations need to reflect this in their data breach response plans.

Do you think that mandatory data breach notification requirements should be introduced in Australia?



Conclusion and recommendations

Information and communications technology is increasingly the backbone of global economic growth. Billions of people across the globe rely heavily on ICT for work, communication, entertainment and almost every other facet of their everyday lives. So it is unsurprising, then, that cyber security is now of critical domestic and international concern.

Our survey results reflect that cyber attacks are occurring on a regular basis, across all organisations types, and in almost every industry; that cyber security is front of mind for many Australian organisations; and that for many (though not all) organisations, cyber resilience is considered a whole-of-enterprise challenge.

Our survey also found that many organisations perceive they have a satisfactory understanding of, and capability to prevent and deal with, cyber attacks. Unfortunately, this is not always reflected in the practical measures that organisations are adopting to mitigate cyber risk and increase their cyber resilience.

In particular, many organisations are not adopting adequate data segmentation practices; consider cyber security to be an issue for the IT department or best left to their outsourced service providers; do not have a data breach response plan in place; do not regularly provide cyber security training to their employees and contractors; have not adequately considered or addressed supply chain risk; and have not adequately turned their mind to their insurance arrangements.

And this is despite the wide range of liabilities that organisations may be exposed to as a consequence of a cyber attack – including severe reputational damage to the organisation, large civil penalties, personal liability for directors and proposed laws for mandatory notification of serious data breaches back on the Federal Government's legislative agenda.

Key areas of focus for organisations over the next 12 months should include at least the following:

- organisations that are subject to specific regulatory regimes should ensure they are fully compliant in relation to the protection of data held by them or their third party service providers
- organisations should assess their current cyber resilience against published frameworks and the Australian Government Information Security Manual
- individuals tasked with developing and monitoring the health of an organisation's cyber security policies and systems should ensure they are clearly aware of what is expected of them and are fully informed of potential vulnerabilities or attacks
- every organisation should ensure that it has a data breach response plan which clearly sets out a framework for identifying, notifying and managing serious data security breaches, as well as business continuity and disaster recovery plans, all of which should be tested regularly to ensure their effectiveness
- organisations should train all staff in cyber security measures, and give individuals an opportunity to report areas of potential cyber vulnerability
- organisations should take prompt steps to assess and mitigate supply chain risk, including:
  - identifying and evaluating cyber risk throughout their supply chain to ensure suppliers, or the systems through which they engage the organisation, do not present unacceptable cyber risks
  - conducting thorough due diligence on new suppliers and key customers (including their cyber security training and screening processes and their general competence to manage and mitigate cyber risk); and
  - incorporating appropriate provisions in contracts (including provisions relating to data ownership and access, privacy and data protection, compliance with specified security standards and disengagement)
- organisations should consider sharing information on cyber security with peers outside their organisation to discuss strategies and enhance preparedness for potential future attacks, and
- organisations should review their insurance arrangements and determine the suitability of cyber insurance (having regard to their risk profile).

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

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

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

Endnotes

[1] Ponemon Institute, 2015 Cost of Data Breach Study: Global (May 2015), available at http://ibm.co/1FStqBu (Ponemon Data Breach Study 2015)

[2] OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, available at http://bit.ly/1RjGk3o, at 4

[3] Department of Defence, 2015 Australian Government Information Security Manual: Executive Companion, available at http://bit.ly/1L2e1ks

[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] World Economic Forum, Global Risks 2015 (10th Edition), available at http://bit.ly/15wPuqV

[9] See, for example, Australian Prudential Regulatory Authority Prudential Standard CPS 231 (Outsourcing), available at http://bit.ly/1XVPI10

[10] Ponemon Data Breach Study 2015, above note 1 at 13

[11] The Australian Securities & Investments Commission's Cyber resilience: Health check (March 2015), available at http://bit.ly/1HyFGJC, provides a useful set of prompts for organisations to conduct a cyber resilience assessment

[12] Objective frameworks for assessing organisational cyber resilience include the US Government's NIST Cybersecurity Framework, available at http://1.usa.gov/1eQYolG; the Australian Department of Defence's Strategies to Mitigate Targeted Cyber Intrusions, available at http://bit.ly/1Owrnxd, and the UK Government's Cyber Essentials Scheme Available, at http://bit.ly/1HA0joM

[13] See Department of Defence, Strategies to Mitigate Targeted Cyber Intrusions, available at http://bit.ly/1Owrnxd

[14] Ibid

[15] Office of the Australian Information Commissioner, Guide to developing a data breach response plan (consultation draft) (October 2015) at 1-2, available at http://bit.ly/1Qkz0Gk

[16] The OAIC considers that organisations not governed by the Privacy Act should nevertheless have a data breach response plan as an incident of good privacy practice: ibid at 1

[17] For a high level guide to developing a data breach response plan, see Office of the Australian Information Commissioner, Guide to developing a data breach response plan (consultation draft) (October 2015), available at http://bit.ly/1Qkz0Gk. The OAIC's has, as an example, posted its own data breach response plan to its website: http://bit.ly/1RDQk7G

[18] CERT-UK, Cyber-security risks in the supply chain (2015), available at http://bit.ly/1BAGZI2

[19] Ibid

[20] Office of the Australian Information Commissioner, Annual Report 2014-5, available at http://bit.ly/1ki6vgt

[21] Privacy consultant Nigel Waters estimates that 'thousands' of breaches go unreported each year in Australia: Sydney Morning Herald, 27 July 2011 (available at http://bit.ly/1SB7dRh), cited in Office of the Australian Information Commissioner, Discussion Paper: Australian Privacy Breach Notification (November 2012), available at http://bit.ly/1S8BENJ

[22] 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

[23] http://www.ag.gov.au/Consultations/Pages/serious-data-breach-notification.aspx