
PLAN
PROTECT
FORTIFY
Perspectives on
Cyber Risk 2021
MinterEllison.

Contents

Paul Kallenbach
Partner
Competition, Risk & Regulatory

> "...more data than ever is being **collected, processed, stored and disseminated** – by local and global suppliers, individuals, employers and government..."

The State of **Cyber Risk in 2021** ›

Welcome to our 6th annual *Perspectives on Cyber Risk* report.

The events of 2020 transformed the way we live and work, including accelerating our use and reliance on information and communications technology.

The COVID-19 pandemic caused much of the world to substitute physical interaction for online – in work, education, commerce and leisure.

This has meant that more data than ever is being collected, processed, stored and disseminated – by local and global suppliers, individuals, employers and government – across all sectors of the Australian and global economy.

This increased reliance on ICT and the flow of data has inevitably brought with it heightened cyber security risks and challenges, including significant data breaches.

This year we combine our research findings with interview insights from Australian General Counsel, Heads of Risk, Data Protection/Privacy Officers and C-suite executives across the health, financial services, energy, education, infrastructure and government sectors.

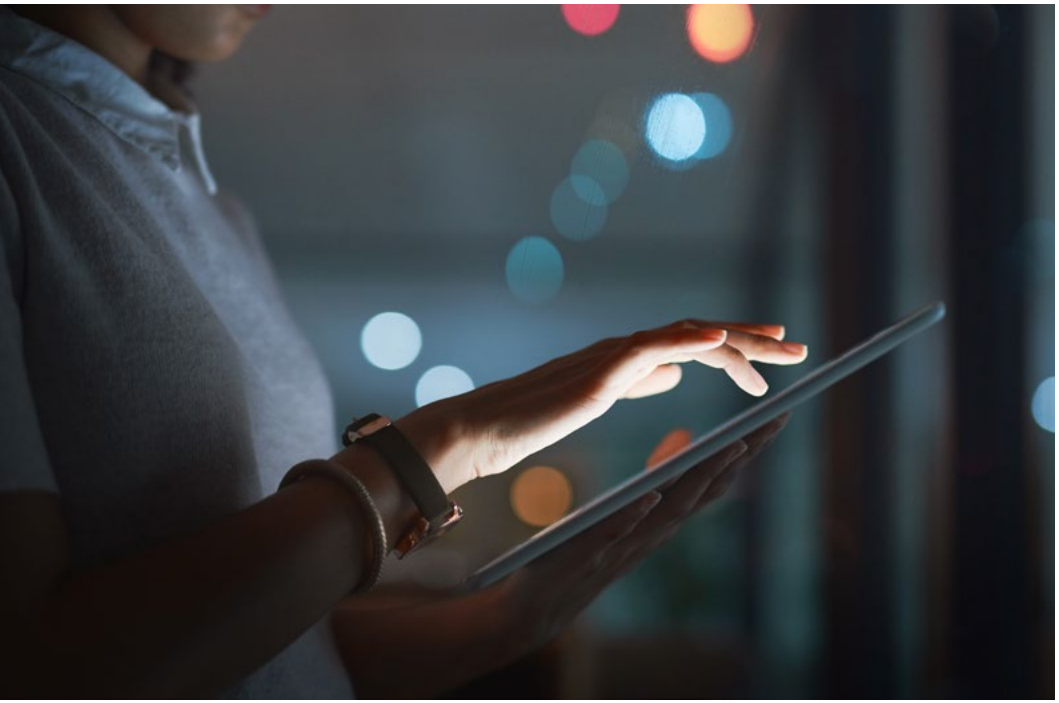
We also share an interview with the Australian Information Commissioner about Australian privacy regulation now and in the future.

The report explores recent developments in Australia's cyber risk landscape and provides insights from industry leaders on how businesses are managing cyber risk.

We highlight areas of risk and focus that are common to businesses across all industry sectors. And we recommend six measures that organisations should adopt as part of their cyber risk regime.

Key takeaways

It's not surprising that new cyber security challenges arising from COVID-19 featured significantly in responses to our cyber risk survey this year and in our interviews with technology executives. With many organisations having transitioned rapidly to a work-from-home environment, in-house IT resources remain stretched. They faced the challenge of facilitating remote access connectivity and secure desktop endpoints for entire workforces – almost overnight.



Key takeaways

Our industry survey found the following four key takeaways:

Testing of data breach response plans growing

More organisations are testing their data breach response plans than ever before (but it's still not enough). An untested data breach response plan may not be effective when dealing with a data breach. Pleasingly this year, 55% of survey respondents indicated that their data breach response plans were being tested at least annually.

Low adoption of external cyber frameworks

The rate of adoption of external cyber frameworks remains low. External frameworks, such as the Australian Signals Directorate's Essential Eight, provide valuable guidance on best practice for managing cyber risk. However, less than 50% of organisations have taken steps to assess their cyber security maturity against such a framework.

People remain prime targets

Despite the high-tech nature of some cyber attacks, people remain the prime targets of attacks, and hence a critical focus of ongoing investment. Again in 2020, both our survey and the Australian Privacy Commissioner's notifiable data breach reports found that human error and phishing emails are by far the most common cyber incidents impacting organisations in Australia.

COVID-19 created security challenges

Almost 40% of survey respondents faced increased cyber security risks due to the shift to remote working. Others found that COVID-19 exposed latent or underappreciated security issues.

Areas of focus

As well as our survey, we dove deeper into interviews with technology leaders across a range of industries. Based on our survey results and our discussions with these leaders we reveal the following areas of focus for organisations in 2021 and beyond:

Focus on the supply chain

Organisations should develop a thorough understanding of their supply chain, including their key vendors' IT security and operational postures – to mitigate against the introduction of weak links, and, for APRA-regulated organisations, in order to discharge their obligations under APRA's Prudential Standards.

Build for resilience

COVID-19 has exposed the critical importance of resilience in the procurement and operation of crucial ICT systems in helping to mitigate against events that may be outside of an organisation's control.

Keep up the training

Most cyber incidents still result from human error. A regular program of security training and awareness is critical to addressing this.

Don't go it alone

Organisations should consider joining an industry group or forum to share intelligence regarding cyber risk and evolving cyber threats.

Recommended measures

We recommend six measures that organisations should adopt as part of their cyber risk planning and governance:

1 ›

Test data breach response plans at least annually

2 ›

Assess the organisation's cyber security maturity against an external risk framework

3 ›

Fully understand the risks posed by the organisations supply chain (including operational and security risks)

4 ›

In procuring key IT systems, ensure that those systems provide adequate resilience to support remote working and to assist in addressing circumstances beyond the organisation's control

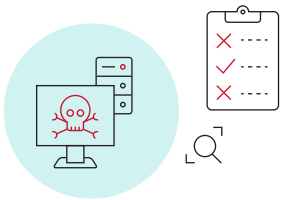
5 ›

Undertake regular and effective staff training on cyber security

6 ›

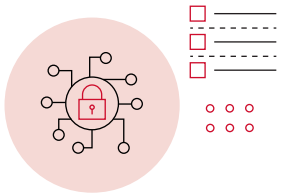
Join an industry forum to share cyber risk intelligence

At a glance



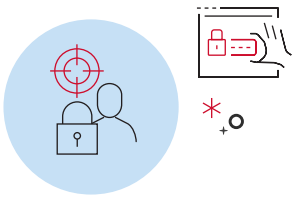
More organisations are

testing their data response plans



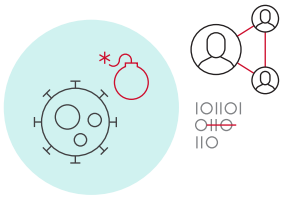
Low rate of adoption of

external cyber frameworks



People

remain the prime target of cyber attacks



COVID

exposed previous security issues

<50%

of respondent organisations assess their cyber security maturity against an external framework

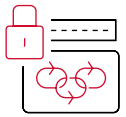
55%

of respondents say their data response plans are tested annually

40%

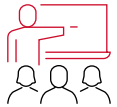
of respondents say their cyber security risks increased due to work from home

Areas of focus



Supply chain

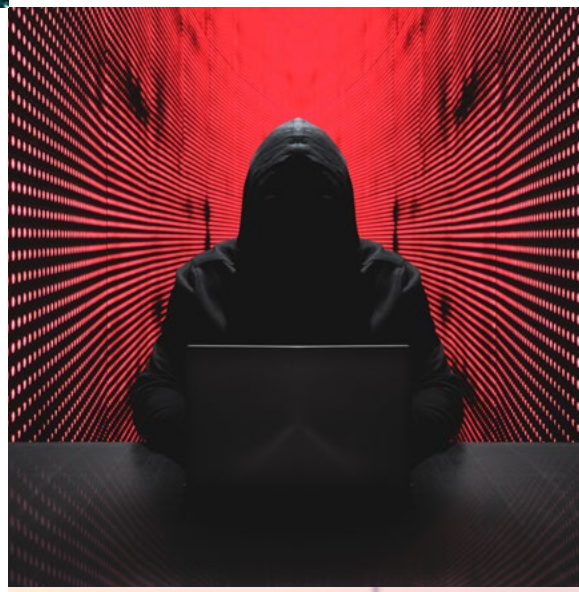
Build resilience



Regular training program

Join an industry group. Share intel.

Recent developments



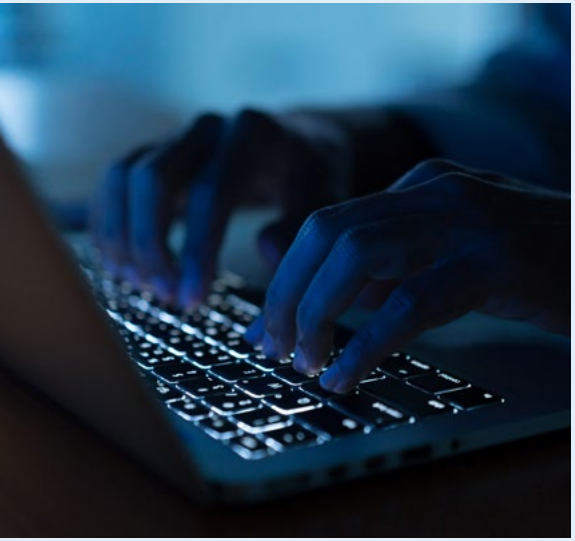
Data breaches continue to impact Australian business

While many of Australia's data breach incidents during the last 12 months were, as in previous years, attributable to human error, many significant incidents were suspected to be the work of nation-states or organised criminal groups. These include:

- The malicious software attack on **Accellion's** legacy file transfer appliance in December 2020 and January 2021. This resulted in breaches of the Reserve Bank of New Zealand, Allens Linklaters, the Australian Securities and Investments Commission (ASIC), and Washington's State Auditor office.
- Breach affecting the **European Medicines Agency** in December 2020, where information was accessed regarding the Pfizer COVID-19 vaccine. The incident raised concerns that documents relating to vaccines and their development could be used for espionage, financial or other attacks.
- The exploitation of Orion's **SolarWinds** products in March 2020, which prompted a US National Security Council Meeting at the White House. Among SolarWinds' 300,000 customers are 425 of the US Fortune 500 companies, all branches of the US military, and a number of the world's telecommunications giants, including Cisco and FireEye.
- A sophisticated ransomware attack on **Channel Nine's** IT systems in March 2021 prevented the broadcaster from airing programs from its Sydney broadcasting facility. The attack disrupted programs over several hours and was described by the network as the largest attack on a media company in the country's history. Support has been sought from the Australian Signals Directorate and the Australian Cyber Security Centre to determine the source of the attack.
- More recently, in May of this year, a cyber criminal group called 'Darkside' forced a six day shutdown of the **Colonial Pipeline**, after successfully deploying ransomware to the company's corporate network. Colonial Pipeline is the largest refined oil pipeline in the US, and carries 45% of the east coast's fuel supply. Concerned that the attack might spread to its operational control systems, Colonial Pipeline initiated a shutdown of fuel pumping operations. Panic-buying ensued, with fuel prices spiking in some areas. On 10 May, President Biden declared a temporary state of emergency. The company subsequently disclosed that it had paid US$4.4 million in ransomware payments to restore affected systems.

Regulatory developments

Australia's privacy laws have undergone incremental change over the past 12 months – most notably, to enact additional privacy safeguards concerning Australia's COVIDSafe app.[i] However, significant changes to Australia's privacy landscape are looming.



ACCC

In the wake of the ACCC's Digital Platforms Inquiry Final Report of July 2019, which examined, among other things, the privacy impact of online search engines and social media and digital content aggregators, the Commonwealth Government's overall review of the Privacy Act has progressed.

In October 2020, the Commonwealth Attorney-General's Department released its Privacy Act Review Issues Paper. Key focuses of that paper included the:

- right of individuals to enforce privacy obligations;
- scope, application and effectiveness of the current regime and enforcement powers; and
- impact and efficacy of the notifiable data breach regime.

The Privacy Act Review

Reflecting on the review, the Australian Information Commissioner and Privacy Commissioner (**Australian Privacy Commissioner**) had this to say to us:

The Privacy Act review is an opportunity for Australia to strengthen its privacy framework for the digital age to ensure fair information handling, prevent harm, protect fundamental human rights and build public trust. Central to that theme of trust, one of the key features of our submission to the review is a greater emphasis on the rights of individuals and the obligations of entities to protect those rights, to ensure the public interest is served by privacy law into the next decade.

Consumer Data Right

Following the commencement of the Consumer Data Right (CDR) in the banking sector in July 2020, the Commonwealth Government released its Report of the *Inquiry into Future Directions for the CDR*. This recommended an expansion of the functionality of the CDR regime and its further integration into the data ecosystem of the digital economy.

The ACCC has also made several important amendments to the CDR rules. These amendments permit accredited intermediaries to collect data on behalf of third party data recipients where the consumer consents (with effect from 2 October 2020), and expand the types of consumers who may use the CDR (with effect from 1 November 2021).

Trends in regulatory enforcement

ASIC has identified 'deterrence-based enforcement action' as one of its critical cyber supervisory projects for 2021.

Cyber resilience

In 2020, ASIC took its first cyber-related enforcement action against RI Advice Group, an Australian financial services licensee (AFSL), alleging various breaches of section 912A (the general licensee obligation provisions) of the *Corporations Act 2001* (Cth) (**Corporations Act**). They alleged the company failed to implement adequate policies and systems and ensure sufficient resources were deployed to manage cyber risk across its authorised representative group.

The action followed various cyber breaches in the company's authorised representative networks. This included a successful 'brute force' attack by an intruder, following which the intruder was logged into a server containing sensitive client information, including identification documents, for over 155 hours.

ASIC has indicated that this action won't be the last.

Consequently, we expect to see a heightened degree of focus on cyber security and resilience policies, governance and documentation developed by AFSL holders, including those with an authorised representative network.

Further, directors and other officers of all corporations must be conscious of the potential for different areas of legal exposure arising from a cyber security incident.

Areas of legal exposure include:

Personal liability

Personal liability for directors for breach of their obligations under section 180 of the Corporations Act to exercise their powers and discharge their duties with reasonable care and diligence, in how they supervise the building of cyber security and resilience and the implementation of defences to what are, today, clearly foreseeable risks. These risks are compounded for accountable persons under the Banking Executive Accountability Regime (BEAR) and under the proposed broader remit of the Financial Accountability Regime (FAR).

Capital raising

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.

Claims against directors

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).

ASX rules

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.

Misleading and deceptive conduct

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).

Contract claims

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.

APRA standards

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 conversation with Angelene Falk

Australian Information Commissioner and Privacy Commissioner

In early 2021, we spoke with the Australian Privacy Commissioner about the impacts of COVID-19 on privacy and upcoming changes to the Australian privacy landscape. This is what she had to say.

Q What were the key impacts of COVID-19 on the Australian privacy framework in 2020? Do you expect these impacts to continue after the pandemic ends?

The COVID-19 pandemic has focused even more attention on the right to privacy, given the heightened need to use personal information to achieve public health and economic outcomes.

The OAIC has played a significant role in supporting public trust and confidence in the use of personal information for initiatives to prevent and manage COVID, such as contact tracing.

The introduction of the COVIDSafe app was one of the most tangible examples of the intersection of COVID-19 and privacy. It was significant that changes were made to the *Privacy Act 1988* that enshrined strict privacy safeguards for COVIDSafe app data in law. These protections were informed by a detailed Privacy Impact Assessment that was released publicly, which sets an important benchmark for similar projects.

The OAIC has an expanded regulatory role and powers in relation to the COVIDSafe app, which extends to the handling of app data by state and territory health authorities. Any unauthorised collection, use or disclosure of COVIDSafe app data is not only a criminal offence, but also triggers my regulatory powers.

We convened a National COVID-19 Privacy Team to bring privacy regulators together to respond to proposals with national implications. For example, we published draft guidelines for state and territory health authorities that aim to harmonise contact tracing orders across state borders.

Internationally, data protection authorities have also collaborated and responded with practical strategies to enable the use and protection of personal information as a key tool in the pandemic response.

The introduction of QR codes to supplement contact tracing efforts and the national vaccination scheme are other examples of how COVID-19 has increased the focus on privacy.

We've produced a range of privacy guidance and advice for businesses, Australian Government agencies and individuals – most recently, guidance for employers on understanding their privacy obligations to staff around COVID-19 vaccinations.

Now the COVID-19 national vaccine rollout is underway, we need to continue to work to ensure personal information is handled consistently and that the privacy of the community is protected. Protecting personal information is central to maintaining public trust and promoting compliance with health orders and contact tracing processes.

We are actively monitoring regulated entities' handling of personal information and will pursue regulatory activities where personal information is at risk.

Ultimately, COVID has highlighted the importance of maintaining public trust and confidence in the handling of personal information. Post pandemic, we expect more organisations will embrace privacy by design, as this is increasingly what the community looks for in products and services.

A conversation with Angelene Falk
Australian Information Commissioner and Privacy Commissioner

Q What do you see are the greatest challenges to promoting and upholding privacy in Australia at the present time?

The privacy landscape has changed significantly since the introduction of the Privacy Act more than three decades ago. Most aspects of the daily lives of Australians have been transformed by innovations in technology and service delivery. This has resulted in a dramatic increase in the amount of data and personal information collected, used and shared – data transfers that no longer stop at national borders. Alongside this significant shift in data handling practices has come an increase in community expectations that their personal information will be protected wherever it flows.

Given the scale and scope of environmental change, the Attorney-General's Department's current review of the Privacy Act is necessary to ensure that our privacy framework is proportionate, sustainable and responsive to emerging privacy risks into the future.

Our Australian Community Attitudes to Privacy Survey 2020 found levels of trust in organisations' handling of personal information are continuing to decline. The community wants more to be done to protect their privacy in the face of new and emerging risks and more choice and control over their personal information.

"

The community wants more to be done to protect their privacy in the face of new and emerging risks and more choice and control over their personal information."

Our recommendations to the review are aimed at addressing this trust deficit. If the community trusts that their data will be protected, they will also have greater confidence in participating in the digital economy.

Greater clarity and common privacy expectations will allow businesses to innovate with confidence and to strengthen the relationship with their customers. And businesses, whether large or small, can build trust and confidence in their brands by developing a reputation for reliable, transparent and effective privacy management.

Legislative reform in the privacy and cyber security space is currently underway in Australia, including a review of the Privacy Act. The OAIC has previously stated (in its media release dated 14 December 2020) that "Australia needs a strong, fair and flexible privacy framework that prevents harm, protects fundamental human rights and builds public trust to support a successful economy."

Q What might an ideal future state of Australia's privacy framework look like?

Strong and effective data protection laws are essential to preventing online harms: they complete the Australian Government's ring of defence for Australians' data and our digital economy.

A stronger privacy framework is also good for business. It supports our COVID-19 response and our economic recovery by helping to increase consumer trust, providing businesses with the clarity to innovate with confidence and to strengthen the relationship with their customers.

It also supports innovation and growth in the Australian digital economy and international trade by connecting with privacy laws around the world – thus reducing regulatory friction for business – and ensuring that personal information is protected wherever it flows.

Importantly, a stronger privacy framework benefits and protects the community, so they can have greater confidence that their information will be handled securely, fairly and reasonably.

This all requires a regulator who can enforce the law in line with community expectations.

We have made a total of 70 recommendations to the review in line with these goals, including changes that would enhance individuals' choice and control over their personal information.

We want to see additional protections that create legal obligations aimed at achieving greater fairness and organisational accountability to address privacy risks and harms. Personal information handling practices should be required to be fair, as well as reasonable. Entities should also be required to demonstrate that they are building in privacy by design.

Q What will be the OAIC's regulatory approach to exercising its powers and functions during 2021?

Our 2020-21 Corporate Plan signals our ongoing commitment to advancing online privacy protections for Australians. The online realm features prominently in our four key areas for regulatory focus this year: online platforms, social media and high privacy impact technologies; security of personal information, particularly in the finance and health sectors; the implementation of the Consumer Data Right; and new personal information handling practices arising from COVID-19, including the COVIDSafe app.

The Privacy Act grants the Commissioner a range of privacy regulatory powers. These include powers that allow the OAIC to work with entities to facilitate legal compliance and best privacy practice, as well as investigative and enforcement powers to use in cases where a privacy breach has occurred.

We continue to use a range of strategies to identify compliance risks and significant or systemic issues, and we take a proportionate and evidence-based approach to taking regulatory and enforcement action to change practices.

As well as driving regulated entities to build in systems and processes to improve compliance and demonstrate accountability for handling personal information, our regulatory action is aimed at giving individuals greater choice and control over the handling of their personal information.

Decisions to undertake regulatory action are taken in line with our privacy regulatory action policy. Key factors that we take into consideration include the seriousness and level of public concern about the incident, the potential educational, deterrent or precedential value; any remedial action taken; and the likelihood of reoccurrence.

Many privacy threats and challenges extend beyond national boundaries. In dealing with an interference with privacy or potential privacy risk that operates across national boundaries, we work in partnership with privacy regulators in foreign jurisdictions to ensure our approach to regulatory action is consistent and harmonised. This can also include taking joint regulatory action into matters of common concern.

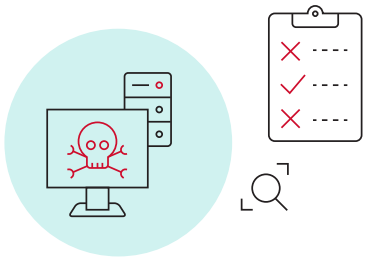
Industry insights

Insights from our sixth annual cyber security survey

In November 2020, we conducted our sixth annual cyber security survey to understand the level of awareness of and importance that organisations place on cyber risk.

FINDING 1 ›

More organisations are testing their data breach response plans than ever before (but it's still not enough)



Pleasingly, our survey has found a year-on-year increase since 2017 in the number of organisations that regularly test their cyber security and data incident response plans.

In 2020, **55%** of respondents stated that these plans were being tested at least annually, compared with only **34%** of organisations that undertook annual testing in 2017.

This increase is likely attributable to a corresponding increase in awareness regarding the frequency and potential consequences of cyber attacks and data breaches. The press attention following high profile data breaches has helped to raise awareness among both organisations and the general public.

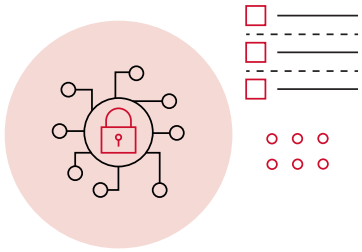
However, increased awareness is not the only factor contributing to organisations' more regular testing of their response plans. In our experience, some have commenced regular testing after contending with a serious cyber incident and discovering that their untested incident response plans were lacking.

Perhaps because of increased testing of incident response plans, we have also seen growth in the number of organisations implementing complementary tools to assist in the management of cyber incidents. This includes incident management playbooks – step-by-step guides to the activities to be undertaken in response to different kinds of cyber incidents.

Our survey results disclosed that **36%** of respondents had developed such complementary tools, an increase from **26%** in 2019.

However, results show that an increased level of preparedness is by no means universal. There remains a significant number of organisations that have no data breach response plan in place. **19%** of respondents told us that their organisations do not have a data breach response plan, or they were unsure whether this was the case.

While this is only a slight decrease from the **24%** of respondents who provided the same response in 2019, it is still a significant improvement on the **59%** of respondents who gave this response in 2016.



FINDING 2 ›

The rate of adoption of external cyber frameworks remains low

Less than **50%** of respondents to our survey stated that their organisation had taken steps to assess its cyber security maturity against an established framework. At the same time, many respondents considered that their organisations should be doing more to audit and review their cyber resilience practices.

External frameworks – such as the Australian Signals Directorate's (ASD's) Essential Eight, the National Institute of Standards and Technology's cyber security framework, and APRA's Prudential Standards (even for non-regulated entities) – can provide significant value to an organisation. These frameworks encourage a best practice approach to:

- **identifying** cyber risk – including identifying key information assets and organisational, supply chain and governance risks, and taking steps to mitigate those risks
- **protecting** against cyber incidents – including implementing technical and organisational controls, processes and procedures (including, critically, by conducting regular staff training on cyber risk and secure information handling practices)
- **detecting and responding** to cyber incidents – including continuous monitoring and detection, by implementing appropriate chains of escalation, and by data breach response planning, analysis and communications
- **recovering** from cyber incidents – including business continuity and disaster recovery planning, and implementing learnings from past incidents

Assessment against these frameworks:

- provides a clear picture of an organisation's cyber security maturity;
- may assist an organisation in targeting its improvement efforts; and
- is likely to increase a Board's confidence in the organisation's executive and security teams.

Such assessments should address the broad range of cyber security considerations, such as asset identification, application and access control, patch management, application hardening, authentication methods, governance and risk management, training and awareness, and post-incident review.

While our survey shows that more organisations than ever are implementing and regularly testing and revising their data breach response plans, adopting best practice external cyber security frameworks is not yet sufficiently widespread.

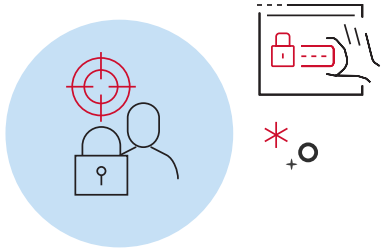
Assessment against an external framework is also a helpful part of an organisation's continuous improvement program, as it allows it to measure improvements in the organisation's cyber risk profile. IT security experts often recommend that security maturity assessments be conducted regularly (for example, annually or bi-annually) to ensure that the organisation's maturity level keeps pace with developments in the industry and evolving cyber risk practices.

Demonstrating alignment with an external framework may also help an organisation in discharging its regulatory obligations, as such frameworks provide an objective standard by which to determine compliance.

For example, implementing the ASD's Essential Eight may assist an organisation in demonstrating that it has discharged its obligation, under Australian Privacy Principle 11.2, to take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Finally, aligning with external frameworks may assist organisations to increase its level of trust with consumers. According to the Australian Privacy Commissioner:

Australian Community Attitudes to Privacy Survey 2020 found levels of trust in organisations' handling of personal information are continuing to decline. The community wants more to be done to protect their privacy in the face of new and emerging risks and more choice and control over their personal information.



FINDING 3 ›

Despite the high-tech nature of some cyber attacks, people remain the prime targets of attacks, and hence a critical focus of ongoing investment

Phishing emails, where malicious actors rely on targets to provide information in response to a fraudulent email, are a far cry from the elaborate hacking efforts depicted by Hollywood. However, these incidents remain the most commonly reported cyber incident.

In our 2020 survey, **70%** of reported incidents originated from phishing messages. A further **17%** of incidents involved invoice fraud, leaving only **13%** of incidents as more technical forms of attack (such as denial-of-service).

These results are consistent with the statistics released by the OAIC for the period July to December 2020, which showed that email-based phishing was the most commonly employed form of malicious attack.

Similarly, human error was the cause of a significant number of data breaches notified to the OAIC from July to December 2020. Compared with the previous reporting period, human error breaches increased in terms of the total number of notifications received (up **18%**) and proportionally (up from **34%** to **38%**).

Perhaps because of the frequency of phishing emails and other attacks seeking to exploit human frailties, the steps being taken by organisations to improve their cyber security are overwhelmingly focused on the human dimension. Our survey found that the majority of respondents who implemented additional security measures as a result of cyber incidents focused on delivering additional staff training or updating internal processes and procedures. Only a minority focused on effecting technical changes to their IT systems.

The Australian Privacy Commissioner had this to say about the privacy risks of human error:

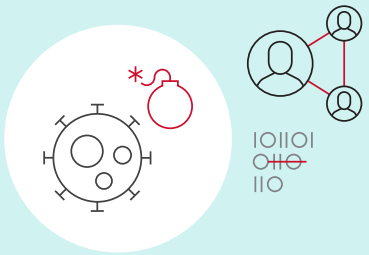
The human factor is also a dominant theme in many malicious and criminal attacks, which remain the leading source of breaches notified to the OAIC.

Organisations need to reduce the risk of experiencing a data breach by addressing human error, including promoting staff awareness about secure information handling practices.

For instance, staff should be educated about how to spot scams and phishing emails. Secure information handling practices should also be regularly reinforced, such as locking workstations and using the blind carbon copy function for emails with multiple external recipients.

This needs to be supplemented with technological solutions that assist staff – for example, multifactor authentication, email filtering and secure options for transmitting personal information.

Implementing the Australian Cyber Security Centre's Essential Eight as a minimum will make it much harder for adversaries to compromise business systems, and reduce the risk of human error breaches.



FINDING 4 ›

COVID-19 created security challenges

Unsurprisingly, a large number of respondents identified COVID-19 as having impacted their cyber security practices.

The Australian Privacy Commissioner told us:

The COVID-19 pandemic has focused even more attention on the right to privacy, given the heightened need to use personal information to achieve public health and economic outcomes.

Many of the impacts felt by organisations stemmed from changes to work patterns and procedures – particularly the significant rise in the number of employees working from home. **38%** of respondents identified that remote working created or increased cyber security risks by introducing potentially insecure platforms, and increasing the number of personal devices used by employees in a work context.

These changes required many organisations to upgrade their remote access systems, revise their internal processes, procedures and incident response plans, and provide additional training to their staff. And some organisations told us that, with the benefit of hindsight, COVID-19 served to expose security issues that were both latent and underappreciated.

Insights from conversations with technology industry leaders

To dig deeper into our survey findings, we consulted with IT executives across a range of industries between December 2020 and February 2021 to discuss the cyber risk issues facing their organisations and the approaches they are taking to manage them.

Q How did organisations' operations change in 2020, and how did those changes impact cyber security practices?

COVID-19 rapidly changed how many organisations operated day-to-day in Australia and around the world. From a cyber risk perspective, the biggest change was the substantial shift to remote working. This gave rise to a range of cyber risk issues and highlighted existing issues that may not have been fully understood or mitigated prior to COVID-19.

Set out below are the key messages we heard from CIOs reflecting on their cyber security experience in 2020.

Resilient systems

When operations are largely or entirely remote, the resilience of IT systems takes on greater importance. Where an on-site system becomes unavailable, organisations may have workarounds or manual processes available to enable work to continue. However, in a remote working context, many of these workarounds or manual processes may not be available or may be impracticable. As such, system downtime may have a much more severe operational and financial impact. In this context, some organisations we spoke to disclosed their renewed focus on procuring and implementing systems that improve their overall resilience.

Supply chains have never been more important

While many Australian organisations were able to move seamlessly (or almost seamlessly) to remote working, a number of CIOs we spoke to experienced issues across their supply chains. In particular, organisations using outsourced service providers in countries such as India or the Philippines experienced service disruption, as providers in those regions were not set up for remote work and did not have appropriate business continuity arrangements in place. Their experience highlights the need for organisations to understand the risk posed by their supply chain – not only in relation to IT security risk but also operational risk.

You can't control what you can't see

Some organisations found that remote working led to an increase in 'shadow IT', where employees use applications or platforms that are not part of the organisation's approved application set. This can give rise to security challenges, as such applications may not have been through standard security assessment and approval processes (and, in many cases, may not even be visible to the organisation). It may also give rise to legal risk, as the use of such 'shadow IT' may cause an organisation to contravene its regulatory requirements or breach contractual obligations that it owes to third parties.

There is strength in numbers

Many of the organisations we spoke to observed that in 2020, even more than in previous years, there was great value in participating in industry groups, such as the Victorian Government's Information Security Advisory Group and equivalent private sector groups. These groups bring together IT leaders to share cyber threat intelligence and security strategies.

Q What proportion of organisations' operations are in the cloud, and how does this affect an organisation's cyber risk profile and practices?

Our discussions with industry confirmed that organisations increasingly rely on cloud technology and data storage. Most organisations we spoke to have at least 50% of their current operations in the cloud.

This increased reliance on cloud-based systems poses several security challenges for organisations. In particular.

Transparency

In many cases, using cloud services means placing trust in a vendor's security controls but without full visibility. In our experience, many large scale cloud vendors will not disclose detailed security information to their customers, nor will they provide them with comprehensive audit rights. Instead, organisations are told that they must rely on the vendor's external certifications or audit reports (such as ISO certifications or SOC 2 reports) to satisfy themselves of the vendor's security arrangements.

Consistency

Achieving consistency of security levels and controls across an organisation's environment is made more difficult when operating in a hybrid cloud and on-premise environment, where the available security options for systems may differ.

Continuous change

Cloud services, of their nature, frequently change and evolve. While changes in security measures are generally aimed at improving the vendor's security posture, such changes create another barrier to customers maintaining an up-to-date understanding of security across their end-to-end platforms and environments.

How can customers of cloud-based services mitigate supply chain risk?

Based on our experience negotiating large-scale cloud service contracts, we recommend that customers consider the following two steps:

Step 1

Conduct thorough due diligence on the vendor (which should be refreshed at appropriate intervals), including:

- the classes and sensitivity of data that will be stored in the cloud.
- the security controls that will be applied by the vendor.
- where the data (including backups) will be held, including whether there is an option to store the data within Australian data centres.
- where the data will travel to or through.
- the vendor's business continuity and disaster recovery arrangements.

Step 2

Incorporate the following provisions in contracts:

- mandated compliance with specified security standards and requirements (including the flow-down of those requirements to key subcontractors), for example, ISO 27001.
- access to the vendor's certification details and external audit reports (such as SOC 2 reports).
- a commitment from the vendor that any changes to its security policies, or changes to how it delivers services during the subscription term, will not materially decrease the level of security that it provides.
- requiring the vendor to take full responsibility and liability for breaches of the contract (including security and privacy provisions) by its subcontractors.
- requiring the vendor to notify the customer should it suffer a data breach.
- allowing for prompt access to the organisation's data in the possession or control of the vendor.

Q What initiatives have organisations undertaken to enhance cyber resilience?

For the IT executives we spoke to, initiatives to enhance cyber resilience were broadly divided into three categories:

1. people and culture
2. assurance and governance processes
3. systems and infrastructure.

However, people and culture initiatives were overwhelmingly the focus of organisations in improving their cyber resilience. Most notably, staff communication and training.

The executives we spoke to also observed that staff communication and training could not be a one-off, nor is there a one-size-fits-all approach to training within the organisation. For example, an organisation may focus training on particular groups, such as finance personnel who are more likely to be the targets of payment redirection scams, or new hires who may have had less cyber security training than others in the organisation.

Processes to deal with cyber incidents are also crucial, according to the executives we spoke with. Organisations generally acknowledged that they would never be able to prevent all potential cyber incidents. Rather, incident detection and organisational response effectiveness will be key to mitigating economic and reputational damage and reducing legal risk. As one CIO said, *"You are going to get attacked. It just depends on how much damage is done and when you find out."*

> **"**
>
> **You are going to get attacked.** It just depends on how much damage is done and when you find out."

Q What are the next areas of focus?

Some interviewees considered that, with significant improvements to internal security practices having been made over recent years, the next frontier for their cyber risk management activities is even greater oversight of supply chain risk.

While detailed IT security audits of suppliers and their subcontractors are common in some industries (such as in financial services), our interviewees consider supply chain risk to be often overlooked. Many told us that a greater focus on supply chain risk, including developing a formalised IT security review process, will be a crucial aspect of their cyber resilience activities in 2021.

This leaves the third of the categories referred to above – systems and infrastructure.

Many of our interviewees considered this low-hanging fruit to have already been picked, and that substantial further investment in security applications and infrastructure is likely to give rise to diminishing returns.

Instead, their focus is moving from security architecture to secure architecture. This includes:

- changes to network architecture (ie, zero trust vs permitter)
- user-centred security (including end-user authentication strategies that reduce the ability of users to engage in risky behaviour)
- improved development lifecycle processes.

And while these focus areas are technical in nature, our interviewees recognised that their successful implementation would require cultural change – so often the more difficult to achieve.

Industry in focus:

- **Financial Services**
- Health
- Higher Education
- Infrastructure

Industry in focus: Financial Services

The Australian financial system consists of an estimated 17,000 interconnected financial entities, markets and platforms that provide products and services to consumers.[ii] In recent years, entities operating in the financial services sector have faced increased pressure to innovate and, in many cases, have taken significant strides in modernising their technology and streamlining their business operations.

However, the complex IT systems required to deliver financial services, coupled with the significant volume of personal information collected, used, disclosed and stored by financial service institutions (FSIs), mean that the sector faces consistent and serious cyber threats.

Data breaches

According to the OAIC's Notifiable Data Breaches Report for July to December 2020, the finance sector reported the second highest number of data breaches (behind the health sector). Importantly, the report disclosed that while human error was the most common source of data breaches across Australia, malicious or criminal attacks were the most common source of data breaches in the finance sector, accounting for 66% of reported breaches. The finance sector also reported the highest number of data breaches resulting from system faults.

Cyber attacks

The number of attempted cyber attacks on FSIs significantly exceeds the number of data breaches reported by the OAIC. ANZ's institutional banking boss, Mark Whelan, has stated that during the COVID-19 pandemic, the number of cyber attacks on the bank escalated to the point where it is receiving 8 to 10 million attacks a month.[iii] Mr Whelan went on to describe cyber attacks as 'the biggest single issue ... or threat if you like, in banking today'.[iv]

Regulators

In response to the cyber threats faced by the sector, regulators including the Australian Prudential Regulation Authority (APRA) have introduced standards and guidelines aimed at ensuring that FSIs implement appropriate security measures to protect consumers' privacy as well as safeguarding the stability of the sector (and, by extension, the economy).

"

...malicious or criminal attacks were the most common source of data breaches in the finance sector, accounting for 66% of reported breaches."

Cyber risks in financial services

In November 2020, former Executive APRA Board Member Geoff Summerhayes observed that although no APRA-regulated bank, insurer or superannuation fund has yet suffered a material cyber breach, it was 'only a matter of time until a major incident occurs'.[v] A number of factors contribute to the grievous cyber threat landscape faced by FSIs.

Growing 'attack surface'

Operating an FSI requires the use of a large number of complex systems and third party services. As FSIs continue to modernise their systems and integrate third party services into their IT and customer environments, the size of 'attack surface' available to be exploited by malicious actors increases[vi] – each integration between systems creates potential new security vulnerabilities. For example, the integration of Internet of Things devices into FSI processes and workflows (such as payment applications for smart watches) may increase the number of endpoints that can be used to access FSI systems.

Cloud adoption

Use of public cloud services is becoming increasingly common in FSIs due to the cost and resource efficiency of solutions – transitioning to public cloud can improve efficiency by 30 to 40 percent compared to traditional hosting for some workloads.[vii] This reflects a significant shift from the traditional FSI approach of using segregated, on-premise systems.

The use of public cloud services by APRA-regulated entities in a material outsourcing context may also raise regulatory issues. While APRA acknowledges the increasing usage of cloud services by FSIs and has issued specific guidance in relation to their use of cloud services,[viii] there remains a tension between the APRA standards and the realities of cloud adoption. For example, Prudential Standard CPS 231 requires that APRA-regulated FSIs must ensure that APRA has certain audit rights in connection with a material outsourcing arrangement. However, in a public cloud context, where hosting environments are shared across many customers, and data storage and support may be provided from locations across the globe, audit rights may be difficult to achieve in contract negotiations and potentially problematic to exercise in practice.

Data stores

FSIs hold a significant volume of customer data. Like health service providers, FSIs hold classes of data that are of inherent value to malicious actors, such as accounts details and identity verification data. In the hands of a cyber criminal, this information can be used to perpetrate identity or financial fraud – making FSIs prime targets for frequent and aggressive cyber attacks. According to National Australia Bank CEO, Ross McEwan, NAB blocked over 41,000 attempts at exfiltrating data in the first quarter of 2020 – he described the attacks as 'ferocious attacks on us as an institution, just as they will be on any other firm, I suspect, that holds customer data for payments'.[ix]

Targeted sector regulation APRA CPS 234

The SolarWinds and Accellion breaches (described on page 6 of this report) both exemplify the way in which a cyber breach can have a cascading effect through broader systems. In recognition of the growing and systemic nature of cyber threats to the financial services sector, APRA issued Prudential Standard CPS 234 (CPS 234), which came into effect in July 2019. The purpose of CPS 234 is to ensure that APRA-regulated entities develop and maintain information security protections that are appropriate given the importance of the data they hold and the seriousness of the threats that they face.

CPS 234 applies to all 'APRA regulated entities', which includes authorised deposit taking institutions (ie, banks), general insurers, life insurance companies, private health insurers and registrable superannuation entity licensees, as well as any third parties that manage these entities' information assets.

Under CPS 234, an APRA-regulated entity must:

- clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals
- maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity
- implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls
- notify APRA of material information security incidents
- review the effectiveness and the design of all information security controls as part of its internal audit activities (encapsulating any controls held by third parties or related parties).

In November 2020, APRA announced that, commencing in 2021, it would be requesting one-off tripartite independent cyber security reviews across all of its regulated industries. As part of this initiative, APRA will be asking the Boards of certain regulated entities to engage an external audit firm to conduct a thorough review of their compliance with CPS 234 and report back to both APRA and the Board.[x]

> "The purpose of CPS 234 is to ensure that APRA-regulated entities develop and maintain information security protections that are appropriate given the **importance of the data they hold and the seriousness of the threats that they face."**

What FSIs should be doing to mitigate cyber risk

Testing and verification

FSIs should regularly test and verify their internal security measures, as well as monitor external sources for information about newly discovered security vulnerabilities.

Review of security practices

FSIs should exercise care and prudence before integrating their systems with those of third parties. This should entail detailed security due diligence on third party systems, including a review of the third party's security practices and certifications, and penetration testing of their systems.

Supply chain protection

FSIs should take steps to ensure that their supply chains do not expose them to systemic vulnerabilities. FSIs should not only conduct security due diligence on their material suppliers, but should also ensure that appropriate contractual protections are in place, including:

- clear provisions regarding data ownership and an unconditional right for the FSI to access its data at any time
- an obligation to only access or store data in approved countries
- requirements for data to be encrypted in transit and at rest
- requirements for suppliers to meet specified security standards and hold any applicable certifications (for example, ISO 27001 certification or PCIDSS certification)
- the right to conduct security audits and provide SOC 2 audit reports if available
- requirements that supplier personnel receive regular and adequate security training (for example, developers should be receive training in relation to secure coding and OWASP top ten vulnerabilities)
- notification and investigation processes to be followed in the event of a data breach or suspected data breach.

As far as possible, these requirements should also be passed through to suppliers' subcontractors.

IoT preparedness

FSIs should maintain adequate security baselines, implement effective perimeter defences, and be cognisant of consumer privacy requirements, when balancing safety and customer convenience through the implementation of mobile technologies.

Mitigation tools

While in some cases rapidly advancing technologies may increase cyber risk, modern technologies can also be employed to strengthen cyber defences. FSIs should consider the use of data analytics and other tools to mitigate against cyber and other risks to their organisations.

Industry in focus:

Financial Services

› **Health**

Higher Education

Infrastructure

Industry in focus: Health

The health sector has increasingly embraced digital solutions to improve patient care and maximise operational efficiencies. The last few years have seen the widespread adoption of Electronic Medical Records, the Internet of Medical Things, and wearable devices.

> **...the significant amount of new information being collected, stored and shared** has amplified the need for robust privacy protections to meet cyber security risks.

Digital solutions

This activity was significantly accelerated during the COVID-19 pandemic, with a substantial increase in the use of telehealth and remote health care technologies.

Data collection

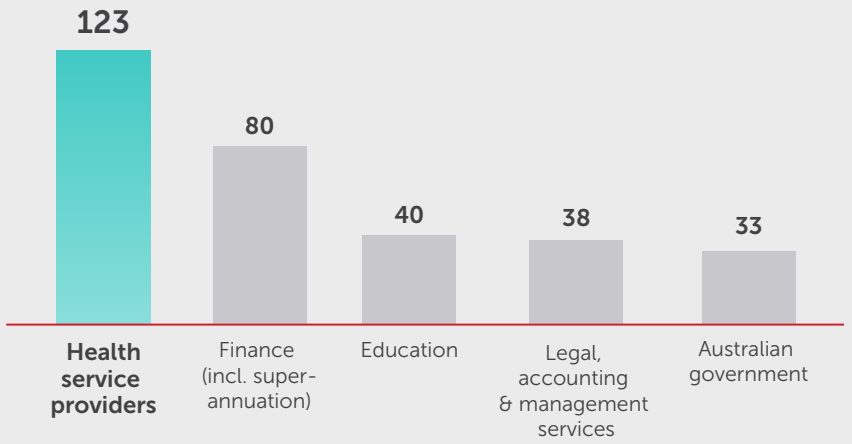
The move to collecting data digitally rather than in paper records has supported the development of artificial intelligence (eg radiology diagnoses and embryo selection) and modelling for service planning and preventative health (eg predicting risk of future hospitalisations). These technologies will continue to be incorporated into practice with the promise of improved patient, population and commercial outcomes.

However, the significant amount of new information being collected, stored and shared has amplified the need for robust privacy protections to meet cyber security risks.

Reporting of breaches in the sector

On statistics alone, the health sector is more exposed to cyber incidents than any other sector. In the OAIC's latest report, 23% of data breaches occurred in the health sector – placing it at the top of the list of affected sectors.[xi]

Number of data breaches reported across top five industries July – December 2020



Source: OAIC Report for July – December 2020.

The high number of reported data breaches may reflect that:

- the compromise of health information is more likely to cause serious harm to an individual (and therefore be reportable under the notifiable data breach scheme)
- all private providers of health services fall within the requirements of the Privacy Act (given that the small business exemption does not apply to health service providers holding health information)
- there is a high level of privacy breach reporting compliance within a sector that operates within a framework of medical ethics (including patient confidentiality).

It may also be, however, that malicious actors are disproportionately targeting health providers. Cybercriminals may be particularly interested in the trove of personal information that may not be readily available from other sources.

The Australian Cyber Security Centre

The Australian Cyber Security Centre (ACSC) has reported that the health sector is most often targeted by ransomware attacks – accounting for 20% of all such attacks in Australia.[xii] The ACSC considers the Australian health sector to be particularly vulnerable to such attacks, including due to outdated infrastructure, the pressure of budgetary constraints, and the proliferation of internet-connected devices.

Indeed, similar warnings in relation to the United States' healthcare system were issued in October 2020 by the Federal Bureau of Investigation – citing research showing that ransomware attacks against US hospitals rose by 71% between September and October 2020.[xiii]

Consequences of data breach in the health sector

Health information is very valuable to cybercriminals because, unlike passwords or credit card details, health information cannot be changed once it has been exposed.

The nature of the industry also makes healthcare providers a particularly unfortunate target for ransomware attacks. In late 2019, computer networks in at least seven major Victorian regional hospitals were locked down due to a ransomware attack that targeted booking and health records systems, and resulted in surgery and treatment delays.

The consequences were not as dire as they could have been when a 2020 ransomware attack closed an emergency room in Dusseldorf, Germany. Patients were rerouted to other hospitals, leading to the death of a woman whose aneurysm was not treated in time.

Even where physical patient harm is avoided, privacy breaches in health care can cause a loss of trust in the therapeutic relationship, reputational harm to the organisation and clinicians, and anxiety for patients.

Legislative and regulatory changes

Privacy Act review

On 12 December 2019, the Australian Government announced that it would review the Privacy Act to ensure that it empowers consumers, protects their data and positively services the Australian economy. The Review has identified a number of issues that go to the heart of the current privacy regime in Australia. Several of these directly impact the healthcare industry, including:

- the scope of 'personal information' is under review
- Permitted Health Situations could be expanded or restricted
- new legal claims for breaches of privacy.

SOCI Act

The *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act) provides that certain 'critical infrastructure assets' must be included on a national register for reasons related to national security. Currently, only the electricity, gas, water and maritime ports sectors are affected.

However, the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (Cth) (SOCI Bill) will, if passed, expand the ambit of the SOCI Act, including to the 'health and medical' sector. It will require controllers of health and medical critical infrastructure assets (such as hospitals) to register those assets and comply with certain security obligations. They will also be able to access government assistance in an incident which would have a serious impact on national security or the country's social or economic stability.

Regulatory changes targeted at software-based medical devices, including software that can be classified as a medical device in its own right (SaMD), took effect on 25 February 2021. The changes mean that software that is subject to the regulatory regime administered by the Therapeutic Goods Administration will be classified according to the intended purpose of the software and the relevant level of risk (particularly where the software malfunctions or provides incorrect information to the user). The higher the level of risk, the higher the classification and, therefore, the more stringent the applicable regulatory requirements.

What should health service providers do?

Key steps that health service providers can take to mitigate the risk of a cyber attack (including ransomware attacks) include:

1. building security awareness of employees through the Commonwealth Government's Digital Health Security Awareness eLearning course

2. installing antivirus protection on all endpoint devices

3. requiring user authentication, including implementing strong passwords and multi-factor authentication

4. ensuring that systems are regularly patched to prevent malicious actors from exploiting known security vulnerabilities

5. identifying and backing up critical information and systems to allow for faster recovery of data after an attack

6. restricting user rights to ensure only necessary individuals have access to particular servers, systems or datasets

7. where a health service provider operates in a public space (such as a hospital), partitioning the provider's networks

8. conducting privacy impact assessments for new projects or processes involving patient information

These are, of course, only a subset of best practices that organisations should adopt in embedding and improving their cyber resilience – as discussed on page 4.

Industry in focus:

Financial Services
Health
› Higher Education
Infrastructure

Industry in focus: Higher Education

Following evidence of growing foreign interference and cyber security threats in the university sector, the Commonwealth Government has introduced significant legislative reforms requiring proactive uplifts to existing university compliance frameworks. These changes have particularly impacted the cyber security and due diligence elements of these frameworks.

This section reviews the new obligations on universities, and the growing threat of foreign interference that has led to these changes.

A growing concern: from foreign influence to foreign interference

Commencing in 2018, the Commonwealth Government has taken significant action to counter the growing threat of foreign interference in Australia. A major catalyst for these actions was the 2018 Australian Security Intelligence Organisation (ASIO) Director General Review, where ASIO recognised that the scale of foreign interference activity against Australia's interests was unprecedented.[xiv] The actions taken by government are summarised in Figure 1.

Foreign interference is distinguishable from foreign influence, which is conducted openly and transparently and is a normal aspect of international relations and diplomacy. Foreign interference occurs where activities are carried out by, or on behalf of, foreign actors. They are coercive, deceptive or corrupting and contrary to Australia's sovereignty, values and national interests.

The key difference between foreign interference and foreign influence is transparency.

Figure 1

Sept 2018	Dec 2018	Aug 2019	Nov 2019	Nov 2020	Dec 2020	Jun 2021
ASIO Director General Review	Foreign influence Transparency Scheme	University Foreign Influence Taskforce	Guidelines to Counter Foreign Intelligence	Parliamentary Joint Comittee on Intelligence and Security Inquiry	Australia's Foreign Relations (State & Territory Arrangements Act 2020	Notify Minister of Foreign Affairs of existing, new and prospective arrangements

Foreign Interference Taskforce

Following growing evidence of foreign interference in the Australian university sector, the Minister for Education announced on 28 August 2019 that the government was establishing a University Foreign Interference Taskforce (UFIT) to provide better protection for universities against foreign interference.[xv] In October 2019, Australia's Director-General of Security confirmed that some foreign actors were pursuing opportunities to interfere with Australian decision-makers across a range of sectors, including the university and research sectors[xvi].

The *Guidelines to Counter Foreign Interference in the Australian University Sector* (Guidelines), developed by UFIT, were released on 13 November 2019. The Guidelines were developed for, and in partnership with, the Australian university sector with the stated purpose to support universities to:

- examine existing tools
- assist decision-makers to assess the risks from foreign interference
- promote greater consistency across the sector.

While the Guidelines are not intended to be exhaustive or place additional compliance or regulatory burdens on universities, it is clear universities are expected to regard the Guidelines in managing foreign interference and cyber security risks.

Recent developments: the increasing expectations of universities

There are currently additional legislative developments underway – including proposed new cyber security obligations for universities – to counter the foreign interference threat. This legislative reform appears predicated on the view that a proactive approach by the university sector in collaboration with government will help safeguard the reputation of Australian universities, protect academic freedom, and ensure that economic benefits are maximised[xvii].

Parliamentary Joint Committee on Intelligence and Security

On 8 September 2020, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) received a letter from the Minister for Home Affairs (Minister) referring an inquiry into foreign interference in Australian universities[xviii]. The PJCIS is viewed by some as one of the most important parliamentary committees, given its role as a key forum for government and the opposition to seek consensus on national security legislation[xix]. To date, two public hearings have been held, and the PJCIS is expected to issue its report in July 2021

Foreign Arrangements Scheme

The latest development impacting universities is *Australia's Foreign Relations (State and Territory Arrangements) Act 2020* (Act), which commenced on 10 December 2020 and established the Foreign Arrangements Scheme (FA Scheme). The FA Scheme requires public universities to notify, through an online public register, new, prospective and existing arrangements with foreign governments and foreign universities 'without institutional autonomy'[xx]. It also allows the Minister for Foreign Affairs to veto certain arrangements between public universities and foreign governments or foreign universities 'without institutional autonomy'[xxi].

SOCI Bill

Universities are also closely monitoring the SOCI Bill. If passed, the SOCI Bill will extend the obligations under the *Security of Critical Infrastructure Act 2018* and introduce new enhanced cyber security obligations to a broader range of sectors including the higher education and research sector.

In its present form, the SOCI Bill will impose obligations on universities to comply with requests for information, directions for action or requested intervention in response to serious cyber security incidents impacting a 'critical education asset'. This term is defined as an institution, such as a university, owned and operated by an entity registered in the Australian university category of the National Register of Higher Education Providers[xxii].

Universities may also need to comply with positive security obligations, including:

- the provision of ownership and operator information
- the adoption and maintenance of a critical infrastructure risk management program
- mandatory reporting obligations about cyber security incidents.

The latter obligations do not arise automatically but may be 'switched on' by the Minister.

What steps should universities take in response to the growing legislative and compliance obligations?

Apparently recognising the need for a collaborative approach to address the growing threats to the university sector, the government has produced guidance materials to assist universities. These include the detailed Guidelines and the sector-specific fact sheets created by DFAT in the context of the FA Scheme. There are also opportunities for universities to participate in workshops with government and organisations such as Universities Australia and UFIT.

Obligation	Application to Higher Education and Research Sector	Potential application to universities
Government Assistance Obligation	Applies to relevant entities in respect of critical infrastructure assets, specifically a critical education asset, impacted by a cyber security incident.	Will apply to universities in the event of a cyber security incident impacting the university.[xxiii]
Positive Security Obligation	If 'switched on' by the Minister, may apply to responsible entities for critical infrastructure assets, specifically a critical education asset.	If 'switched on' by the Minister, may require universities to provide ownership and operator information, adopt and maintain a critical infrastructure risk management program and report cyber security incidents.
Enhanced Cyber security Obligations	If the Minister declares a critical infrastructure asset to be a system of national significance (no systems of national significance have been declared at this stage).	Suppose the Minister declares a university a system of national significance. In that case, universities may need to work closely with the Australian government to adopt and maintain incident response plans, undertake cyber security exercises (potentially under Department observation), undertake and report on vulnerability assessments and provide the government with access to system information.

Industry in focus:

Financial Services
Health
Higher Education
› **Infrastructure**

Industry in focus: Infrastructure

Operational technology

More than perhaps any other industry, the infrastructure industry relies on operational technology (OT) to monitor and control physical processes or devices. OT is widely deployed within critical infrastructure and can be used in a wide range of applications – for example:

- industrial control systems that monitor and control water flow, power delivery and the operation of trains and other transport networks
- distributed control systems that monitor and control manufacturing processes
- building management and automation systems that monitor and control building systems such as climate control, lighting and security.

OT has traditionally operated in isolation from enterprise or broader networks. Increasingly, however, OT is converging with Internet-of-Things (IoT) enabled devices. This can give rise to significant benefits.

For example, in the mining industry, in response to the COVID-19 pandemic, IoT devices have been integrated with machinery to deliver real time information to maintenance technicians who cannot attend onsite. This protects staff whilst facilitating the real-time monitoring of mission-critical mining systems.

However, this convergence significantly increases the risk of a cyber attack or other cyber incident – including the risk that electricity, gas, water, telecommunications or other critical infrastructure may be disrupted or damaged.

The recent Colonial Pipeline ransomware attack (discussed on page 6 of this report) highlights the practical impact of IT network vulnerabilities on critical OT networks as well as the broader economy. In that instance, the Colonial Pipeline Co shut down its fuel pumping operations for six days in order to mitigate the potential spread of ransomware to its operational controls network. The effects of the attack rippled across the East Coast economy, with fuel prices rising an average of six cents during that week.

> "...this **convergence of Operational Technology and Internet of Things** significantly increases the risk of a cyber attack or other cyber incident..."

Industry in focus: Infrastructure

"...in December 2015, a cyber attack on Ukraine's power grid, the first such known attack on electricity infrastructure, resulted in **over 200,000 people being without power for several hours."**

OT and the risks of interconnectedness

A network-connected OT environment may expose legacy security vulnerabilities that subsist within critical infrastructure.

Because of the need for 24/7 uptime, system availability for critical infrastructure has often taken priority over IT security – meaning that the software in OT devices or systems may not have been regularly updated or patched. This may leave these systems or devices vulnerable to ever-more sophisticated hackers.

Cyber attacks

Cyber attacks against OT systems can be financially motivated (for example, the theft of confidential or sensitive data or the deployment of ransomware against critical systems). They can also be undertaken for political or other reasons – with potentially dire health and safety impacts. For example, in December 2015, a cyber attack on Ukraine's power grid, the first such known attack on electricity infrastructure, resulted in over 200,000 people being without power for several hours.

IoT – significant opportunities but significant risks

IoT refers to the network of physical devices connected to the internet and embedded with technologies such as software and sensors that enable the automated collection and analysis of large volumes of data.

IoT is increasingly being used in the property, energy, agriculture and mining sectors to monitor conditions and automate related operations.

For example, in the agriculture industry, IoT devices are used to monitor soil moisture and climate data to allow farmers to more efficiently control irrigation systems and improve crop output.

Cyber security risks

The cyber security risks associated with the use of IoT devices arise, in part, as a consequence of the incipient nature of the IoT industry. This may mean that performance and cost pressures take priority over cyber security. Exacerbating this is the large number of IoT devices deployed globally (which currently exceeds the global human population), meaning that there are many potential infiltration points. For example, in 2016, millions of vulnerable smart baby monitors, smart fridges and webcams were used to carry out distributed denial-of-service attacks against major websites, including Twitter and Pinterest.

How should organisations respond?

As one CIO we interviewed observed, "You can't protect what you don't know that you have".

Organisations must develop an understanding of their OT and IoT environments and devices to assess potential weaknesses and vulnerabilities. This needs to occur continually, not just when a device is first deployed. For example, an organisation we spoke with deployed a thermal camera for site monitoring. The Department of Defence later identified the camera as containing potential security vulnerabilities. The organisation consequently implemented additional security monitoring, as well as isolating the device from its network.

More generally, organisations should:

- adopt a structured and documented approach to the assessment and deployment of IoT devices (for example, individuals should not be permitted to purchase IoT devices and connect them to an organisation's network without appropriate approvals)
- implement active monitoring of attacks against IoT devices
- specifically contemplate such attacks (and their consequences) in their data incident response planning.

Commonwealth Government response

As OT used in critical infrastructure becomes increasingly connected to the internet and other networks, and as IoT technology continues to be adopted and relied on, critical infrastructure is becoming an increasing target for private and state-based cyber attackers.

In June 2020, the Prime Minister announced that Australian organisations, including essential infrastructure operators, were the target of a state-based cyber actor.

In its Cyber Security Strategy 2020, the Commonwealth Government recognised the threat posed by cyber attacks to Australia's critical infrastructure, particularly as the devices become ever more interconnected and our reliance on the internet increases. To this end, the Government has committed to investing $1.67 billion over ten years for "protecting and actively defending the critical infrastructure that all Australians rely on".[xxiv]

Critical Infrastructure Centre

The Critical Infrastructure Centre was established in January 2017 to safeguard Australia's critical infrastructure from the risks of foreign interference. The centre has released best practice guidance for owners and operators of critical infrastructure in respect of supply chains,[xxv] and is continuing to develop best practice guidance to life industry security practices.

The centre has a role in monitoring compliance of entities with critical infrastructure register obligations. It also conducts proactive risk assessments, with a focus on the high-risk sectors of telecommunications, electricity, water and ports.

Security Legislation Amendment (Critical Infrastructure) Bill 2020

The SOCI Bill was introduced into Commonwealth Parliament on 10 December 2020.

The Bill seeks to expand the scope of the Security of Critical Infrastructure Act 2018 (Cth), which currently only applies to the electric, gas, water and maritime ports sectors, to a further 11 sectors. These include higher education, communications, data storage and processing, energy, transport, water and sewerage. The Bill also seeks to introduce many positive security obligations that may apply to those in critical sectors responsible for 'critical infrastructure assets'.

The Bill is discussed further on page 27 and page 31.

How we can help

MinterEllison provides a unique, full-service IT legal and consultancy practice with extensive experience in privacy, data protection and software and IT service procurement.

Our team works with clients across the public and private sector to manage the full lifecycle of IT projects – from initial market approaches to ongoing implementation and performance management. We understand the unique features of the technology sector: the drivers, the innovations and the trends. We bring deep industry experience, technical knowledge and legal expertise together to deliver the best possible outcomes for our clients.

Appendix A – Methodology

Our study commenced in 2015, and is in its 6th year. From December 2020-March 2021, MinterEllison canvassed the opinions of General Counsel, Heads of Risk, Data Protection/Privacy Officers and C-suite executives in Australia in ASX 200 companies, private companies, government and not-for-profit organisations.

The majority of respondents come from organisations with more than 1,000 employees.

Participants were issued a survey seeking feedback on:

- their organisation's cyber security exposure over the past 12 months
- whether cyber risk ranks highly on their organisation's risk register
- their use of an established risk framework
- whether their organisation has a cyber security plan
- the regularity of testing their cyber plan
- the measures their organisations have in place to address a cyber security attack.

Respondents provided quantitative and qualitative results. These were supplemented with in-depth interviews with leaders from industry.

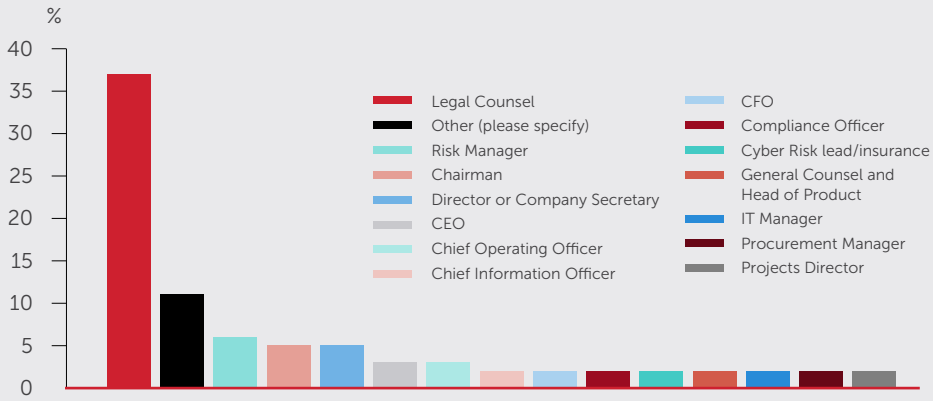
All information provided by participants is confidential and reported primarily in aggregate form.

The views expressed in this report do not necessarily reflect the views of the individual respondents, unless otherwise stated.

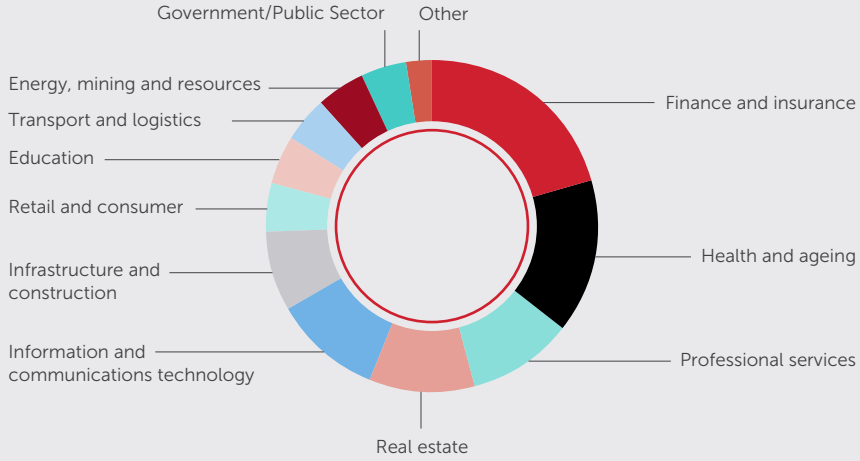
We make no representation or warranty about the accuracy of the information, or about how closely the information gathered will reflect actual organisational performance or effectiveness,

This report contains general advice only, and does not take into account your organisation's particular circumstances or objectives.

Respondent positions



Respondent industries



Endnotes

i See Privacy Act 1988 (Cth) pt VIIIA.

ii Geoff Summerhayes, (Speech, Financial Services Assurance Forum, on 26 November 2020).

iii James Frost and Jonathan Shapiro, 'Cyber attacks 'the biggest risk in banking'', Australian Financial Review (30 March 2021) <https://www.afr.com/companies/financial-services/cyber-is-the-biggest-risk-in-banking-today-20210330-p57f5n>.

iv Ibid.

v See above n ii.

vi PwC Financial Services, Top financial services issues of 2018 (December 2017) 19 <https://www.pwc.com/il/he/bankim/assets/2018/Top%20financial%20services%20issues%20of%202018.pdf>.

vii McKinsey & Company, Next-gen Technology transformation in Financial Services (April 2020) 49 <https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Next-gen%20technology%20transformation%20in%20financial%20services/Next-gen-technology-transformation-in-financial-services.pdf>.

viii APRA, 'Outsourcing Involving Cloud Computing Services' (Information Paper, 24 September 2018) <https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services.pdf>.

ix Ry Crozier, 'NAB blocked 41,000 data theft attempts in a three-month period', itNews (15 September 2020) <https://www.itnews.com.au/news/nab-blocked-41000-data-theft-attempts-in-a-three-month-period-553353>.

x See above n ii.

xi Office of the Australian Information Commissioner, 'Notifiable Data Breaches Report: July–December 2020', Notifiable data breach statistics (Online Report, 28 January 2021) <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2020/>.

xii Australian Cyber Security Centre, Ransomware in Australia (Website, October 2020) <https://www.cyber.gov.au/sites/default/files/2020-10/Ransomware%20in%20Australia%20%28October%202020%29.pdf>.

xiii Check Point Software Technologies, Hospitals Targeted in Rising Wave of Ryuk Ransomware Attacks (Blog Post) <https://blog.checkpoint.com/2020/10/29/hospitals-targeted-in-rising-wave-of-ryuk-ransomware-attacks/>.

xiv Australian Security Intelligence Organisation, Annual Report 2017-18 (Annual Report, 25 September 2018) <https://www.asio.gov.au/sites/default/files/ASIO%20Annual%20Report%20to%20Parliament%202017-18.pdf>.

xv Department of Education Skills and Employment, 'Establishment of a University Foreign Interference Taskforce' (Announcement, 28 August 2019) <https://www.dese.gov.au/guidelines-counter-foreign-interference-australian-university-sector/announcements/establishment-university-foreign-interference-taskforce>.

xvi Evidence to Senate Legal And Constitutional Affairs Legislation Committee, Parliament of Australia, Canberra, 21 October 2019, 64 (Mike Burgess, Australian Security Intelligence Organisation Director-General of Security).

xvii Department of Education Skills and Employment, Guidelines for countering foreign interference in the Australian university sector 6 (Website) <https://www.dese.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector>.

xviii Parliament of Australia, 'Foreign interference in universities inquiry under consideration' (Media Release, 8 September 2020) <https://www.aph.gov.au/About_Parliament/House_of_Representatives/About_the_House_News/Media_Releases/Foreign_interference_in_universities_inquiry_under_consideration>.

xix Anthony Galloway, 'Liberal senator James Paterson to lead Parliament's intelligence and security committee' The Sydney Morning Herald (online, 4 February 2021) <https://www.smh.com.au/politics/federal/liberal-senator-james-paterson-to-lead-parliament-s-intelligence-and-security-committee-20210204-p56zh9.html>.

xx Department of Foreign Affairs and Trade, What does the scheme do? (Website) <https://www.foreignarrangements.gov.au/about-the-scheme/what-does-the-scheme-do>.

xxi Supplementary Explanatory Memorandum, Australia's Foreign Relations (State And Territory Arrangements) Bill 2020 (Cth).

xxii Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth).

xxiii Provided the safeguard measures against the abuse of these powers are met as defined in s35AB.

xxiv Department of Home Affairs, Australia's Cyber security Strategy 2020 (Cyber Security Strategy, 6 August 2020) <https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf>.

xxv Department of Home Affairs, Protecting your critical infrastructure asset from foreign involvement risk (Website) <https://www.homeaffairs.gov.au/nat-security/files/cic-best-practice-guidance-supply-chains.pdf>.

At MinterEllison we are driven to deliver solutions that create lasting impacts. We start by listening: we ask questions that challenge the status quo, then come up with solutions that help clients manage risk, realise efficiencies, grow and contribute back to their stakeholders and communities.

Paul Kallenbach
Partner
Competition, Risk & Regulatory

E paul.kallenbach@minterellison.com
P 03 8608 2622