Perspectives on Cyber Risk 2025

10 Years Perspectives on Cyber Risk

MinterEllison.

Contents

Contents

Contents

Reflections... on a decade of **Perspectives on Cyber Risk**

Cyber security is no longer just an IT issue, but a fundamental business, legal, societal, and geopolitical imperative. To mark the tenth anniversary of our annual cyber security report, we reflect on the last decade that has reshaped not only the digital risk landscape, but also the technological, organisational and regulatory responses to it.

The pace and scale of digital transformation have been remarkable – enabling unprecedented innovation, productivity and connectivity across the global economy.

But these gains have come at a cost: a dramatic escalation in data breaches and other cyber threats, coupled with rising Board-level accountability, regulatory complexity, and significant economic and reputational harm.

Our **2025 Perspectives on Cyber Risk survey** responses reveal that **76%** of organisations rank cyber risk among their top five priorities, up from 56% just two years earlier. This shift is unsurprising. These days, data breaches occur with alarming frequency, and ransomware costs the Australian economy around **A$3 billion** annually. Furthermore, a single security failure can have catastrophic consequences: the 2017 WannaCry and NotPetya ransomware attack exemplified this, rapidly spreading across more than 150 countries, disrupting critical services including hospitals, transport systems, and governments, and causing an estimated US$14 billion in global damages.

Organisations today manage and store vast volumes of data – data that must be protected not only to ensure operational continuity, but to maintain customer trust, preserve corporate reputation, and comply with increasingly stringent legal obligations. Yet, concerningly, more than half of our 2025 survey respondents still lack high confidence in their

Respondents ranking cyber risk as a 'top five' priority: the 2-year leap

56% 2023

76% 2025

Reflections... on a decade of **Perspectives on Cyber Risk**

organisation's knowledge of what data it holds, where it is stored, or how it is secured.

This represents an alarming gap in an era of increasing regulatory scrutiny and heightened public expectation.

This special '10 year edition' of our report traces the evolution of cyber threats and breach tactics, spotlighting some of the most significant incidents here in Australia and overseas.

We examine what the data from our latest cyber survey tells us about progress in cyber resilience, how regulators have responded, and how organisations have adapted. Finally, we provide forward-looking insights for Boards, executives and legal advisers so that they can navigate the next era of digital risk with greater confidence.

As we look back on the lessons learned and ahead to the various threats and opportunities, one theme is clear: **cyber security is more than just a defensive necessity**. It is a shared, strategic responsibility that must be embedded across governance, risk, technology and culture – and is critical to the resilience and success of every organisation in today's digital age.

Paul Kallenbach
Partner
Technology and Data

Shannon Sedgwick
Partner
Cyber Security

A

A decade of data breaches

Data breaches are ***the*** defining cyber security challenge of the modern era

Over the past ten years, data breaches have grown markedly in frequency, scale, and sophistication.

From state-sponsored espionage and supply chain compromises to double-extortion ransomware and insider threats, the nature of these incidents continues to evolve – and what was once primarily a technical problem is now a mainstream business risk, with impacts spanning financial, regulatory, reputational, and national security domains.

This report section examines breach trends across Australia and globally, spotlighting some of the most high-profile and consequential incidents. We analyse how attacker tactics and organisational responses have shifted, distilling key lessons from the past decade and exposing the persistent and emerging risks that remain as the cyber threat landscape becomes ever more complex and perilous.

Quick facts:

Top 5 sectors to notify data breaches July – December 2024[1]

121
HEALTH SERVICE PROVIDERS

100
AUSTRALIAN GOVERNMENT

54
FINANCE
(INCL. SUPERANNUATION)

36
LEGAL, ACCOUNTING AND MANAGEMENT SERVICES

34
RETAIL

[1]OAIC, Notifiable data breaches report: July to December 2024 (Report, 13 May 2025)

A decade of data breaches: global and local lessons learned

No longer simply a byproduct of poor patching or misconfigured systems, many recent data breaches stem from systemic organisational weaknesses – including in data governance, incident response, and strategic oversight. They reveal just how interconnected and vulnerable our digital ecosystems have become. As attackers grow more strategic, sophisticated, and opportunistic, the volume, scale and impact of breaches continue to rise, challenging even the most prepared organisations to keep pace.

From oversights to systemic failures

Some of the decade's most damaging breaches stemmed from basic but consequential failures in patching, configuration, and access control.

For example, the 2017 **Equifax** breach exploited an unpatched vulnerability, exposing the personal data of 147 million individuals.

Similarly, in 2019, **Capital One** fell victim to a firewall misconfiguration, exposing 100 million records. Large-scale incidents like the **Alibaba** cloud breach and the Indian government's **Aadhaar** exposure highlight how scale and centralisation can amplify risk, particularly when combined with insufficient oversight or weak access controls.

Other examples reveal systemic breakdowns in detection, governance, and accountability. The 2018 **Facebook-Cambridge Analytica** scandal exposed how platform design and permissive data access policies enabled the unauthorised harvesting of personal data from over 87 million users. The 2017 **Yahoo** breach, compromising 3 billion accounts, went undetected for years due to delayed internal escalation and poor visibility. Furthermore, the 2018 **Australian National University** breach demonstrated how attackers can dwell undetected in networks for months, exfiltrating sensitive data accumulated over a 19-year span.

These global and local incidents underscore that data breaches often result as much from organisational blind spots as from attacker sophistication.

These and other data breaches are detailed further here.

The weaponisation of cyber operations

Nation-states have intensified cyber operations as tools of economic and geopolitical influence. This is confirmed by CrowdStrike's 2025 analysis, which noted a dramatic increase in espionage and disruption campaigns attributed to Russian and Chinese actors. China-nexus activity alone surged 150%, targeting key sectors like healthcare and government.

These campaigns are not only more frequent but also faster and harder to detect.

Cyber attacker 'breakout time' – how quickly an intruder moves laterally from the initial point of compromise to other systems within the network after intrusion – has dropped to an average of just 48 minutes, with the fastest observed at a mere 51 seconds. For defenders, this translates to having only minutes, not hours, to detect and contain a breach.

The rise and resilience of ransomware

Ransomware remains the most common and costly form of data breach, both globally and domestically.

In Australia, the **Medibank** breach served as a watershed moment due to its scale and the resulting public, political, and legal reactions. In October 2022, attackers accessed Medibank's systems and exfiltrated data affecting around 9.7 million customers. Instead of encrypting systems, the attackers threatened to release stolen data unless a ransom was paid. Medibank refused, leading to the publication of personal and health information on the dark web and triggering widespread calls for regulatory reform.

Globally, major ransomware attacks have also continued to escalate:

WannaCry (2017):

200k

computers infected across

150 **countries**

severely disrupting critical services, including the UK's National Health Service.

Colonial Pipeline (2021):

Ransomware forced the shutdown of the largest fuel pipeline in the United States, prompting a

US$4.4m

ransom payment and triggering fuel shortages across the East Coast.

Kaseya (2021):

REvil ransomware

exploited a vulnerability in the company's remote management software to affect up to

1,500 **downstream organisations**

via managed service providers.

NotPetya (2017):

Originated as a supply chain attack on Ukrainian accounting software, but rapidly spread worldwide causing over

US$10b

in estimated damages

and impacting multinationals such as Maersk, FedEx, and Merck.

JBS Foods (2021);

The world's largest meat processing company paid a

US$11m

ransom after an attack disrupted operations across North America and Australia

DHL (2022):

Frequently impersonated in

ransomware and phishing operations,

was directly targeted by malware campaigns **affecting logistics and customs processing globally.**

Garmin (2020):

Experienced a widespread service outage following a

WastedLocker attack that disrupted its navigation and fitness tracking systems

CNA Financial (2021)

US$40m

ransom payment following an attack that **encrypted thousands of devices** and disrupted operations for weeks.

Medibank (2022):

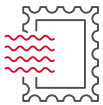
One of Australia's most consequential ransomware and extortion incidents

9.7m **customers health data published**

on the dark web after the company refused to pay the ransom.

These incidents, across diverse industries and sectors, highlight the growing prevalence of 'double extortion' tactics, in which attackers not only encrypt systems but also exfiltrate sensitive data – leveraging the threat of publication to increase pressure on victims.

The convergence of ransomware with supply chain compromise, cloud infrastructure vulnerabilities and identity-based intrusion techniques has further amplified the intensity, complexity and consequence of these attacks.



Royal Mail (2023):

Targeted by the

LockBit group

causing international mail services to be suspended

across the UK.

Healthcare (2024):

Experienced a widespread service outage following a

ransomware attack

by the BlackCat/ALPHV group

crippling operations and leading to widespread disruption in healthcare services.

Ahold Delhaize (2024):

The global food retailer confirmed

sensitive data was stolen during a **ransomware attack**

on its US business, affecting internal systems and leading to disruptions in pharmacy services and e-commerce operations.

Latitude Financial (2023):

Suffered a significant

ransomware

related breach in Australia, with over

14m **personal data records accessed**

including copies of indentification documents

CDK Global (2024):

A major software provider for auto dealerships was attacked by the **BlackSuit ransomware group** disrupting operations at

1000s of dealerships across North America

DaVita (2025):

The kidney dialysis firm disclosed a

ransomware attack

that encrypted parts of its network and impacted some of its operations.

Change Healthcare (2024):

A subsidiary of UnitedHealth Group and a major processor of American medical claims, fell victim to a

ransomware attack

by the BlackCat/ALPHV group

crippling operations and leading to widespread disruption in healthcare services.

Alder Hey Children's Hospital (2024):

The **INC Ransom group** claimed to have

stolen data from the Liverpool-based hospital,including **patient records and financial information,** and published it on the dark web.

Survey spotlight: **confidence, fatigue and the 'new normal'**

Insights from our 2025 cyber risk survey reveal concerning and persistent weaknesses:

36%
of respondents
were very confident in understanding their data holdings or where data is stored

70%
of respondents
test their incident response plans at least annually

52%
of respondents
reported low or partial confidence in meeting post-breach regulatory obligations

> **"Insights from our 2025 cyber risk survey reveal concerning and persistent weaknesses in data mapping and governance. These findings underscore the urgent need for robust data governance frameworks and regular testing of incident response plans to enhance organisational resilience."**
>
> **Shannon Sedgwick**
> Partner, Cyber Security

These figures align with recent findings, such as the Splunk CISO Report, indicating a critical disconnect between where Board attendance by CISOs is high (83%), but Board-level cyber security expertise remains low (29%).

Meanwhile, 53% of CISOs report their role has become materially harder, reflecting heightened expectations and resource constraints.

Evolving tactics and expanding threat surfaces

Attacker methods have grown more sophisticated.

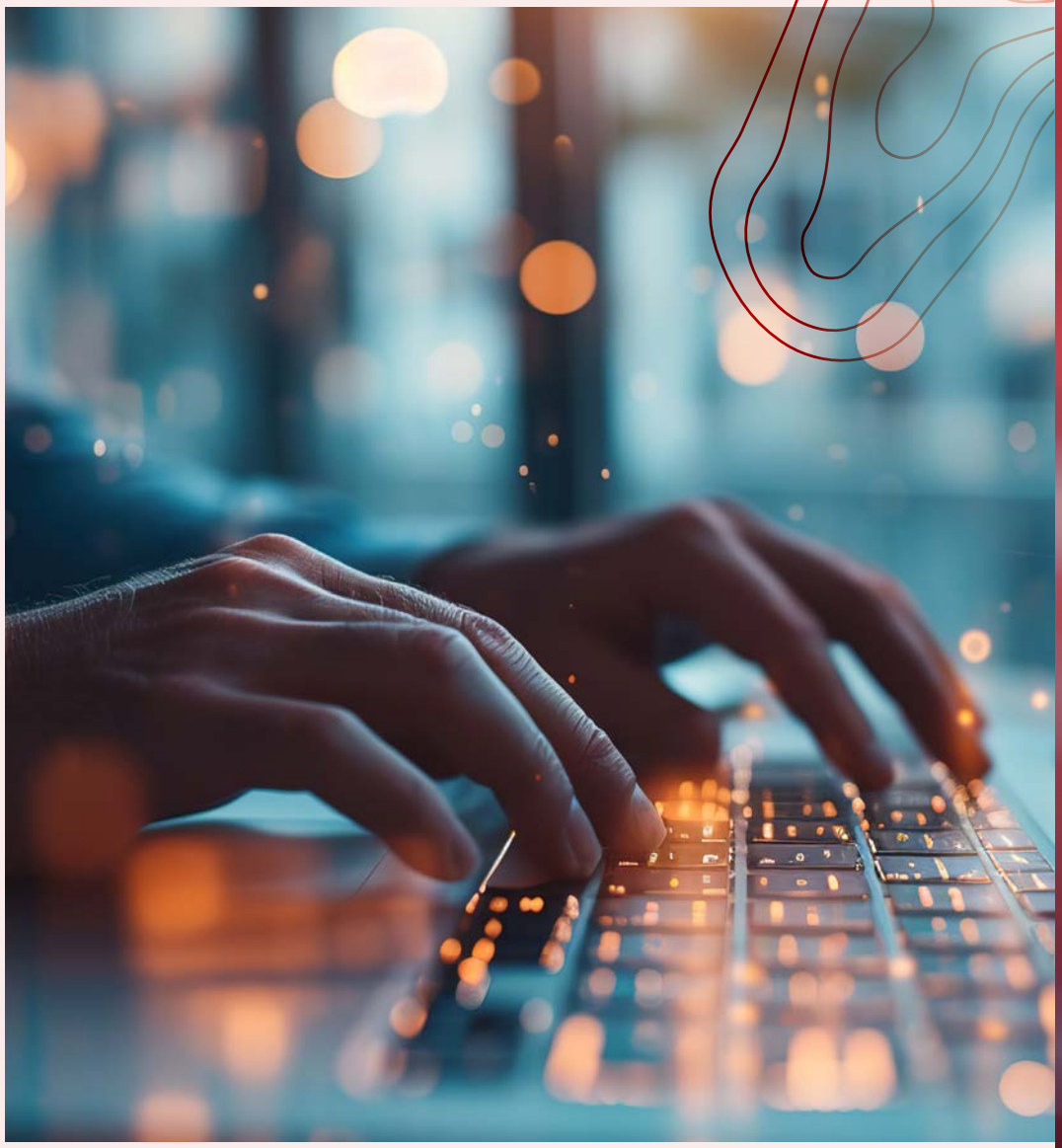
Traditional phishing has yielded to callback scams, phishing-as-a-service, remote monitoring tool abuse, and identity compromise. According to CrowdStrike, 79% of breaches in 2024 were malware-free, relying instead on legitimate tools and stolen credentials to bypass detection. Threat actors like CURLY SPIDER use real-time social engineering to gain remote access in under four minutes.

AI is emerging as a force multiplier. Both CrowdStrike note the growing use of GenAI tools by adversaries to enhance their phishing, automate reconnaissance, and scale influence operations –while still targeting known weaknesses like multi-factor authentication (**MFA**) bypass, misconfigured cloud services, and legacy infrastructure.

Targeted sectors

Certain sectors have borne the brunt of these developments.

- The **healthcare** sector remains the most targeted industry, accounting for 19% of the 527 notifiable data breaches reported to the Office of the Australian Information Commissioner (**OAIC**) between January and June 2024. Its persistent vulnerability reflects a combination of factors: the mission-critical nature of healthcare services, the high value and sensitivity of personal health data, and the sector's frequent reliance on fragmented and legacy infrastructure.
- The **finance sector** continues to be targeted for both fraud and disruption. The **First American Financial** breaches in 2019 and 2023 show that legacy systems, document-heavy platforms, and insider threats remain key areas of risk in this sector. Regulatory risk is also increasing, in light of new standards such as **CPS 230**, which mandates heightened accountability for operational resilience; and the proactive enforcement stance taken by the Australian Securities and Investments Commission (**ASIC**), which has pursued legal action in two high profile cyber matters: against **RI Advice Group** for failing to adequately manage cyber risk across its financial planning network; and against Latitude Financial following its 2023 data breach.
- The **education** and **government** sectors continue to be key targets for nation-state actors seeking to gather intelligence, disrupt operations, or exert influence. These sectors consistently rank among the top three for espionage-motivated intrusions, with adversaries often remaining undetected for extended periods. The 2018 breach at the **Australian National University** exemplifies this threat: attackers infiltrated the network and exfiltrated nearly two decades' worth of personal and academic records over several months before detection. Government department and agencies that have been impacted by significant breaches over the past decade include the **Commonwealth** and **NSW Departments of Education**, the **US Office of Personnel Management**, the **UK National Health Service** (**NHS**) and **UK Foreign Office,** the **NZ Stock Exchange**, and the **German Budestag** and **Federal Foreign Office**.



The road travelled and the road ahead

Over the past ten years of our Perspectives on Cyber Risk series, one trend has remained constant: the widening gap between risk awareness and risk readiness. Each report has captured a moment in the cyber landscape – from the first inklings of ransomware-as-a-service and the early stages of notifiable breach regulation, to the wave of high-profile supply chain attacks and, more recently, the emergence of AI-powered threat vectors.

Across this body of work, several consistent themes have emerged:

Faster, stealthier and more challenging

The threat landscape has become ever **faster**, more **decentralised**, **commercialised**, **stealthier**, and **strategically damaging**.

Uneven organisational responses

Organisational responses have been **uneven**, with some sectors adapting quickly while others struggle with legacy systems, under-resourced teams, and reactive cultures.

All eyes on board and senior management

Expectations on Boards and senior executives have expanded significantly. Cyber risk is now firmly understood as a matter of **corporate governance**, **regulatory accountability**, and **institutional trust**.

There is little doubt that the future threat landscape will continue to be shaped by the accelerating use of AI – both by defenders and adversaries. While AI offers the promise of detection, analysis and response, it equally enables scalable, adaptive attacks, from hyper-personalised phishing to deepfake-enabled fraud and generative misinformation.

Crucially, cyber and security leads within every organisation need to be supported and empowered with the mandate, resources, and influence to drive change – fostering a culture where cyber security is a shared responsibility, embedded in decision-making at all levels, and seen as vital for an organisation's reputation, resilience, and long-term success.

"**Organisations must continuously evolve and adapt their security strategy to an increasingly complex environment – especially in the face of AI and its benefits and risks.**

This means continuously investing in the fundamentals: timely patching, comprehensive asset and data visibility, rehearsed incident response, supply chain assurance, robust access controls, user awareness training, and reliable backup procedures.

Cyber considerations must be embedded into strategic planning and boardroom dialogue, not just compliance checklists."

Paul Kallenbach
Partner, Technology and Data

A timeline of Australian and overseas data breaches

Data breach milestones

In the early 1970s

Creeper was discovered on ARPANET. It spread between mainframes with a simple message: "I'm the creeper: catch me if you can".

First major online data breach

In **2005** DSW Shoe Warehouse exposed over 1.4 million credit card numbers after attackers accessed its payment systems.

Most expensive cyber attack

NotPetya (2017), masquerading as ransomware but designed for destruction, caused over US$10 billion in damage globally – affecting Maersk, Merck, FedEx and more.

Largest insider data theft

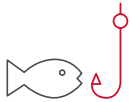
Between 1976 and 2006, aerospace engineer Greg Chung stole an estimated US$2 billion worth of classified Boeing documents and provided them to China. He was later sentenced to over 15 years in prison.

Largest retail data breach

In **2006-2007** TJX Companies (owner of T.J. Maxx and Marshalls) suffered a breach affecting over 94 million credit and debit card accounts.

First GDPR fine over €1 billion

In **2023** TJX Meta was fined €1.2 billion by Ireland's Data Protection Commission for transferring EU user data to the US in breach of GDPR rules – the largest GDPR penalty to date.



First known phishing attack

In **1996** hackers targeted AOL users with fake emails to harvest login credentials – a technique that still dominates today.

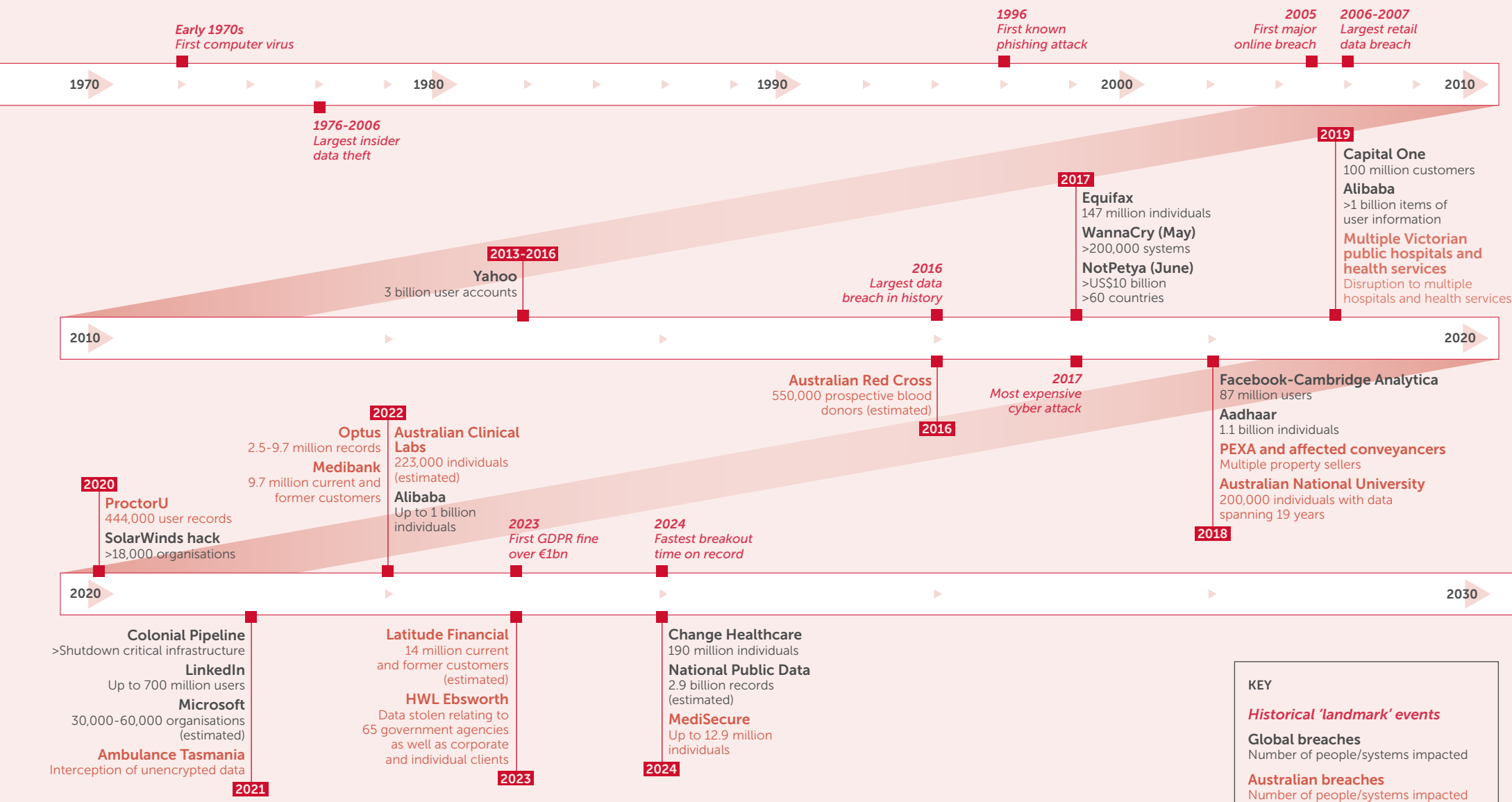
Largest data breach in history

Yahoo's breaches, disclosed in 2016 but dating back to **2013-2014** compromised all 3 billion user accounts – the most ever recorded.

Fastest breakout time on record

According to CrowdStrike, the fastest lateral movement from initial access was just 51 seconds, observed in a **2024** ransomware incident – leaving defenders no time to respond.

A decade of data breaches 2015-2025



14 major overseas data breaches in the past 10 years

Affected entity or event

01. Yahoo

Date

2013-2016

Attributed cause

Russian State-sponsored group.

Magnitude of impact

3 billion user accounts

Affected information

Names, phone numbers, password challenge questions and answers, password recovery emails and a cryptographic value unique to each account

Attack vector

Spear phishing

Significance

Widely considered to be the largest known data breach in history, the Yahoo breach compromised the personal data of all 3 billion user accounts.

Initially underestimated, the true scale of the breach was not disclosed until years later, after multiple incidents were combined and publicly confirmed. Investigations revealed that Yahoo failed to properly assess and escalate the incident internally, delayed notifying affected users and regulators, and lacked adequate detection capabilities.

Yahoo faced widespread criticism, regulatory fines, and over 40 class action lawsuits as a result of the breach.

Affected entity or event

02. Equifax

Date

2017

Attributed cause

Russian State-sponsored group.

Magnitude of impact

147 million affected individuals

Affected information

Social security numbers, birth dates, addresses, driver's licence numbers and credit card details

Attack vector

Software vulnerability exploit, poor security controls

Significance

Attackers exploited a known vulnerability in the Apache Struts software used by Equifax's online dispute portal. Although a patch had been issued months earlier, Equifax failed to apply it, allowing the attackers to gain entry.

Once inside, the attackers moved laterally across systems due to weak network segmentation, and discovered usernames and passwords stored in plain text. Undetected for several months, they exfiltrated large volumes of data. Compounding the issue, Equifax had failed to renew an encryption certificate on one of its internal security tools, which prevented its own monitoring systems from identifying the breach.

The company was widely criticised for its delayed response and lack of transparency. In 2019, it reached a global settlement of up to US$425 million with US regulators, including the Federal Trade Commission and the Consumer Financial Protection Bureau, as well as 50 US states and territories. The breach led to significant reputational damage and a lasting spotlight on corporate accountability for cyber risk.

Affected entity or event

03. WannaCry

Date

2017 (May)

Attributed cause

Lazarus Group

Magnitude of impact

>200,000 infected systems

Affected information

Varied (data on individual PCs was encrypted by hackers)

Attack vector

Ransomware

Significance

The 2017 WannaCry ransomware attack showed how rapidly a known vulnerability can be weaponised at scale. Exploiting the EternalBlue flaw in Windows – originally developed by the National Security Agency (**NSA**) and later leaked – WannaCry spread autonomously, infecting over 200,000 systems across 150 countries in a matter of days.

The malware encrypted files and demanded Bitcoin payments, halting operations across logistics, healthcare, finance, and telecommunications. The UK's NHS was among the hardest hit, cancelling thousands of appointments and reverting to manual processes. The estimated cost to the NHS was £92 million, and global economic losses exceeded US$4 billion.

The attack exposed widespread failures in patch management and highlighted the systemic risks posed by outdated infrastructure and leaked cyber weapons. Although an accidental kill switch eventually slowed the spread, much of the damage had already been done.

Affected entity or event

04. NotPetya

Date

2017 (June)

Attributed cause

Russian State-sponsored group.

Magnitude of impact

Over US$10 billion in estimated global damages; affected government and private sector organisations across more than 60 countries

Affected information

Operational systems and data were rendered inaccessible; no exfiltration of personal data reported

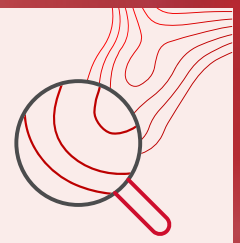
Attack vector

Supply chain compromise via malicious update to Ukrainian tax software (MeDoc); exploited the EternalBlue vulnerability

Significance

In terms of economic damage, NotPetya is widely regarded as the most devastating cyber attack in history. Although it appeared to be ransomware, its purpose was entirely destructive: the malware encrypted in NotPetya's systems had no intention of allowing recovery. It rapidly spread across corporate networks worldwide, affecting companies including Maersk, Merck, FedEx, Mondelez, and Saint-Gobain.

The incident prompted a global reckoning with the risks of supply chain compromise, lack of segmentation, and the militarisation of malware. Its unprecedented scale and collateral impact influenced national cyber strategies and incident response frameworks globally.



Affected entity or event

05. Facebook-Cambridge Analytica scandal

Date

2018

Attributed cause

Meta (Facebook)

Magnitude of impact

87 million affected Facebook users

Affected information

Profile information including names, genders, locations, birthdays, and education details, personal information from users' Facebook friends and data from personality quiz responses used to build detailed psychographic profiles.

Attack vector

Data harvesting

Significance

The 2018 Facebook-Cambridge Analytica scandal was a defining moment in global conversations about data privacy, platform responsibility and digital influence.

The controversy centred on how the political consulting firm Cambridge Analytica obtained personal information from around 87 million Facebook users without their knowledge or consent. This was enabled by a third party quiz app, "This Is Your Digital Life," which was installed by around 300,000 users; and collected not only data from those users, but also from their Facebook friends – due to Facebook's permissive data-sharing policies at the time.

Although no technical breach occurred, the incident revealed systemic issues with Facebook's platform governance, consent architecture and enforcement of developer access restrictions. The data harvested was allegedly used to build detailed psychographic profiles of voters and influence political campaigns, including the 2016 US presidential election and the UK Brexit referendum.

The fallout was extensive. Facebook CEO Mark Zuckerberg testified before US Congress and faced questioning from regulators and legislators around the world. The company was also fined US$5 billion by the US Federal Trade Commission for privacy violations – one of the largest penalties ever imposed for data misuse.

In Australia, the OAIC launched an investigation and, in March 2020, initiated civil penalty proceedings against Facebook, alleging serious and/or repeated interferences with privacy under the *Privacy Act 1988* (Cth) (**Privacy Act**). The OAIC estimated that while only 53 Australians had installed the app, the personal information of approximately 311,127 Australian Facebook users was exposed.

On 17 December 2024, the OAIC and Meta reached a settlement through an enforceable undertaking. Meta agreed to establish a A$50 million payment program for affected Australian users, marking the largest privacy-related settlement in Australian history. The program, to be administered by an independent third party, offers compensation to users who held a Facebook account between 2 November 2013 and 17 December 2015, were present in Australia for more than 30 days during that period, and either installed the app or were friends with someone who did.

This case underscores the critical importance of robust data governance and the need for platforms to ensure transparency and accountability in handling personal information.

Affected entity or event

06. Aadhaar

Date

2018

Attributed cause

Various

Magnitude of impact

1.1 billion affected individuals

Affected information

Names, addresses, phone numbers, Aadhaar numbers, passport numbers. Biometric data (iris scans and fingerprints) may also have been affected.

Attack vector

Data leaks, poor access control

Significance

The Aadhaar data exposure, linked to India's national digital identity system, raised global concerns about biometric data security and the risks of centralised identity infrastructure.

Launched in 2009, Aadhaar is the world's largest biometric ID program, assigning a 12-digit identification number to over 1.3 billion Indian residents. It stores personal, demographic, and biometric data, including fingerprints and iris scans, in a centralised government database managed by the Unique Identification Authority of India (**UIDAI**).

Between 2017 and 2018, multiple media investigations and independent researchers exposed serious vulnerabilities and lapses in access control. In one widely reported instance, journalists were able to purchase unauthorised access to the Aadhaar database for as little as ₹500 (around A$12), gaining the ability to retrieve demographic data using Aadhaar numbers. In another case, a breach at a state-owned utility provider enabled access to the ID numbers and personal data of millions of users via a public website.

Although UIDAI denied that the core biometric database was breached, estimates suggest that over **1.1 billion individuals' data** was potentially exposed through poorly secured APIs, leaked credentials, and unauthorised access points. The Indian government later acknowledged issues with security practices and imposed restrictions on data access while enhancing audit and oversight mechanisms.

The Aadhaar exposure became a flashpoint in global privacy discourse, prompting constitutional challenges in India's Supreme Court and widespread scrutiny of government surveillance, consent and data protection frameworks. It also influenced policy reforms, including the introduction of India's Digital Personal Data Protection Act (2023), discussed here.

Affected entity or event

07. Capital One

Date

2019

Attributed cause

Individual threat actor

Magnitude of impact

100 million customer records

Affected information

Names, addresses, phone numbers, email addresses, birth dates, annual income, credit information, social security numbers and bank account numbers

Attack vector

Misconfiguration exploit

Significance

The 2019 Capital One breach exposed the sensitive personal and financial information of more than 100 million customers across the US and Canada, highlighting the risks of cloud misconfiguration and insider threats.

The attacker, a former employee of Amazon Web Services (**AWS**), exploited a firewall misconfiguration to access Capital One's cloud-hosted environment. The breach involved over 140,000 US Social Security Numbers, 1 million Canadian Social Insurance Numbers, and extensive credit application data.

The attacker used legitimate credentials and tools to extract the data, underscoring how even organisations with strong technical protections can be vulnerable to gaps in access control and monitoring.

The breach led to intense regulatory scrutiny and class actions. Capital One ultimately agreed to pay US$190 million in a class action settlement, and US$80 million in civil penalties to US regulators, for failing to establish effective risk management prior to migrating sensitive data to the cloud. The case is a cautionary tale of balancing cloud adoption and innovation with rigorous oversight and internal governance.

Affected entity or event

08. Alibaba

Date

2019 and 2022

Attributed cause

2019: insider threat / affiliate misuse.
2022: security misconfiguration.

Magnitude of impact

2019: over 1 billion items of user information scraped.
2022: potentially up to 1 billion individuals (23+ terabytes of data).

Affected information

2019: Taobao user IDs, mobile phone numbers, user comments.
2022: comprehensive personal details, including names, addresses, national ID numbers, phone numbers, criminal case details.

Attack vector

2019: web scraping via customer crawler.
2022: unauthorised access to allegedly misconfigured and unsecured police database.

Significance

These two distinct cyber attack incidents highlighted different risks.

The 2019 event showed vulnerability to large-scale scraping by insiders and affiliates targeting a major e-commerce platform, while the 2022 leak represented a catastrophic failure in securing highly sensitive government data hosted on a commercial cloud.

The 2022 leak is potentially one of the largest data breaches of personal information in history, exposing the data of a vast portion of China's population.

The latter incident led to significant scrutiny of Alibaba Cloud's security practices and controls, particularly the 2022 incident, which prompted high-level government attention in China regarding data security on cloud platforms.

Affected entity or event

09. SolarWinds hack

Date

2020

Attributed cause

Russian State-sponsored group

Magnitude of impact

>18,000 organisations

Affected information

Highly sensitive internal company information and classified government records

Attack vector

Supply chain attack

Significance

The SolarWinds supply chain attack was one of the most sophisticated cyber espionage campaigns of the last decade, compromising US federal agencies, Fortune 500 companies, security vendors, and many others. The attack was attributed to a Russian state-sponsored group (APT29/Cozy Bear) who gained access to SolarWinds' software development environment and inserted malicious code into updates of its Orion IT monitoring platform.

The compromised software was downloaded by around 18,000 customers, providing attackers with a covert entry point into the networks of some of the world's most sensitive government institutions, including the US Departments of Treasury, Commerce, and Homeland Security, as well as major global corporations.

The attack went undetected for months and was ultimately discovered by a private sector security firm investigating unrelated anomalies. Its success lay not only in the technical complexity of the supply chain compromise, but also in the attacker's stealth: once inside a victim network, they used legitimate credentials, minimal malware, and advanced operational security to avoid detection.

The SolarWinds incident exemplifies the systemic risk posed by software supply chains, and contributed to major reforms in both public and private sector cyber practices – including enhanced vendor and third party risk assessments, mandatory incident reporting (e.g. under the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**)), and greater scrutiny of remote access and software monitoring tools. It also helped accelerate the development of operational resilience frameworks, such as APRA's Prudential Standard CPS 230.

Affected entity or event

10. Colonial Pipeline

Date

2021

Attributed cause

Russian State-sponsored group

Magnitude of impact

Shutdown of critical infrastructure

Affected information

IT and operational technology (**OT**) systems

Attack vector

Compromised credentials, ransomware

Significance

The Colonial Pipeline ransomware attack was a watershed moment in critical infrastructure cyber security, causing the shutdown of the largest fuel pipeline in the US and sparking widespread fuel shortages across the its eastern seaboard. The attack, attributed to the criminal ransomware group DarkSide, used compromised credentials to gain access to Colonial's IT systems and deploy ransomware that encrypted key operational data.

Although the OT systems controlling pipeline flows were not directly compromised, Colonial shut them down pre-emptively to contain the attack – a decision that halted the flow of gasoline, diesel and jet fuel across 8,800 kilometres of pipeline. The resulting disruption caused panic buying and fuel shortages in multiple states, and prompted emergency measures from the US Federal Government.

Colonial Pipeline paid a ransom of US$4.4 million in Bitcoin to the attackers (although part of that payment was later recovered by the US Department of Justice).

The breach revealed critical gaps in infrastructure cyber resilience, including the lack of segmentation between IT and OT environments, and prompted major efforts (including in Australia) to improve incident reporting and enhance security standards for owners and operators of critical infrastructure assets.

Affected entity or event

11. LinkedIn

Date

2021

Attributed cause

Attribution complication; data offered for sale by hacker alias 'TomLiner'

Magnitude of impact

Up to 700 million users (approx. 92% of LinkedIn's user base at the time)

Affected information

Primarily publicly available profile data scraped at scale and potentially aggregated with data from other sources. Included: full names, email addresses, phone numbers, physical addresses, geo-location records, LinkedIn profile URLs, personal and professional backgrounds/ experience, gender, links to other social media accounts

Attack vector

Misuse of LinkedIn's API, resulting in data scraping

Significance

Although this large-scale exposure resulted from data scraping, and not a breach of internal systems, the incident highlighted significant risks associated with API security and the potential for mass harvesting of publicly available user information.

The aggregated dataset, containing details for the vast majority of LinkedIn users in 2021, was offered for sale on dark web forums – increasing the risk of sophisticated phishing campaigns, social engineering, identity theft attempts, and business email compromise (**BEC**) scams targeting affected individuals, even without password exposure.

LinkedIn confirmed that no private data (such as password data) was exposed, and took steps to halt the activity, including taking legal action against scraping entities.

The incident underscored the ongoing challenge platforms face in preventing large-scale scraping and the need for users to carefully manage the visibility of their public profile information.

Affected entity or event

12. Microsoft

Date

2021

Attributed cause

Chinese State-sponsored group

Magnitude of impact

Estimated 30,000 to 60,000 organisations

Affected information

Full access to compromised servers, enabling theft of entire email mailboxes, extraction of credentials stored in memory, deployment of web shells for persistent access, and potential lateral movement within victim networks

Attack vector

Exploitation of server-side request forgery (**SSRF**) and other vulnerabilities

Significance

This was a major global incident demonstrating the rapid, widespread exploitation of critical zero-day vulnerabilities in widely used enterprise software.

The attackers gained deep access, allowing extensive data theft and establishing backdoors before patches were available, leading to protracted cleanup and ongoing risk for compromised organisations. The incident prompted emergency patch releases from Microsoft and urgent warnings from cyber security agencies globally.

The incident underscored the importance of timely patching, robust monitoring, and network segmentation to limit the blast radius.

Affected entity or event

13. Change Healthcare

Date

2024

Attributed cause

ALPHV/ BlackCat ransomware group

Magnitude of impact

190 million individuals (over half of US population)

Affected information

Extensive personal (including sensitive) information including names, addresses, dates of birth, phone numbers, email addresses, Medicaid ID numbers, Medical record numbers, healthcare providers, diagnoses, medicines, test results, images, billing, claims, payment information, payment card details, financial and banking information, social security numbers, driver's licence or state ID numbers, and passport numbers.

Attack vector

Ransomware deployment following initial access via compromised credentials without MFA protection

Significance

This was a catastrophic cyber attack and the largest healthcare data breach in US history. It demonstrates the systemic risk and interdependence within the US healthcare IT infrastructure, with a single breach crippling core functions nationwide and threatening the financial viability of numerous healthcare providers.

The incident exposed critical security failures, notably the lack of MFA on a remote access portal at a systemically important entity.

Change Healthcare's parent company, UHG, confirmed that it had paid a US$22 million ransom, although complexities arose with the ransomware group's subsequent actions (with data potentially reappearing with another group).

The incident led to intense scrutiny from regulators and lawmakers, billions in recovery costs for UHG, and widespread calls for improved cyber security standards, third party risk management, and resiliency mandates across the healthcare sector.

Affected entity or event

14. National Public Data (a data broker operated by Jericho Pictures Inc)

Date

2024

Attributed cause

Malicious actor gaining unauthorised access to NPD systems.
Data later leaked by hacker group 'USDoD'.

Magnitude of impact

~2.9 billion records exposed, potentially affected up to 170 million individuals across the US, UK and Canada

Affected information

Names, social security numbers, current and past addresses (spanning decades), dates of birth, phone numbers, email addresses and personal information on relatives

Attack vector

Unauthorised access to and exfiltration of data

Significance

This 2024 data breach involving NPD, a US-based data broker, highlighted ongoing concerns surrounding the data brokerage and aggregation industry. The incident resulted in unauthorised access to a substantial volume of personal information, including social security numbers and historical address records covering a significant portion of the US population.

The breach raised questions about security practices in the sector, particularly in relation to the collection and storage of large-scale personal information. NPD and its parent company subsequently faced multiple class action lawsuits, filed for bankruptcy in October 2024, and ceased operations in December 2024.

12 major Australian data breaches over the past 10 years

Affected entity or event

01. Australian Red Cross

Date

2016

Attributed cause

N/A (human error)

Magnitude of impact

~550,000 prospective blood donors

Affected information

Names, contact details (address, email, phone), date of birth, gender, blood type, donor ID, appointment details, and answers to sensitive donor eligibility questions

Attack vector

Human error

Significance

This data breach was not deliberate. An employee of a third party provider to the Red Cross inadvertently saved a database backup file onto a publicly accessible part of a web server during development and testing. The breach was discovered by an external security researcher scanning the internet.

Although not intentional, this incident highlighted the risks associated with third party vendor management and security practices, and demonstrated the potential for accidental exposure of large volumes of health and other sensitive health information through simple human error in IT processes.

The incident also showcased a rapid and effective incident response by the Australian Red Cross, including prompt notification to the public, well managed support channels, and cooperation with the security researcher, all of which, according to the OAIC investigation, mitigated harm and meant adverse consequences for individuals were less likely.

Affected entity or event

02. PEXA and affected conveyancers

Date

2018

Attributed cause

Unconfirmed (likely cybercriminals using phishing)

Magnitude of impact

Multiple property sellers

Affected information

Property settlement funds

Attack vector

Phishing

Significance

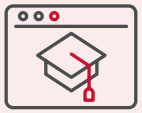
A phishing attack on the PEXA e-conveyancing platform led to property settlement funds being diverted to a fraudulent bank account.

The incident exposed vulnerabilities in the e-conveyancing ecosystem, specifically related to the security practices (email security, credential management) of practitioners using the platform, and raised concerns about the security of high-value digital property transactions.

It prompted PEXA to enhance security measures and introduce the PEXA Residential Seller Guarantee (offering financial protection for sellers against specific types of fraud occurring within the platform) and the PEXA Key app for secure communication of bank details, both of which aimed to restore confidence with the platform.

Affected entity or event

03. Australian National University (ANU)



Date

2018

Attributed cause

Unconfirmed (sophisticated actor suspected, likely State-sponsored)

Magnitude of impact

200,000 affected staff, students and visitors, with the data spanning 19 years

Affected information

Extensive personal information, including names, addresses, dates of birth, phone numbers, personal emails, emergency contacts, tax file numbers, bank account and other payroll details, passport details, student academic records

Attack vector

Advanced spear phishing attack

Significance

This was one of Australia's most significant university breaches, impacting a high-profile national institution, and demonstrated the capabilities of sophisticated threat actors to achieve deep, persistent access and steal vast quantities of data.

It highlighted the cyber security challenges faced by large, complex university environments, and led to a major investment to uplift cyber security practices at ANU, as well as closer scrutiny of its data retention practices.

Affected entity or event

04. Multiple Victorian regional public hospitals and health services

(Gippsland Health Alliance, South West Alliance of Rural Health)

Date

2019

Attributed cause

Unconfirmed (ransomware operators)

Magnitude of impact

Disruption to multiple hospitals and health services across regional Victoria. Specific patient number impact not publicly detailed, but involved critical systems

Affected information

Some patient data was potentially accessed or exfiltrated, though the primary impact was operational disruption

Attack vector

Ransomware

Significance

This ransomware attack demonstrated how vulnerable critical regional healthcare infrastructure can be to disruptive ransomware attacks. It caused significant operational impacts, forcing hospitals to disconnect systems, revert to manual processes, and delay patient care and services.

The incident occurred shortly after the release of an Auditor-General report highlighting cyber security weaknesses in the Victorian public health system, including insufficient staff awareness of cyber security issues.

Affected entity or event

05. ProctorU

Date

2020

Attributed cause

Unconfirmed (data posted on dark web forum)

Magnitude of impact

444,000 user records, including students from multiple universities

Affected information

Names, usernames, email addresses, physical addresses, phone numbers and hashed passwords

Attack vector

Unclear

Significance

ProctorU, an online proctoring service, suffered a data breach impacting numerous university students using its widely adopted service, particularly during the COVID-19 pandemic.

The incident highlighted cyber security and privacy risks associated with third party vendors, including those handling student data.

Affected entity or event

06. Ambulance Tasmania

Date

2021

Attributed cause

Unconfirmed individuals intercepting radio communications

Magnitude of impact

Unspecified, but impacted individuals who requested ambulance services between November 2020 and January 2021

Affected information

Sensitive information transmitted via the radio network, including names, age, gender, address of incident, medical conditions (e.g. HIV status)

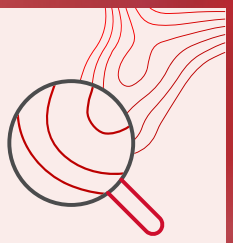
Attack vector

Interception of unencrypted data

Significance

The incident exposed a critical privacy failure resulting from the use of outdated, unencrypted communication technology for transmitting highly sensitive patient information in an emergency services context.

It highlighted the urgent need for modernisation and enhanced security in critical telecommunications infrastructure.



Affected entity or event

07. Optus

Date

2022

Attributed cause

Unconfirmed

Magnitude of impact

2.5 to 9.7 million records

Affected information

Names, birth dates, phone numbers, email addresses, physical addresses; and for a subset of individuals, identity documents (driver's licences, passports and Medicare numbers)

Attack vector

Unsecured API endpoint connected to a customer identity database

Significance

This was one of Australia's largest ever data breaches, impacting a significant portion of the population.

It triggered significant consequences, including costly remediation efforts (such as identity document replacement), regulatory investigations by the OAIC and ACMA, class action lawsuits, and reputational damage repair.

It also acted as a major catalyst for Australian government action, including significantly increased penalties under the Privacy Act and a heightened focus on critical infrastructure cyber security (see page 52).

Affected entity or event

08. Medibank

Date

2022

Attributed cause

Russian hacking group REvil

Magnitude of impact

9.7 million current and former customers

Affected information

Extensive personal information (names, dates of birth, Medicare numbers, passport numbers for some) and sensitive information (claims data, including medical service provider details, diagnosis and procedure codes)

Attack vector

Stolen high-privilege credentials (reportedly lacking MFA)

Significance

After gaining initial access to Medicare's systems using stolen high-privilege credentials, the attacker dwelled in the network, exfiltrating large amounts of data before deploying ransomware (though encryption wasn't the primary lever). The attacker demanded A$10 million in ransom, which Medibank refused to pay, resulting in the data being leaked on to the dark web.

The incident is widely regarded as one of the most damaging cyber attacks in Australian history, given the scale and sensitivity of the health data compromised. It underscored the risks associated with credential theft, the absence of MFA, and insufficient network monitoring and segmentation.

The attack also raised difficult ethical questions about ransom payments in the context of cyber extortion, caused significant distress to affected Medibank customers and prompted multiple class actions.

It led to a major regulatory response, including an investigation by the OAIC, and civil penalty proceedings commenced in the Federal Court, alleging that Medibank failed to take reasonable steps to protect personal information.

Notably, it also marked the first invocation of Australia's cyber sanctions regime against an individual hacker.

Affected entity or event

09. Australian Clinical Labs

Date

2022

Attributed cause

Quantum ransomware group

Magnitude of impact

~223,000 individuals

Affected information

Mix of personal information (names), health information (medical records, pathology results), identity information (Medicare numbers), and financial information (credit card numbers, some with CVVs)

Attack vector

Unknown

Significance

The Australian Clinical Labs (**ACL**) breach marked another significant incident within the healthcare sector, involving the compromise of highly sensitive patient information, including pathology results and financial data. Approximately 86GB of personal data was ultimately published on the dark web.

The incident underscored the difficulties organisations face in detecting and responding to data exfiltration in the context of ransomware attacks. It also raised concerns about the timeliness of both internal investigations and external notifications, particularly given the sensitive nature of the data involved.

The breach prompted an investigation by the OAIC, focusing on whether ACL took reasonable steps to secure personal information and whether it complied with the assessment and disclosure timeframes under the notifiable data breaches (**NDB**) regime.

Affected entity or event

10. Latitude Financial

Date

2023

Attributed cause

Unconfirmed

Magnitude of impact

~14 million current and former customers

Affected information

Primarily identity documents: ~7.9 million Australian and NZ driver licence numbers (mostly provided since 2013), ~53,000 passport numbers. Also included ~6.1 million records (dating back to at least 2005) containing names, addresses, phone numbers and dates of birth. A smaller subset had financial statements exposed

Attack vector

Stolen employee credentials

Significance

The breach – one of Australia's largest by number of individuals – originated through the compromise of a third party vendor, again highlighting the risks associated with supply chain vulnerabilities.

The incident affected a significant volume of historical customer records, some dating back more than a decade, raising questions about Latitude's data retention practices, including whether the long-term storage of personal information was necessary or consistent with data minimisation obligations under Australian privacy law.

The breach prompted multiple class action investigations, and triggered an ongoing investigation by the OAIC, focusing on the adequacy of Latitude's security measures and its compliance with the Privacy Act, including obligations to take reasonable steps to protect personal information, and to delete or deidentify data when no longer required.

Affected entity or event

11. HWL Ebsworth

Date

2023

Attributed cause

ALPHV/ BlackCat ransomware group

Magnitude of impact

Data stolen relating to over 65 government agencies, as well as corporate and individual clients

Affected information

A mix of legal files, personal information, corporate and government records, including sensitive information associated with Commonwealth departments, state agencies, regulators, and private sector clients

Attack vector

Unknown

Significance

After breaching the legal firm's systems, the ALPHV/ BlackCat ransomware group exfiltrated and published over 1.4 terabytes of data on the dark web.

The breach highlighted both the criticality of legal service providers in sensitive information ecosystems and the cascading risks to public and private sector clients from a single compromise.

The incident also reinforced the importance of rigorous third party and professional services supply chain oversight, especially where privileged, sensitive or classified material is at risk.

HWL Ebsworth undertook extensive forensic investigation and client notification efforts, and was subject to scrutiny by the OAIC and other federal agencies regarding its response and security controls.

Affected entity or event

12. MediSecure

Date

2024

Attributed cause

Unidentified cybercriminal group (ransomware)

Magnitude of impact

Up to 12.9 million individuals

Affected information

Historical electronic prescription information, including patient names, addresses, dates of birth, phone numbers, Medicare numbers, healthcare identifiers, and specific prescription details (medication, dosage, date, prescribing doctor)

Attack vector

Unknown

Significance

The MediSecure incident highlighted the risks associated with the long-term storage of sensitive health data. The breach involved historical prescription and health-related information, raising broader questions about data minimisation, legacy system security, and the justification for retaining sensitive information over extended periods of time.

The financial and operational impacts were immediate and severe: MediSecure was unable to meet the considerable costs of breach containment, forensic investigation, legal compliance, and stakeholder communication – ultimately entering voluntary administration shortly after the incident.

The incident triggered a national response due to the sensitivity of the health information involved and its implications for trust in the Australian healthcare system. Multiple federal agencies, including the National Cyber Security Coordinator (**NCSC**), Australian Signals Directorate (**ASD**) and Australian Federal Police (**AFP**) were engaged to support incident response efforts and assess potential systemic risks within the broader health data supply chain.

B

Cyber risk survey 2025 highlights

Introduction

For the tenth consecutive year, MinterEllison has surveyed Australian business leaders, C-suite executives, directors, legal counsel, and risk managers to capture their perspectives on the evolving cyber risk landscape.

Conducted in February and March 2025, this year's survey not only provides a snapshot of current organisational sentiment and practices, but also informs reflections on a decade of profound digital transformation, geopolitical shifts, and regulatory evolution.

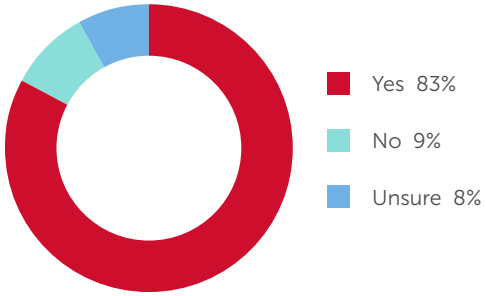
For Australian organisations and leaders, cyber risk now sits at the intersection of national security, regulatory scrutiny, and operational resilience.

The Russia-Ukraine war has shown how cyber operations can be weaponised alongside conventional conflict – a reality mirrored in China's sustained cyber espionage targeting Australia's government, education and critical infrastructure sectors. These are not isolated threats but part of a broader strategic contest, where data, systems and trust are all targets. Boards are increasingly expected to navigate this complexity – making decisions not just about protection, but about cyber resilience in the face of persistent, state-linked adversaries and a rapidly hardening global regulatory environment.

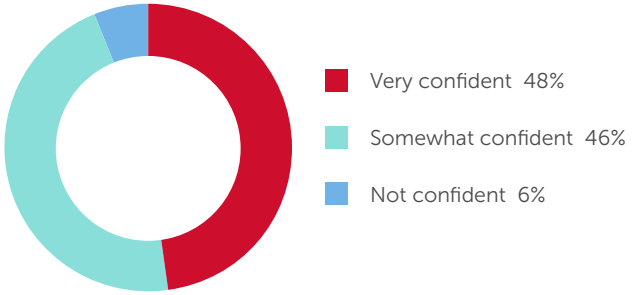
This report section presents the key findings from our 2025 survey, situating them within the context of the past decade and incorporating insights from the evolving cyber security landscape.

Survey highlights 2025

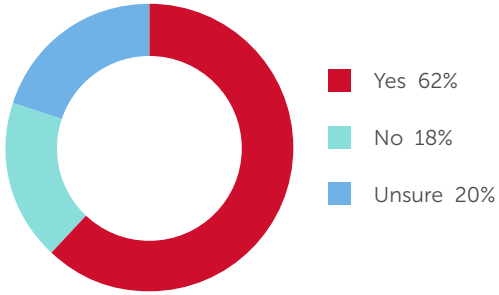
Does your organisation measure its cyber maturity against an established framework?



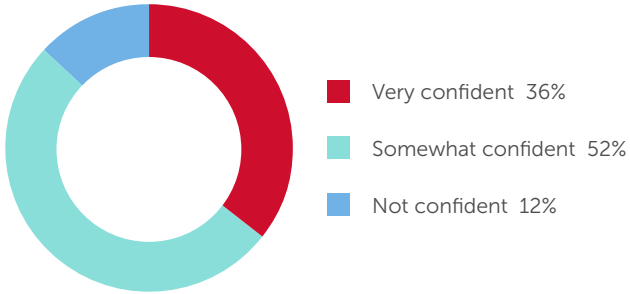
How confident are you that your organisation understands its regulatory and contractual obligations in the event of a cyber attack or data breach?



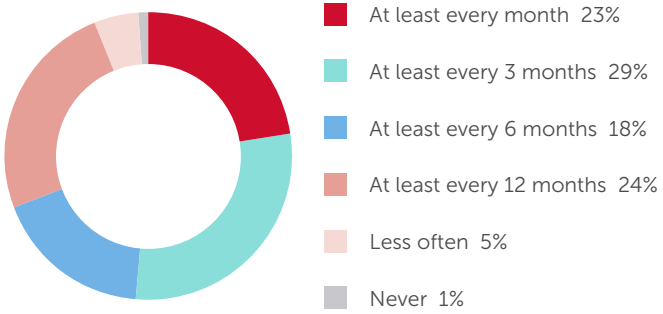
Is your organisation sufficiently staffed to monitor and manage cyber security needs effectively?



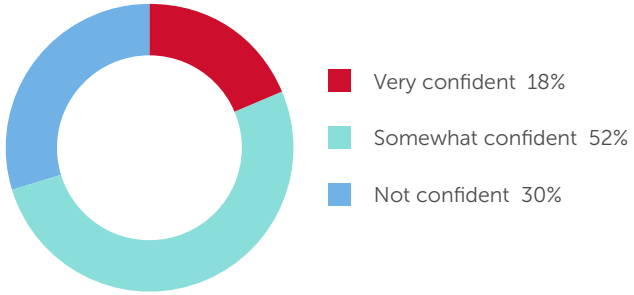
How confident are you that your organisation knows what data it stores, where it is stored, what controls protect it and who has access to it?



How often does your organisation conduct staff training or awareness activities on cyber risks?



How confident are you that your organisation is prepared to adopt emerging AI platforms, such as generative AI?



Key findings and decade-long trends

1. Cyber risk: from emergent threat to enduring top-tier priority

The most striking trend over the past decade is the dramatic elevation of cyber risk within organisational priorities.

2025 finding: **76% of respondents** now rank cyber risk as a "high risk" (within their top 5) on their corporate risk register.

Decade trend: In 2015, only **29%** of surveyed organisations believed cyber was a top-tier risk. The near tripling of this figure highlights the rapid escalation of digital threats. This increase aligns with the growing frequency, cost and visibility of cyber incidents, further accelerated by high-profile Australian breaches including **Optus**, **Medibank** and **Latitude**. Cyber security has become a major boardroom concern.

Insights: While cyber risk is now firmly on the Board agenda, awareness does not readily translate into action. Multiple studies highlight a persistent gap between Board engagement on cyber issues and cyber literacy. For example, an analysis by Diligent and NightDragon in 2023 found that only **12% of S&P 500 companies** had a Board member with specialised cyber security expertise. It's unsurprising then that the 2024 What Directors Think survey found that **35% of directors** cited cyber security as one of the biggest challenges to oversee.

The picture is even bleaker in Australia: a 2022 study of **ASX 100 companies** revealed that fewer than **2% of non-executive directors** had a background in cyber security. However, CISOs are gaining greater visibility. According to Splunk's 2025 CISO Report, **83% of CISOs now regularly present to the Board**. Juxtaposed, these figures reveal a critical disconnect: CISOs are being seen, but not necessarily heard. Without deeper cyber education and capability at Board level, organisations risk overestimating their resilience, underinvesting in uplift, or misjudging regulatory exposure.

ASIC's enforcement actions in **RI Advice Group** (see page 37) and **FIIG Securities** (see page 39), and the impending commencement of APRA's CPS 230 framework, clearly indicate that directors are expected to not only oversee cyber risk – but to do so with genuine competence and accountability.

76% **of respondents** now rank cyber risk as a "high risk" (within their top 5) on their corporate risk register.

29% **of surveyed organisations** in 2015 believed cyber was a top-tier risk. The near tripling of this figure highlights the rapid escalation of digital threats.

but only 12% of S&P 500 companies had a Board member with specialised cyber security expertise.

35% **of directors** cited cyber security as one of the biggest challenges to oversee.

fewer than 2% of non-executive ASX 100 directors had a background in cyber security.

83% **of CISOs** now regularly present to the Board.

2. Data governance: a persistent blind spot

Despite a decade of heightened breach activity, regulatory pressure, and organisational investment in cyber capabilities, confidence in basic data governance remains unacceptably low.

2025 finding: Only **36%** of respondents say they are "very confident" that their organisation knows exactly what data it holds, where it resides, and how it is secured.

Decade trend: This figure has barely moved over recent years – in fact, in 2024 the stats were the same – and pointing to enduring structural shortcomings. Despite the ongoing focus on addressing cyber threats, many organisations continue to struggle with fundamental cyber security hygiene measures such as data mapping, visibility, and access control.

Insights: Weak data governance remains one of the most significant barriers to cyber resilience in Australia. It complicates breach response, frustrates compliance efforts, and increases the blast radius of any incident.

High-profile global breaches offer stark reminders:

- the 2017 **Equifax** incident exploited a known but unpatched vulnerability – yet its impact was amplified by poor data segmentation and access controls, enabling the exfiltration of data on 147 million individuals;
- the 2019 **Capital One** breach compromised over 100 million customer records due to a misconfigured firewall and inadequate cloud protections; and
- **Facebook's Cambridge Analytica** scandal in 2018, though not a technical breach, revealed how permissive platform settings and lax oversight allowed third party access to tens of millions of user profiles without informed consent.

Closer to home, recent Australian breaches have raised similar concerns – whereby cyberattackers accessed and exfiltrated identity documents and other personal information that, in many cases, appeared to have been retained beyond necessity.

While APP 11.3 already requires entities to take reasonable steps to destroy or de-identify personal information when no longer needed, the OAIC's recent post-incident regulatory responses suggest an enhanced enforcement focus on retention and disposal practices. This trend aligns with the **second tranche** of proposed Privacy Act reforms, which the government has confirmed will enshrine **data minimisation**, **purpose limitation**, and **enhanced organisational accountability** as core statutory principles.

Closing the governance gap, however, requires more than just policy updates. It demands investment in enterprise-wide data mapping, system architecture that supports secure access and automated deletion, ongoing monitoring, and a culture of accountability. Without those foundations, even the most sophisticated cyber security controls risk being built on sand.

only 36% of respondents say they are "very confident" that their organisation knows exactly what data it holds, where it resides, and how it is secured.

3. Beyond the plan: building response readiness

Organisations have made clear strides in incident response planning over the past decade. But having a plan is not the same as being ready. True cyber resilience demands more than documentation – it requires rehearsed, cross-functional capability. On this front, many organisations continue to fall short.

Respondents reporting adoption of response plans

42% in 2016

91% in 2025

Respondents reporting incident plan testing

34% in 2017

70% in 2025

2025 finding: While **91%** of organisations report having a cyber security incident response plan, only **70%** regularly test or rehearse it at least annually. Our results revealed, however, that **83%** formally assess their cyber maturity against an established framework such as the NIST Cyber security Framework or the ASD Essential Eight, which is promising.

Decade trend: While there is still some way to go, these numbers represent significant progress. The adoption of response plans has steadily increased over the past decade – from just **42%** in 2016, to **54%** by 2017, and reaching **91%** in 2025. Testing has also become more widespread: only **34%** of organisations reported regular incident plan testing in 2017, compared with **70%** in 2025.

Insights: Despite the widespread adoption of response plans, many organisations remain underprepared. Only **70%** of this year's survey respondents reported that they regularly test their incident plans. This is echoed by ASIC's 2023 Cyber Pulse Survey, which reported a weighted average maturity score of just **1.66 out of 4** – placing most organisations in the early, reactive stages of capability.

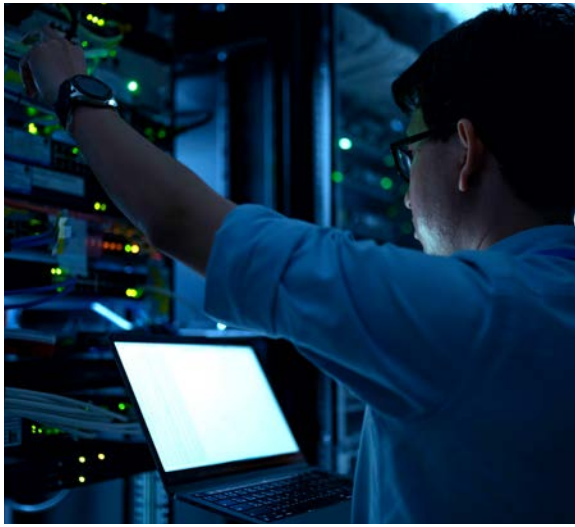
Moreover, while annual testing is a solid foundational component, effective preparedness also requires realistic, scenario-based simulations. The most resilient organisations involve legal, communications, senior leadership, and business continuity in their exercises – not just IT or security.

The regulatory consequences of poor incident readiness are becoming increasingly severe. Following its 2022 cyber incident, **Medibank** was subjected to intense scrutiny by APRA, which imposed a A$250 million increase to its capital adequacy requirement. This mandated uplift reflected deficiencies in Medibank's information security and broader risk management practices – particularly its inability to detect and contain the breach before attackers exfiltrated sensitive customer health data.

While 91% of organisations report having a cyber security incident response plan

only 70% regularly test or rehearse it at least annually.

and 83% formally assess their cyber maturity against an established framework



A parallel example is ASIC's enforcement action against **RI Advice Group**, which followed multiple breaches across its authorised representative network. In that case, the Federal Court found that RI Advice had failed to implement adequate cyber security controls – including incident detection and response processes – in breach of its obligations under the *Corporations Act 2001* (Cth) (**Corporations Act**). The Court's decision reinforced that failure to maintain cyber resilience may constitute a breach of financial services licence conditions and expose directors to potential liability.

More broadly, both **APRA** and **ASIC** have emphasised the importance of embedding cyber resilience at the governance level. APRA has called for regular, scenario-based testing that involves Boards and executives, warning against 'set-and-forget' approaches where response plans are treated as compliance artefacts rather than dynamic capabilities.

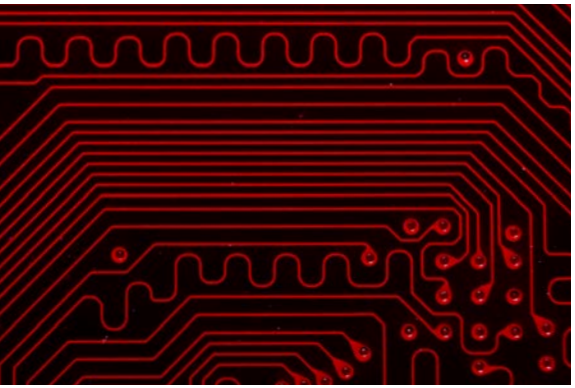
ASIC's growing use of enforcement powers – most recently in its 2025 civil penalty proceedings against **FIIG Securities** – reinforces that cyber risk management is a legal obligation, not a discretionary best practice.

Meanwhile, attackers are accelerating their pace. CrowdStrike reports an average breakout time of **48 minutes**, with the fastest observed to date being **51 seconds**. In such a short window, vague plans and unclear decision-making leave no room for error.

Organisations must treat incident response as an agile process – continuously tested, measured, and improved. In today's threat environment, a well-practised response is not just good hygiene – it's the difference between containment and crisis.

4. Regulatory compliance: a widening gap between expectation and readiness

Despite many years of high profile cyber incidents and an ever expanding regulatory landscape, many organisations remain ill-prepared to meet their legal obligations in the aftermath of a breach. Confidence levels have flatlined, suggesting that regulatory change is outpacing organisational readiness.



2025 finding: **52%** of survey respondents report being only "somewhat confident" or "not confident" in their organisation's ability to meet regulatory and notification obligations after a cyber incident.

Decade trend: This figure has shown little movement over recent years, pointing to a persistent disconnect between the increasing complexity of regulatory requirements and the maturity of operational compliance capabilities. Even as cyber risk has climbed corporate risk registers, too few organisations appear to have embedded compliance into their incident response functions.

Insights: The regulatory consequences of cyber incidents are intensifying. Over the past decade, Australian organisations have become subject to a growing matrix of breach reporting and legal obligations, including:

52%

of respondents report being only "somewhat confident" or "not confident" in their organisation's ability to meet regulatory and notification obligations after a cyber incident.

- mandatory notification of eligible data breaches to the OAIC and affected individuals under the Privacy Act;
- **Prudential Standards CPS 234** and **CPS 230**, which together impose strengthened requirements on APRA-regulated entities. **CPS 234** requires the timely reporting of material information security incidents (within 72 hours), while **CPS 230** – taking effect from July 2025 – introduces broad operational risk management obligations, including requirements for incident response planning, scenario testing, and assurance over material service providers;
- the SOCI Act, which imposes dual-layer reporting for cyber incidents affecting critical infrastructure (within 12 and 72 hours, depending on severity);
- State-based regimes, such as the ***Privacy and Personal Information Protection Act 1998*** **(NSW)**, ***Privacy and Data Protection Act 2014*** **(Vic)**, and the forthcoming ***Privacy and Responsible Information Sharing Act 2024*** **(WA)**, all of which include data breach notification obligations;
- the ***Cyber Security Act 2024*** **(Cth)** (**Cyber Security Act**), which introduces ransomware payment reporting requirements for large businesses and critical infrastructure entities from May 2025;
- the **ASX Listing Rules**, which may require immediate disclosure of price-sensitive cyber incidents under continuous disclosure obligations;
- the ***My Health Records Act 2012*** (**Cth**), which imposes mandatory data breach notification obligations on organisations, registered repository and portal operators, and contracted service providers, in connection with the handling of My Health Record data; and
- for some Australian organisations, the **General Data Protection Regulation (GDPR)**, which applies extraterritorially to organisations that offer goods or services to, or monitor the behaviour of, individuals in the EU. The GDPR imposes strict breach notification obligations, requiring controllers to notify supervisory authorities within 72 hours of becoming aware of a personal data breach that is likely to result in a risk to individuals' rights and freedoms.

In March 2025, ASIC initiated its second-ever cyber security enforcement action, filing proceedings in the Federal Court against FIIG Securities Limited, a fixed-income broker and Australian Financial Services (AFS) licensee.

ASIC alleges that between March 2019 and June 2023, FIIG failed to implement adequate cyber security risk management systems (including properly managed and configured firewalls, timely software patching, mandatory cyber-security training, and sufficient resource allocation), leading to a significant data breach.

The breach, which went undetected for nearly three weeks, and resulted in the theft of approximately 385GB of confidential data, affecting around 18,000 clients.

The compromised information included driver's licences, passports, bank account details, and tax file numbers.

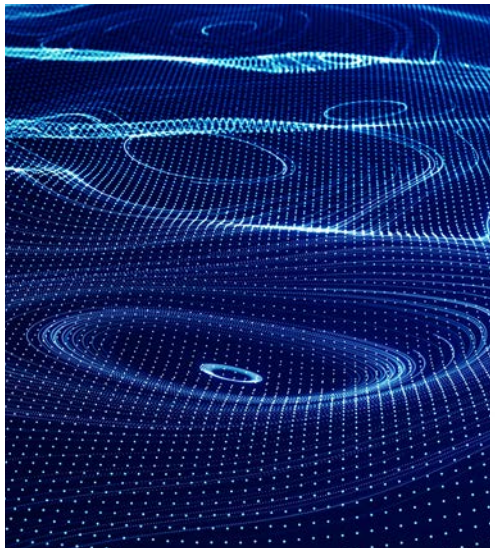
ASIC is seeking declarations of contraventions, civil penalties, and compliance orders.

These obligations sit alongside an increasingly assertive enforcement posture:

- **ASIC** has reinforced that cyber risk is governance risk. In **RI Advice Group** (2022) and **FIIG Securities** (2025), it brought proceedings against licensees for failing to implement adequate cyber controls – raising implications for both organisational systems and directors' duties under the Corporations Act.
- The OAIC has escalated its enforcement approach, launching civil penalty proceedings (**Meta**, **Medibank** and **Australian Clinical Labs**), and issuing determinations against entities such as **Pacific Lutheran College** and **Datateks** for failing to assess, notify or respond to breaches appropriately.
- The newly established **Cyber Incident Review Board (CIRB)** under the Cyber Security Act will conduct post-incident reviews of significant cyber events. While it does not wield enforcement powers, its published findings and recommendations are expected to shape regulatory expectations and boardroom practice over time.

These developments signal a structural shift: cyber compliance is no longer limited to privacy legislation – it now intersects with corporate governance, financial regulation, critical infrastructure obligations, and national security law. For many organisations, particularly those in highly regulated sectors, the regulatory stakes have never been higher.

In this context, confidence gaps are not a minor weakness – they are a material risk. Organisations that aren't adequately prepared may face delayed or inaccurate notifications, regulatory scrutiny, public criticism, litigation (including under the proposed statutory tort for serious invasions of privacy), and reputational fallout that lingers long after the event.



To close the readiness gap, compliance must be operationalised – not siloed. That means:

- embedding legal and regulatory response procedures into cyber incident plans;
- mapping obligations across overlapping regimes, and clearly assigning internal accountability for each;
- training legal, executive and communications teams on evolving requirements and regulator expectations; and
- testing breach reporting and decision-making processes regularly through cross-functional simulation exercises.

As regulatory expectations rise, so too does the cost of getting it wrong. The real test is no longer whether an organisation has the right policies, but whether it can act swiftly, lawfully and confidently under pressure – all while engaging its stakeholders and protecting its brand.

5. The supply chain: acknowledged risk, persistent vulnerability

Supply chain security has emerged as one of the most enduring and complex challenges in cyber risk management. As digital ecosystems become ever more interconnected and reliant on third party services, the vulnerability of those providers increasingly becomes the organisation's own.

2025 finding: **50%** of survey respondents reported that a third party supplier or vendor in their supply chain had suffered a cyber attack or data breach in the past year. This aligns with global trends – Panorays reports that **91%** of CISOs observed a rise in third party incidents.

Respondents reporting breach affecting third-party supplier

50%

This figure is consistent with global data.

Decade trend: While the number of direct attacks on organisations has fluctuated, third party compromises have remained a constant vector. High profile incidents such as the SolarWinds compromise and the Latitude Financial breach have exposed the systemic and reputational risks associated with embedded vendor relationships.

Insights: Despite growing awareness, deep visibility into the supply chain remains elusive. Global research suggests only **3%** of CISOs claim full visibility into their vendor ecosystems. In Australia, Boards are being urged to take a more proactive oversight role – including ensuring contracts contain clear cyber security obligations, audit rights, and breach notification terms.

The regulatory stakes have risen accordingly. APRA's CPS 234 requires regulated entities to ensure that information assets managed by third parties are subject to the same standard of protection as those managed internally. Under CPS 230, effective from July 2025, APRA expects entities to maintain comprehensive registers of material service providers, conduct rigorous due diligence, and implement assurance mechanisms such as scenario testing and termination plans.

Meanwhile, under the Privacy Act, organisations remain responsible for the acts and omissions of overseas vendors handling personal information, unless specific exceptions apply. The OAIC has emphasised that regulated entities should not treat third party breaches as out-of-scope, and expects prompt assessment, notification, and remediation regardless of whether the incident occurred within the organisation's direct control.

Breach case studies – including SolarWinds, Latitude Financial, the Australian Red Cross and HWL Ebsworth – demonstrate the multifaceted consequences of supplier exposures, ranging from operational disruption and legal exposure to reputational damage and regulatory action.

Closing the supply chain exposure gap requires more than due diligence at onboarding. It demands ongoing risk governance, including:

- maintaining up-to-date registers of material third party service providers;
- conducting periodic security audits or requesting external assurance reports (e.g. SOC 2, ISO 27001);
- embedding clear cyber security obligations, reporting requirements, and audit rights into contracts;
- requiring timely incident notification and response coordination provisions; and
- including third party breach scenarios in tabletop exercises and business continuity testing.

As regulatory scrutiny intensifies and attacker tactics evolve, supply chain risk must be treated as a first order cyber threat – and not a peripheral concern. Visibility, control, and accountability cannot stop at the organisation's perimeter. Boards and executives must demand assurance that critical vendors are not only contractually bound, but operationally capable of meeting heightened cyber security expectations. In an ecosystem defined by interdependence, complexity, and cascading consequences, trust in suppliers is no substitute for rigorous oversight.

6. Artificial intelligence: rising optimism tempered by risk awareness

GenAI has rapidly moved from being in the margins to becoming mainstream – transforming how organisations think about both opportunity and risk. While confidence in adopting AI is growing rapidly, so too is recognition of the importance of its security, privacy, and governance challenges.

2025 finding: **70%** of survey respondents report being at least "somewhat confident" in their organisation's preparedness to adopt GenAI platforms. However, **84%** cite privacy risks – particularly data compromise – as their top concern, followed closely by cyber security risks, such as attacks on or manipulation of AI systems.

Decade trend: These figures represent a dramatic shift from **2018**, when fewer than **15%** of respondents reported any active use of AI solutions. Adoption has grown rapidly, driven by advances in Large Language Models (**LLMs**), increased commercial availability, and a broadening array of use cases across sectors.

Insight: While organisations are optimistic about AI's potential to improve efficiency, enable insight, and enhance threat detection, they are equally alert to its darker side. AI is now both a security tool and a security target.

External research underscores this duality. According to CrowdStrike, threat actors in 2024 used GenAI to assist in developing phishing emails, fake personas, and even attempted malware design. Splunk reports that over half of CISOs now believe AI gives attackers an edge, citing concerns about highly realistic deepfakes, AI-crafted social engineering, and scalable attack automation.

Even well-intentioned AI use can amplify risk: AI models may inadvertently memorise or leak training data, propagate bias, or be manipulated through prompt injection and adversarial machine learning. As discussed in last year's report, technical debt, legacy infrastructure, and inadequate testing have further complicated secure deployment.

Regulators are responding at pace. The **EU AI Act**, discussed on page 46, is currently the most comprehensive framework globally, imposing mandatory risk assessments, security testing, and governance controls for high-risk AI systems. In Australia, regulatory discussions are accelerating, with increasing calls for AI-specific obligations around transparency, accountability, and safe design – potentially as an extension of existing privacy and consumer protection regimes.

Internally, organisations are starting to move from experimentation to organised structure. According to Splunk, 65% of CISOs are now training security teams in prompt engineering, and 56% are establishing policies to define which tasks are appropriate for AI tools – as opposed to which should remain human-led. The emerging best practice is clear: a **security-first posture** that embeds AI security throughout the design, development, and deployment lifecycle.

Culture and clear roles and responsibilities remain as important as code. Effective AI governance requires not only technical guardrails, but also shared accountability, cross-functional input (including legal, risk, and ethics teams), and proactive engagement with regulators, peers, and standards bodies. In this rapidly evolving field, no organisation has all the answers – and those that **learn, adapt and collaborate** will be best placed to reap AI's benefits while managing its unprecedented risks.

70%
of respondents
report being at least "somewhat confident" in their organisation's preparedness to adopt GenAI platforms.

84%
of respondents
cite privacy risks – particularly data compromise – as their top concern

Final word: navigating a decade of cyber risk

Over the past decade, cyber risk has evolved from an emerging concern to a defining feature of organisational resilience. This year's survey results affirm this trajectory, while also highlighting areas where momentum is still lacking.

Data governance remains a structural weakness. Incident readiness is uneven. Regulatory obligations are outpacing preparedness.

Third party risk is growing in scale and complexity. And GenAI is both amplifying opportunity and compounding threat.

What's clear is that cyber is no longer a discrete technical domain. It is a strategic, operational and legal imperative – one that Boards, executives and risk leaders must engage with directly, confidently, and continuously. Closing the capability gap requires more than awareness.

It demands action: embedding security into architecture and accountability into leadership. The organisations that make this shift will not only be best placed to weather the risks ahead – they'll help set the standard for resilience in the decade to come.

C

A decade of rapid regulatory change

Introduction

Few areas of law have evolved as rapidly or expansively over the past decade as **privacy**, **data protection** and **cyber security**.

In Australia and abroad, governments and regulators have responded to escalating cyber threats, transformative technologies, and shifting public expectations, by enacting increasingly complex and far-reaching legal frameworks.

Through a combination of omnibus and sector-specific measures, jurisdictions worldwide have sought to regulate matters such as online privacy, online safety, critical infrastructure, AI, automated decision making, consumer data rights, children's privacy, and mandatory cyber incident reporting.

As Australia edges closer to the most significant overhaul of its privacy laws in decades, and enforcement appetite strengthens across multiple regulators, organisations must grapple not only with what compliance means today, but how best to position themselves for a more regulated – and more accountable – future.

In this report section, we examine key regulatory developments in Australia and internationally over the past ten years, and share some insights on what may lie ahead.

Around the (global) grounds

The global trajectory of data, privacy and cyber security regulation over the past decade is a study in both convergence and complexity, as jurisdictions respond to shared risks but within diverse legal, cultural and political frameworks.

The United Nations Conference on Trade and Development's (UNCTAD) Global Cyberlaw Tracker offers a useful snapshot of this evolution:[2]

- in 2015, **55%** of member states had enacted some form of data protection and privacy legislation. By late 2021, that figure had increased to **71%**, with a further **9%** considering draft legislation;
- similarly, in 2015 **71%** of member states had some form of cybercrime legislation. By late 2021, this had increased to **80%**, with another **5%** considering draft laws.

These numbers have likely continued to climb in recent years, as jurisdictions have progressed these draft laws.

Against this backdrop of global regulatory reform, we've highlighted 10 key regulatory developments from the past decade. Each represents a milestone – whether for setting international trends, influencing the adoption of similar laws in other jurisdictions, or marking a significant turning point in their own domestic legal landscape.

1. General Data Protection Regulation

Regulation EU (2016/679)

When: Adopted 27 April 2016, enforceable 25 May 2018
Where: European Union (**EU**)
What: The *General Data Protection Regulation* (**GDPR**) marked a transformative moment in global privacy regulation, replacing a patchwork of national data protection laws across EU member states with a single, harmonised legal framework. GDPR is widely regarded as the 'gold standard' for privacy legislation, introducing several landmark features:

- **extra-territorial reach**, in some cases, applying to organisations outside the EU that process the personal data of EU residents;
- **expanded individual rights**, such as the right to erasure (the 'right to be forgotten'), the right to data portability, and enhanced consent requirements; and
- **significant enforcement powers**, with penalties of up to €20 million or **4%** of global annual turnover, whichever is higher.

Its global influence cannot be overstated: the GDPR has shaped the direction of privacy law reform in jurisdictions around the world, including Australia, and continues to serve as a benchmark for legislative design and regulatory expectations.

[2] UNCTAD, 'Global CyberLaw Tracker' (18 February 2025); see also: UNCTAD, 'Data and privacy unprotected in one third of countries, despite progress' (29 April 2020)

2. Artificial Intelligence Act

(Regulation EU 2024/1689)

When: Adopted 21 May 2024, enforceable 1 August 2024 (noting that the Act's requirements will be progressively introduced)
Where: European Union
What: We first explored the emerging contours of the Artificial Intelligence Act (**AI Act**) in our 2023 *Perspectives on Cyber Risk* report, prior to its formal adoption.

The AI Act represents a watershed development in global technology regulation, establishing the world's first comprehensive legal framework specifically designed to govern AI. Its stated objective is to foster innovation and uptake of AI, while safeguarding health, safety and the fundamental rights of individuals.

The AI Act introduces a harmonised, risk-based regulatory model across EU member states. AI systems are categorised into four risk levels – unacceptable, high, limited and minimal – with corresponding legal obligations tailored to the nature and impact of the system.

Notably, the framework includes specific provisions for general-purpose AI models, alongside restrictions on certain prohibited practices.

The AI Act also establishes a centralised supervisory authority – the **AI Office** – tasked with monitoring compliance, handling complaints, and coordinating enforcement across the EU.

Importantly, the AI Act has extra-territorial effect: non-EU organisations, including those in Australia, may be subject to its requirements where their AI systems are deployed in the EU or impact individuals within the Union.

While still in its early implementation phase, the AI Act is expected to shape the global trajectory of AI regulation as a legislative model or reference point for regulators in other jurisdictions.

3. *California Consumer Privacy Act 2018*

When: Enacted 28 June 2018; enforceable 1 January 2020
Where: California, USA
What: As the first comprehensive, state-level data privacy legislation of its kind, the California Consumer Privacy Act 2018 (CCPA) marked a foundational shift in US privacy law. The CCPA introduced new rights for California residents regarding the collection, use, and disclosure of their personal information, and imposed a set of obligations on certain businesses operating in the state.

Under the CCPA, California re residents have the right to:

- know what personal information is being collected, used and disclosed;
- request deletion of their personal information held by a business; and
- opt out of the sale or sharing of personal information.

Although narrower in scope than the GDPR – particularly in its original form – the CCPA has nevertheless had significant ripple effects. Domestically, it catalysed a wave of privacy reform across the US, with numerous other states enacting or considering similar legislation.

Internationally, it has been viewed as a key milestone in the development of consumer privacy rights and regulatory models outside of the EU framework.

The CCPA has since been expanded and modified by the California Privacy Rights Act (**CPRA**), which came into effect in 2023, further aligning California's privacy regime with global best practice and establishing the **California Privacy Protection Agency** as a dedicated regulator.

4. American Data Privacy and Protection Act 2022

When: Introduced 21 June 2022; failed to pass on 3 January 2023 (at the conclusion of the 117th Congress)
Where: USA
What: Unlike jurisdictions with comprehensive national privacy frameworks, the US has long relied on a fragmented patchwork of sector-specific federal laws and state-level legislation. The *American Data Privacy and Protection Act* (**ADPPA**) emerged in 2022 as the most promising attempt to establish a comprehensive US federal privacy law.

The ADPPA aimed to create baseline obligations for the collection, processing and transfer of personal data, while strengthening individual rights. It included provisions broadly aligned with international standards – including rights of access, correction, deletion, and limitations on secondary uses of data. Notably, the ADPPA introduced a data minimisation principle as a core compliance obligation, shifting the focus from 'notice-and-choice' towards 'purpose-and-necessity' limitations.

Despite bipartisan support and substantial momentum, the ADPPA failed to progress through Congress in 2023. However, the push for federal privacy reform has continued. In April 2024, a new draft bill – the *American Privacy Rights Act* (**APRA**) – was introduced with bipartisan support from the chairs of the House Committee on Energy and Commerce, and the Senate Committee on Commerce, Science and Transportation.

The APRA retains many features of the ADPPA, and its progress will be closely watched by regulators both domestically and internationally. A successful enactment would mark a significant milestone in the evolution of privacy regulation in the US, with implications for global data governance frameworks and international data flows.

5. Digital Personal Data Protection Act 2023

When: Enacted 11 August 2023, effective date to be determined
Where: India
What: The *Digital Personal Data Protection Act 2023* (**DPDA**) is India's first comprehensive data protection law. It marks a pivotal step in the evolution of data governance in the world's most populous nation and one of its largest digital economies. Enacted following years of consultation, legislative redrafting, and public debate, the DPDA reflects many of the principles found in the GDPR, while incorporating features specific to India's legal and administrative context.

The DPDA is an omnibus statute that applies across sectors to the processing of digital personal data. It introduces a set of foundational privacy principles – including purpose limitation, data minimisation, and requirements for notice and consent – and confers rights on Indian data principals (individuals), such as access, correction, erasure, and grievance redress.

Like the GDPR, the DPDA has extra-territorial application: it extends to entities outside India where personal data is processed in connection with offering goods or services to individuals in India. It also establishes a central regulator – the **Data Protection Board of India** – with powers to investigate breaches, impose penalties and issue directions.

While implementation and enforcement remain at an early stage, the DPDA represents a significant shift in India's regulatory posture, with implications for multinational organisations processing data from or about Indian individuals. It is expected to influence the evolution of privacy and data governance frameworks across the Indo-Pacific and beyond.

6. Cyber Security Act 2018

When: Enacted 2 March 2018, enforceable 31 August 2018 (with certain provisions coming into effect on 11 April 2022)
Where: Singapore
What: Singapore has long been recognised as a regulatory leader in cyber security and data protection within the Asia-Pacific region. The *Cyber Security Act 2018* was a pivotal step in establishing a legislative framework to protect critical information infrastructure (**CII**) – defined as systems necessary for the continuous delivery of essential services – from cyber threats, and to coordinate incident response at the national level.

The Act imposes obligations on owners of designated CIIs, including requirements for risk mitigation, incident reporting, and compliance with directions issued by the **Cyber Security Agency** of Singapore (**CSA**). It also empowers the CSA to investigate and respond to cyber security incidents, and to conduct audits and inspections of CII operators.

In 2024, amendments to the Act significantly broadened its scope: key changes included the expansion of the CSA's regulatory remit and enforcement powers, and the extension of the Act's application beyond traditional CII sectors to include digital infrastructure service providers (such as cloud and data centre operators).

These reforms reflect Singapore's continuing efforts to modernise its cyber regulatory architecture and maintain resilience across both public and private digital infrastructure. The enhanced framework has been closely observed by other jurisdictions in the region (including Australia) who have enacted, or are considering enacting, similar critical infrastructure regulatory frameworks.

7. Cyber Security Framework Law 2024

(Law No 21.633)

When: Enacted 26 March 2024, enforceable 1 January 2025 (with certain provisions coming into effect on 1 March 2025)
Where: Chile
What: The *Cyber Security Framework Law* has positioned Chile as the first Latin American country to introduce dedicated cyber security legislation. The law establishes a national regulatory framework aimed at safeguarding critical infrastructure, and responding to escalating cyber threats across both the public and private sectors.

The law creates the **National Cyber Security Agency**, a central authority tasked with oversight, enforcement, and incident coordination. Regulated entities – including operators of critical infrastructure – are required to implement cyber security measures proportionate to their risk exposure. These include:

- developing and maintaining incident response plans;
- conducting cyber security risk assessments; and
- complying with mandatory cyber incident notification requirements to the Agency.

In parallel, Chile also enacted the *New Data Protection Law* (Law No. 21.719) in 2024, which modernises the country's privacy and data protection regime.

Drawing inspiration from the GDPR, the new law strengthens individual rights, clarifies data controller and processor obligations, and introduces enhanced enforcement powers. Together, these laws reflect the broader shift towards regulatory alignment with the GDPR and other international privacy and cyber security standards.

8. UN Convention against Cybercrime

When: 2024
Where: International – the Convention applies to those countries that accede to the Convention
What: The *UN Convention against Cybercrime* is the first international treaty developed under the auspices of the United Nations to comprehensively address cybercrime through a criminal justice lens. It represents a significant multilateral effort to establish a coordinated and cooperative global approach to cybercrime prevention, enforcement and capacity-building.

The Convention provides a legal framework for the criminalisation of both cyber-dependent offences (such as unauthorised access and illegal system interference) and cyber-enabled offences (including online child sexual exploitation, information and communications technology (**ICT**) related fraud, and identity-related crimes). It also emphasises:

- international cooperation, including streamlined mechanisms for mutual legal assistance and cross-border evidence sharing;
- preventive measures, encouraging signatories to adopt domestic safeguards to reduce cybercrime risks; and
- capability building, with a particular focus on supporting developing countries to strengthen legal, institutional and technical capabilities.

By addressing long-standing jurisdictional and procedural barriers, the Convention seeks to enhance global responsiveness to increasingly sophisticated, transnational cyber threats. While the Convention has been welcomed as a step towards harmonising global cybercrime standards, its effectiveness will ultimately depend on the breadth and depth of international adoption – and the extent to which it can complement existing regional frameworks such as the Council of Europe's Budapest Convention.

9. Product Security and Telecommunications Infrastructure Act 2022

When: Enacted 6 December 2022, enforceable 29 April 2024
Where: United Kingdom
What: The *Product Security and Telecommunications Infrastructure Act 2022* (**PSTI Act**) was a pioneering development in the regulation of connected devices, establishing mandatory cyber security standards for consumer connectable products – commonly referred to as smart or Internet of Things (**IoT**) devices.

The legislation, considered a world-first in this domain, aims to reduce systemic vulnerabilities in everyday digital products by imposing baseline security obligations on manufacturers, importers and distributors operating within the UK market. Many of its requirements are reflected in Australia's more recent *Cyber Security Act*, discussed on page 55.

Key provisions of the *PSTI Act* include:

- a prohibition on default or easily guessable passwords (e.g. 'admin' or '12345');
- requirements to provide a clear vulnerability disclosure mechanism for reporting security issues; and
- obligations to communicate transparently about product security updates, including minimum support periods for security patches.

The law covers a broad spectrum of consumer devices, including smart TVs, connected toys, smartphones, and home automation products.

Responsibility for enforcement rests with the **Office for Product Safety and Standards**, which may issue compliance notices, impose monetary penalties or direct the withdrawal of non-compliant products from the market. The PSTI Act also imposes criminal liability for non-compliance in certain circumstances.

10. Cyber Security Law 2017

When: Enacted 7 November 2016, enforceable 1 June 2017
Where: People's Republic of China
What: The *Cyber Security Law* was the first foundational piece of legislation in mainland China to systematically address cyber security, data governance and the regulation of digital infrastructure. It forms the cornerstone of China's increasingly complex and interlocking framework for digital and information regulation.

The law introduced a broad regulatory regime applicable to network operators – a term encompassing owners, administrators and providers of networks and network services – and imposes obligations in relation to:

- the protection of CII;
- network security risk mitigation and monitoring;
- data localisation, requiring certain categories of data to be stored within China; and
- the collection, use and protection of personal information, including consent and purpose limitation principles.

Over time, the law has been supplemented and significantly expanded by a suite of sectoral and cross-cutting legislation, including the:

- *Data Security Law 2021* (**DSL**), which introduced classification-based management of data and national security-focused obligations;
- *Personal Information Protection Law 2021* (**PIPL**), China's closest analogue to the GDPR, establishing a comprehensive regime for personal data protection and cross-border transfers; and
- *Security Protection Regulations on Critical Information Infrastructure*, which specify operational requirements for CII operators.

Most recently, in 2024, China enacted the *Network Data Security Management Regulation*, which clarifies and integrates compliance obligations under the *Cyber Security Law*, DSL, and PIPL – particularly in relation to cross-border data transfers, algorithmic governance, and risk assessments for 'important' and 'core' data.

Together, these instruments form a dense and evolving regulatory architecture that reflects China's twin priorities: enhancing cyber sovereignty, and securing its digital economy. Multinational organisations with operations or supply chains involving China must navigate this evolving framework carefully, particularly in light of heightened enforcement and state security considerations.

Australia: a decade in review

Not to be outpaced by international developments, Australia has undergone its own decade of significant privacy and cyber reform.

2024 marked a particular turning point, with the long-anticipated amendments to the Privacy Act and the SOCI Act, the introduction of world-first age verification requirements for social media platforms under amendments to the *Online Safety Act 2021* (Cth) (**Online Safety Act**), and the passage of new cyber legislation in the form of the Cyber Security Act.

We take a closer look at each of these reform measures below.

1. Privacy Act 1988

The Privacy Act underwent a series of important reforms over the last decade, reflecting an increasingly complex and fraught environment in how personal information is collected, used and stored.

The most significant of these was the introduction of the NDB scheme, which commenced on 22 February 2018. The NDB scheme requires entities regulated by the Privacy Act to notify the OAIC and affected individuals of data breaches that are likely to result in serious harm. This shift to mandatory notification marked a turning point in privacy regulation in Australia, aligning it more closely with the GDPR and embedding transparency and accountability into the response to privacy incidents.

Other amendments over the last decade have strengthened enforcement powers, raised civil penalty thresholds, and broadened the OAIC's ability to hare information with domestic and international regulators.

In 2022, the maximum penalty for serious and repeated interferences with privacy was increased to the greater of A$50 million, three times the benefit obtained, or 30% of adjusted turnover.

More recently, the *Privacy and Other Legislation Amendment Act 2024* (Cth) (**POLA Act**) was enacted on 10 December 2024. The POLA Act introduced a suite of reforms aimed at further strengthening the protection of individuals' personal information by amending both the Privacy Act and the *Criminal Code Act 1995* (Cth) (**Criminal Code**).

Several provisions commenced in December 2024, with others set to take effect in 2025 and in 2026.

Key amendments introduced by the POLA Act that are now in force include:

Changes to civil penalties: The threshold for the highest tier of civil penalties has been lowered: a data breach need now only be serious – rather than serious and repeated – in order to attract the top-tier penalty provisions. While repeated contraventions are no longer a prerequisite, they may still be considered in assessing the overall seriousness of the breach.

The POLA Act also introduces a new mid-tier civil penalty for interferences with privacy, carrying a maximum penalty of 10,000 penalty units (currently A$3.3 million) for bodies corporate.

In addition, lower-tier penalties may now be imposed for contraventions of specified Australian Privacy Principles (**APPs**), including:

- the obligation to have a clearly expressed and up-to-date privacy policy (APP 1.3);
- prescribed content requirements for the privacy policy (APP 1.4); and
- obligations relating to direct marketing opt-outs (APPs 7.2, 7.3 and 7.7).

These attract a maximum penalty of 1,000 penalty units (currently A$330,000) for bodies corporate;

Infringement and compliance notices: The **Privacy Commissioner** is now empowered to issue both compliance notices and infringement notices in response to various contraventions of the Privacy Act (including contraventions of various APPs and a failure to provide a compliant data breach notice). Infringement notices may also be issued for failures to provide information, or to comply with a compliance notice. These notices attract penalties of up to 60 penalty units (currently A$19,800) per contravention for bodies corporate, and up to 200 penalty units (currently A$66,000) for listed companies;

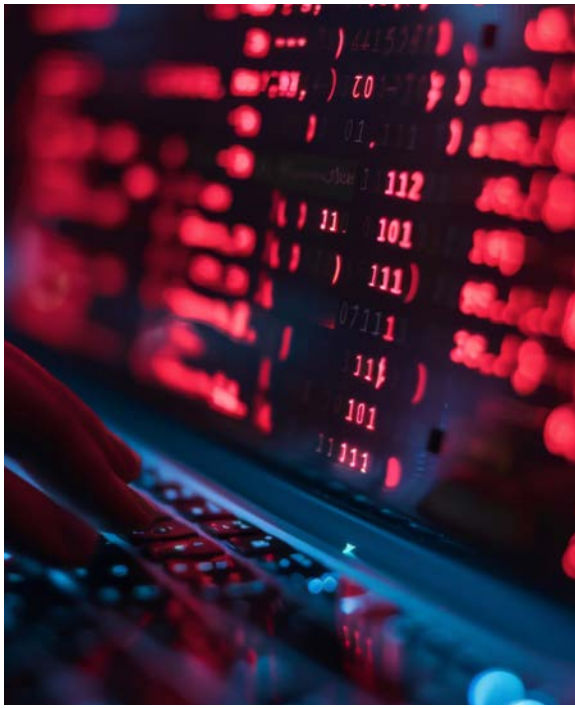
Other enforcement powers: The POLA Act expands the range of remedies available for breaches of civil penalty provisions under the Privacy Act, empowering the Federal Court and the Federal Circuit and Family Court of Australia to make orders for redress, compensation and public statements in relation to a contravention. It also introduces new general investigation and monitoring powers for the Privacy Commissioner, which replace the existing entry and inspection provisions in the Privacy Act. In addition, the Privacy Commissioner may, with the Minister's approval or direction, conduct public inquiries into specified privacy matters and is not bound by the rules of evidence in doing so;

APP codes: While APP codes already exist, the POLA Act introduces new powers enabling the Minister to direct the Privacy Commissioner to develop and register both permanent and temporary APP codes. A dedicated Children's Online Privacy Code is also anticipated; however, it is not required to be developed and published until 2026;

Technical and Organisational Measures: APP 11 requires APP entities to take reasonable steps to protect personal information from misuse, interference, and loss, as well as from unauthorised access, modification, or disclosure. The POLA Act introduces APP 11.3, which clarifies that such reasonable steps include the implementation of both technical and organisational measures to safeguard personal information;

Doxxing: A new criminal offence of 'doxxing' has been introduced into the Criminal Code. The offence captures the use of a carriage service to make available, publish, or distribute personal information of a group or individual, where the conduct would be regarded by a reasonable person as menacing or harassing. It carries a maximum penalty of six years' imprisonment; and

White list: A new mechanism allows for the prescription of countries and binding schemes that provide protection substantially similar to the APPs, to assist entities in assessing whether it is appropriate to disclose personal information to overseas recipients (in accordance with APP 8). The list of prescribed countries is yet to be developed.



2. Corporations Act 2001

Although not the subject of a specific legislative amendment, the past decade has seen increasing regulatory focus on cyber security as a matter of directors' duties under the Corporations Act, particularly by ASIC. At a minimum, Boards are now expected to implement, oversee and actively manage appropriate cyber security risk frameworks. A failure to do so may constitute a breach of directors' duties.

MinterEllison's *Perspectives on Cyber Risk* series has documented the elevation of cyber risk to a core governance priority for Boards and senior executives over the past 10 years.

3. SOCI Act 2018

In March 2018, the Australian Government enacted the SOCI Act, establishing a regulatory framework for the protection of critical infrastructure assets across 11 designated sectors, including communications, energy and healthcare. The SOCI Act defines critical infrastructure broadly to encompass physical facilities, supply chains, and IT systems whose disruption would have a significant impact on national security or economic stability.

The SOCI Act empowers the Federal Government to collect information from asset owners and operators to mitigate risks such as sabotage, espionage, and coercion. It imposes obligations including registration on the Register of Critical Infrastructure Assets, mandatory cyber incident reporting, and the development, maintenance, and implementation of a written risk management program.

The SOCI Act was significantly amended in late 2024 as part of the broader Cyber Security Legislative Package. Key amendments include:

Data Storage Systems: The definition of a 'critical infrastructure asset' under the SOCI Act has been expanded to include data storage systems that store or process business-critical data. As a result, the obligations under the SOCI Act now extend to such systems where they meet the following criteria:

- the responsible entity owns or operates the data storage system;
- the system is used (or is intended to be used) in connection with a primary critical infrastructure asset;
- it stores or processes business-critical data; and
- vulnerabilities, impacts, or unauthorised access to the system could affect the availability or integrity of the relevant critical infrastructure asset.

A clear nexus must exist between the data storage system and the critical infrastructure asset. This amendment addresses prior uncertainty regarding the regulatory status of data storage systems and reinforces protections for business-critical data – an ongoing target for cyber criminals;

Protected Information: The SOCI Act contains a regime governing the handling of 'protected information', which imposes restrictions on its recording, use, and disclosure. Recent amendments introduced a revised definition of 'protected information' that now incorporates the concept of 'relevant information'. The intent is to enable both entities and government agencies to undertake a harms-based assessment when determining whether, and how, such information may be used or disclosed.

Under the amended regime, *protected information* is defined as *relevant information* that is either confidential commercial information or information the disclosure of which could reasonably be expected to prejudice:

- national security or the defence of Australia;
- the availability, integrity, reliability, or security of a critical infrastructure asset; or
- Australia's social or economic stability, or the safety of its people.

Relevant information is broadly defined and includes (but is not limited to) any document or information obtained or generated for the purposes of complying with, or in the course of exercising powers or performing functions under, the SOCI Act;

Telecommunications security: Key telecommunications security obligations, previously located in Part 14 of the *Telecommunications Act 1997* (Cth) (commonly referred to as the *Telecommunications Sector Security Reforms* or **TSSR**) have now been incorporated into the SOCI Act. This integration reduces regulatory overlap and addresses prior confusion stemming from the division of core security obligations across separate legislative frameworks.

Notably:

- all carriers and carriage service providers are now classified as managing a critical telecommunications asset under the SOCI Act;
- new and amended rules apply to a defined subset of these assets – from 4 April 2025, the *Telecommunications Security and Risk Management Rules* extends security obligations by requiring mandatory cyber incident reporting and the development of a tailored telecommunications critical incident risk management program (**CIRMP**); and
- breaches of the former TSSR – now embedded in the SOCI Act – are subject to the SOCI Act's compliance and enforcement regime, including civil penalties.

While the new framework commenced on 4 April 2025, the obligation to implement a CIRMP will not take effect until 4 October 2025.

Other amendments to the SOCI Act include:

- a new power to direct responsible entities to remedy deficiencies in their risk management programs;
- streamlined reporting requirements for *systems of national significance*; and
- expanded powers for the Secretary of Home Affairs to collect information and take action in response to all-hazards incidents – extending beyond cyber risks to include threats such as natural disasters and acts of terrorism that may affect the availability, reliability, or integrity of critical infrastructure.

4. Cyber Security Act

In November 2024, the Australian Government passed Australia's first standalone cyber-related legislation – the Cyber Security Act 2024 (Cth).

The Cyber Security Act is intended to provide a framework to address cyber security issues, enhance protections, mitigate risks, and improve the government's visibility of the threat environment, ensuring Australia is better prepared for future cyber threats.

Key features of the Cyber Security Act include:

Secure-by-design standards for smart devices: Manufacturers and suppliers of *relevant connectable products* – devices that connect to the internet to send or receive data, either directly or via another device – will be required to meet minimum cyber security standards. These include:

- a ban on default or easily guessable passwords (e.g. 'admin' or '12345');
- a requirement for manufacturers to provide a statement of compliance, confirming that the device meets the relevant standards (and notably, the content of the statement of compliance aligns with equivalent UK requirements under the *Product Security and Telecommunications Infrastructure Act 2022*); and
- obligations on suppliers to ensure they supply compliant products are sold in Australia, supported by either a manufacturer's statement or independent third party verification.

These obligations will come into effect on 4 March 2026.

Mandatory ransomware reporting obligations: From May 2025, 'reporting business entities' will be required to notify the Department of Home Affairs of ransomware and cyber extortion payments. This is intended to address the current under-reporting of such incidents and improve the government's situational awareness. A 'reporting business entity' is defined as:

- an organisation that carries on business in Australia with an annual turnover exceeding A$3 million (excluding Commonwealth or State bodies); or
- is a 'responsible entity' for a critical infrastructure asset under the SOCI Act.

A ransomware payment report must be submitted if:

- a cyber security incident has occurred, is occurring, or is imminent;
- the cyber security incident had, is having, or could reasonably be expected to have, a direct or indirect impact of the entity;
- a ransom or extortion demand is made; and
- a payment or benefit is provided in response to that demand.

Reports must be submitted within **72 hours** of either making the payment or becoming aware that the payment has been made. These obligations operate alongside existing reporting requirements under the Privacy Act, the SOCI Act, APRA Prudential Standard CPS 234, and (for some Australian entities) ASX Listing Rule 3.1 and the EU or UK GDPR.

'Limited use' of information provided to the National Cyber Security Coordinator (NCSC): The Cyber Security Act restricts how information shared with the NCSC may be used or disclosed, depending on whether the incident qualifies as a 'significant cyber security incident'. An incident will meet this designation where:

- there is a material risk that the incident has seriously prejudiced, is seriously prejudicing, or could reasonably be expected to prejudice, Australia's social or economic stability, defence, or national security; or
- the incident is, or could reasonably be expected to be, of serious concern to the Australian public.

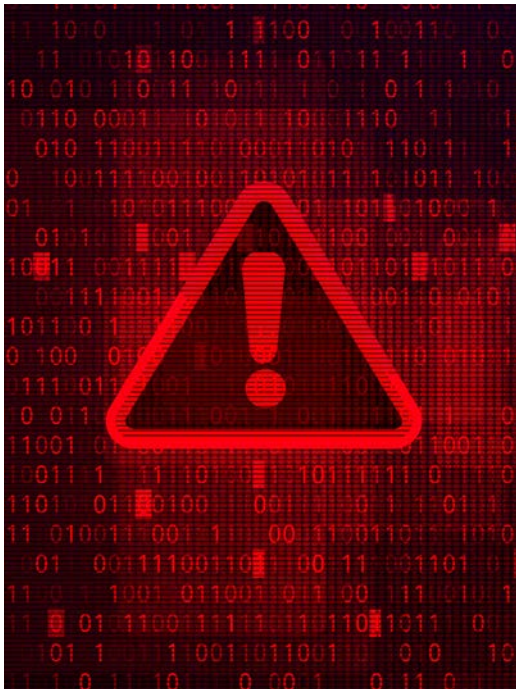
In such cases, the NCSC may use the information to assist the entity, prevent or mitigate material risks to critical infrastructure, or support the functions of intelligence and law enforcement agencies.

For other incidents, the NCSC's role is more limited – it may coordinate government support, refer the entity to appropriate services, or notify the Minister for Cyber Security of the incident;

Cyber Incident Review Board: The Cyber Security Act establishes an independent advisory body – the Cyber Incident Review Board (**CIRB**) – to conduct *post-incident reviews* of major cyber incidents. The Board, comprising of a Chair and up to six other members, may be activated via referral from the Minister, the **Australian Cyber Security Centre**, impacted entities, or Board members. Key features of this process include that:

- reviews are conducted on a no-fault basis, with no attribution of blame or legal liability;
- reports exclude personal, confidential, commercially sensitive or national security-related information; and
- recommendations are shared with both government and industry, with the aim of improving collective cyber resilience; and

Penalties and enforcement: Non-compliance with the Cyber Security Act may result in a range of enforcement actions, including compliance notices, stop notices, recall notices, and civil penalties. For serious contraventions, penalties may reach up to 60 penalty units (currently equivalent to approximately A$1.127 million).



Our watch list: 2025 and beyond

2025 is set to be a significant year for compliance in Australia, with several major legislative reforms – particularly in the areas of privacy and online safety – scheduled to commence following their passage in 2024.

In this report section, we outline the key regulatory changes taking effect over the coming year and their implications for organisations operating in Australia.

We also consider additional reforms that may be on the agenda following the Federal election, including the second tranche of the Privacy Act amendments and the government's response to the statutory review of the Online Safety Act.

Privacy Act: key forthcoming changes

Significant reforms to the Privacy Act are scheduled to come into effect later in 2025 and in 2026, including the introduction of a statutory tort for serious invasions of privacy, and new obligations relating to automated decision-making. These developments reflect the growing recognition of privacy harms beyond data misuse, and the need for transparency in increasingly automated decision environments.

Tort for serious invasions of privacy:
A new statutory tort for serious invasions of privacy will commence on 10 June 2025.

The tort provides individuals – but not corporations – with the right to sue where their privacy has been seriously violated either through **intrusion into seclusion** or **misuse of information relating to them**.

To succeed, a plaintiff must prove the following elements:

- the defendant has invaded their privacy;
- the plaintiff has a reasonable expectation of privacy in all of the circumstances;
- the defendant's conduct was intentional or reckless (i.e. rather than merely negligent);
- the invasion of privacy was serious; and
- the public interest in protecting the plaintiff's privacy outweighs any competing public interest (such as freedom of expression or the media).

While this sits within the Privacy Act, it applies broadly – the defendant need not be an 'APP entity', meaning that the cause of action is available against both individuals and organisations (including government).

The tort includes several **statutory exemptions**, notably for:

- journalists, publishers, and (in certain circumstances) their employers;
- law enforcement bodies and intelligence agencies;
- minors; and
- State and Territory authorities acting in good faith in the exercise or purported exercise of their functions or powers.

A number of **statutory defences** also apply, including:

- consent;
- where the invasion of privacy was required or authorised by law; and
- where the defendant reasonably believed the invasion of privacy was necessary to prevent a threat to life or safety.

Defences **mirroring defamation law** – such as absolute privilege, publication of public documents, and fair report of proceedings of public concern – also apply.

Despite the exceptions and defences, this tort introduces a powerful new avenue for individuals to seek redress. Organisations that collect, use or disclose personal information should closely monitor its early application and consider reviewing existing practices and risk frameworks accordingly; and

Transparency obligations for automated decision-making: From 10 December 2026, APP entities are required to update their privacy policies under new provisions relating to automated decision-making.

Where decisions that significantly affect individuals' rights or interests are made, or are substantially influenced by computer programs, including AI or other automated systems, entities must disclose in their privacy policies:

- the types of personal information used in such decision-making processes; and
- the kinds of decisions made using that information.

Importantly, the obligation applies even if human involvement is present, so long as the decision-making process is **substantially automated**.

These changes reflect growing regulatory focus on algorithmic transparency and accountability. APP entities should begin mapping current and future uses of automated decision-making technologies to ensure readiness for these obligations ahead of the commencement date.

Online Safety Act 2021 (Cth): key forthcoming changes

Australia's online safety framework continues to evolve, with **legislative amendments** and **regulatory reviews** aimed at strengthening protections – particularly for children and vulnerable users – and enhanced accountability for digital platforms:

Minimum age for social media use: The *Online Safety Amendment (Social Media Minimum Age) Act 2024* (**SMMA Act**) was passed by Federal Parliament on 29 November 2024, with commencement expected approximately 12 months post-enactment. The Act introduces a minimum age requirement of 16 years for the creation of social media accounts, in response to growing concerns about the impact of digital platforms on children's wellbeing and development.

Under the *SMMA Act*:

- age-restricted social media platforms will need to take reasonable steps to prevent children aged under 16 years from creating social media accounts. The eSafety Commissioner will provide guidance on what constitutes 'reasonable steps';
- a service will be an age-restricted social media platform if:
  - the sole or significant purpose of the service is to enable online social interaction between two or more end users;
  - it enables end users to link or interact with others; and
  - it allows users to post material.

Exemptions apply to:

- messaging apps;
- online gaming services;
- services with health or education as their primary purposes; and
- services assessed as 'low risk' by the eSafety Commissioner.

Importantly, platform operators will be prohibited from using **government-issued identification** for age verification, although alternative age assurance methods may be accepted where approved.

The amendments carry significant penalties for non-compliance, with fines of up to A$49.5 million for platform operators who fail to meet their privacy obligations.

Over the horizon: emerging reforms in privacy and cyber law

Further regulatory change is firmly on the horizon. The coming years are likely to see further legislative activity in privacy, online safety, AI and broader digital regulation – driven by evolving technologies, geopolitical pressures, and heightened public and regulator expectations.

In particular, the **second tranche of reforms to the Privacy Act** remains under consideration, along with the government's response to the **statutory review of the Online Safety Act**.

Artificial intelligence is also an area of increasing policy focus, with the potential for new regulatory frameworks or targeted amendments to existing regimes:

Privacy Act – second tranche: While the first tranche of the Privacy Act reforms (discussed above) is now or will shortly be in force, a second tranche remains on the table. The Australian Government's 2023 response to the Privacy Act *Review Report* endorsed, or agreed in principle to, a broad range of additional proposals aimed at modernising the Privacy Act for the digital age. These include expanding the definition of 'personal information', introducing enhanced organisational accountability measures, and shortening the notification period for notifiable data breaches from **30 days to 72 hours** to align with the SOCI regime and international norms (including the GDPR). The Government also supported new obligations for privacy-by-design, including the requirement for entities to conduct Privacy Impact Assessments for high-risk activities and to appoint senior privacy officers.

If progressed, the second tranche will also significantly expand individual rights, including a direct right of action for individuals to seek redress for interferences with their privacy (which will be in addition to the statutory tort for serious invasions of privacy, also discussed above).

Further reforms under consideration include increased regulatory clarity through simplification of the APPs, and targeted regulation of high privacy risk activities, such as the use of biometric data and facial recognition technologies.

While these proposals remain subject to further public consultation and policy refinement, they collectively signal a shift toward a more rights-based, risk-responsive privacy framework, with stronger alignment to global standards and heightened expectations on regulated entities; and

Statutory review of the Online Safety Act: In parallel, a statutory review of the Online Safety Act was undertaken in 2024, culminating in a final report containing 67 recommendations. The review advocates for a **'systems-based' regulatory approach**, shifting from reactive content removal to proactive harm prevention. Key recommendations include:

- the introduction of a statutory duty of care, requiring online services to take reasonable steps to prevent foreseeable online harm to users;
- expanding the investigatory, enforcement and litigation powers of the eSafety Commissioner; and
- imposing significant penalties, of up to A$50 million or 5% of global annual turnover, for breaches of the duty of care.

What comes next?

Looking beyond the known legislative proposals, we anticipate AI will remain a key focus for federal and state governments in 2025 and beyond.

Possible options for regulating AI in Australia include adapting existing regulatory frameworks to introduce additional guardrails addressing AI, or creating new regulatory frameworks through specific legislation (similar to the European Union's *Artificial Intelligence Act*, which is considered to be the regulatory high water mark).

While the precise contours of future regulation remain to be seen, one trend is unmistakable: each passing year has brought a more intense, more expansive, and more coordinated regulatory focus on cyber security, privacy and data protection.

What were once emerging policy areas are now firmly at the centre of legislative and enforcement agendas, both in Australia and globally. For organisations, the compliance burden is no longer incremental – it is cumulative and accelerating, driven by the convergence of **technological innovation, geopolitical tension, rising public expectations, regulatory ambition** and **harmonisation, and increasing economic and national security dependency on digital infrastructure.**

D

Emerging threats: preparing for tomorrow

The future of cyber security will be shaped by the convergence of rapidly evolving technologies, increasing geopolitical instability, and expanding digital frontiers.

The pace of change presents both opportunities and profound risks. From AI-powered attacks and quantum threats to space systems and neural interfaces, organisations must anticipate a world where digital complexity grows faster than the pace at which traditional risk management frameworks can adapt.

This report section explores significant emerging threats shaping the next decade of cyber risk – and what organisations should do now to prepare.

1 › ARTIFICIAL INTELLIGENCE: ACCELERANT AND ATTACK VECTOR

AI is a double-edged sword: while it holds promise for cyber defence, it's already transforming the threat landscape.

In 2024, threat actors increasingly leveraged foundation models to automate attacks, create realistic deepfakes, and scale disinformation. For example, according to CrowdStrike, adversaries are now using GenAI to craft phishing content, impersonate IT job candidates, and conduct influence operations around elections.

AI-driven malware is now capable of swiftly adapting to host environments in real time, while phishing-as-a-service kits use LLMs to craft credible 'lures' at scale.

In our 2025 survey, **84%** of respondents identified AI-related privacy and security risks as their top concern in adopting this technology.

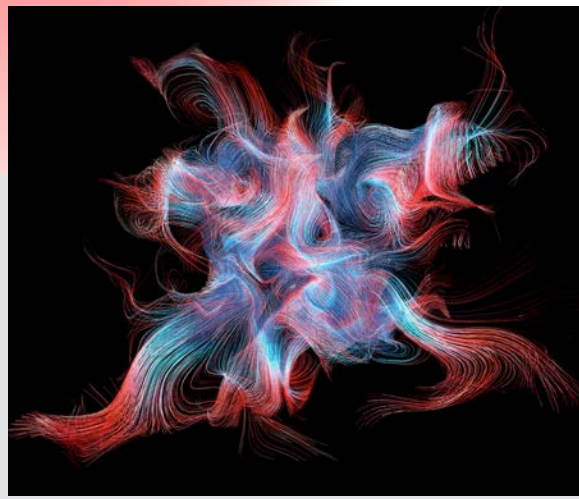
From a legal perspective, regulatory frameworks are struggling to keep pace. The EU's *AI Act*, discussed on page 46, is one of the first comprehensive attempts to regulate high-risk AI systems. But significant gaps remain around enforcement, redress and ethical governance – particularly in cross-border and national security contexts.

2 › DEEPFAKES AND THE EROSION OF TRUST

In 2024, a year in which half of the world's population voted in elections, deepfakes and the dissemination of fake information became mainstream threats.

Synthetic media was used to impersonate leaders, disrupt elections, and extort organisations. In one high-profile incident, a voice-cloned message impersonating former US President Joe Biden circulated days before the presidential election.

As detection struggles to keep pace with realism, the risk shifts from mere impersonation to systemic loss of trust – in video evidence, digital identities, and communication channels. This creates new imperatives for authenticity verification, identity assurance frameworks, and regulatory oversight of synthetic content.



3 ›
QUANTUM COMPUTING AND THE RACE TO Q-DAY

Quantum computing promises revolutionary benefits in medicine, materials, and optimisation – but also poses an existential risk to current encryption standards.

The prospect of 'Q-Day' looms large – the moment when quantum systems can break RSA and elliptic curve encryption. State actors are already harvesting encrypted datasets for future decryption.

While functional quantum computers are not yet mainstream, the urgency is clear: organisations must begin migration planning for post-quantum cryptography, including algorithm agility, asset classification, and supply chain dependencies.

4 ›
SPACE AS A CYBER DOMAIN

The militarisation and privatisation of space is giving rise to a new domain of cyber conflict.

Satellites, launch infrastructure, and ground stations are increasingly targeted in geopolitical cyber operations. The **Viasat** incident during the Russia-Ukraine war – which disabled broadband communications across Europe – underscored how critical space systems are to both civilian and military functions.

Space-based infrastructure must now be considered part of national critical infrastructure, with end-to-end security controls, sovereign capability planning, and coordinated regulatory frameworks across commercial, defence, and civilian agencies.

5 ›
NEURAL INTERFACES: COGNITIVE LIBERTY AND BIO-DIGITAL RISK

Neural technologies, including brain-computer interfaces (BCIs), are moving from science fiction to reality.

Companies like Neuralink, Synchron and Meta are advancing wearable and implantable tech that connects the human brain to digital systems.

This creates a new attack surface – not just for data, but for human thought. Neural data is intimate and immutable. The potential misuse of this data for profiling, manipulation, or unauthorised control poses profound risks to privacy, autonomy, and safety.

Secure design, data governance, and legislative protections for 'cognitive liberty' must accompany these innovations. Risks of developer insolvency or discontinuation – with devices still implanted – call for legal frameworks mandating support continuity and possible open-source fallback mechanisms.

6 ›
GEOPOLITICAL FRAGMENTATION AND CYBER ESCALATION

Cyber operations are increasingly a tool of geopolitical strategy – not only in active conflicts, but also in influence, espionage, and economic disruption.

Geostrategic tensions in the Indo-Pacific have led to state-sponsored targeting of critical infrastructure, while proxy cyber groups blur the lines of attribution and retaliation. Boards must now treat geopolitical risk as an intrinsic element of their cyber strategy – integrating it into threat intelligence, business continuity planning, and supply chain due diligence.

7 ›
THE EXPANDING ATTACK SURFACE: IOT, CLOUD AND IDENTITY

Attackers continue to exploit expanding digital perimeters – particularly IoT devices, cloud workloads, and identity systems.

CrowdStrike found that 79% of incidents in 2024 were malware-free, relying instead on legitimate tools and credential abuse. Identity compromise is now the preferred vector for lateral movement and persistence.

IoT devices often lack secure-by-design principles, with patching and authentication controls lagging behind – a shortfall that the *Cyber Security Act* seeks to address (see page 55).

Cloud environments, meanwhile, face risks from misconfiguration, third party access, and complex entitlement models. In this context, organisations must invest in zero trust architectures, identity-centric security models, and continuous posture assessment across hybrid environments.

Conclusion: from horizon-scanning to readiness

Emerging threats are no longer distant possibilities. They are reshaping the risk landscape in real time.

What is needed is not just foresight, but a clear strategy, responsibilities and actions: embedding emerging risk into strategic planning, updating frameworks to reflect new realities, and elevating the role of cyber leaders in governance and decision-making.

Preparing for tomorrow's cyber risks means strengthening today's foundations – and looking beyond today's playbook.

How we can help

We have brought together an unmatched team of cyber security experts under one roof, combining the dynamism of a human-centred, specialised boutique business, with the power of a large Australian law firm.

Find out more 〉

Proactive cyber security

Incident response, digital forensics, breach coaching, and crisis management

Cyber risk Board governance

Privacy and data regulation

Procurement structuring and probity

Software and ICT service procurement

Digital transformations and outsourcing

Telecommunications regulation

IP protection and enforcement

Investigative support

IP commercialisation

Dispute resolution

Strategic risk guidance and integration

Meet our team

Report authors

Paul Kallenbach
Partner
Technology and Data
M +61 412 277 134

Shannon Sedgwick
Partner
Cyber Security
M +61 481 102 121

Acknowledgments
Thank you to all those who contributed to the 10 year anniversary edition of Perspectives on Cyber Risk Report 2025:

- Nami Burns, Lawyer
- Kate Dimes Letters, Senior Asociate
- Jack Goldsmith, Senior Consultant
- Luci Guyot, Special Counsel
- Maria Rychkova, Lawyer
- Tulin Sevgin, Director
- Jasmine Tait, Lawyer

Jonathon Blackford
Partner
MinterEllison Consulting
M +61 415 837 221

Ashish Das
Partner
MinterEllison Consulting
M +61 424 289 204

Helen Lauder
Legal Consultant
M +61 2 9921 4689

Lisa Jarrett
Partner
Technology and Data Law
M +61 448 880 530

Vanessa Mellis
Partner
Technology and Data Law
M +61 434 658 811

Nicholas Pascoe
Partner
Technology and Data Law
M +61 403 857 529

Sonja Read
Partner
Technology and Data Law
M +61 411 276 772

Tulin Sevgin
Director
MinterEllison Consulting
M +61 468 863 620

In the event of a cyber security incident, please contact MinterEllison's incident response team at

cyberincident@minterellison.com

Cyber risk and cyber resilience are more pressing than ever for Australian organisations. Heightened geopolitical factors, new regulatory requirements, an increasing prevalence of cyber attacks, and an increasing reliance on technology and data mean that organisations must take proactive steps to build and maintain their cyber resilience.

Paul Kallenbach
Partner, Technology and Data
M +61 412 277 134