HERBERT
SMITH
FREEHILLS
CYBER

ARE YOU CYBER READY?

Australian businesses grapple with cyber resilience in 2024

Herbert Smith Freehills Cyber Risk Survey

Contents

03 Are you cyber ready?

04 Survey results at a glance

06 Cyber risk escalates

11 On the minds of General Counsel

17 Keeping watch

21 How we can help you

Are you cyber ready?

Twelve months ago, our survey told us that corporate Australia had a lot of work to do to improve its cyber resilience – is this still the case?

Today, almost 80% of respondents to our Cyber Risk Survey believe the cyber threat to their organisation has increased compared with last year. However, our data shows that many are still not undertaking crucial preparatory work – perhaps one of the most jarring findings from our survey was that 58% of respondents said it would take an actual cyber attack to motivate their organisation to meaningfully improve their data risk management.

The traditional view of cyber risk and resilience is becoming harder to sustain. As companies continue to transform their digital capabilities, handle ever-greater data volumes, and transact with a complex array of third parties, their supply chains are subject to growing cyber vulnerability. Their attack surface has increased (and become less visible) and many are faced with the real prospect of regulatory intervention, cyber-related class action claims and long-term reputational damage.

Robust cyber resilience involves many parts of a business, but we believe it is time to acknowledge that technology and IT plays a disproportionate role in building cyber resilience. Many of the incidents we see could have been avoided through basic cyber hygiene and good technology or IT solutions.

We also observe that legal teams are increasingly front and centre. This was evident in our survey last year and is reinforced in 2024. In the immediate aftermath of an incident, legal expertise is essential in assessing the impact of an attack, preserving evidence, ensuring regulatory compliance, navigating communications, managing notifications and helping the business engage with stakeholders.

Boards also play a significant role. Key decisions, including those relating to disclosure, threat actor engagement and extortion payments often reside with the board. Despite this, half of our respondents say their boards have not been through a cyber simulation, 30% have not been educated about cyber risk in the last year and 36% have not yet decided whether they were open to paying an extortion demand. Clearly there is a lot more to do.

We can always work harder or spend more on the technical side of the ledger. The challenge for many organisations is whether the investment is sufficient to align with the company's risk profile – what does good look like? What resilience measures are sufficient? Many are turning to the Government for guidance, and more than 50% of our respondents think the Government needs do more to address cyber risk.

Throughout 2024, we interviewed high profile cyber leaders (in the private and public sector). Similar messages are coming through: protect the network you have, not the network you think you have, select a standard and measure yourself against it, invest in early detection tools and basic cyber hygiene, review your supply chain and have a good incident response plan.

58%

of respondents consider it would take a **cyber attack** to meaningfully improve their **organisation's focus on data risk management**

This year, we surveyed more than 160 legal leaders, with the overwhelming majority comprising group general counsel, senior legal counsel, divisional general counsel or equivalent. Sectors represented include financial services, consumer and retail, infrastructure, private capital, technology, and energy and resources.

This report tracks the evolving perspectives of in-house legal teams amid a rapidly changing cyber landscape. Fresh data is supported by insights from our firm's industry-recognised experts from across the Asia-Pacific region in cyber, regulatory, corporate advisory, dispute resolution and insurance. Our research reveals that while Australian organisations are becoming increasingly concerned with cyber risk, their legal preparations and activities are not yet proportionate to the severity of the threat.

Cameron Whittfield
Partner – APAC Cyber Security Head

Survey results at a glance

Top 3

aspects of cyber risk that cause greatest concern:

1. Reputational risk
2. Third-party risk
3. Underinvestment in systems / infrastructure

ALMOST **80%**

believe the **cyber threat** to their organisation has **increased** compared with 12 months ago.

93%

of companies impacted by a cyber extortion incident **did not pay ransom demands**.

OVER **70%**

of boards have been **educated about cyber risk** in the past 12 months.

50%

have **not held a board simulation**.

36%

of respondent boards have not decided whether they are **open to paying an extortion**.

35%

of organisations have a director with **cyber expertise or experience on the board**.

75%

of respondents said the **legal team is a key member of the crisis response team** in the event of a cyber extortion incident.

54%

of **legal teams** have **never participated in a simulation**.

59%

do not have a specific **legal cyber incident response plan**.

OVER

80%

of respondents **do not have a budget** for the legal team **specifically dedicated** to spend on cyber risk.

40%

have an **individual tasked** with covering data and cyber risks.

14% have a **resource dedicated solely** to these risks.

Majority of respondents are now concerned about **class action risk**.

79%

believe cyber is a **CIO risk to own**.

ONLY

27%

are satisfied with their organisation's **data collection and retention** practices.

58%

of respondents consider it would take a cyber attack to meaningfully improve their **organisation's focus on data risk management**.

MORE THAN

50%

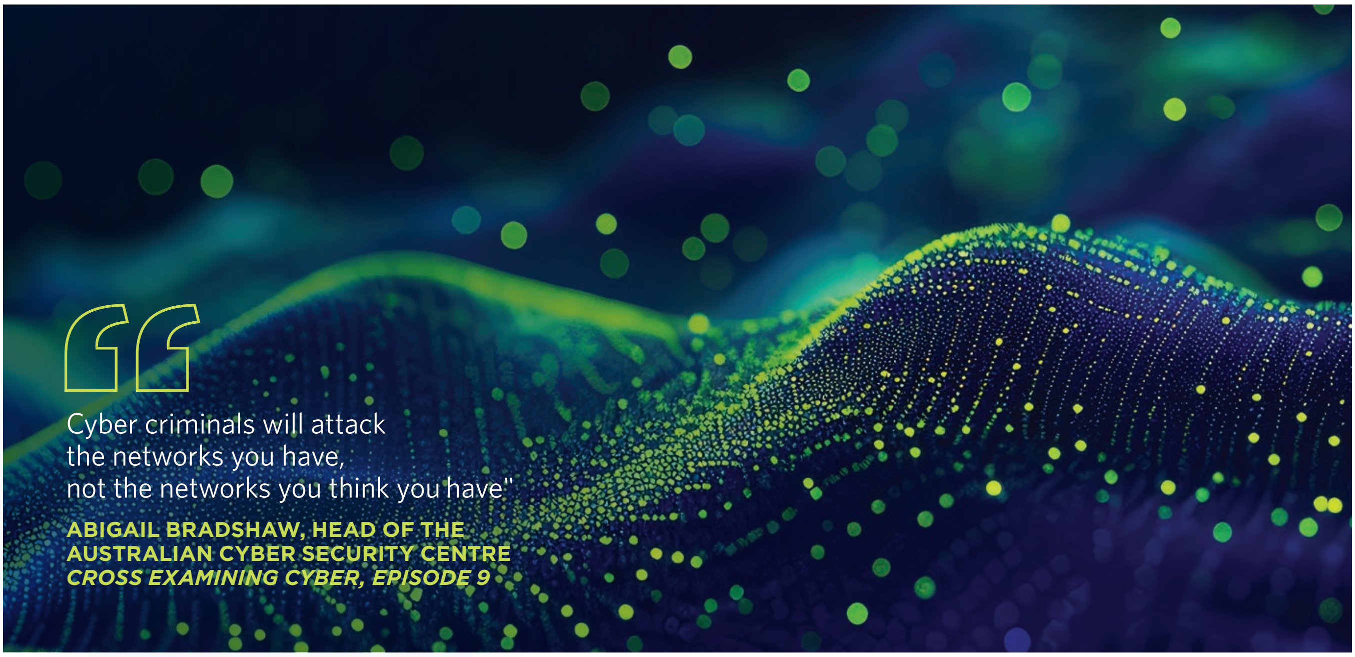
say **Government could do more** to address cyber risk.

80%

say they **would not engage** a law firm from an **insurer's panel**.

Cyber risk escalates

Are Australian businesses keeping up?



> Cyber criminals will attack
> the networks you have,
> not the networks you think you have"
>
> **ABIGAIL BRADSHAW, HEAD OF THE AUSTRALIAN CYBER SECURITY CENTRE**
> ***CROSS EXAMINING CYBER, EPISODE 9***

Many Australian organisations are now attuned to the criticality of cyber resilience. Approximately 80% of respondents believe the cyber threat to their organisation has increased compared with 12 months ago, and 33% go further, saying this threat has materially increased.

This is consistent with our professional experience and reflects the escalation and rising complexity of the threat landscape. In July 2024, we spoke with Abigail Bradshaw, Head of the Australian Cyber Security Centre.[1] She described a recent proliferation in activity by both criminal (that is, financially-motivated) actors and state-based actors, with a blurring of the lines between the two types.

Surveyed organisations also vary in their approach to prioritising cyber risk mitigation strategies. In the main, they are focused on updating their IT infrastructure, IT policies, procedures and incident response plans, as well as staff education. These strategies sit squarely within the wheelhouse of an organisation's IT security function, which may explain why 79% of survey respondents continue to see cyber risk as owned by their Chief Information Officer (CIO) or Chief Information Security Officer (CISO). There is little doubt that the IT team and associated experts play a critical role in building cyber resilience and responding to cyber incidents. However, a mindset that puts IT at the centre can put an organisation at risk of falling short on the enterprise-wide preparation required to meet cyber threats. This includes building the confidence of its board, testing its incident responders and upskilling the legal team.

ALMOST
80%

of respondents believe the **cyber risk threat** to their organisation has **increased** in the past 12 months.

Top 3

cyber risk priorities in the past 12 months have been:

1. Updating IT security infrastructure
2. Updating relevant policies, procedures or response plans
3. Staff engagement and/or education

79%

perceive cyber risk as a technology risk.

[1] Herbert Smith Freehills, Cross Examining Cyber: Conversations on Cyber Law, 'Episode 9: Cross Examining Ms Abigail Bradshaw - Part 2'.

In saying this, we understand why managing cyber risk often falls to the CIO or CISO. In our experience, many incidents could have been prevented with basic IT hygiene, such as keeping software updated by promptly rolling out patches, deploying enterprise-wide multi-factor authentication systems, restricting and regularly reviewing privileges and putting your remote desktop protocol behind the organisation's firewall.

Like our survey respondents, we also believe cyber security is, at its core, an IT risk. But cyber risk is also no different to any other risk. Boards, executives and legal leaders need to understand cyber risk so they can fully participate in discussions about it and to meaningfully respond to threats.

One of the most acute challenges to the effectiveness of organisations' responses to cyber risk is language: technical teams and boards are still struggling to understand each other. "There is a language disconnect," says Herbert Smith Freehills Partner and APAC Cyber Security Head Cameron Whittfield. "CISOs give briefings, and boards ask questions, but it is not clear to us whether ultimately there is shared understanding, and often we play the role of translator."

> There is a language disconnect. CISOs give briefings, and boards ask questions, but it is not clear to us whether ultimately there is shared understanding, and often we play the role of translator."
>
> **CAMERON WHITTFIELD, PARTNER – APAC CYBER SECURITY HEAD**

VIEWS FROM ASIA

Asia-based respondents are less concerned about cyber risk, with only around 60% of respondents saying cyber risk has materially or somewhat increased compared to 12 months ago. In comparison almost 80% of Australian respondents say cyber risk has increased.

Rising regulatory focus

Regulatory scrutiny in Australia is only increasing as a multitude of regulators take action on cyber. And while upcoming law reform may provide the guidance that businesses crave, it will also increase the regulatory burden and associated legal risks.

The Office of the Australian Information Commissioner (OAIC) commenced civil penalty proceedings against companies following major data breaches.

The Australian Communications and Media Authority (ACMA) is pursuing a high profile company for failing to adequately protect customer data.

In May 2024, the **Australian Stock Exchange (ASX)** updated its advice on how companies should manage continuous disclosure obligation**s** during a fast-moving data breach.

In November 2023, the **Australian Securities and Investments Commission (ASIC)** called on organisations to prioritise cyber security in light of capability gaps revealed by its cyber pulse survey.

The Australian Prudential Regulatory Authority (APRA) wrote to its regulated entities in 2024 to clarify its expectations regarding data backups and to identify common cyber control weaknesses.

Each of **APRA** and **ASIC** emphasise that cyber resilience is a key area of focus and investment in their respective Corporate Plans for 2024-25.

Boards remain underprepared

Staging a simulated cyber incident in a near real-life environment is an essential way to meaningfully test an organisation's incident response capabilities. We identified this in last year's report and it remains true today.

Simulations give participants a risk-free opportunity to clarify roles and responsibilities and to practice delegations and decision-making. They also shine a light on weaknesses in an organisation's cyber resilience program. This leads to a renewed focus and investment in systems and processes, in advance of a real-life crisis. And yet too many organisations are still only turning their attention to cyber preparedness when an attack occurs.

This is particularly the case with boards. This year's survey shows that 70% of boards have been educated about cyber risk, but only 40% have participated in a simulation exercise. Participation in simulations was notably higher for executive teams, at 69%.

The appropriate delineation of roles and responsibilities between the board and the executive team in a cyber crisis can be markedly different from everyday operations – particularly for 'active' boards.

70% of boards have been **educated about cyber risk** in the past 12 months.

ONLY 40% of boards have participated in a **simulation**.

35% of organisations have a director with **cyber expertise or experience on the board**.

36% of respondent boards have not decided whether they are **open to paying an extortion.**

"It can come as a surprise to directors that they play a relatively limited role in responding to a cyber crisis. While they must proactively supervise the response, very few decisions bubble up to board level. Boards must have confidence in management's ability to respond, and the interplay between management and the board is critical," Whittfield says. Ironing out creases in a simulated environment facilitates a smoother response in a real crisis.

Indeed, in our practice, we observe that sophisticated boards often bring a welcome sense of calm and strategic clarity to cyber incident response.

It is perhaps not surprising that boards have been reviewing their skill matrices and expending energy seeking new directors with cyber expertise or experience. Notably, 35% of organisations have done so. But there is a risk that complacency can stem from appointing a dedicated or uniquely qualified individual. "Effective incident response is multi-disciplinary," Whittfield says. "Relying on an individual or taking comfort in a particular individual's expertise can lead to a false sense of security. Cyber is like any area of business risk, and all directors should be armed with the skills to interrogate and actively participate in discussions. It is also entirely appropriate for a board to have the ability to directly interrogate cyber experts brought in to assist the organisation."

VIEWS FROM ASIA

Asian boards are less likely to have participated in cyber simulations than Australian boards and are also less likely to have been educated about cyber risk in the past 12 months.

Boards must have confidence in management's ability to respond, and the interplay between management and the board is critical"

CAMERON WHITTFIELD, PARTNER – APAC CYBER SECURITY HEAD

An essential role for legal teams

Lawyers are downplaying their relevance and deprioritising their preparedness. Our survey indicates that over 80% of respondents do not have a legal team budget dedicated to cyber risk. Furthermore, half of legal teams have never participated in a cyber simulation.

"These investment decisions echo the intense resourcing pressures imposed on in-house legal teams in the current environment. However, they do not sit comfortably alongside the integral role played by legal advisers in a cyber crisis," says Senior Associate, Heather Kelly, who brings expertise in both corporate law and at the frontline of cyber incident management, as an in-house lawyer. This observation is not lost on many survey respondents: 75% of respondents regard the legal team as "central" to their organisation's crisis response in the event of a cyber incident.

Lawyers may be intimately involved in reviewing compromised data, engaging with regulators; drafting communications for staff, customers and suppliers; assessing compliance risk and operational impacts; responding to contractual claims; and engaging with insurers. "Missteps managing the legal side of each incident response workstream can have significant regulatory and commercial consequences," says Kelly.

75%

of respondents say the **legal team is a key member of the crisis response team** in the event of a cyber extortion incident.

OVER 80%

of respondents **do not have a legal team budget specifically dedicated** to cyber risk.

59%

do not have a specific **legal cyber incident response plan.**

OVER 50%

of **legal teams** have **never participated in a simulation.**

ONLY 14%

of organisations have someone in the **legal team dedicated** to or **specialising** in **data/cyber risk**.

40%

have someone in the team tasked with **covering data/cyber as part of a broader remit,** but almost the same number (36%) have no one at all.

“These investment decisions echo the intense resourcing pressures imposed on in-house legal teams in the current environment. However, they do not sit comfortably alongside the integral role played by legal advisers in a cyber crisis.”

HEATHER KELLY, SENIOR ASSOCIATE

> Privilege should not get in the way of an effective response."
>
> **CHRISTINE WONG, PARTNER**

Christine Wong, a disputes partner with expertise in contentious privacy and data disputes, also raises the role of lawyers in managing legal professional privilege. In Wong's view, "privilege should not get in the way of an effective response, but given the real risks of follow-on litigation, whether and how privilege applies should be considered in incident planning ahead of time and modified as needed when a live issue arises".

Lack of expertise is an aspect of cyber risk giving rise to great concern among survey respondents. Only 14% of organisations have a resource in their legal team dedicated to or specialising in cyber and data. In our view, this concern is somewhat misplaced. It may sound comforting and indeed prove useful having such an individual available day-to-day. But engaging a trusted external adviser may support a more efficient and effective incident response, particularly where their expertise comes from deep experience across a broad range of incidents and industries.

The use of a preferred, trusted adviser needs to be managed in the context of any insurance policies. 76% of respondents have cyber insurance that often refers the policyholder to a list of the insurer's panel advisors. However, 80% say they would not engage a law firm from their insurer's panel.

Our survey data indicates this position arises, in part, due to a conflict of interest (perceived or real) between the policyholder and insurer on the extent of coverage or the management of any incident response. Our clients often express concerns about this issue and query whether cyber insurance panel law firms are acting in their best interests. While this may be confronting, it is a conversation unfolding regularly in boardrooms, as directors look to ensure they have the right type of support. Senior Associate Laura Newton brings deep expertise in regulatory and incident response across the public and private sectors. She believes that "it is imperative that businesses understand, practically, what a conflict of interest in the insurance panel model might mean for them – for example, understanding if the panel firm also advises their insurer on coverage determinations, and what information the panel law firm will share with the insurer, including any legal advice".

Obtaining adviser pre-clearance from insurers, in advance of an incident, puts an organisation in a strong position to be supported before, during and after an event, by a team that understands their people, processes and business strategy. The fly-in-fly-out cyber triage approach is certainly losing favour with large corporates.

VIEWS FROM ASIA

Australia-based respondents are much more likely to say they are central to the organisation's response in the event of a cyber event, with only 45% of respondents based in Asia saying they are central to the organisation's response. More Asia-based respondents consider themselves "important but not central" to the crisis response than Australia-based respondents.

> It is imperative that businesses understand practically what a conflict of interest in the insurance panel model might mean for them – for example, understanding if the panel firm also advises their insurer on coverage determinations, and what information the panel law firm will share with the insurer, including any legal advice."
>
> **LAURA NEWTON, SENIOR ASSOCIATE**

On the minds of General Counsel

> ...even companies that have heavily invested in cyber protections may well have an incident"
>
> CAROLYN PUGSLEY, PARTNER

Reputational risk of greatest concern

Reputational risk is the aspect of cyber risk causing organisations most concern. Putting the organisation in a strong position to withstand a reputational backlash following a cyber incident is now a critical task for boards.

This comes down to building internal 'muscle memory' and ensuring that businesses are prepared to navigate difficult judgment calls with poise in the heat of an incident response. "As a community, we've crossed the Rubicon in terms of recognising that even companies that have heavily invested in cyber protections may well have an incident," says Carolyn Pugsley, a senior partner in Herbert Smith Freehills' corporate governance team. "Now is the time to focus on what a good response looks like from a reputational perspective."

Accountability, transparency and empathy are guiding principles in protecting reputation and re-establishing trust in the aftermath of a crisis. Companies need to balance obligations to agencies and regulators, alongside communicating with customers and the public. Minimising potential legal losses should be a factor, but not the primary lens through which decisions are considered. Being seen as transparent and empathetic to stakeholders affected by a data breach may remain the right path, even if it impacts the organisation's legal rights and entitlements, including its ability to claim against a third-party.

In a crisis, organisations are pushing uphill to re-establish the trust that has been eroded by the breach. Reputation is critically linked to organisational survival. In a crisis response, stakeholders are given a clear view of the company's narrative, and its alignment or misalignment, with actions. Values-based communications are inextricably linked with a company's public license to operate, and this can be more critical in a crisis than simply minimising your legal exposure.

Legal teams have an important role to play in framing disclosures and disseminating accurate information. "Jumping out too fast, to push out information that isn't reliable and from which the business may need to backtrack only feeds a perception that you're not on top of the incident and not credible," Pugsley says.

Top 5

cyber risk concerns:

1. Reputational risk
2. Third-party risk
3. Underinvestment in systems or infrastructure
4. Aged data stores
5. Lack of expertise

VIEWS FROM ASIA

Our survey uncovered a major difference between Asia and Australia. More than 20% of Asia-based respondents say their organisation does not have a legal specific cyber incident response plan, while most Australia-based respondents say their organisation does.

Ransom payments fall out of vogue

We expect many Australian organisations will soon be required to disclose any extortion payments made in the context of a cyber incident. However, our survey data suggests a sustained trend away from paying ransom.

Consistent with last year's findings, a significant minority of those surveyed are aware of ransoms being paid in the context of cyber incidents. This is consistent with our experience. "The starting point in almost all cases is that organisations won't pay a ransom. Whereas if you rewind 12 or 18 months, that issue was up for grabs," Pugsley says.

This trend is generally consistent with recent findings from the global incident response firm, Coveware, whose Q2 2024 report depicts a general decline in the proportion of clients choosing to pay a ransom since Q1 2023.[2] Coveware reported that: "In Q1 2024, the proportion of victims that chose to pay touched a new record low of 28%."[3]

Our survey reveals that nearly 40% of boards have not decided (in advance of any cyber-attacks) whether they would be open to paying a ransom. However, it is unclear whether this cohort has the decision-making tools and legal advice needed to help them navigate this complex topic in the heat of an incident, or whether these boards intend to adopt a reactive approach. What we do know is that ransom discussions are complex. Paying a ransom can itself be an offence, under instrument of crime or terrorism financing law, for example, or if the organisation or individual receiving the funds is sanctioned (a strict liability offence).

The Australian Government established a thematic autonomous sanctions regime in 2021. This was first used on two individuals in 2024. Newton says, "the use of thematic autonomous sanctions adds a new component to the risk framework relevant to paying a ransom demand, as there is a heightened risk that a ransom payment may be directly or indirectly going to one of these individuals".

In our view, these concerns must be balanced against the operational impact of an attack, including on health and safety, and the overall best interests of the company. Indeed, paying a ransom demand may be the right path for an affected company.

New mandatory disclosure laws in Australia will hopefully shine a light on the scale of the problem, and this data can be effectively used by government to deliver targeted support for vulnerable sectors, particularly small-to-medium sized businesses.

"The starting point in almost all cases is that organisations won't pay a ransom. Whereas if you rewind 12 or 18 months, that issue was up for grabs"

CAROLYN PUGSLEY, PARTNER

A sobering wake-up

Third-party risk is a key cyber concern identified by respondents in this year's survey, second only to reputational risk.

The vulnerability of organisations to third parties is particularly topical in light of the CrowdStrike global outage in July 2024. "While not a cyber incident, CrowdStrike has shown how interdependent we all are," says Peter Jones, a corporate partner who specialises in complex technology and information transactions. "In a different context that could have been a cyber-driven impact. For example, the effect could have been materially worse had it been a malicious third-party that co-opted the platform."

Despite ranking as a key concern, addressing third-party risk was not prioritised by surveyed organisations in the past 12 months. There are lots of possible explanations but confusion over ownership of this risk within the business is likely to blame. Possibly, the CrowdStrike outage may be the sobering wake-up call that refocuses attention.

Mitigation of third party-related software risk is now a cornerstone of effective cyber risk management. "Given the interconnectedness of commercial relationships, it's not just the entity with which you directly deal, it's the entity beyond that and the one beyond that and so on," Jones says. Third-party risk extends to understanding how data is shared and managed by external parties. Many organisations provide highly sensitive commercial content to third and fourth-party service providers while conducting business. "These vendors are often the weakest link in the data management chain, and security controls must be implemented to manage these relationships and risks," Jones says. It is also necessary that relevant insurance programs are set up such that the loss caused by a third-party is adequately covered.

These weak links have not escaped government and regulatory attention. In the 2023–2030 Cyber Strategy, the government acknowledged the issue with insufficiently secure products and services being made available to businesses (and consumers), describing it as a 'market failure' that it is seeking to address. In July 2025, we expect Prudential Standard CPS 230 to take effect, which would require APRA-regulated organisations to effectively manage operational risks arising from service providers.

There are many ways that a company can build a more robust supply chain. These include thorough due diligence, comprehensive onboarding and enforceable standards in vendor contracts. Contract privity between different parties in a supply chain can make it hard to flow through legal obligations. However, as ASIC Chair Joseph Longo said in 2023,[4] "[it]'s not enough to sign a contract with a third-party supplier – you need to take an active approach to managing supply chain and vendor risk. Setting it and forgetting it, does not, cannot, and will not work."

It is possible for a company to be subjected to customer claims in connection with the impacts on affected customers of poor supply chain management. Additionally, relevant regulators could bring an action against an organisation that had not discharged its obligation to manage third-party risk, especially given the role of directors to provide supervision of the corporate entity. "Good risk management would look at third-party risk issues. It comes back to organisations making general decisions about their risk exposure and what they can do to mitigate this," Jones says.

Addressing **#7**
third-party risk ranks in terms of surveyed organisations' **cyber risk priorities** in the past 12 months,

despite ranking **#2**
risk of greatest concern

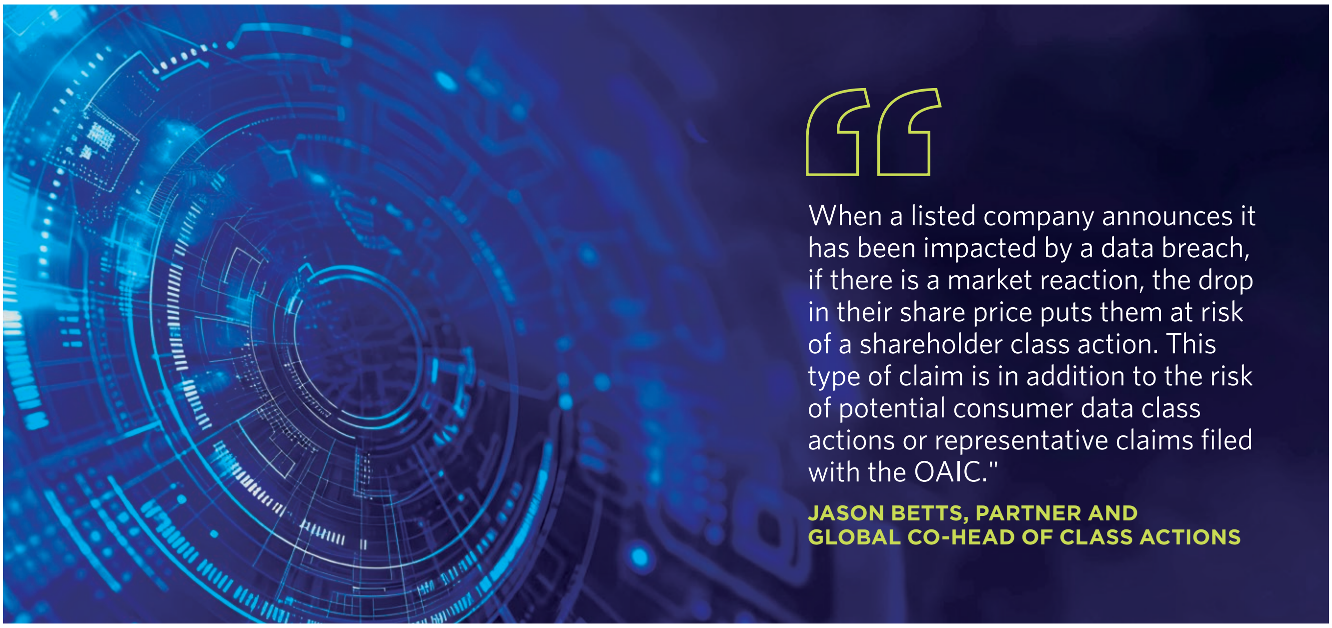
"The CrowdStrike incident has shown how interdependent we all are ... In a different context that could have been a cyber-driven impact. For example, the effect could have been materially worse had it been a malicious third-party that co-opted the platform"

PETER JONES, PARTNER

[2] Coveware, July 2024, 'Ransomware actors pivot away from major brands in Q2 2024'.

[3] Coveware, April 2024, 'RaaS devs hurt their credibility by cheating affiliates in Q1 2024'.

[4] Address by ASIC Chair Joe Longo at the Australian Financial Review Cyber Summit, 18 September 2023, 'Marconi's illusion: What a 120-year-old magician's trick can teach us about cyber preparedness'.



> When a listed company announces it has been impacted by a data breach, if there is a market reaction, the drop in their share price puts them at risk of a shareholder class action. This type of claim is in addition to the risk of potential consumer data class actions or representative claims filed with the OAIC."
>
> **JASON BETTS, PARTNER AND GLOBAL CO-HEAD OF CLASS ACTIONS**

Potential for cyber class actions looms large

Over half of survey respondents are concerned about the risk of class actions from cyber incidents. Perhaps unsurprisingly, concern is highest among organisations that hold a lot of consumer personal information, including banks, telcos and health providers.

The law with respect to class actions involving cyber incidents remains untested as no such case has proceeded to judgment. There is also currently no actionable tort for invasions of privacy. But just as threat actors are entrepreneurial and looking for opportunities, so too are plaintiff law firms.

According to Herbert Smith Freehills' Partner and Global Co-Head of Class Actions Jason Betts, listed organisations are particularly vulnerable. "When a listed company announces it has been impacted by a data breach, if there is a market reaction, the drop in their share price puts them at risk of a shareholder class action," he says. "This type of claim is in addition to the risk of potential consumer data class actions or representative claims filed with the OAIC."

58% of organisations are **concerned about class action risk.**

33% are concerned about their **data retention** practices.

46% have a poor understanding of the scale of their **organisation's current data footprint.**

83% of organisations that are "**very concerned**" about their **data collection and retention** practices are also concerned about **classactions**.

58% of respondents consider it would take a **cyber attack** to meaningfully improve their **organisation's focus on data risk management**.

5 Australian Prudential Regulatory Authority, 3 June 2024, 'Security and adequacy of backups'.

* Starting October 2024

The boundaries being tested by plaintiff firms are by no means static. For example, in June 2024, the ASX updated its Listing Rule Guidance Note 8 to include an example of managing continuous disclosure obligations during a fast-moving data breach. APRA has also emphasised its "heightened supervisory focus on cyber resilience, ensuring that all entities meet the requirements"[5]. Anticipated reforms to the *Privacy Act* are expected to introduce a direct right of action for individuals, paving the way for class action claims for breaches of privacy. The key issue will become proving loss in quantifiable dollar terms. According to Betts, "once you have a legislated right to privacy that, if breached, leads to a remedy, causation will be an easier element to prove than it is now. Suddenly you have a clear head of loss to sue under, which can lead to damages".

Christine Wong has advised on OAIC representative privacy actions and investigations. She agrees with Betts that the change is significant, given that "recovery for breaches of privacy is broader than for many other potential causes of action" such that "individuals can recover non-economic losses such as anxiety or embarrassment." Wong emphasises that potential regulatory action, with significant associated civil penalties and ongoing compliance burdens from enforceable undertakings may also be material issues for organisations, alongside class action risks.

While class action plaintiff law firms have been testing the strength of the data security obligations of impacted organisations, in time this may evolve into an examination of whether the data needed to be collected in the first place. 46% of respondents say their organisation has a poor understanding of their organisation's data footprint, and that this is a key barrier to improving data collection and retention practices. However, according to Betts, the mere act of probing data storage systems and practices may carry an obligation to resolve any issues identified as part of that exercise. Otherwise, organisations may leave themselves vulnerable to the discovery of documents highlighting a failure to take action. In this context, it is perhaps unsurprising that 83% of organisations who are 'very concerned' about their data collection practices are also concerned about class actions.

Class action risk is being used by threat actors themselves to increase pressure on their targets to pay ransoms. We have seen cases of threat actors warning corporate victims they should expect to lose material amounts in the courts if they decline to co-operate. We have also seen threat actors notify regulators of a breach, again to put pressure on the corporate victim. These are compounded by the escalating cost and complexity of navigating regulatory investigations and related litigation including class actions.

"Getting data right is critical. Data is the blast zone of a cyber incident."

MAGDALENA BLANCH-DE WILT*, CYBER RISK ADVISORY LEAD

"The mere act of probing data storage systems and practices may carry an obligation to resolve any issues identified as part of that exercise. Otherwise, organisations may leave themselves vulnerable to the discovery of documents highlighting a failure to take action."

JASON BETTS, PARTNER AND GLOBAL CO-HEAD OF CLASS ACTIONS

Data management in the spotlight

When an attack occurs, organisations have an immediate challenge to identify and interrogate compromised data. Getting a handle on their data footprint and the extent of any exposure is vital. This is so they can meet their regulatory obligations to notify stakeholders expeditiously, then focus on managing the regulatory, financial and reputational fallout.

Emily Coghlan, Director, Legal & Legal Technology, Digital Legal Delivery, leads a team at Herbert Smith Freehills that helps organisations identify compromised datasets, and triage and interrogate them quickly. The team can isolate particular sensitive types of data – for example, data containing personal information – using the latest technology tools, and then analyse it. This informs advice regarding the potential impact of the breach, and subsequent obligations such as notifying impacted individuals. "Over the last 12 months, we've had to review significant datasets where data has been exfiltrated from businesses and either dumped on the dark web or this has been threatened," Coghlan says. "The challenge of understanding your data footprint and being able to isolate and extract data really comes into play during a cyber incident where time is of the essence."

If gigabytes or terabytes of data have been compromised, the task of assessing the loss could involve sifting through millions of documents to extract potential personal information. AI tools that leverage pre-trained models are helping to scan data more efficiently and cull the documents that require review. "The technology is coming along quickly. These tools didn't exist a few years ago and they will get better. Machine learning, large language models and generative AI will help to extract personal information in these massive datasets much more quickly," Coghlan says.

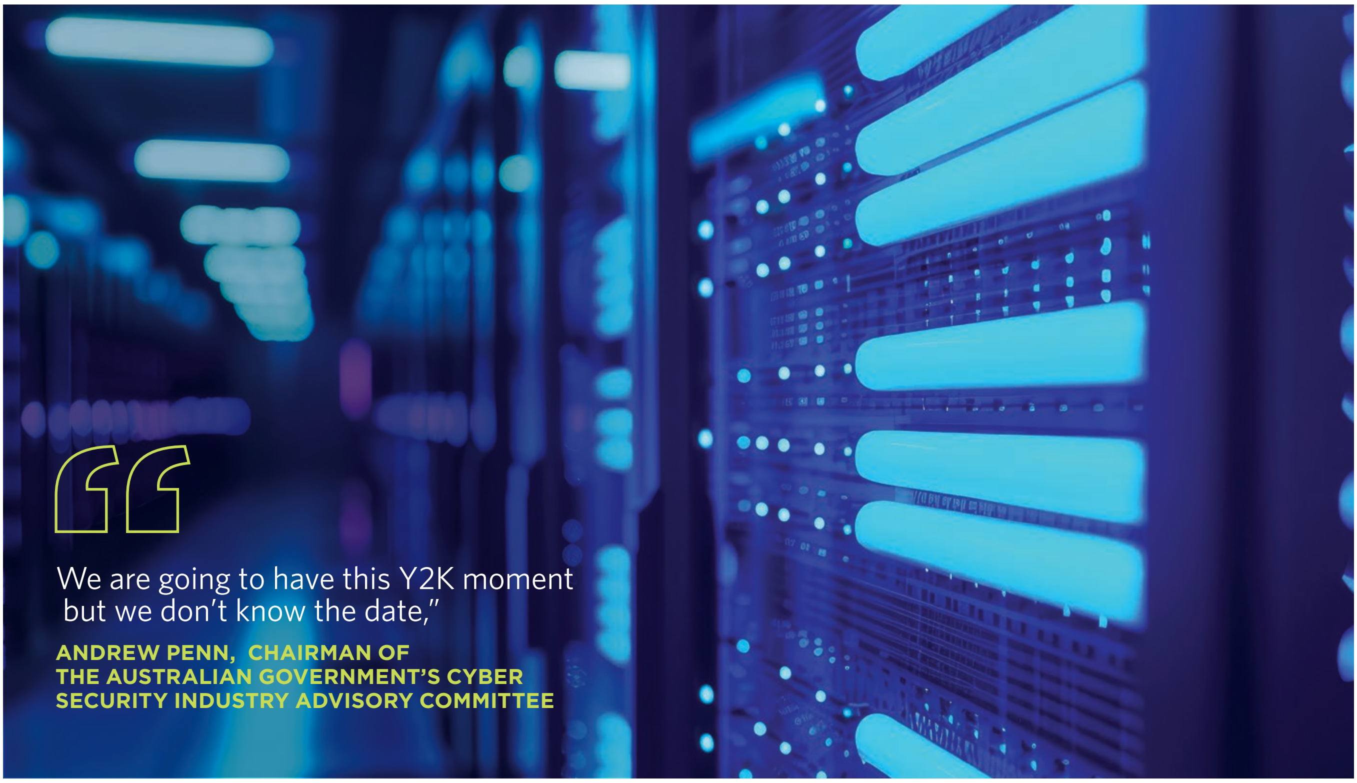
> It is not possible to protect something you don't know you have"
>
> **ANDREW PENN, CHAIRMAN OF THE AUSTRALIAN GOVERNMENT'S CYBER SECURITY INDUSTRY ADVISORY COMMITTEE**
> ***CROSS EXAMINING CYBER, EPISODE 6***

Getting a handle on your data footprint ahead of an incident is a critical part of cyber resilience. In May 2024, we spoke with Andrew Penn, former CEO of Telstra and recently Chair of the Australian Government's Cyber Security Industry Advisory Committee for the development of the 2023–2030 Cyber Strategy. Penn highlighted that "it is not possible to protect something you don't know you have".[6] He also emphasised the importance of creating a comprehensive inventory of digital assets to best protect them.

> Over the last 12 months, we've had to review significant datasets where data has been exfiltrated from businesses and either dumped on the dark web or this has been threatened..."
>
> **EMILY COGHLAN, DIRECTOR, LEGAL & LEGAL TECHNOLOGY, DIGITAL LEGAL DELIVERY**

Keeping watch

An evolving set of risk and regulatory changes on the horizon



> We are going to have this Y2K moment but we don't know the date,"
>
> **ANDREW PENN, CHAIRMAN OF THE AUSTRALIAN GOVERNMENT'S CYBER SECURITY INDUSTRY ADVISORY COMMITTEE**

Fast moving technology

In many respects, we are all still learning about the future technology impacts on cyber risk. Many commentators cite AI and generative AI, as both a force for good in fighting cyber crime, and as a force for bad in being exploited by threat actors. One thing we can all be sure of: emerging technologies will move at pace.

Recently, we have seen the mass compromising of business emails involving deepfake technology, not dissimilar to the attack suffered by engineering company Arup, in February 2024. This resulted in a HK$200 million fraud. We are aware of threat actors joining incident response video conferencing. It is fair to say that our adversaries are looking to exploit this development, which has accelerated even in the last few months due to rapid technology advancements.

The fact remains that many threat actors would prefer to attack using minimal effort. Indeed, this is why basic phishing exploits remain common place and effective. However, as AI becomes more accessible and deepfake technology proliferates, we can certainly expect this to become an increasing part of the threat actor arsenal.

The development of quantum computing should be watched with interest. In our recent conversation with Penn, he drew attention to a concern that many organisations have deprioritised: the vulnerability caused by reliance on encryption to advancements in AI and quantum computing. "We are going to have this Y2K moment but we don't know the date," he said.[7] In the context of an evolving threat landscape, Penn suggested that "success can't be defined as eliminating the digital threat; it has to be defined by learning to live with it".[6]

[6] Herbert Smith Freehills, Cross Examining Cyber: Conversations on Cyber Law, 'Episode 5: Cross Examining Andy Penn - Part 1'.

[7] Herbert Smith Freehills, Cross Examining Cyber: Conversations on Cyber Law, 'Episode 6: Cross Examining Andy Penn - Part 2'.

Privacy reform

75%

of organisations have taken steps to **review their data collection and holding practices**, but the projects are not yet complete.

58%

of respondents consider it would take a cyber attack to meaningfully improve their **organisation's focus on data risk management.**

Of the organisations taking steps to review their data collection and holding practices:

ALMOST 80%

are **focused on reducing aged data stores.**

71%

are **reviewing security and privilege setting** applied to important or sensitive data.

66%

are **reducing data collection/reviewing data collection practices.**

"For a little while there has been a culture that more data is better," says Special Counsel Kaman Tsoi, who advises clients on privacy and data protection. "It was fuelled by the boom in data analytics and cloud services. Companies where thinking 'Storage space is cheap, let's hang onto our data just in case. And we might find some way to monetise it down the track'. Keeping it all became easier than deciding what to get rid of and when."

Unfortunately, as many companies experiencing large-scale data breaches have found: too much data can be a problem when things go wrong, especially when the data is personal information. Several incidents have had consumers and media questioning why companies held such old data in the first place. In this context it is not surprising that, of the 75% of organisations taking steps to review their data collection and holding practices, 78% are focusing their efforts on reducing aged data stores.

Data retention has been a sleeper issue in relation to Privacy Act compliance for some time. However, we expect it will be brought back into focus in upcoming law reform. Specifically, certain companies may be required to establish minimum and maximum retention periods for personal information, as well as to specify retention periods in their privacy policies. The reforms may also create more flexible enforcement options for the Information Commissioner, including low and mid-level breaches. "At the moment, enforcement tends to be more focused on bigger incidents so there is a lot going under the radar," Tsoi says.

According to Emily Coghlan, the volume of data stored by businesses continues to mushroom. Data sources are also expanding, with new and emerging technologies creating additional challenges. This means organisations that have not been systematically reviewing and deleting their aged data have extraordinarily backlogged volumes. These companies are also potentially highly exposed in the event of a cyber incident.

> At the moment, enforcement tends to be more focused on bigger incidents so there is a lot going under the radar"
>
> **KAMAN TSOI, SPECIAL COUNSEL**

This will not come as a surprise to our survey respondents: while only 33% express concern regarding their organisation's data collection and retention practices, 58% consider it would take a cyber attack to meaningfully improve their organisation's focus on data risk management.

These statistics paint a sobering picture of complacency and inertia. But they should be taken in the context of protracted delays to anticipated reform. "Many legal leaders have not had the bandwidth, budget or executive buy-in to meaningfully address data concerns in a privacy landscape in limbo. In particular, we know clients are waiting to see words on a page and bipartisan support for the proposed reforms before green-lighting the adoption of certain AI tools." says Heather Kelly.

Developing ethical frameworks around the use of data is becoming important as more organisations contemplate use cases involving machine learning and generative AI according to Coghlan and Tsoi. This will involve balancing the opportunities from AI with the risks that come from hanging on to potentially irrelevant data. For example, it may be possible for a business to de-identify all its customers transactions for the purposes of generating insights from an AI model. However, attempting to obtain insights at the individual customer level will more likely require greater risk assessment, transparency and fairness under new privacy provisions.

VIEWS FROM ASIA

Asia-based respondents are relatively more concerned than those based in Australia regarding their organisation's data practices. However, reducing aged data stores and reviewing data collection practices have not been priority steps for managing data risk. Instead, many organisations are focusing their efforts on managing privilege settings and other security infrastructure solutions. It seems they see it as predominantly a technical issue.

> Many legal leaders have not had the bandwidth, budget or executive buy-in to meaningfully address data concerns in a privacy landscape in limbo."
>
> **HEATHER KELLY, SENIOR ASSOCIATE**

The 2023–2030 Cyber Strategy: A quick fix or a slow burn?

Implementation of the 2023–2030 Cyber Strategy is taking shape, albeit very slowly. It was released in November 2023 and we are yet to see meaningful legislative outcomes from an ambitious two-year Action Plan.

Our survey shows that most participants are familiar with the strategy, but do not have a view on it. Of those who are familiar with it, 17% support its reform agenda, while the same percentage (17%) think its proposals did not go far enough in addressing cyber risk relevant to their organisation. Concerns about the strategy shared via the survey are consistent with what we are hearing from clients – in particular, concerns about information (including threat intelligence) sharing and a lack of clarity around 'no fault' reporting. We share these concerns and look forward to further guidance in the months ahead.

More than 50% of survey participants believe the Government could do more to address potential cyber security risks to the Australian economy.

Whittfield is concerned that the Australian Government has bundled the Minister for Cyber Security in with a number of other portfolios, following a ministerial shake-up announced on 28 July 2024. "While we may not need a standalone Cyber Security Minister, cyber is now simply one of a large number of significant portfolios assigned to a single minister. There is a risk of cyber being deprioritised at a time when we need it to be front of mind," Whittfield says.

The ministerial restructure is noteworthy given the emphasis placed on strengthening the Australian Government's cyber resilience in the 2023–2030 Cyber Strategy. In July 2024, the Department of Home Affairs acknowledged it had made limited to no progress against the majority of action items pertaining to public sector security and sovereign capabilities in the Horizon 1 Action Plan, including uplifting the cyber security of the Australian Government[8].

This follows a report published in June 2024 by the Australian National Audit Office,[9] which identified ongoing low levels of cyber resilience in non-corporate Commonwealth entities.

But credit where credit is due. In the time Clare O'Neil MP, now federal Minister for Housing, held the country's first cyber ministry portfolio, we believe the Government demonstrated great focus and engagement regarding cyber. It appointed an Expert Advisory Board to advise on the development of the 2023–2030 Cyber Strategy, and released the strategy and accompanying Action Plan. It established a National Office of Cyber Security and appointed a National Cyber Security Coordinator. It also introduced new cyber security legislation to improve information sharing and mandate the disclosure of ransom payments.

VIEWS FROM ASIA

Similar to Australia-based respondents, Asia-based respondents want more specific guidance on building cyber resilience. But unlike Australia-based counterparts, they would like specific regulation to help them achieve it – something that is not a top 3 priority for Australian respondents.

MORE THAN

50%

say the **Government could do more** to address cyber risk.

Less than a third say they are very or quite familiar with the **Australian Government's Cyber Security Strategy.**

> There is a risk of cyber being deprioritised at a time when we need it to be front of mind"
>
> **CAMERON WHITTFIELD, PARTNER – APAC CYBER SECURITY HEAD**

[8] Hansard - Senate Estimates, 25 July 2024, 'Department of Home Affairs response to Portfolio Question Number BE24-0018'.

[9] Australian National Audit Office (ANAO), 14 June 2024, 'Management of Cyber Security Incidents'.

How we can help you

At Herbert Smith Freehills, we understand that managing cyber risk is one of the highest priorities for our clients. This is why we have built a dedicated cyber practice to provide 360-degree advice on all aspects of cyber preparedness and response.

We equip organisations to prepare for incidents and manage cyber risks before they arise. Our multi-disciplinary team have backgrounds in IT, forensics and cyber security, and can 'speak the same language' as your technical teams.

Offering a full range of cyber risk management solutions, our worldwide network provides a 'follow-the-sun' model that can support clients anytime, anywhere. Should an incident arise, we will immediately mobilise the right team of specialists to be by your side in those crucial first hours and days of a crisis. Whether your challenge relates to ransomware, cyber extortion, corporate espionage, inadvertent disclosure, advanced persistent threat, or something else – we have the subject matter expertise to assist you.

After an incident, we work with you to support with recovery activities, including through post-incident reporting, regulator engagement, insurance claims and dispute management.

Our dedicated cyber team is supported by a 350+ strong global team of data and technology specialists providing the full suite of data breach analytics services, to get to the heart of compromised data and to understand the issues it presents.

Our cyber offering

Cyber risk management and advisory

- Incident response/crisis management plans/playbooks/checklists
- Cyber simulations and tabletop exercises
- Data collection/retention/compliance advice
- Privacy impact assessments
- Board/ELT advisory and training
- Cyber due diligence assessments
- 3rd party risk management reviews
- Supplier and customer contract reviews
- Insurance advisory and negotiation
- FIRB compliance assessment
- Security of Critical Infrastructure Act advice

Post-incident response

- Data breach notification management
- Post-incident reviews
- Insurance claim management
- Realising insurance recoveries
- Litigation support including class actions
- Ongoing regulatory engagement support
- Post-incident contractual uplift advice

Incident response

- Response coordination ('breach coach')
- Legal and regulatory advice including market disclosure/directors' duties/regulatory and contractual compliance
- Extortion negotiation management
- Communications/media/PR management
- Regulatory and law enforcement engagement
- Forensic investigation management
- Impacted data hosting/analysis/review
- Emergency injunctions and take-down notices
- Insurance advisory

Our team

Australia

Cameron Whittfield
Partner – APAC
Cyber Security Head
T +61 3 9288 1531
M +61 448 101 001
cameron.whittfield@hsf.com

Peter Jones
Partner
T +61 2 9225 5588
M +61 436 320 477
peter.jones@hsf.com

Carolyn Pugsley
Partner
T +61 3 9288 1058
M +61 438 074 738
carolyn.pugsley@hsf.com

Jason Betts
Partner, Global Co-Head
of Class Actions
T +61 2 9225 5323
M +61 400 078 976
jason.betts@hsf.com

Priscilla Bryans
Partner
T +61 3 9288 1779
M +61 419 341 400
priscilla.bryans@hsf.com

Anne Hoffmann
Partner
T +61 2 9225 5561
M +61 418 906 447
anne.hoffmann@hsf.com

Merryn Quayle
Partner
T +61 3 9288 1499
M +61 405 538 746
merryn.quayle@hsf.com

Christine Wong
Partner
T +61 2 9225 5475
M +61 423 891 933
christine.wong@hsf.com

Kaman Tsoi
Special Counsel
T +61 3 9288 1336
M +61 412 687 842
kaman.tsoi@hsf.com

Jacques Giuffre
Executive Counsel
T +61 8 9211 7680
M +61 424 149 014
jacques.giuffre@hsf.com

Guy Narburgh
Special Counsel
T +61 2 9322 4473
M +61 447 393 645
guy.narburgh@hsf.com

Emily Coghlan
Director,
Legal & Legal Technology,
Digital Legal Delivery
T +61 3 9288 1474
M +61 412 958 233
emily.coghlan@hsf.com

Heather Kelly
Senior Associate
T +61 3 9288 1260
heather.kelly@hsf.com

Laura Newton
Senior Associate
T +61 2 9322 4120
M +61 460 817 111
laura.newton@hsf.com

Magdalena Blanch-de Wilt*
Cyber Risk Advisory Lead
**starting October 2024*

Marine Giral
Senior Associate
T +61 3 9288 1496
M +61 411 811 765
marine.giral@hsf.com

Josh Kain
Senior Associate
T +61 3 9288 1351
M +61 484 910 098
josh.kain@hsf.com

Caitlyn Bellis
Solicitor
T +61 2 9322 4579
M +61 447 829 506
caitlyn.bellis@hsf.com

Annie Zhang
Solicitor
T +61 3 9288 1133
M +61 432 724 968
annie.zhang@hsf.com

UK

Andrew Moir
Partner, Global Head of Cyber and Data Security
London
T +44 20 7466 2773
M +44 7 809 200434
andrew.moir@hsf.com

Peter Dalton
Partner, Cyber
London
T +44 20 7466 2181
M +44 7 818 764209
peter.dalton@hsf.com

Miriam Everett
Partner, Global Head of Data and Privacy
London
T +44 20 7466 2378
M +44 7 545 300862
miriam.everett@hsf.com

Asia

Peggy Chow
Of Counsel, Cyber and Data
Singapore
T +65 6868 8054
M +65 9757 7966
peggy.chow@hsf.com

Hannah Cassidy
Partner, Head of Financial Services Regulatory – Asia
Hong Kong
T +852 2101 4133
M +852 6392 3519
hannah.cassidy@hsf.com

24/7/365 Cyber Hotline

Contact us any time and day of the year. With a 'follow-the-sun' model, we will immediately assemble the right team to be by your side in the crucial first hours and days of a crisis.

T +61 3 9288 1000
hsfcyberhotline@hsf.com
cyber.australia@hsf.com

HERBERT
SMITH
FREEHILLS

CYBER

HERBERTSMITHFREEHILLS.COM