HERBERT SMITH
FREEHILLS
KRAMER

ARE YOU CYBER READY?

The cyber challenge through the eyes of Australia's legal leaders

Herbert Smith Freehills Kramer
Cyber Risk Survey Report 2025

Contents

02 The road to cyber agility
04 Survey results at a glance
06 The state of play
08 Supply chain insecurity
10 What do boards want?
12 Dealing with data risk
14 Practice makes perfect
15 Regulation driving uplift
16 Spotlight on SOCI
18 Legal team outlook
21 Ready or not?
22 Our team
23 How we can help you

The road to cyber agility

In a global climate characterised by escalating conflict, geopolitical tensions, economic headwinds and rapid technological advances, cyber security continues to dominate the corporate risk management agenda.

Australian businesses continue to grapple with their cyber resilience and contend with new cyber threats, all in a financially constrained environment. We have observed two significant challenges: How to maximise cyber investments and how to support organisations avoid 'cyber fatigue'? These challenges are exacerbated when cyber attacks fall out of the headlines and return on investment is hard to quantify.

Now in its third year, the HSF Kramer Cyber Risk Survey serves as a unique touchstone, seeking the views and experiences of legal leaders across corporate Australia.

This year, we received more input from general counsels (or equivalent) than ever before, from a diverse range of sectors including consumer services, financial services, resources, health and energy.

Consistent with our experience, legal leaders continue to play a central role in organisational cyber security, with a significant uptick in their own cyber education, simulation participation and incident response involvement. This reflects the role legal experts play, especially when an incident occurs, often being called upon to navigate complex regulatory compliance, urgently finalise critical communications, engage with key stakeholders and assess impacts, and lead remediation and recovery workstreams. It also reflects the magnitude of legal risks – and the long legal tail – inherent in any material incident.

This year, 68% of respondents believe cyber threat has increased in the past 12 months compared with 80% in 2024. One may perceive this as running contrary to the evidence, including the Australian Signals Directorate (ASD) reporting that the number of ransomware attacks and common vulnerabilities and exposures increased from 2023-24.[1] It is possible some respondents are experiencing cyber fatigue, or simply acclimatising to the risk. What is clear is that more than two thirds of respondents believe cyber risk is growing year-on-year.

Last year, we focussed on the technology challenges and the need for basic cyber hygiene, often solved with fundamental technology investment and practices. This year, we see a significant shift back to individuals: the human element. This is seen both in terms of: (a) cyber resilience, with responsibility to defend against cyber risks required across all individuals in an organisation, and (b) on the attack side, where we are now seeing highly sophisticated social engineering techniques, exacerbated by the use of AI and attacks perpetuated by criminals whose first language is English.

When it comes to maintaining cyber risk management and enhancing resilience, organisations can't afford to get comfortable. Cyber risk management must be fully embedded in daily operations across all business functions, with a continuous commitment to scrutiny and improvement. Regrettably, we must adopt a position of zero-trust.

In an environment characterised by rapid digital transformation, increasing data volumes and reliance on complex supply chains, there also needs to be a shift in how cyber security is approached. In particular, in relation to third-party and data-related risks, which rose to the top two cyber risks for organisations this year.

I recall discussions 15 years ago, where experts warned cyber risks involved people, process and technology. Nothing has changed.

This is why the management of this risk needs to be democratised across the business. It is as much a risk for the Chief Information Security Officer (CISO), as it is for leaders dealing with data governance, human resources, procurement, legal and finances, to name a few.

This democratisation has now made it to the board room. We are now seeing boards reviewing their reporting processes around cyber, stepping back from traffic-light metrics focussed on technology projects, to reports that appreciate cyber risk is being managed across all aspects of the business.

Technology risk assessments are also shifting. The rise of generative and agentic artificial intelligence is similarly an 'all company' opportunity and risk, and we are seeing the assessment combine with cyber security. That's because we can't assess our approach to AI without considering the security elements.

Of course, our adversaries are also experimenting with AI. This year's survey found that, of respondents who believe cyber risk has increased, 75% attribute the increase to the emergence of new and more sophisticated tech driven cyber threats. However, while there is no doubt emerging technology does present new risks, many organisations are still failing to get basic cyber hygiene right.

Of concern, only 45% of respondents believe their boards are 'cyber mature' and fewer than 40% of boards participated in a simulation in the last 12 months. The number of boards receiving cyber education dropped from 70% in 2024 to 59% in 2025.

Through this survey, we aim to make a meaningful and thought-provoking contribution to Australia's cyber security discourse. We also hope to support legal leaders by giving them the confidence to play a central role in protecting our nation's companies and their customers from cyber threats.

In an uncertain world, one thing we can be sure of is that cyber security will remain central to managing and mitigating organisational risk.

We hope this report goes some way to help avoid complacency and shine a light on new cyber challenges, through the lens of our legal leaders – those who are invariably on the front line.

Cameron Whittfield
Partner – Head of Asia-Pacific Cyber Security

5 key themes

This year's survey results highlighted the following overarching themes:

1. The challenge in managing third-party and supply chain risks
2. Boards and management embedding cyber in the corporate DNA
3. Information risk convergence as a driver of cyber readiness
4. Incident response planning and the power of the simulation
5. Increase in regulatory complexity and a focus on enforcement

1 ASD, Annual Cyber Threat Report 2023-2024.

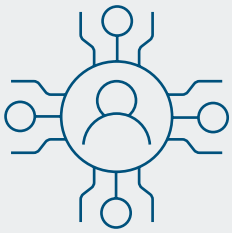
Survey results at a glance

68%

believe the **cyber threat has increased** compared to 12 months ago

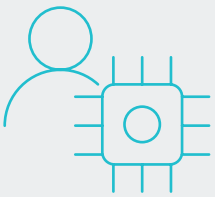
38%

are **not confident** their organisation is well placed to **manage and mitigate cyber risk**



45%

do not believe their board is **'cyber mature'**

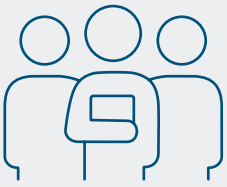


39%

of SOCI Act-regulated respondents believe the regime has had a significant influence on their **cyber risk management strategy**

70%

said their organisation had **cyber insurance**



76%

see Legal as a key member of the **crisis response team**

26%

did not know whether their organisation was captured by **operational resilience obligations**

33%

believe their boards have not decided whether they are open to paying an **extortion demand**

25%

of respondents' organisations were directly impacted by a **cyber incident** in the past 12 months

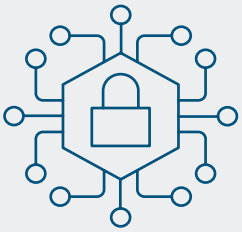
13% of those involved a **ransom**

75%

of respondents' organisations were impacted by a **third-party incident** in the past 2 years

63%

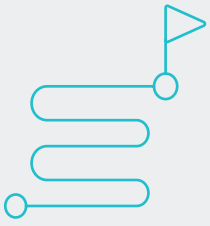
believe it would take a **cyber attack** to meaningfully improve focus on **data risk management**



36%

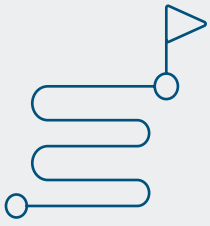
of boards have participated in a **cyber simulation** in the past year

Top 3



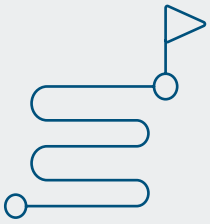
Cyber concerns

1. Third-party risk
2. Data-related risk
3. Technology/infrastructure risk



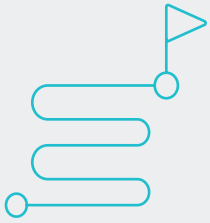
Cyber investment priorities

1. Reviewing or uplifting IT security infrastructure
2. Creating or uplifting cyber incident response plans
3. Testing relevant plans (eg simulations)



Internal drivers of cyber risk

1. Increased reliance on technology and outsourcing
2. IT security vulnerabilities arising from business transformation projects
3. Inadequate investment in IT security infrastructure



External drivers of cyber risk

1. New and evolving cyber threats (including AI)
2. Rising number of reported attacks
3. Recent regulatory scrutiny

The state of play

In our digitally-reliant and data-saturated world, the intersection between the law and cyber security has never been more important – it is a space where operational and legal risks truly converge.

From ensuring compliance with complex regulatory regimes to providing support and advice when responding to significant cyber incidents, the centrality of legal teams in an organisation's cyber risk management strategy has continued to strengthen across all sectors.

It is important to understand how lawyers consider cyber security at an organisational level – what are the key risks, what are the key opportunities, and how are the executive and board performing?

The HSF Kramer Cyber Risk Survey is unique. It specifically explores the perspectives of Australian legal leaders on organisational cyber risk maturity and strategy. This makes it a valuable tool – not only to measure sentiment, but also to consider areas of strength and areas where improvement is required.

Over the past 12 months, a lot has changed. The world is in a state of geopolitical flux. Inevitably, this impacts the cyber threat environment.

While we may naturally look to areas of conflict, shifts in US politics have had global ramifications, with realignment of security priorities and funding cuts to the US Cybersecurity and Infrastructure Security Agency (CISA). We have seen key initiatives come to an end or put in abeyance. All the while, our adversaries appear to be investing more than ever before.

The domestic regulatory environment has also continued to evolve, with the passage of Australia's *Cyber Security Act 2024*, updates to the *Security of Critical Infrastructure Act 2018* (SOCI Act) coming into force, and *Privacy Act 1988* (Privacy Act) reform still high on the Federal Government's agenda.

Technological advances have marched on, with increasingly sophisticated GenAI and agentic AI models ushering in new and concerning cyber risks.

Teamed with economic uncertainty, increasing compliance and increasing supply chain complexity, it is undoubtedly a challenging environment for cyber security professionals.

This report addresses these issues and also provides unique insights from some of the country's foremost cyber leaders from across the public and private sectors, as well as HSF Kramer's cyber experts.

It also provides a longitudinal view of the evolving attitudes, understanding and concerns of Australian lawyers in relation to organisational cyber risk management and strategy, which can help inform and improve these practices into the future.

The social engineering threat

Organisations should be acutely aware of the threat posed by sophisticated social engineering campaigns being launched by cyber criminals via deep fakes and tailored communications exploits.

In particular, board directors, senior executives, system administrators, contact centres and IT help desks staff are key targets.

Social engineering techniques are used by threat actors to gain access to systems, reveal credentials, disclose sensitive information or steal money, among other things.

According to the ASD: "Malicious actors often go to great lengths to make their communication seem legitimate and trustworthy, increasing the chances that targeted personnel will follow their instructions. Recent advancements in AI have amplified the effectiveness of social engineering techniques".[2]

"We are now being confronted with an attack vector that is immune to traditional cyber defence techniques. When an English-speaking individual impersonates a staff member, often using information in the public domain, the organisation's security perimeter changes. It now includes any individual in a customer or employee support role," Whittfield observed.

> We are now being confronted with an attack vector that is immune to traditional cyber defence techniques."
>
> **CAMERON WHITTFIELD, PARTNER**

CISO insights

HSF Kramer spoke to some of Australia's leading CISOs about how they believe cyber security risk can be better managed and shared across organisations. These are their five key takeaways:

1. Cyber security is now viewed as a whole-of business risk – but getting organisations on the same page, from top to bottom, remains challenging.
2. Partnership is important. Lawyers and CISOs have to work better together, by communicating more effectively to understand complementary and competing goals.
3. CISOs need more oversight and insight into an organisation's systems, controls and policies than ever before to effectively evaluate risk.
4. CISOs and risk & compliance teams should work hand in glove to evaluate and mitigate against risk and ensure regulatory compliance.
5. Third-party risk is significant and, at present, best managed through rigorous due diligence, regular auditing and tight contracting.

2 ASD, Social Engineering (29 May 2025).

Supply chain insecurity

The perils of third-party risk

Digital supply chains are increasing in scale and complexity, forming an interconnected network of hardware, software, personnel and data flows that deliver digital products and services, from development through to deployment and ongoing support. These functions touch every part of the digital ecosystem relied upon by organisations, from cloud providers, computer hardware and software, and managed service providers.

A spate of recent cyber incidents has illustrated that complex supply chains have significantly expanded the cyber attack surface, providing new avenues for malicious actors to exploit. Indeed, 75% of respondents reported their organisation had been impacted by a third-party incident over the past two years.

In this year's survey, third-party risk ranks as the top cyber-related risk, closely followed by data-related risks. An increased reliance on technology and outsourcing was identified by respondents as the key internal driver of the increase in cyber risk.

This expanding risk profile has coincided with a rising regulatory focus on third-party risk, via the SOCI Act and the Australian Prudential Regulatory Authority's CPS230 and CPS234, which variously emphasise the need for businesses to conduct third-party risk assessments, establish clear contractual obligations and proactively map critical business services and dependencies.

Chair of the Australian Securities Investments Commission, Joe Longo, has specifically called out third-party risk, noting that: "none of us has control over the security of a third-party provider ... If we rely solely on the security measures those providers have in place, we leave a wide opening for a data breach if those measures are compromised".[3]

According to HSF Kramer's Magdalena Blanch-de Wilt, Executive Counsel and APAC Cyber Risk Advisory Lead, "If you experience a third-party incident, it can often be no different to an incident impacting your organisation directly. The impact on your operations may be the same, as may be the need to muster an incident response team, and you may need to invest the same type of resources and effort to manage the issues".

This sentiment is shared by Partner and corporate governance expert at HSF Kramer, Carolyn Pugsley, who said, in the

3 key

considerations we continue to see when a third-party cyber incident occurs

1. When a cyber incident impacting a third-party has a downstream operational impact
2. When a cyber incident impacts a third-party that holds or has access to another organisation's data, and that data has been accessed by a threat actor
3. When a cyber incident impacts a third-party that holds or has access to an organisation's data, and that organisation is subject to extortion as a result ie the threat actor has sought out the deepest pockets

3 Address by ASIC Chair Joe Longo at the AFR Cyber Summit, 'Marconi's illusion: What a 120-year-old magician's trick can teach us about cyber preparedness' (18 September 2023).

event of a breach "the general population don't really care if it was a third-party risk system failure that caused the incident".

"Reputationally you are carrying the can and reputationally the impact is the same as if it's your system ... Contractually, you may well be protected, you may well be insured, but really that's not what keeps boards awake at night. It's reputational and brand damage and the impact on that for customers or clients," Pugsley said.

It is surprising, therefore, that many companies are not investing in third-party risk management with the same focus as other activities. Despite significant concerns, addressing these risks was low on uplift priorities, ranking seventh in this year's survey. Ultimately, when it comes to the views of respondents as they pertain to third-party risk, the message is clear – the risk is well understood, but managing the risk is proving challenging.

These results are not surprising, says Heather Kelly, Senior Associate in HSF Kramer's cyber practice.

"Demonstrating a return on investment can be a real pain point. Third-party risk is somewhat intangible, and there is currently little regulatory guidance on what 'good' looks like. When coupled with economic uncertainty, it is no wonder that data risk management investment proposals are losing out to other, more established activities, such IT security infrastructure upgrades," Kelly said.

Blanch-de Wilt believes the dial might shift "when we see enforcement of a higher order", for example meaningful action taken by the ASIC, including when an incident involves a third-party.

To date, ASIC has only pursued Australian Financial Services Licence (AFSL) holders for breaches of licence obligations related to alleged failures to implement adequate cyber security measures. However, since late 2023, ASIC has emphasised it is actively investigating directors and executives for deficiencies in this area. We are yet to see anything come of this, but we know it remains a focus area for ASIC.

An emerging trend: third-party simulations

To support organisations better manage third-party risks and prepare for a significant cyber incident that may involve one, HSF Kramer's practice has expanded to run simulation exercises based on third-party incidents.

For example, some of HSF Kramer's clients are preparing for scenarios where their suppliers deliberately cut off the organisation's access to affected supplier systems during third-party attacks, in a good faith attempt to limit the impacts of the attack. Even if the customer does not receive a ransom demand, preventative measures such as these can present significant business continuity challenges for companies down that supply chain.

While this is still an emerging trend, Blanch-de Wilt said a movement towards using simulation scenarios involving a third-party incident is shifting the conversation and educating organisations about the cascading impact of such an event.

"I think we're slowly seeing that pivot away from organisations planning and testing only direct attacks on their own systems," she said.

"It is particularly important for organisations with complex supply chain, ownership and operational arrangements, like infrastructure, where you might have an owner, an operator and other stakeholders. To me, the next part of the evolution will be getting our third-parties involved in simulations. It would be great to see supply chain and partner ecosystem cyber incident response mechanisms being routinely tested through a simulation."

"If you experience a third-party incident, it can often be no different to an incident impacting your organisation directly."

MAGDALENA BLANCH-DE WILT, EXECUTIVE COUNSEL AND APAC CYBER RISK ADVISORY LEAD

What do boards want?

Despite a significant focus over the past several years on the importance of cyber preparedness for boards and a spotlight on overarching cyber governance practices, this year's survey found board maturity is still not where it needs to be, with 45% of respondents reporting they would not describe their board as cyber mature.

This trend was backed up by other data, which may signal cyber fatigue at the board level. For example, 32% of respondents did not believe their board had a clear understanding of the delineation between board and management roles and responsibilities during incident response. This may indicate that boards are not being familiarised with cyber incident response plans (CIRP), or that CIRPs do not clearly articulate 'who owns what' in the event of a cyber incident.

This dynamic may also be exacerbated by lack of exposure and upskilling via simulations: only 36% of boards participated in a cyber simulation in the past 12 months, and 18% have never participated in a simulation.

Courts and regulators expect boards to play a critical, but limited, role in incident response. One key decision usually reserved for the board is the decision to pay, or not to pay, a ransom demand. This decision requires directors to engage with a complex set of considerations, including an assessment based on directors' duties, reputational matters and the legality of payment.

Despite this, the survey found only 33% of boards have a ransom payment decision-making framework, and 33% of boards have not formed a view as to whether they would be open to paying a ransom. This latter statistic has not meaningfully shifted in the last 12 months (36% in 2024) and leaves us with a recurring problem: discussions in relation to payment may occur for the first time when an incident actually hits. We believe that many of these considerations can (and should) be addressed prior to any extortion demand.

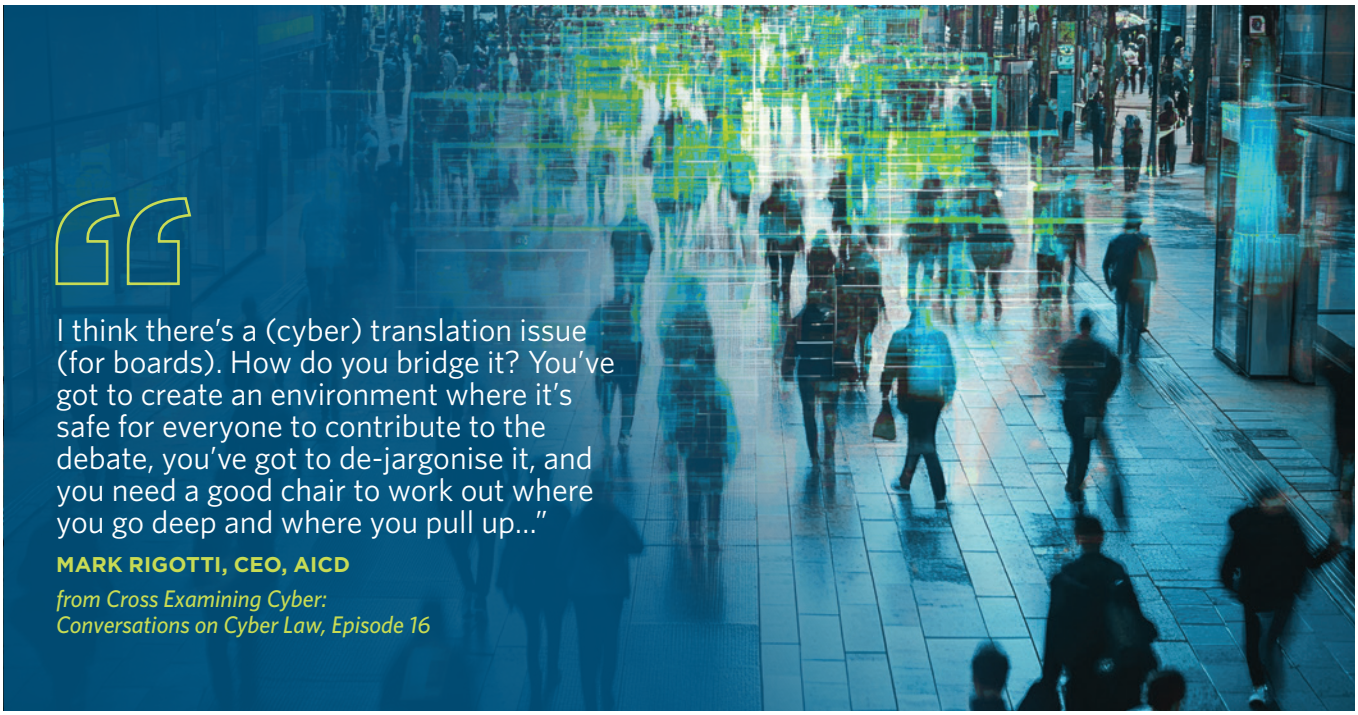
These results also suggest that boards may not possess the necessary agility to effectively respond to a cyber ransom demand acting consistently with their duties, noting that threat actors typically do not afford their victims much time to deliberate. Importantly, organisations with an annual turnover of greater than $3 million (and many SOCI Act-regulated entities) are now required to report payment of a ransom in connection with a cyber security incident within 72 hours under the *Cyber Security Act 2024*.

There is also a possibility cyber security has dropped in priority for boards amid an environment of competing demands. This plays out, for example, in the Australian Institute of Company Director's *Director Sentiment Index* for H1 2025: after holding the top spot for several years, cyber security dropped to third in order of priority.

Pugsley believes cyber risk is still a top concern for boards, with the shift in risk prioritisation reflecting the fact organisations are embedding cyber as a standard risk type.

She observed: "Cyber risk isn't going anywhere – it's here to stay. Boards are focusing on cyber reporting cadence and what effective cyber reporting looks like, while recognising the threat landscape and organisational risk will continue to change. For boards, cyber risk management has to be in your DNA".

> Good reporting draws out how the threat is changing, how well the business is (or isn't) prepared, how cyber preparedness intersects with other risks and opportunities and what further actions are recommended."
>
> **CAROLYN PUGSLEY, PARTNER**



How to report well

When it comes to board reporting, and presenting meaningful and useful information to the board, the first consideration should be who is leading and contributing to the report.

Cyber reporting was traditionally the domain of the CISO. However, as observed by Whittfield, siloed reporting can result in boards being presented with "vanity metrics" and not getting the "full organisational picture".

"Who's marking the marker? One thing we are seeing when an organisation comes to us and asks, 'what does good board cyber reporting look like?', is the need to look beyond the CISO report. How is the whole organisation considering and managing cyber risk? Each division of the business needs to 'own' cyber risk management in their area of responsibility," Whittfield said.

Pugsley notes that boards want to see the right kind of combination of stakeholders engaged around cyber as a risk area and know how those people and teams are working together to manage and mitigate risk.

"We've also moved beyond board reports that are just a list of actions that have been taken since the last update. Good reporting draws out how the threat is changing, how well the business is (or isn't) prepared, how cyber preparedness intersects with other risks and opportunities and what further actions are recommended. Fitting all of this into a punchy, digestible report is not easy, but directionally we are seeing a desire for and a shift toward more mature board reporting," she said.

Top 3 considerations for board reporting

1. **Who holds the pen?** Look beyond the CISO because cyber resilience extends to all aspects of the business.
2. **Be concise and to-the-point when considering:** What does the threat look like? What's the risk for our business? And how are we managing it?
3. **Provide solutions for the board to consider.** This may include options for resources to support cyber uplift, suggested updates to policies and procedures for approval, and gap analysis.

Dealing with data risk

While data is highly valuable, it can also increase the attack surface – a sentiment clearly expressed in this year's survey, where data's risk profile is rated second only to third-party risk.

Despite the risks, an alarming 63% of respondents reported that organisations often only start addressing data risk management and uplifting data governance after experiencing a cyber incident. More concerning is that this rate has risen from 58% in the past 12 months, reflecting a broader trend observed by the HSF Kramer team.

Heather Kelly notes the team recently coordinated several data governance projects, of various levels of complexity, for clients spurred into action following disruptive and distressing attacks on themselves or their competitors.

"Even though the public is accustomed to hearing about cyber attacks in the news, there is a sense that the public, and potentially regulators, will not be as forgiving when the next incident impacting their sector rolls around. Good data governance is now a critical part of cyber risk management," she said.

Furthermore, the survey found that while 85% of respondents reported their organisation had taken steps to improve data governance over the past year, approximately a third of respondents remained concerned that their data management practices were inadequate.

Kaman Tsoi, HSF Kramer privacy specialist and Special Counsel, said tackling data governance was a "daunting task" for some organisations, given the vast amounts of data that organisations hold in 2025. Data mapping and audits can also be cost prohibitive.

"If you step back and look at the totality of what you're trying to achieve as part of a data audit, that can scare organisations off. That's why we work hard to support clients by breaking the task up into smaller, more achievable tasks. You need to start somewhere, and it can help to approach things iteratively," Tsoi said.

In a positive sign, however, Emily Coghlan, Partner in HSF Kramer's Digital Legal Delivery practice, said she had experienced an uptick in the number of clients seeking to unpick and map their data footprint, including data flows to third parties.

"There's been a rise in work around information governance. That means organisations are looking much earlier on, before a breach occurs, as to where their data sits. They're also considering questions like: What does that then look like from a redundancy, resilience and information security perspective? Does that meet our data retention and privacy obligations?" she said.

It is possible this interest has been spurred on in part by recent changes in domestic privacy regulation. This includes the introduction of a new tiered penalty regime under the Privacy Act, which provides the Office of the Australian Information Commissioner more opportunities to pursue 'lower-order' privacy breaches, and clarification that under the Australian Privacy Principles 'reasonable steps' – in relation to obligations to secure personal information – include technical and organisational measures.

> "There's been a rise in work around information governance. That means organisations are looking much earlier on, before a breach occurs, as to where their data sits."
>
> **EMILY COGHLAN, PARTNER**

Christine Wong, HSF Kramer Partner and specialist in regulatory investigations and enforcement, said data risk was top of mind for corporate Australia due to the long tail of legal risks it can involve.

"The understanding of the level of risk associated with cyber security has certainly heightened – regulators like ASIC, APRA and OAIC are looking at considering enforcement from a range of angles (sector specific laws, privacy, prudential standards, directors duties). They're actively taking on significant cases. The financial implications of an enforcement action are more acute with increased civil penalties, and the ever present risk of class actions," Wong said.

> If you step back and look at the totality of what you're trying to achieve as part of a comprehensive data audit or data mapping exercise, that can scare organisations off."
>
> **KAMAN TSOI, SPECIAL COUNSEL**

So you've been hacked... now what?

A quick Q&A about injunctions with Tamir Maltz

Barrister at 12 Wentworth Selborne Chambers, Sydney

Why injunct a threat actor when you strongly suspect they won't comply with it?

It's true that a threat actor will likely ignore a court's injunction to take down stolen data posted on the 'dark' web. However, the injunction can be effective to dissuade third parties from going onto the dark web and accessing or disseminating the stolen data, and to encourage publishers not to publish (or to take down ASAP) any stolen data. This is because a third-party that's aware of the injunction can be in contempt of court if they take steps to knowingly undermine the injunction's effect. A data-breach injunction is not a 'silver bullet' – there are some drawbacks and limitations, some aspects remain untested, and it will not suit everyone. But it is now part of the breach-responders' legal armoury.

What are the qualities of a corporate victim that pursues an injunction?

As I mention earlier, a data-breach injunction will suit some corporations and not others. There are several circumstances that seem to lead victim corporations to take this course:

- the victim cannot or does not wish to pay a ransom demand
- the exfiltrated data's confidential nature has been substantially maintained
- the exfiltrated data is primarily of local interest (ie less likely to be published by overseas media entities, against whom it is more difficult to enforce an Australian court's injunction)
- the victim is the custodian of others' highly-sensitive data and feels almost a moral obligation to do 'everything possible' to protect the stolen data
- the exfiltrated data contains privileged or priceless trade-secret information
- the victim has substantial resources, and is seen as a motivated and credible legal 'threat', discouraging third parties from 'trying their luck' against the injunction

Do threat actors appear at injunction proceedings?

Perhaps unsurprisingly, these applications are invariably conducted 'ex parte'. Nevertheless, some anonymous threat actors have 'promised' to attend court if they are sent large amounts of bitcoin (necessary they claim, to cover the cost of flights to and accommodation in Australia...).

If you want to hear more, listen to Tamir Maltz speak with Christine Wong and Cameron Whittfield, on *Cross Examining Cyber: Conversations on Cyber Law, Episode 18*.

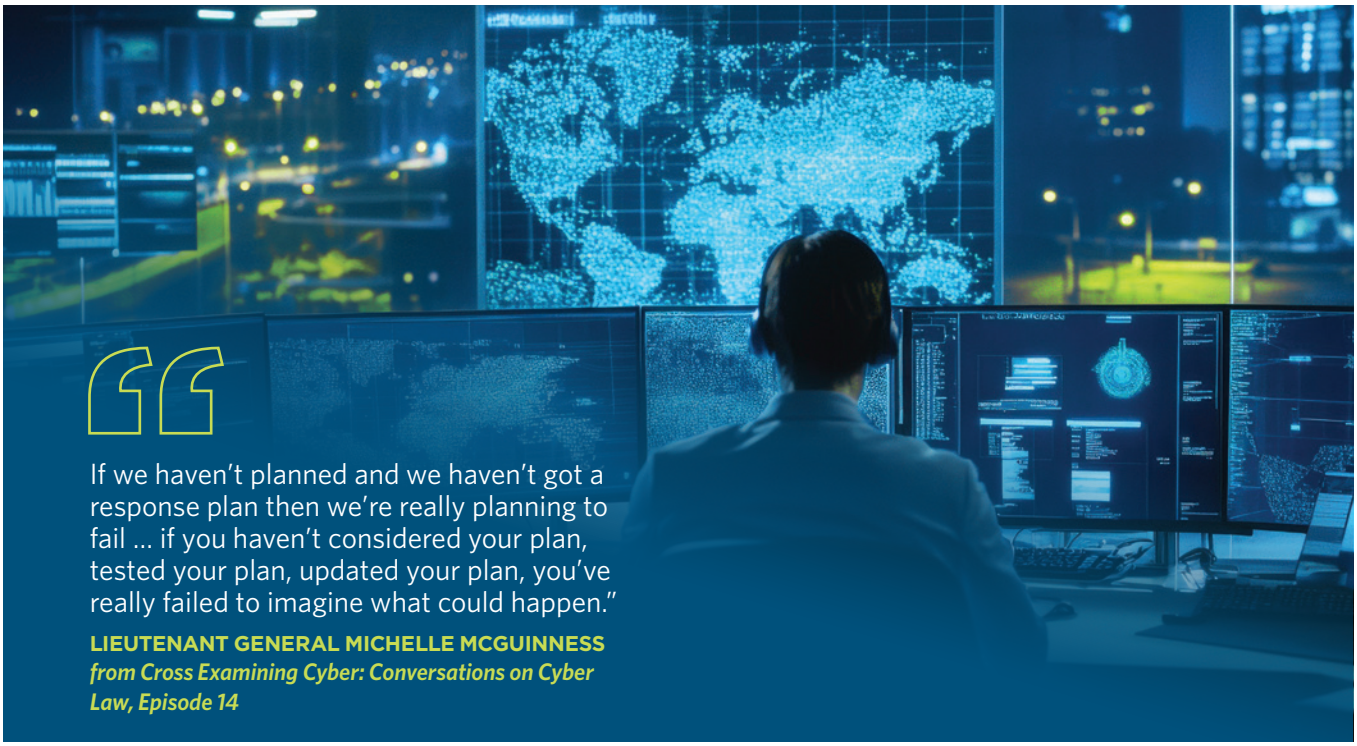
Class actions in focus

Cyber-related class actions are emerging as a material class action risk in the Australian market, as highlighted in Australian Class Action Risk Report 2024. Plaintiff law firms and litigation funders are increasingly targeting cyber incidents, particularly in sectors such as healthcare, insurance, and government, where sensitive information is heavily concentrated.

Australia's class action landscape is broadening to encompass cyber security breaches, driven by evolving case law, legislative reforms and expanding funding avenues. This growing threat is reflected in the results of the 2025 HSF Kramer Cyber Risk Survey, where 21% of respondents who reported an increased perception of cyber risk cited the potential for class actions as a contributing factor.

According to Jason Betts, HSF Kramer Partner and Global Co-Head of Class Actions, "organisations must adopt proactive safeguards – such as robust data governance, timely breach response protocols, and transparent communication strategies – to reduce legal vulnerability and maintain stakeholder confidence".

Practice makes perfect



> If we haven't planned and we haven't got a response plan then we're really planning to fail ... if you haven't considered your plan, tested your plan, updated your plan, you've really failed to imagine what could happen."
>
> **LIEUTENANT GENERAL MICHELLE MCGUINNESS**
> ***from Cross Examining Cyber: Conversations on Cyber Law, Episode 14***

The importance of simulations

Cyber simulations are an increasingly important part of organisational cyber preparedness, building the muscle memory necessary to drive effective decision-making in the event of a cyber attack.

This year's survey found in the 12 months prior, 53% of respondents had participated in a cyber simulation, which represents a significant increase in participation by legal teams from previous surveys.

However, only 52% of boards had ever participated in a simulation, with just 36% taking part in one in the last 12 months. The survey found 18% of boards had never been involved in a simulation, despite encouragement from industry bodies such as the AICD and increasing emphasis from regulators such as ASIC about the importance of incident response testing.

Whittfield noted that simulations are an effective way of engaging boards, particularly those less familiar with cyber risk.

"There is usually a 'Eureka moment' in these simulations. Board members previously lacking confidence in the subject matter suddenly click into the room, become fully engaged and then we're off," he said.

HSF Kramer's Peter Jones, Partner and telecommunications and financial services expert, highlighted the need to ensure simulations remain "fresh", so participants do not become complacent.

"If you don't actually learn anything from a simulation, then it's not a useful test. A well-developed simulation should stress-test areas that are in need of improvement and encourage participants to engage in some uncomfortable decision-making. Participants should not expect to walk away from a simulation patting themselves on the backs," he said.

"Simulations have evolved significantly. We're now designing tailored simulations that are plausible and align with an organisation's sector, functions and specific operations. They also need to test the parameters of people's understanding and how they want to go about managing risk as a part of an integrated enterprise."

"In addition, the importance of simulations is also being recognised by regulators. There's an expectation, whether it's explicit or implicit, that organisations should be testing incident response plans and undertaking simulation activities, particularly in and around cyber risk and resilience."

Whittfield noted for listed companies, continuous disclosure obligations were a key topic.

"We spend a lot of time with listed company boards, engaging with issues related to trading halts and ASX disclosures as a result of a cyber incident. As recently as twelve months ago, boards would default to a trading halt and disclosure. Now, we are seeing a more considered approach, applying the appropriate legal tests and acknowledging that many cyber incidents are not price sensitive. Each incident must be considered on its facts," he said.

Regulation driving uplift

While there has been significant reform of Australia's cyber-related laws over the last several years – as well as increased signalling from regulators that action will be brought against organisations not fulfilling their obligations – attitudes towards regulation were generally positive.

Jones said there is broad acceptance that appropriate regulation is a good thing, and clear regulation can create certainty for organisations as they invest in regulatory compliance, including cyber uplift programs.

He also noted that progress on recent cyber regulatory reform had been marked by high levels of consultation, which had facilitated increased collaboration and enhanced trust between government and industry.

"When it comes to certain regulatory reform areas in Australia, we have seen a degree of genuine consultation and willingness to have open conversations. However, I do think that improved coordination and prioritisation across the different regulators, when they are looking at major reform, would be viewed as a useful development," Jones said.

The survey results also suggest that there is some confusion when it comes to terminology used in the regulation of cyber risk in Australia. 26% of respondents admitted to not knowing whether operational resilience obligations applied to their organisation. However, there was greater awareness among organisations captured by the SOCI Act (53% of respondents), with just 6% of those respondents uncertain about their operational resilience obligations.

Despite the comparatively positive outlook in relation to certain aspects of the regulatory environment, Jones noted that, for organisations operating in an internationally competitive environment, overly-onerous domestic compliance requirements or ones which have significant productivity impacts could result in "regulatory arbitrage".

"If a regulatory regime becomes too difficult and costly to comply with, then international organisations may refocus investment in offshore locations which may have lighter handed regimes," Jones said.

"While there are challenges in that space however, no one is saying 'get rid of regulation'. Rather, I think people are saying we need appropriately calibrated regulation that is focused on a proportional response to risk. And it can never be zero risk."

"The regulators are not usually starting with an enforcement or investigation mindset. Very few incidents (relative to the total number of incidents) lead to investigations and, in our experience, a constructive relationship with regulators, whether before, during or after an incident, can be a very useful approach. Misunderstandings can occur 'on the papers' and a combative approach to engagement can lead to unnecessary scrutiny."

CAMERON WHITTFIELD, PARTNER

"I do think that improved coordination and prioritisation across the different regulators, when they are looking at major reform, would be viewed as a useful development."

PETER JONES, PARTNER

Spotlight on SOCI

In terms of regulatory regimes impacting organisational cyber security practices, the survey found the SOCI Act has had a marked impact on driving uplift.

According to respondents regulated by the SOCI Act, 88% reported the regime had an influence on their approach to cyber security.

There is also evidence that SOCI Act regulation correlates with respondents reporting higher rates of cyber readiness.

For example, according to respondents regulated by the SOCI Act:

69%
believe their boards are **cyber mature**

90%
view Legal as a **key member of the crisis response team**

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

46%
of boards have **participated in a simulation** in the past 12 months

Consistent with the broader survey results, the top 3 cyber concerns are

1. Third-party risks
2. Data-related risks
3. Technology/infrastructure risks

The top 3 cyber investment priorities are

1. Creating or uplifting cyber incident response plans
2. Testing relevant plans; Reviewing or uplifting IT security infrastructure (tied)
3. Board/management engagement or education

SOCI sector comparison

Energy and infrastructure

Top 3 cyber-related risks

1. Third-party risks
2. User-related risks
3. Business continuity risks

54%
believe their boards are **cyber mature**

40%
of boards have **participated in a simulation** in the past 12 months

Top 3 cyber priorities

1. Testing relevant plans
2. Reviewing or uplifting IT security infrastructure
3. Creating or uplifting cyber incident response plans

72%
boards have been **educated about cyber risk** in the past 12 months

88%
view Legal as a **key member of the crisis response team**

Financial services

Top 3 cyber-related risks

1. Data-related risks
2. Third-party risks
3. Technology/ infrastructure risk

69%
believe their boards are **cyber mature**

54%
of boards have **participated in a simulation** in the past 12 months

Top 3 cyber priorities

1. Managing data-related risks
2. Testing relevant plans
3. Board/management engagement or education

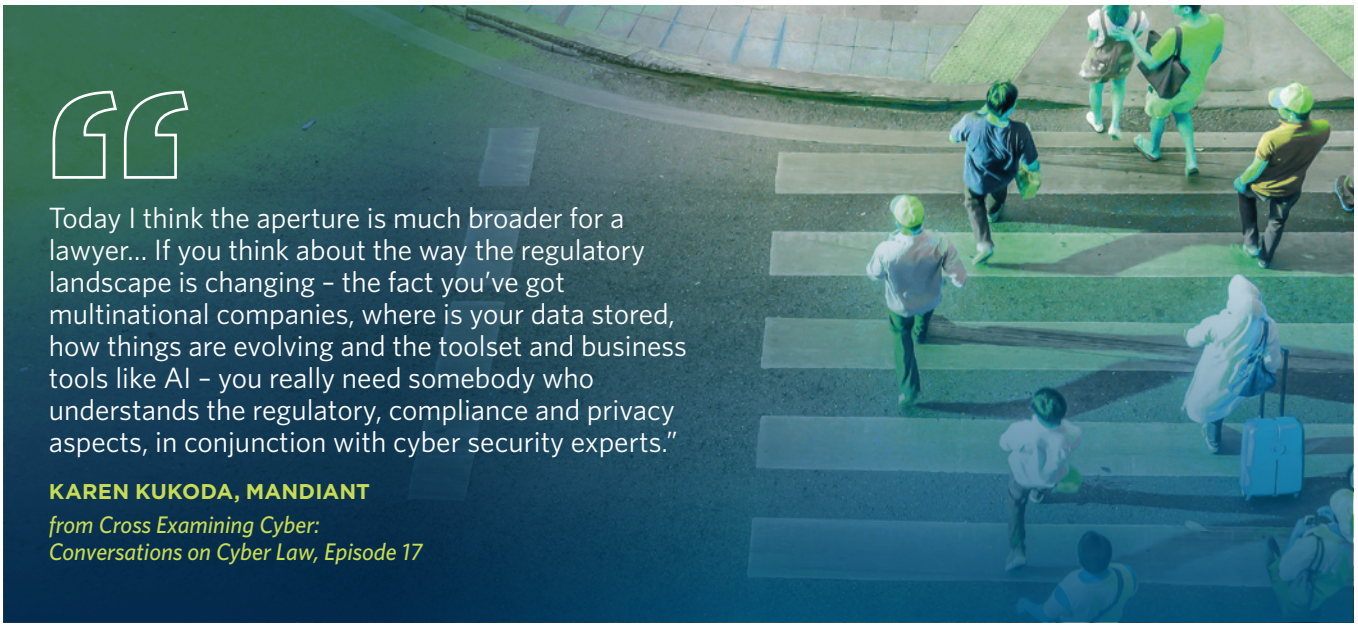
54%
boards have been **educated about cyber risk** in the past 12 months

95%
view Legal as a **key member of the crisis response team**

"The banks are acutely aware of their regulatory obligations but across the financial services sector, there is a divide. Concerns have been raised about superannuation funds because it's an area where there have been issues and a need for the regulator to play a stronger role. There would be huge social effects in the event of a serious cyber impact on a super fund, and if significant amounts of money were stolen."

PETER JONES, PARTNER

Legal team outlook



> Today I think the aperture is much broader for a lawyer... If you think about the way the regulatory landscape is changing – the fact you've got multinational companies, where is your data stored, how things are evolving and the toolset and business tools like AI – you really need somebody who understands the regulatory, compliance and privacy aspects, in conjunction with cyber security experts."

KAREN KUKODA, MANDIANT

from Cross Examining Cyber: Conversations on Cyber Law, Episode 17

The role of legal teams as key players in managing organisational cyber risk is clear, with 76% of respondents reporting that legal functions are central to incident response.

Notably, there are two key areas where the importance of the legal-cyber nexus are best highlighted – the increase in legal-focussed cyber incident response plans (CIRP) and simulation participation.

These figures clearly illustrate legal expertise is valued and, in many organisations, viewed as critical to cyber security risk management, incident response, regulatory compliance and reputation management.

Jones reflected that one of the key strengths of a general counsel during a cyber crisis is the ability to manage stressful situations analytically and objectively, enhancing clarity and assurance for boards.

"They are good at taking the heat out of situations and focussing on the matter at hand," he said.

"I also think the ability many lawyers have to manage multiple streams of work is also something that is typically very important, and critical when an incident has occurred. They can balance the need to move quickly with best protecting an organisation."

The number of respondents reporting their organisation has a legal-focussed CIRP has increased significantly, from

19% in 2023 to **51%** in 2025

And the rate of legal teams participating in simulations has jumped over the last two years, increasing from

38% in 2023 to **53%** in 2025

Organisational structure can create siloes

The HSF Kramer team has observed some general counsel still report a disconnect between cyber, digital teams and broader business operations. A key reason for this disconnect was identified as the existence of multiple overlapping teams across cyber and digital, compliance, legal and IT, which can result in coordination difficulties, opposing priorities and duplication. In addition, third-party involvement adds complexity.

However, despite their growing importance, in-house legal teams are also stretched.

Heather Kelly observed a pervasive climate of economic and geopolitical uncertainty was impacting the role of legal teams, expanding their remit and forcing them to become more reactive to risks, including cyber.

"The evolving role of the general counsel – from ring-fenced lawyer to risk advisor – means that legal teams are stretched very thin. They don't have the capacity to invest in the myriad of risk management activities they would like to. So, it is very heartening to see that there has been an uptick in their preparedness in relation to cyber. Their budget and bandwidth are precious resources," Kelly said.

Christine Wong said that she had noticed general counsel and in house legal leaders were increasingly focussed on getting a handle on data, which represents a significant challenge for organisations, especially those with legacy systems and large data stores.

"Organisations are grappling with the Hydra like nature of their data – so much data across so many systems has given rise to significant complexity in understanding what is there and whether the control and security settings are adequate. Given recent law reforms and the prevalence of data extortion attacks, I think data risk management will continue to be a real driver of concern for in-house teams," Wong said.

Kelly noted the rise of AI had also made many organisations focus on data in a way the risk of a potential future cyber attack had not, with "legal teams harnessing the newfound momentum to spearhead projects aimed at cleaning up aged and inaccurate data".

> The evolving role of the general counsel – from ring-fenced lawyer to risk advisor – means that legal teams are stretched very thin."
>
> **HEATHER KELLY, SENIOR ASSOCIATE**

Cyber insurance

Anne Hoffmann, Partner in HSF Kramer's Disputes and insurance practice, shared the following insights regarding the cyber market:

- The market continues to grow. One insurer projects that the global cyber insurance market will reach USD 16.3 billion in 2025, driven by increasing digitisation and the growing frequency and severity of cyber incidents.
- Underwriters continue to expect that organisations commit significant investment to cyber security as a pre-requisite for coverage.
- As the threat landscape evolves, policy wordings should be reviewed and amended to ensure adequate coverage.
- Legal risks from class actions and regulatory scrutiny are becoming more prominent. We have now seen a number of cyber-related class actions emerge, though the loss is difficult to quantify.
- The market is seeing new entrants, increasing capacity and competition. We have generally observed a soft market which should be in policyholders' favour, decreasing premiums and increasing limits.

"We are sadly seeing time and time again that our clients' expectations of what is covered by their cyber policy does not keep up with the pace at which threat actors change their tactics," Hoffmann said.

Is legal professional privilege under threat?

On 4 April 2025, the Federal Court published its judgment on the application of a consumer class action to access a suite of technical reports from Deloitte, who provided expert cyber and IT support to Medibank after it suffered a significant cyber attack in October 2022.

Medibank asserted these materials were privileged and therefore did not need to be discovered. However, the Court found that privilege did not apply over three reports prepared by Deloitte: a root cause analysis, a post incident review and a report on compliance with APRA's CPS234.

Medibank is currently appealing the decision, which has set an important precedent for privilege and how it applies in the context of cyber incidents.

According to Wong, privilege is often more complex in cyber contexts due to the overlay of the issues being operational in nature, blurring the lines between communications that are privileged and not privileged.

"Even if business continuity isn't impacted by a cyber event, the issues are still occurring in the context of an IT security environment having been impacted. Following a significant event, many corporates understandably want to review their position, to ensure that settings are appropriate and consider whether some defences need to be strengthened," Wong said.

"As soon as you're thinking about things against that background, there are likely to be multiple purposes. For privilege to apply, legal purpose must be king."

Jones highlighted "legal professional privilege is not a service we can sell as lawyers".

"We can't just emblazon 'Legally Privileged' on documents – that's not how it works. Organisations need to be aware of the limits of privilege and that is certainly something lawyers should be communicating," he said.

> Legal professional privilege is not a service we can sell as lawyers."
>
> **PETER JONES, PARTNER**

> Even if business continuity isn't impacted by a cyber event, the issues are still occurring in the context of an IT security environment having been impacted. Following a significant event, many corporates understandably want to review their position, to ensure that settings are appropriate and consider whether some defences need to be strengthened,"
>
> **CHRISTINE WONG, PARTNER**

Ready or not?

Cyber security is now a standard business risk – one that legal teams must play a key role in managing and mitigating and, in the event of a cyber incident, responding to, recovering from, and learning from.

Cyber security and its intersection with the law has never been more important. This will only become more central in an uncertain world, with data volumes exploding, new threats emerging and sophisticated technologies increasingly adopted.

By developing a clearer understanding of the attitudes and maturity of legal teams as they relate to cyber security and related issues – as the HSF Kramer Cyber Risk Survey does – organisations can holistically enhance cyber uplift and education. In addition, insights can be gained into areas where organisations are perceived to be performing well and where further improvement is needed, ultimately supporting effective allocation of resources and technology investments.

As Australia's cyber-related regulatory environment continues to expand and mature, HSF Kramer's Cyber Risk Survey will continue to provide key insights into how general counsel are adapting and responding. Ultimately, this will provide not just important data to drive continuous improvement, but also information to support business leaders and policy makers better understand the opportunities and challenges facing legal teams in the cyber realm.

Our cyber simulation offerings

As this report has demonstrated, the evolving cyber threat landscape has materially changed how organisations approach cyber risk. This is why organisations are turning to HSF Kramer as their trusted adviser to educate and stress test their crisis management response capabilities.

How we deliver

No two organisations are the same, which is why we tailor our simulation exercises to your unique requirements.

We provide education workshops focussed on the threat landscape, legal and regulatory considerations, and the operational impacts of various cyber attacks. These workshops typically run for 60 to 90 minutes and are an ideal way to refresh your board or management on the current cyber risks.

> "...this was the best, most detailed, well thought through and executed simulation I have ever been a part of..."
>
> **ASX TOP 10 CRISIS MANAGEMENT LEAD**

Our most popular exercises include:

Education workshop and mini simulation
We will take you through a 2-hour education session covering the cyber threat landscape, the legal and regulatory issues arising from a cyber incident, and a simple hypothetical to educate on the key issues and decisions during a cyber incident.

Customised tabletop simulation
We will design a 3-hour bespoke exercise around the cyber threat issues relevant to your organisation. This will feature a series of interactive 'injects', each building upon the last, to test key processes and decision making. Suitable for management, the board, or both.

Full incident response plan test
A comprehensive, often unannounced, real-world cyber simulation which can be performed over multiple days. This exercise requires the Crisis Response Team to fully enact the response to a simulated cyber attack. It involves high collaboration, potentially including multiple service providers, and may be designed for management, the board or both.

Our team

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

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

Jason Betts
Partner
T +61 2 9225 5525
M +61 400 078 225
jason.betts@hsfkramer.com

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

Magdalena Blanch-de Wilt
Executive Counsel and APAC Cyber Risk Advisory Lead
T +61 3 9288 1350
M +61 410 646 267
magdalena.blanch-dewilt@hsfkramer.com

Heather Kelly
Senior Associate
T +61 3 9288 1260
M +61 477 886 470
heather.kelly@hsfkramer.com

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

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

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

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

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

Emily Coghlan
Partner
T +61 3 9288 1474
M +61 412 958 233
emily.coghlan@hsfkramer.com

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

Rebecca Gill
Senior Associate
T +61 3 9288 1229
M +61 455 331 704
rebecca.gill@hsfkramer.com

Annie Zhang
Senior Associate
T +61 3 9288 1133
M +61 432 724 968
annie.zhang@hsfkramer.com

Brooke Crenfeldt
Solicitor
T +61 2 9225 5187
M +61 494 029 821
brooke.crenfeldt@hsfkramer.com

How we can help you

In a world where data, digital systems and regulation increasingly intersect, HSF Kramer's dedicated multidisciplinary cyber practice provides advice on all aspects of cyber risk and preparedness, using a 'follow the sun' model that can support our clients anytime and anywhere.

We offer a full range of cyber risk management solutions with a worldwide network comprising more than 350 experts who can mobilise to support clients should a cyber incident arise.

From data governance through to incident response, our team can support your organisation to go from strength to strength in the ongoing cyber risk challenge that faces us all.

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

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.

Phone +61 3 9288 1000

Email cyberhotline@hsfkramer.com
cyber.australia@hsfkramer.com

HERBERT SMITH
FREEHILLS
KRAMER