
HERBERT SMITH
FREEHILLS
KRAMER
Are you cyber ready?
Australian legal leaders' views on the cyber risk landscape and outlook
Cyber Risk Survey Report 2026

Contents

Foreword

Now in its fourth year, the HSF Kramer Cyber Risk Survey remains a unique lens through which to examine how Australia's legal leaders perceive, prepare for and respond to cyber risk. This year's survey attracted responses from general counsel, divisional general counsel and senior legal counsel across a diverse cross-section of sectors.

Financial institutions (including banking, insurers and superannuation funds) again dominated the respondent pool at 35%, reflecting the sector's acute exposure to cyber risk and its comparatively high levels of regulatory maturity. Energy, health, consumer goods and retail, and infrastructure also featured prominently, providing a meaningful view of the cyber landscape across these important sectors.

The defining story of 2026 is AI. Technology-related risks (including AI) have surged to become the second most-cited concern among respondents, displacing data-related risk from that position for the first time. Addressing AI-related cyber security risks is the second-highest investment priority and AI-related cyber risks have become the single greatest pain point in cyber resilience programs. While third-party and data risks continue to feature, it is the convergence of AI with those established threat categories that is reshaping how organisations must think about and resource their cyber risk programs.

Yet for all the urgency of the AI story, the fundamentals of cyber risk management remain consistent. Organisations are alive to some of the key risks: third-party risk retains its position as the number-one concern, and the lived reality behind that statistic is stark: 62% of respondents experienced a third-party cyber incident in the past 12 months alone. However, this year's results suggest that there is more work needed to enable organisations to manage risk they cannot see (for example, many of the significant incidents in the past year have been people driven – social engineering, insider threats). People-related risk ranks as a top three concern, yet it remains absent from the top investment priorities, revealing a gap between risk recognition and directed action.

The legal team's criticality to incident response has strengthened further, with 77% of respondents reporting that their legal team is a key member of the crisis response team. The legal-cyber nexus is no longer an emerging concept; it is an operational imperative.

The road to effective cyber resilience is through deliberate, tested and whole-of-company preparedness. This report sets out where Australia's legal leaders stand today, and the distance that remains to be travelled.

Cameron Whittfield
Partner – Cyber, Data and Emerging Technologies

2026 survey: key themes

1. **AI as the key cyber risk**: the emergence of AI-driven threat vectors and the challenge of AI risk in existing cyber frameworks
2. **The human element as a persistent vulnerability**: people-related risk ranks as a top-three concern, yet remains absent from top investment priorities, revealing a disconnect between risk recognition and directed action
3. **Third-party risk entrenched at the top**: persistent supply chain exposure, with 'fourth-party' risk visibility emerging as the dominant pain point
4. **Board maturity improving, but gaps remain**: increasing confidence in Board cyber maturity, yet simulation participation and ransom preparedness still fall short
5. **Data risk management**: while most respondent organisations have taken steps to review data management practices in the past 12 months, 59% of respondents believe it would take a cyber incident to meaningfully drive greater focus on data risk management
6. **Legal teams as essential crisis responders**: deepening integration of legal functions into incident response, simulations and cyber incident response frameworks

Survey results at a glance

Cyber readiness in 2026: stronger governance, persistent exposure

Risk landscape

71%

of respondents cited **third-party risk** as their organisations' top cyber concern.

Supply chain exposure remains the dominant risk, with visibility into fourth-party relationships the key challenge.

62%

of respondent organisations were **impacted** by a third-party **cyber incident** in the past 12 months.

The lived reality of supply chain risk is being felt across sectors.

94%

of respondents have taken steps to **review data management practices** in the past 12 months.

Review activity is near-universal, but only 31% of organisations are satisfied with their data risk management practices.

Preparedness

69%

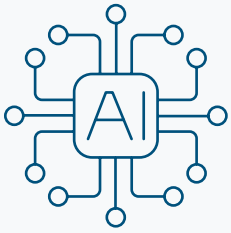
of respondents rated their Board's **cyber maturity** as 'high' or 'very high'.

Respondents describe their Board's cyber risk maturity positively, but gaps remain.

50%

of respondent Boards participated in a **cyber simulation** in the past 12 months.

While Board participation has increased in comparison to previous years, testing readiness remains a key gap.



97%

of respondents are aware of how AI is changing the **cyber threat landscape**.

Only 20% report having a detailed understanding of AI risks.

Response & regulation

77%

of respondents see Legal as **central to incident response.**

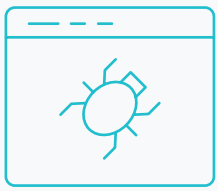
The legal-cyber nexus is now an operational imperative, not an emerging concept.

72%

of respondents regulated by the SOCI Act said that the SOCI regime had a **'moderate' or 'minor' influence** on their cyber risk management strategy, while 28% reported 'significant' influence.

As reforms progress, regulatory impact on cyber strategy is expected to deepen.

59%



of respondents believe it would take a **cyber incident** to meaningfully drive greater focus on **data risk management**.

A reactive posture persists, with many organisations waiting for a catalyst before prioritising data governance.

Top 3

Top 3 cyber concerns

1. Third-party risk
2. Technology-related risks, including AI
3. People-related risk

Top 3 cyber investment priorities

1. Uplifting and/or testing IT security infrastructure and systems
2. Addressing AI-related cyber security risks
3. Updating security posture/strategy

Top 3 pain points in cyber resilience programs

1. Addressing AI-related cyber risks
2. Implementing effective third-party risk management strategies
3. Implementing appropriate data risk management strategies

Artificial Intelligence

The defining story of 2026

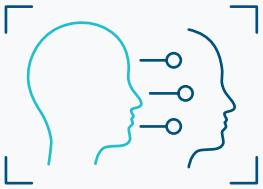
This year's survey results show that awareness of AI-driven cyber risks among legal leaders is near-universal, however, the gap between awareness and proportionate readiness measures is the defining challenge.

Respondents are increasingly concerned with technology (including AI) risks, which rose to second place (versus third place in our 2025 survey) when respondents were asked about their top organisational concerns. Organisations are conscious of the threat but have not yet developed the frameworks, skills or tooling to manage it with confidence. This finding is consistent with our client conversations over the last 6 to 9 months, and the work we have been doing to uplift cyber resilience programs in the era of AI.

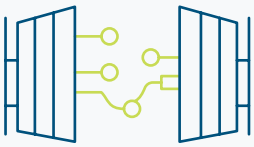
While 97% of respondents are aware of how AI is changing the cyber threat landscape, only 20% report having a detailed understanding of those risks. As AI adoption accelerates, including with the rapid advancement of frontier AI models such as OpenAI, Claude Mythos, Gemini, Grok, DeepSeek and Doubao, legal leaders are increasingly being asked to navigate a new generation of cyber threats.

The challenge is no longer awareness. It is ensuring organisations have the governance, controls and response capabilities needed to keep pace with a rapidly evolving threat environment. Organisations that can translate awareness into practical preparedness will be better positioned to manage the cyber risks emerging alongside the AI opportunity.

Top AI-specific concerns



Deepfakes/executive impersonation

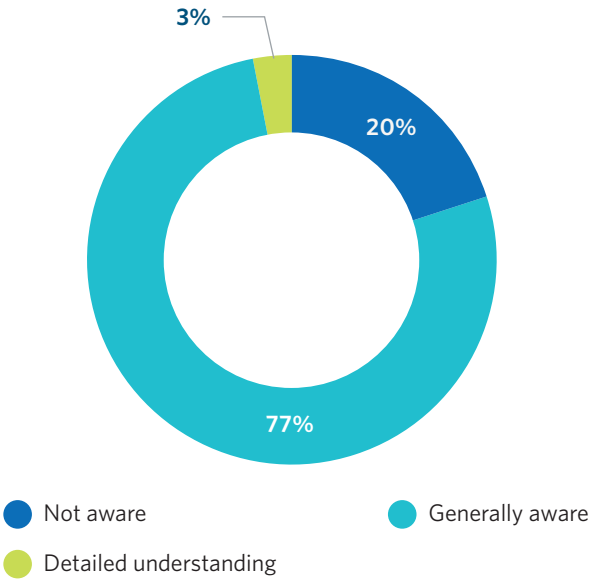


AI lowering barrier to entry for criminal threat actors

AI accelerating vulnerability detection and exploitation

AI-enhanced phishing attacks

Awareness of how AI is changing the cyber threat landscape



"We are seeing our clients lean into the assessment of AI-driven cyber risks, with conversations about the impact on cyber security programs and priorities routine at Board and C-suite level. We see organisations continuing to grapple with the prioritisation of resourcing and capability in the cyber and AI space. The desire to embrace productivity, remain secure and act with financial discipline will create ongoing friction in a world of frontier and agentic AI models."

HEATHER KELLY, SENIOR ASSOCIATE

The human element

People remain a persistent vulnerability

People-related risk – encompassing social engineering, insider threats, key person dependencies and cultural factors – is the third most-cited cyber concern among respondents. Yet despite this recognition, this year's survey shows that people-related risk does not feature in the top three investment priorities or the top three pain points in cyber resilience programs.

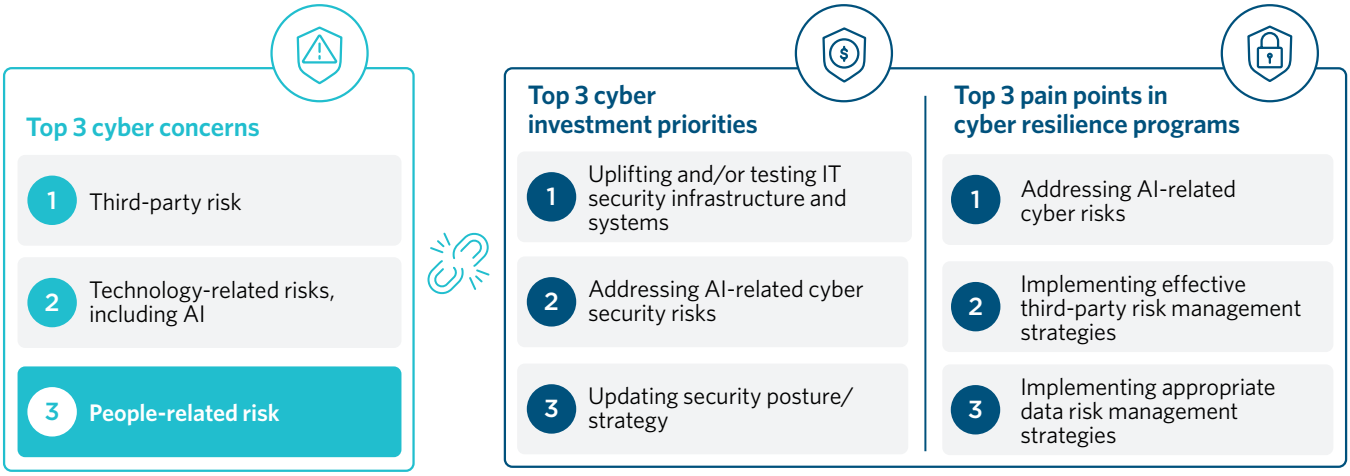
This disconnect between perceived risk and directed action is notable, and suggests that many organisations may be underestimating the action required to address what remains a significant exposure point.

The survey results are consistent with what we are observing in practice: the most consequential incidents we have seen over the past year have been people-driven – for example, resulting from sophisticated social engineering or insider threat. As AI lowers the barrier to realistic phishing and deepfake-enabled impersonation, the human element is becoming more, not less, critical to organisational resilience.

Organisations that treat people risk as a standing investment priority, including through effective training, and understand that the drivers of this risk are distributed across the organisation, will be materially better positioned to withstand the threats that are already at their door. The most mature organisations will also factor the human element into their Board cyber risk reporting.

People-related risk is the third most-cited cyber concern among respondents

But addressing this risk was not featured in the top three investment priorities or top three pain points in cyber resilience programs.



The chain reaction

Supply chain risks remain

Third-party risk is again the number-one cited concern, and in 2026, the visibility problem is the central obstacle. Nearly four in five respondents cited difficulty obtaining sufficient information from the affected third party to mount an effective response.

This reinforces a structural problem that organisations remain heavily dependent on counterparties whose cooperation cannot be guaranteed in a crisis, and whose own supply chains remain largely opaque. Until that information asymmetry is addressed, third-party risk will remain as much a governance challenge as a technical one.

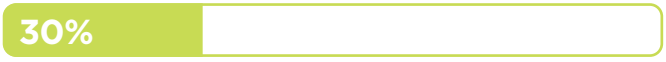
of respondents were impacted by **a third-party cyber incident** in the past 12 months

Greatest challenges in third-party risk management

'Fourth-party' risk: lack of visibility into suppliers' own supply chains

Lack of transparency/over-reliance on supplier questionnaires

Challenges securing appropriate contractual rights



Resourcing constraints limiting use of existing contractual rights

Difficulty transitioning away from suppliers

Top 3 third party incident pain points

Of the 62% who experienced a third party incident in the past 12 months, the top 3 pain points were:

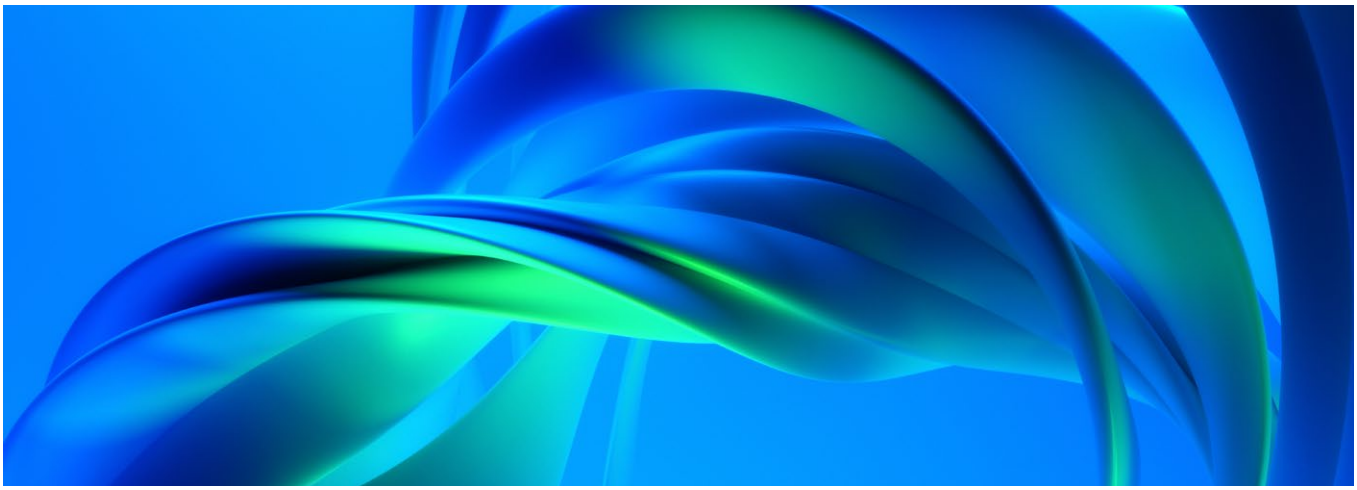
1. Effective **cooperation by the third-party**
2. Effectiveness of the **organisation's incident response coordination** (given third-party involvement)
3. Managing **operational disruption**

"Solving the challenge of visibility of third party cyber and data risks grows even more acute in an AI-dependent world where third and fourth-party technology are critical dependencies."

CAITLYN BELLIS, SENIOR ASSOCIATE

Board governance

Maturity and remaining challenges



Board cyber maturity perceptions have improved materially, but simulation participation remains a critical gap.

Notably, we have observed a number of Boards reflecting on their approach to cyber governance in the wake of *ASIC v Bekier* [2026] FCA 196 (the Star Decision), interrogating whether their existing frameworks meet evolving expectations of director oversight. This has driven a renewed focus on the nature and quality of Board reporting on cyber, with organisations reassessing the depth, frequency and strategic orientation of the information flowing to directors.

The results point to a significant uplift in Board level cyber governance. More Boards are considered cyber mature, and understanding of cyber risk has increased substantially since 2025. However, while awareness and oversight continue to strengthen, practical preparedness appears to be lagging. Only half of respondent Boards participated in a cyber simulation during the past 12 months, suggesting that translating cyber awareness into tested readiness remains a key opportunity for organisations. Equally, as the complexity and velocity of cyber incidents increase, there is a growing need for structured decision-making frameworks at a Board level to enable directors to make informed, timely decisions during a crisis rather than relying on ad hoc processes under pressure.

Our 2025 survey found Board maturity was still not where it needed to be, with 55% of respondents reporting they would not describe their board as cyber mature. In 2026, this picture has improved markedly to 69% (14% increase).

of respondents describe their board as being cyber mature
Up from 55% in 2025 (+14%)

of respondents believe their board has a clear understanding of cyber risk
Up from 68% in 2025 (+22%)

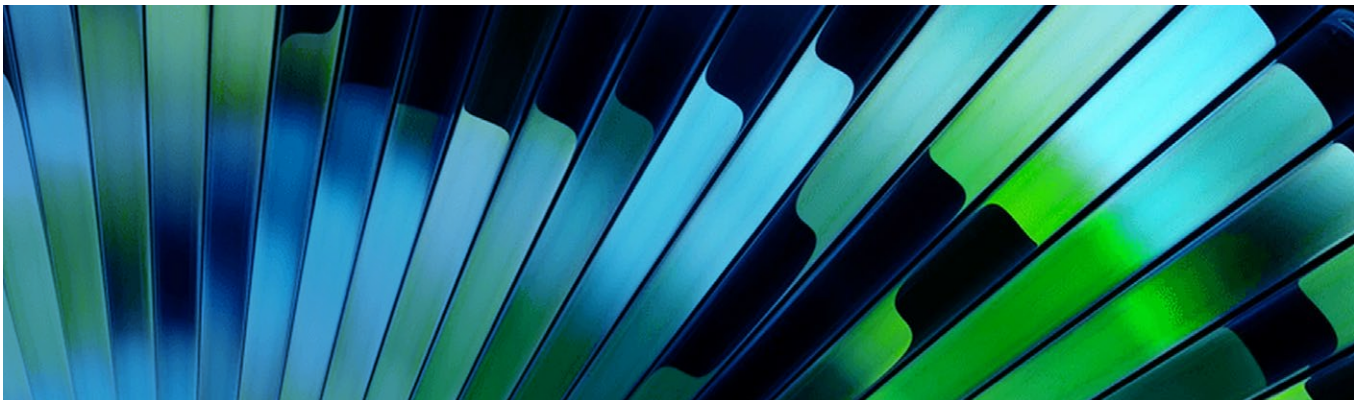
While the survey findings around increased Board maturity are aligned with our own observations around the uplift in the cadence and focus of reporting being provided to Boards, in our experience many companies are still working to bridge the gap between 'information' and 'insight' in their Board cyber reporting."

CAROLYN PUGSLEY, PARTNER

of respondent Boards participated in a cyber simulation in the past 12 months
Up from 36% in 2025 (+14%)

Data management

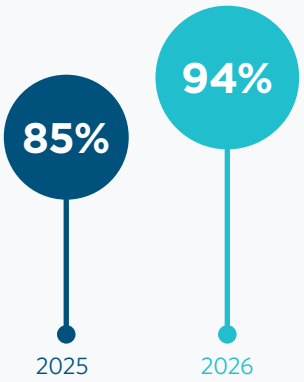
The risk you already hold



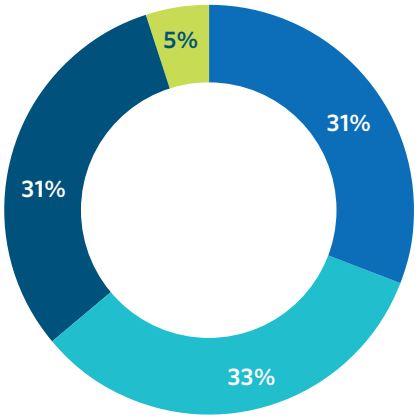
Nearly all organisations reviewed their data management practices in the past 12 months, yet confidence remains mixed. The fact that 59% of respondents believe it would take a cyber incident to meaningfully drive greater focus on data risk management suggests many organisations are still motivated by events rather than prevention.

The findings point to a disconnect between recognising data risk and prioritising it. While organisations are taking steps to review their data management practices, many appear to be waiting for a catalyst before making data risk a strategic focus. The continued absence of data risk from the top three investment priorities, despite its prominence as a pain point, indicates that competing demands are crowding out sustained data governance investment.

Respondent organisations who took steps to review data management practices in the past 12 months

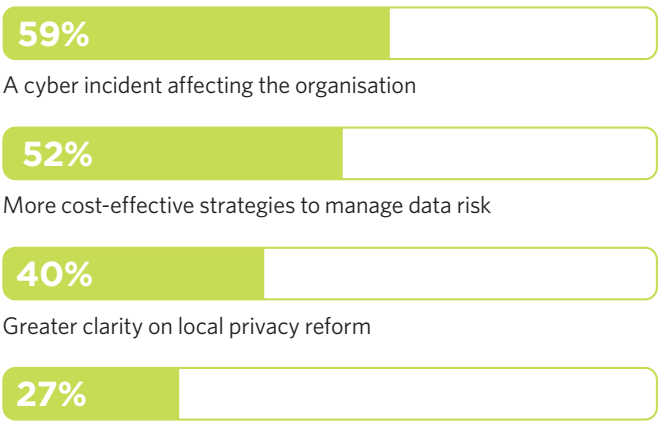


How satisfied are you with your organisation's data management practices?



- Very satisfied/Satisfied
- Neutral
- Concerned/Very concerned
- Prefer not to say

What would drive greater focus on data risk?



Regulation in an active landscape

Driving cyber resilience

The regulatory landscape continues to shift, moving from the Independent Review into the *Security of Critical Infrastructure Act 2018* (SOCI Act), into the current multi-tranche reforms to the *Privacy Act 1988* (Cth) (Privacy Act) and SOCI Act, and further focus on the *Cyber Security Act 2024* (Cth) (Cyber Security Act) and broader legislation as part of Horizon 2 of the 2023–2030 Australian Cyber Security Strategy.

This year's survey findings provide a timely snapshot of regulation's growing influence. An overwhelming majority of SOCI-regulated respondents reported that the regime has had a meaningful impact on their organisation's cyber resilience programme, offering valuable insight as policymakers consider the next phases of reform.

Regulation is becoming a major driver of cyber risk management

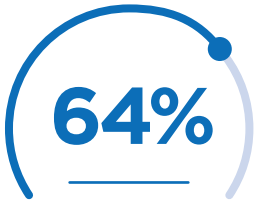
The majority of organisations surveyed now operate within a regulated cyber environment, and the impact is increasingly being felt beyond compliance functions. Respondents reported that regulatory obligations are influencing cyber strategy, governance and operational decision-making, particularly among organisations subject to the SOCI Act regime. As new incident reporting requirements and sector-specific standards continue to mature, regulation is playing a growing role in shaping organisational cyber resilience. 64% of respondents recognise regulation as a meaningful driver of cyber posture.

Tens of millions of dollars in penalties were imposed in the last year alone following enforcement action by regulators, a figure we expect to rise as enforcement activity intensifies. Notably, regulatory penalties represent only a small fraction of the materially more significant costs of incident response, containment and recovery, business interruption, reputational damage, and the broader litigation risk and claims exposure that typically follow a major cyber event.

Being ready to manage regulatory obligations in a cyber incident, including SOCI, CPS 230/234 and Privacy Act obligations, is non-negotiable. SOCI Act and Privacy Act compliance in the face of reform, as well as regulatory enforcement generally, will remain key areas of focus. The proposed change to a 72 hour eligible data breach notification timeframe will also add moderate complexity, although well prepared organisations will be able to meet the challenge.

of respondents are subject to cyber-related regulation

of respondents subject to the SOCI Act report that the regime has had an influence on their cyber risk management strategy



of respondents recognise regulation as a meaningful driver of cyber posture

"Despite concerns about fitness for purpose, SOCI is clearly contributing to cyber resilience uplift, joining privacy and financial services and prudential regulation as key regulatory drivers of cyber readiness."

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

Looking ahead

The results from our 2026 HSF Kramer Cyber Risk Survey paint a clear picture that Australian organisations are more aware of cyber risk than ever, but awareness alone is not enough. The gap between recognition and readiness (whether in relation to AI-driven threats, people risk, third-party exposure or data governance) remains the central challenge.

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 increasing, new threats emerging and sophisticated technologies increasingly adopted.

While Boards are more engaged, regulation is sharpening focus, and investment in cyber security is increasing, the threat landscape is evolving at pace and organisations that treat cyber resilience as a periodic exercise rather than a continuous discipline will find themselves exposed.

The organisations best positioned for what lies ahead will be those that move beyond awareness to action, embedding cyber resilience into governance, culture and operational decision-making, stress-testing their preparedness through simulation, and building the frameworks needed to respond decisively when, not if, an incident occurs.

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 Australian legal leaders are adapting and responding. Ultimately, this will provide important data to drive continuous improvement, and information to support business leaders and policymakers better understand the opportunities and challenges facing organisations.

> The work done by a company to respond to an incident brings into sharp focus two questions: (1) What should a company investigate as part of a proper corporate governance response? (2) What parts of that investigation can and should be privileged? These aren't straightforward questions because of the plethora of activities involved in responding to an incident and the potentially significant legal exposures for the company. However, how companies answer them is under increasing scrutiny and may impact on reputation as well as exposure to future legal risks. Legal leaders and companies should consider the relevant factors thoughtfully in advance of a crisis."
>
> **CHRISTINE WONG, PARTNER**

Our team

Cameron Whittfield
Partner, Cyber, Data and Emerging Technologies
T +61 3 9288 1531
M +61 448 101 001
cameron.whittfield @hsfkramer.com

Peter Jones
Partner
T +65 6868 8093
M +65 9137 1472
peter.jones @hsfkramer.com

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

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

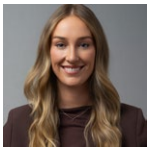
Anne Hoffmann
Partner
T +61 2 9225 5561
M +61 418 906 447
anne.hoffmann @hsfkramer.com

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

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

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



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

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

Christina Knezevich
Senior Associate
T +61 2 9322 4689
christina.knezevich @hsfkramer.com

Brooke Crenfeldt
Solicitor
T +61 2 9225 5187
M +61 438 538 966
brooke.crenfeldt @hsfkramer.com

Amelia Frey
Solicitor
T +61 2 9225 5162
M +61 407 038 959
amelia.frey @hsfkramer.com

Annabelle L'Estrange
Solicitor
T +61 2 9322 4450
M +61 461 461 973
annabelle.lestrange @hsfkramer.com

Leana Lim
Solicitor
T +61 3 9288 1442
M +61 492 003 878
leana.lim @hsfkramer.com

Claire Tucker-Morrison
Solicitor
T +61 3 9288 1472
M +61 455 659 220
claire.tucker-morrison @hsfkramer.com

Andrew Moir
Partner, Intellectual Property and Head of Cyber Security, London
T +44 20 7466 2773
andrew.moir @hsfkramer.com

Miriam Everett
Partner, London
T +44 20 7466 2378
miriam.everett @hsfkramer.com

Peter Dalton
Partner, London
T +44 2074 662 181
peter.dalton @hsfkramer.com

Austin Manes
Special Counsel, Silicon Valley
T +1 650 752 1718
austin.manes @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 and data risk and preparedness, using a 'follow the sun' model that can support our clients anytime and anywhere.

We offer a full range of cyber and data 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, build cyber resilience and enable effective response to the ongoing cyber risk challenge.

1

Cyber readiness

- Cyber incident response plans and crisis management plans, playbooks, checklists
- Cyber incident simulations and tabletop exercises
- Board/ELT advice and training
- Extortion payment decision frameworks
- BCP review and training
- Data collection and retention advice
- Privacy impact assessments
- Privacy and data governance policies
- Cyber due diligence
- 3rd party risk reviews
- Contract reviews
- Board reporting and governance advice
- Insurance advisory
- Regulatory advisory (including SOCI, Cyber Security Act)

2

Cyber crisis

- Response coordination ('breach coach')
- Board engagement support and advice
- Continuous disclosure advice
- Regulatory and law enforcement engagement
- Communications advice
- Insurer engagement and insurance advice
- Forensic investigation management
- Extortion negotiation management
- Impacted data hosting and review
- Support services engagement
- Injunctions and take-down notices
- Regulatory notifications (Australia and overseas)

3

Post-incident

- Post-incident reviews
- Insurance claim management and recovery realisation
- Regulatory engagement support (including CPS 230/234, reportable situations)
- Regulatory compliance advice (including Privacy Act, AFSL, SOCI and prudential obligations)
- Directors' duties advice and governance reviews
- Litigation support
- Class actions
- Contractual compliance advice
- Contractual uplift advice
- Post-incident data management reviews
- Law reform advice and submissions

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 CYBER SECURITY EXECUTIVE**

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.

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.

Telephone +61 3 9288 1000
Email cyberhotline@hsfkramer.com
cyber.australia@hsfkramer.com

HERBERT SMITH
FREEHILLS
KRAMER

HSFKRAMER.COM