



HERBERT
SMITH
FREEHILLS

CYBER READY? AUSTRALIAN BUSINESSES RISE TO THE CHALLENGE

Herbert Smith Freehills Cyber Risk Survey 2023

Contents

02 On the front lines

03 Our survey results at a glance

05 The buck stops here

07 Are you cyber ready?

11 Empowering legal teams to tackle cyber-attacks

14 Emerging themes in insurance and regulation

16 How we can help you

On the front lines

Views from in-house legal teams on cyber risk

From engaging regulators and government to managing communications and compliance, the list of responsibilities has grown long.

Australian organisations face a perilous, rapidly evolving cyberthreat landscape. Over the last 12 months, the national discourse has shifted into hyperdrive in the wake of global geopolitical instability and a spate of high-profile attacks. Businesses are also subject to increased regulatory scrutiny as well as growing expectations from government, consumers and other stakeholders.

As a wealthy nation committed to digitalisation, Australia is a prime target for a new wave of cyberthreat actors. The consequences of cyber-attacks are soaring, along with their scale, frequency and sophistication. Encryption events can bring businesses to a standstill. Data breaches undermine consumer confidence and cause real harm through identity theft and financial loss. There is even the potential for operational shutdowns to bring vital infrastructure such as hospitals, airports and utilities to a halt. Compounding matters, our adversaries are continually adapting and looking to leverage new capabilities such as generative AI.

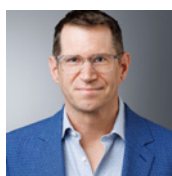
Historically, the task of coordinating cyber incident response fell to an organisation's IT security team under the oversight of its Chief Information Officer (CIO) or Chief Information Security Officer (CISO). Today, the unmistakable trend is that lawyers are joining them at the forefront of the response.

When a crisis occurs, more lawyers are taking on the high-pressure role of 'breach coach'. This involves coordinating critical activities such as engaging with the board, government, regulators and insurers, assessing operational impacts, reviewing compromised data, ensuring regulatory and contractual compliance, overseeing communications and executing a cyber extortion response strategy. Failure to appropriately manage these workstreams can have significant legal and regulatory ramifications.

Until now, qualitative research has focused largely on the views of boards, a variety of executives and technology teams, rather than the legal leaders so often front-and-centre when a cyber-attack occurs.

In 2023, Herbert Smith Freehills decided to take a fresh perspective. We conducted a landmark survey of over 120 legal leaders from businesses based in Australia. More than 67% of respondents held the position of General Counsel or equivalent, while 51% of the surveyed organisations were ASX-listed entities, 71% had international operations and more than 33% had in-house legal teams with 25 legal staff or more. Sectors represented included financial services, consumer goods and retail, energy, technology, media, telecommunications, transport, healthcare, pharmaceutical, infrastructure and resources.

This report highlights some of the survey's most fascinating – and sobering – findings. It is supported by insights from our firm's industry-recognised experts across the Asia-Pacific region in cyber, corporate, disputes resolution and insurance. Overall, while organisations have recognised the need to increase cyber resilience and have taken some positive steps, there is still much work to do.



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

Our survey results at a glance



122

in-house legal leaders
from Australia business

67%

General Counsel
or equivalent



25%

have been
directly impacted
by a cyber
extortion incident



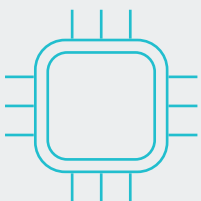
Top 3

aspects of cyber risk that
are of greatest concern:

- 1 Reputational risk
- 2 Third party risk
- 3 Aged data stores

32%

have cyber
expertise
on the board



47%

have held a board
cyber simulation



38%

of respondent legal teams
have not yet participated in
a cyber simulation



58%

of respondents have an
individual tasked with
covering data and cyber risks

21%

now have a resource
dedicated solely to
these risks



Most respondents have a
cyber incident response plan,
but only

19%

 have a
legal-specific plan

11%

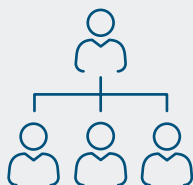
of respondents
impacted by a cyber
extortion demand paid
a ransom

**48%**

of respondent boards have
not settled on a formal
position regarding
ransom payments

**42%**

expressed concern about their
organisation's data collection and
retention practices

**68%**

find regulations helpful
to guide internal policy
and investment

**79%**

believe we
do not need more

85%

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

**70%**

believe cyber is
a CIO risk to own

**5 most
impacted
sectors**

Financial Institutions
Pharmaceutical
Consumer goods
Tech
Media



The buck stops here

Regulators have sent directors a clear message on cyber resilience as threats increase



It should always be remembered that businesses subjected to a cyber-attack are the victims of a crime. As noted by Cameron Whittfield, Herbert Smith Freehills Partner and APAC Head of Cyber Security, “we are dealing with attacks from cyber criminals based in foreign jurisdictions. Few people have been educated or trained to deal with this type of threat before and corporates are grappling with this new paradigm in real time”.

Nonetheless, while affected organisations would once have been met with sympathy, it is clear that this has changed. Regulators now believe organisations have had ample warning to improve their security and prepare for incidents when they arise. Effective preparation enables an organisation to fulfil its legal obligations, limit regulatory and litigation risks, as well as to protect individuals and shield itself from reputational damage.

As an indication of the costs that businesses can face, Latitude Financial reported \$76 million of pre-tax costs and provisions related to the cyber-incident in March this year.¹ The Australian Prudential Regulation Authority (APRA) also imposed an increase on Medibank’s capital adequacy requirement of \$250 million

following its cyber incident in November 2022. We note that various consequential impacts are also playing out with the regulators and in the courts.

Amidst rapid technological change, an evolving regulatory landscape and a patchwork of regulators zeroing in on cyber resilience, organisations must recognise that accountability ultimately sits with the board. The Australian Securities and Investments Commission (ASIC), the Office of the Australian Information Commissioner (OAIC) and APRA have all emphasised the requirement for boards to have a clear understanding of their organisation’s cyber resilience as a fundamental component of business risk management.

¹ Latitude Group Holdings, 18 August 2023, ‘ASX Announcement’.

This sentiment was reinforced at the Australian Institute of Company Directors' Australian Governance Summit on 2 March 2023 where ASIC Chair Joseph Longo emphasised that cyber preparedness is squarely a board-level issue. "How the board ensures sufficient oversight of threats, vulnerabilities and mitigating controls will set the tone for the cyber resilience of an organisation," he said.²

Under the Corporations Act 2001 (Cth), directors must discharge their duties with care and diligence. In practice, ASIC's view is that boards need to address reasonably foreseeable non-financial risks. "If ever there was such a risk, cyber risk falls into that description quite nicely," says Tony Damian, Partner at Herbert Smith Freehills and trusted adviser to many Australian boards. Reiterating the judgment of Justice Helen Rofe in *ASIC v RI Advice Group Pty Ltd*,³

Whittfield adds that it is not possible to reduce the chances of a cyber-attack to zero. Rather, it is the role of the board to make a risk-based assessment and set the company's risk appetite so decisions can be made on investment in security, people and processes.

This is a fast-evolving area of law where general principles may apply but the circumstances of every business and industry are different.

Damian notes that the duty of a board is to ask how their organisation is addressing "foreseeable non-financial risk" in the way that ASIC and the law require. "Have we done everything we can as a board, in case there are hostile actors trying to get into our systems, shut us down and take our data?" he asks. "That's the legal duty and from there you can plot a pretty good roadmap of how a board can do its job, make sure the company is ready and prepared, and sleep well at night."

“

Have we done everything we can as a board, in case there are hostile actors trying to get into our systems, shut us down and take our data?"

TONY DAMIAN, PARTNER

² <https://asic.gov.au/about-asic/news-centre/speeches/chair-s-remarks-at-the-aicd-australian-governance-summit-2023/>

³ *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* [2022] FCA 496, [58].



“

We are dealing with attacks from cyber criminals based in foreign jurisdictions. Few people have been educated or trained to deal with this type of threat before and corporates are grappling with this new paradigm in real time"

**CAMERON WHITTFIELD,
PARTNER - APAC
CYBER SECURITY HEAD**

Are you cyber ready?

A Herbert Smith Freehills survey shows we must do more to prepare our companies

The importance of cyber crisis simulation exercises

Staging a simulated cyber-attack is a key way for organisations to test their incident response, yet 28% of respondents indicated their board had not yet done so. In reality, this could be higher, as an additional 25% of respondents had no visibility of this aspect of their organisation's cyber resilience strategy.

In our experience, cyber simulation exercises can help both management and boards prepare for the rhythm and challenge of a crisis. First, these simulations often show that the board may not be able to convene or form a quorum quickly enough. As a result, they may need to create a sub-committee or some other form of delegated authority. Second, only a small number of key decisions likely require escalation to the board. While it varies by organisation, boards are typically involved where there are complex regulatory issues around continuous disclosure, significant financial and reputational impacts and discussions about whether to pay a ransom demand. Third, important differences of opinion may exist between board and management on issues such as ransom payments, communications strategies and the level of market disclosure required.



"When you put management or a board through a simulation, they get to exercise or test their cyber crisis response. Key issues can be considered in advance, and this preparation can be incredibly valuable when an actual incident occurs"

**CAMERON WHITTFIELD, PARTNER
- APAC CYBER SECURITY HEAD**

28%

**OF RESPONDENTS SAY
THEIR BOARDS HAVE
NOT YET HELD A CYBER
SIMULATION EXERCISE**

32%

**SAY THEIR BOARDS NOW
HAVE CYBER EXPERTISE**

Cyber simulation exercises bring these matters to the fore. They can be constructively debated and resolved in advance of a crisis, to the extent foreseeable. Although each incident will present unique facts and challenges, pre-considering some key issues that are likely to arise will assist the board's interaction with management when faced with a real-life cyber-attack.

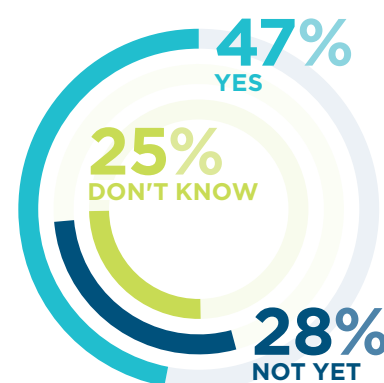
"When you put management or a board through a simulation, they get to exercise or test their cyber crisis response. Key issues can be considered in advance, and this preparation can be incredibly valuable when an actual incident occurs," Whittfield says.

Conducting a cyber simulation exercise is far from the only step a management team or a board should take to address foreseeable non-financial risk. What is reasonable will depend on the particular circumstances of a company and its industry. Some businesses will have a large data footprint to manage, while for others, ensuring protection against operational impacts will be key.

Our experience is that many well-prepared boards are upskilling, seeking external cyber security advice and testing to see how well internal systems and processes hold up. "If a board had not turned their mind to this, not even asked management what is being done and then there is a cyber-attack, I think in those circumstances there is not much debate the board has not complied with its statutory and common law duties to act with care and diligence," Damian says.

He observes that the finding that 28% of boards are yet to hold cyber simulation exercises illustrates that some companies are not as prepared as they could be, and as ASIC and other regulators may expect them to be. "Companies might be doing other good things, but it's an important statistic because it indicates we haven't quite matched our awareness with action. It raises the question of how ready we are."

Board has held a cyber simulation



“

... Companies might be doing other good things, but it's an important statistic [28% of boards yet to hold cyber simulation] because it indicates we haven't quite matched our awareness with action. It raises the question of how ready we are"

TONY DAMIAN, PARTNER

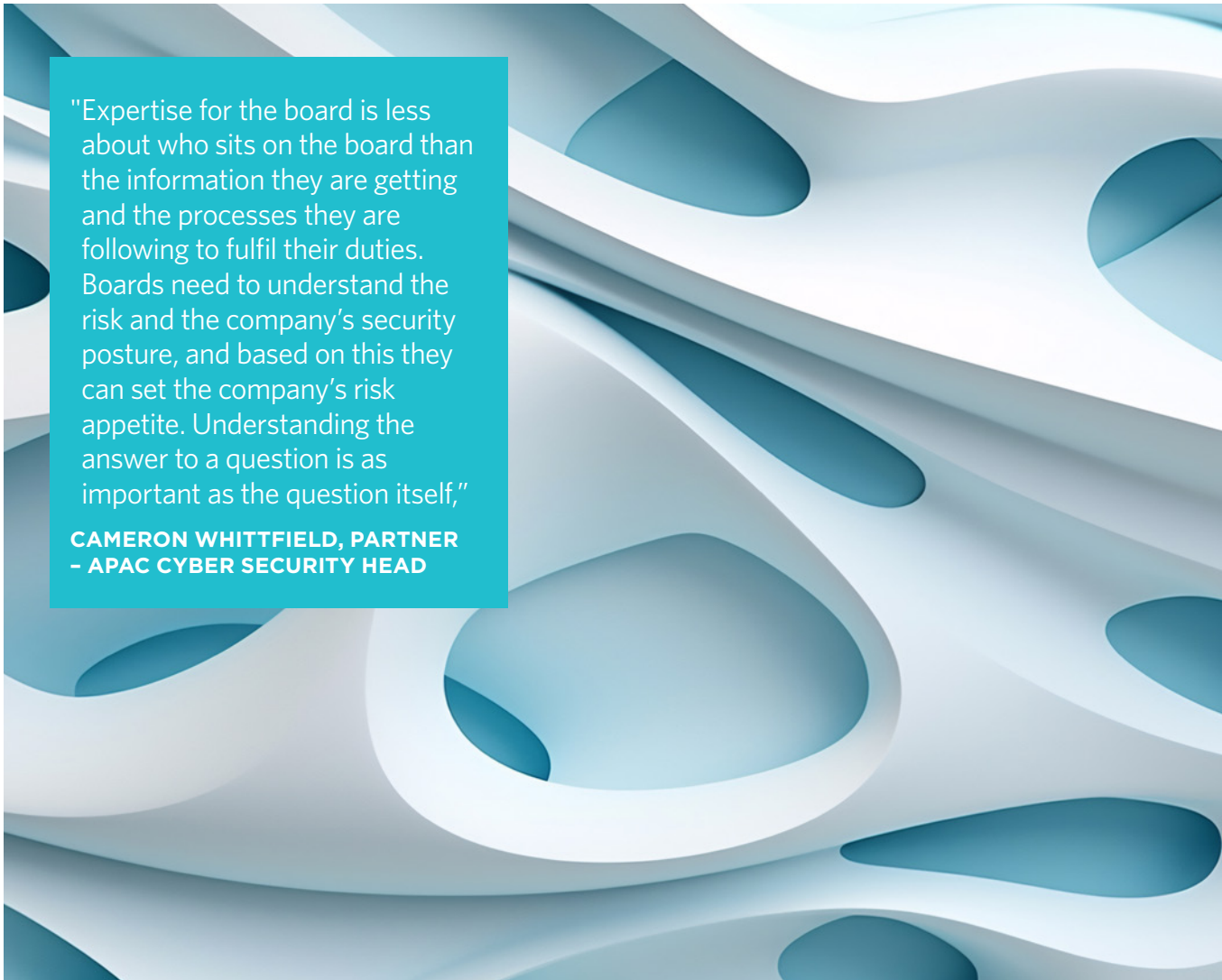
Getting the right expertise

Boards that are educated in cyber security matters are better able to fulfil their legal responsibilities. Of the respondents, 68% indicated that their boards do not have directors with specialist cyber expertise. This is not surprising given this skillset is currently being built out, in real time, at both an executive and board level.

Nonetheless, formal qualifications and specific experience are not ultimately required. What matters is that directors have access to the relevant information to understand the cyber risks relevant to their organisation. It is also important they can call upon appropriate expertise to assess and inform key decision-making relevant to those risks. This may come from a source at the executive level such as the CIO, CISO, General Counsel, or from external advisors.

As Whittfield observes, the key issue is whether companies are prepared. "Expertise for the board is less about who sits on the board than the information they are getting and the processes they are following to fulfil their duties. Boards need to understand the risk and the company's security posture, and based on this they can set the company's risk appetite. Understanding the answer to a question is as important as the question itself," he says.

In encouraging findings, 75% of survey respondents said their organisation's boards had been educated about cyber risk in the past 12 months. Only 7% said their board had never been educated at all. Board education levels were significantly higher among listed companies, reflecting the higher level of market disclosure obligations, public scrutiny and analyst coverage these organisations attract.



"Expertise for the board is less about who sits on the board than the information they are getting and the processes they are following to fulfil their duties. Boards need to understand the risk and the company's security posture, and based on this they can set the company's risk appetite. Understanding the answer to a question is as important as the question itself,"

**CAMERON WHITTFIELD, PARTNER
- APAC CYBER SECURITY HEAD**

Formalising a position on ransom

Of those surveyed businesses that had been impacted by an extortion event, 11% paid a ransom demand. This low percentage is consistent with recent findings from the global incident response firm, Coveware, reporting that “in the second quarter of 2023, the percentage of ransomware attacks that resulted in the victim paying fell to a record low of 34%”.⁴

These figures may come as a surprise to many, but they are broadly consistent with our own professional experience. As companies build cyber resilience (including through effective back-ups, improved recovery solutions and business continuity planning), they are able to better manage any encryption event. And, in our experience, those companies dealing with a data breach alone are unlikely to pay.

Ransom discussions are complex and typically require elevation to the board. “You want to get legal advice on what is the current state of the law. However, the devil is always in the detail when it comes to the legality of a payment applied to the specific facts,” says Christine Wong, Partner at Herbert Smith Freehills with specialist expertise in regulatory matters and investigations.

There are several situations where paying a ransom can itself be an offence – for example, if the organisation or entity receiving the funds is sanctioned. This is a strict liability offence. Without a valid defence, anyone who has facilitated the payment such as the Chief Executive Officer (CEO), Chief Financial Officer (CFO), CIO or third-party advisor could be found an accessory to the crime. In addition, instrument of crime or terrorism financing offences may be activated.

While questions of legality are important, directors also have to consider a range of commercial, practical and reputational matters to discharge their directors’ duties. Acknowledging the extreme sensitivity of this position, our survey indicates that many boards have not settled on a formal position regarding ransom payments. For many company lawyers it remains unclear whether the board would be open to payment. “There is a lack of clarity at board and management level about how different factors should be prioritised by a particular business” Wong says. “Some organisations have done that work and have very detailed models, whereas with others it’s quite reactive.”

11%

OF RESPONDENTS
IMPACTED BY A CYBER
EXTORTION DEMAND PAID

48%

OF RESPONDENTS SAY
THEIR BOARD HAVE NOT
SETTLED ON A FORMAL
POSITION REGARDING
RANSOM PAYMENTS

66%

OF RESPONDENTS SAY
THEIR BOARDS HAVE NOT
GIVEN MANAGEMENT
FORMAL GUIDANCE ON
THEIR EXTORTION-
PAYMENT VIEWS

⁴ Coveware, July 2023, ‘Ransom monetization rates fall to record low despite jump in average ransom payments’.



“

There is a lack of clarity at board and management level about how different factors should be prioritised by a particular business”

CHRISTINE WONG, PARTNER

Empowering legal teams to tackle cyber-attacks

Front-and-centre lawyers must be activated to manage digital risks

Take ownership

We found that 70% of respondents view cyber security as the primary responsibility of the organisation's CIO or information security team. This is not surprising given executive ownership of cyber security often rests with the CIO.

We note, however, that cyber risk is an enterprise-wide risk. Various critical functions across the organisation, including legal, compliance and risk, corporate affairs, public relations and human resources, serve an important role in deciding the best course of action.

In our experience, particularly working with ASX-listed clients, a legal lens needs to be applied not just to preparations before an attack, but in the complex aftermath of an incident where many regulatory and litigation risks may be in play. This is why legal teams, given their level of visibility and engagement, are often uniquely positioned within the organisation to coordinate the overarching response and ultimately serve as the 'breach coach'.

We are also seeing a change in focus within the legal teams themselves. Based on our survey, 58% of respondents have an individual tasked with covering data and cyber risks and 21% now have a resource dedicated solely to these risks.

Know your data footprint

Our survey suggests that businesses remain focused on data collection and retention. While 85% of respondents have a data retention policy in place, a notable 42% expressed concern about their organisation's data collection and retention practices.

"So, you must ask yourself, 'What information are we collecting and why? How long are we keeping it? And once we've achieved the purpose for which we collected it, why are we still holding onto it?' Organisations need to ensure they're not sitting on troves of data unnecessarily."

Emily Coghlan, Director of Herbert Smith Freehills' Alternative Legal Services practice in Australia agrees: "It is critical for an organisation to be across its data footprint and have a robust and defensible process to manage the data associated with a breach."

Businesses faced with exponentially growing data volumes must understand how this data is stored, secured and destroyed once it is no longer required. This 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," Coghlan says.



One of the best ways to reduce the impact from a data breach is to reduce your attack surface,"

**CAMERON WHITTFIELD, PARTNER
- APAC CYBER SECURITY HEAD**

58%



**OF RESPONDENTS
HAVE AN INDIVIDUAL
TASKED WITH
COVERING DATA AND
CYBER RISKS**

42%

**EXPRESSED CONCERN
ABOUT THEIR
ORGANISATION'S DATA
COLLECTION AND
RETENTION PRACTICES**



The vulnerability to third-party providers has played out in a number of recent cyber incidents including the Accellion, GoAnywhere MFT and MOVEit attacks.

Diligent front-end preparations are highly valuable if a cyber-attack occurs. An affected organisation needs to understand exactly what data has been accessed or exfiltrated, the impact to individuals, the legal ramifications of this, and potential exposure to regulatory and litigation risk.

As an example of how rapid response can work in practice, Coghlan's team can be quickly mobilised to help clients retrieve and interrogate compromised data following a breach. "Once you have that

compromised dataset, a key focus is determining what personal and commercially sensitive information it may contain," she says. "You do this by engaging a team of data breach analytics experts to manage the review workflow – often through bespoke tools which increase the efficiencies of the review process." Businesses can then notify stakeholders as needed and focus on managing the regulatory, financial and reputational fallout.

An ASX-listed company may also be obligated to publicly disclose cyber incidents that may affect its share price. However, the duty to report a cyber incident depends on its nature, scale and severity. Our survey finds that 29% of respondents

impacted by a cyber incident did not make a public statement. This should not be surprising as many events can be appropriately managed with minimal impact. In July 2023, the Securities and Exchange Commission in the US adopted rules requiring disclosure of material cybersecurity incidents and annual reporting of cybersecurity risk management, strategy, and governance.⁵ While similar obligations do not exist in Australia, there is increasing community and regulator expectation that cyber incidents are publicly disclosed.

⁵ <https://hsfnotes.com/cybersecurity/2023/08/31/the-secs-new-cybersecurity-disclosure-rules-new-requirements-for-foreign-private-issuers/>



It is critical for an organisation to be across its data footprint and have a robust and defensible process to manage the data associated with a breach"

**EMILY COGHLAN, DIRECTOR
ALTERNATIVE LEGAL SERVICES**

Have a comprehensive legal playbook

Our survey found that 90% of respondents have a cyber incident response plan, but only 19% have a legal-specific response plan or playbook. The consequence for legal teams is that they may not have key information at their fingertips in the critical minutes and hours after an incident occurs.

When considered alongside our survey finding that 38% of respondent legal teams have never participated in a cyber simulation exercise, many legal teams may be significantly under-prepared for a material, time-sensitive cyber-attack.

As Phillip Magness, Herbert Smith Freehills APAC Cyber Risk Advisory Lead observes, "you've got a percentage that don't have a plan and a percentage that have never experienced even a mock exercise. The clients we work with recognise this. They are taking a proactive role in preparatory activities where they soon learn if their plans and playbooks are fit for purpose or not."

Whittfield notes that a legal-specific response plan or playbook might involve several critical steps, including establishing engagement protocols, coordinating regulatory notifications, managing insurance obligations and engaging with customers, suppliers, investors and other stakeholders. "You look at all the different moving parts in the aftermath of an incident and each one has a legal component," he says.

If the breach requires key customer services or accounts to be shut down or impacts customer data, effective communication is vital. Wong notes "there should be a focus on factual and consistent messaging." It's also important for the business to be clear on what documents might be disclosable in a class action or regulatory investigation. This is because legal professional privilege won't necessarily apply; best practice is to record matters factually, and not speculate or offer unnecessary commentary.



21%
**NOW HAVE A RESOURCE
DEDICATED SOLELY TO
DATA AND CYBER RISKS**



Our clients are taking a proactive role in preparatory activities where they soon learn if their plans and playbooks are fit for purpose or not"

PHILLIP MAGNESS, CYBER RISK ADVISORY LEAD

Emerging themes in insurance and regulation

As attack vectors multiply, carefully consider your cover and support

70%

OF SURVEYED
BUSINESSES HOLD
CYBER INSURANCE

85%

OF RESPONDENTS SAY
THEY WOULD NOT ENGAGE
A LAW FIRM FROM AN
INSURER'S PANEL

79%

BELIEVE WE DO NOT
NEED MORE
REGULATION

The insurance tightrope

According to our survey, 70% of respondents hold cyber insurance. While this might seem like a high proportion, we believe it reflects the overall maturity of those surveyed. Furthermore, while many large organisations have invested in internal expertise and have their own protocols to handle cyberthreats, we note that other companies are taking out cyber insurance to ensure they have ready access to incident response support.

Despite the above, we understand that only 20% of Australian SMEs hold cyber insurance.⁶ Many companies are also looking to self-insure, particularly as premiums, exclusions and retention amounts impact on the value proposition.

For Anne Hoffmann, Herbert Smith Freehills Partner specialising in cyber insurance claims, the first priority is for organisations to be across their insurance program and to fully understand which policy will respond to which loss. The effects of a cyber incident can vary markedly, from incident response costs to business interruption,

reputational damage, and regulator or class action risk. This means different policies may come into play. Businesses are well advised to work with their brokers to ensure their cover reflects what they believe they have. "I have seen time and again that companies are surprised by what their policies cover and what they do not. And that is not a situation you want in the aftermath of a cyber incident," Hoffmann says.

⁶ Insurance Council of Australia, Cyber risk, <https://insurancecouncil.com.au/issues-in-focus/cyber-risk/>



“

I have seen time and again that companies are surprised by what their policies cover and what they do not. And that is not a situation you want in the aftermath of a cyber incident”

ANNE HOFFMANN, PARTNER



Another important finding from our survey is that 85% of respondents do not intend to use a law firm from their insurer's panel. Instead, they are seeking legal advice from existing advisers. "Notwithstanding the number of companies that hold cyber insurance, many companies want to be advised by their existing advisers. Those who understand their business, people, processes and risk appetite," Whittfield says. "They also want to be supported before, during and after an event, including in the claim process itself, not just for the immediate incident triage."

Using an existing trusted advisor also helps mitigate any potential conflict of interest between the policyholder and insurer on the extent of coverage or the direction of any incident response. As Whittfield notes, "this is an issue getting increasing focus at a board level as companies look to ensure they have absolute independence of advice". However, if the vast majority of respondents are looking to engage their existing advisers, it is important they take preparatory steps prior to an incident. "We often seek pre-clearance from insurers to ensure there are no coverage issues in relation to our engagement if an event occurs," he adds.

A role for regulation?

Regulation can play a useful role in uplifting cyber resilience. Currently, the Australian Government is developing an update to its national cyber security strategy, and this may herald material legislative reform. We believe it is likely to draw upon recent developments overseas, including in Europe and the US.

Based on our survey, 68% of respondents say that regulations have been helpful when guiding internal cyber security policies and investment, but 79% do not want to see further regulation. This suggests that the right balance has been struck. We note that respondents from the energy and financial services sectors – both of which are conditioned to high regulation – appear more open to additional regulatory requirements than those from other sectors.

Given that cyber security is often a multinational issue and many Australian companies have international operations (including 71% of the respondents to our survey), many organisations already deal with regulatory regimes across multiple jurisdictions. This is in addition to oversight from ASIC, APRA, the Australian Competition and Consumer Commission (ACCC), ASX, OAIC, industry bodies and other government agencies.

"We've got a complex threat environment, a complex supply chain, digitising businesses and an overlay of complicated regulations. There is a general sense of regulatory fatigue," Whittfield says. Simplifying regulation would be preferable to "compounding more on top of organisations", he believes. Magness adds that increased government guidance, as opposed to regulation, would be easier to update in an evolving threat landscape. "It would help Australian businesses understand what good cyber security looks like."

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 provide 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



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



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



Emily Coghlan
Director, Alternative Legal
Services, Australia
T +61 3 9288 1474
M+61 412 958 233
emily.coghlan@hsf.com



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



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



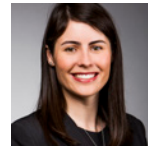
Phillip Magness
Cyber Risk Advisory Lead
T +61 3 9288 1395
M +61 419 247 070
phillip.magness@hsf.com



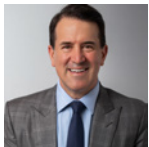
Priscilla Bryans
Partner
T +61 3 9288 1779
M+61 419 341 400
priscilla.bryans@hsf.com



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



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



Tony Damian
Partner
T +61 2 9225 5784
M+61 405 223 705
tony.damian@hsf.com



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



Maddison Ryan
Solicitor
T +61 3 9288 1541
M+61 408 085 215
maddison.ryan@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