HERBERT SMITH FREEHILLS

CYBER

ARE YOU CYBER READY?

Asia Pacific businesses vulnerable to escalating cyber threats

Herbert Smith Freehills Cyber Risk Survey

Contents

Are you cyber ready?

Herbert Smith Freehills recently surveyed a number of its Asia Pacific and global clients across a range of sectors, seeking their perspective on their organisation's approach to cyber risk.

The respondents shared a sense of increased cyber threat, with most believing cyber risk has increased compared to 12 months ago. However, our data shows that many are still not undertaking crucial preparatory work – perhaps one of the most jarring findings from our survey was that 69% of respondents said it would take an actual cyber attack to motivate their organisation to meaningfully improve their data risk management.

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

Adding further complexity is the patchwork of regulations and laws governing data privacy and cyber security across Asia Pacific. While some jurisdictions have established frameworks with sector-specific requirements, others are still in the process of developing or implementing legislation. This evolving regulatory landscape continues to shift, as regulators enhance legislation and step up enforcement against organisations.

The results also highlighted a need among survey participants for:

1. More dedicated cyber support
2. Increased education and engagement
3. Rising focus on data practices

We also observe that legal teams in Asia Pacific are perhaps unaware of the crucial role they play in a cyber crisis, with less than half of respondents saying they think legal is a key member of the incident response team in a cyber crisis. This is a notable difference to what in-house legal teams have told us in other regions of the world, where lawyers are becoming increasingly front and centre and playing the role of "breach coach".

In the immediate aftermath of an incident, legal expertise is essential in assessing the impact of an attack, ensuring regulatory compliance, navigating communications, managing notifications and helping the business engage with stakeholders. Lawyers in Asia Pacific may be underprepared to support their organisations in this way, given they are underinvesting in their own preparedness: 52% of respondents have never participated in a cyber simulation exercise and most organisations do not have a legal cyber incident response plan.

Boards also play a significant role. Key decisions, including those relating to disclosure, threat actor engagement and extortion payments often reside with the board. Despite this, almost half of our respondents say their boards have not been through a cyber simulation and 35% have not yet decided whether they were open to paying an extortion demand. Clearly there is a lot more to do.

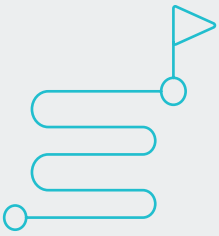
This report tracks the evolving perspectives of in-house legal teams in Asia Pacific amid a rapidly changing cyber landscape. Our research reveals that while organisations in Asia Pacific are becoming increasingly concerned with cyber risk, their preparations are not yet proportionate to the severity and complexity of the threat.

Cameron Whittfield
Partner, Head of Cyber Security – Asia Pacific

Asia survey results at a glance

Top 3

aspects of cyber risk that are greatest concern:

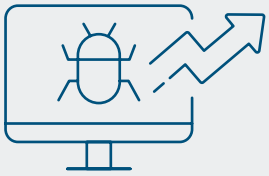


1. Lack of expertise
2. Underinvestment in systems/infrastructure
3. Limited or no testing of policies and procedures

ALMOST

60%

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



55%

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

44%

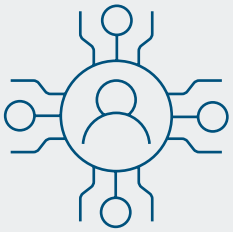
have **not held a board simulation**.

35%

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

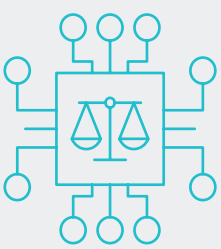
36%

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



45%

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



52%

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

58%

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

OVER 75%

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

33%

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

30%

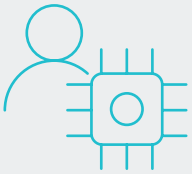
have a **resource dedicated solely** to these risks.

ONLY 77%

of organisations have **a cyber incident response plan**

61%

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



ONLY 29%

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

69%

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

MORE THAN 56%

say **more could be done to support cyber resilience** in their jurisdiction.

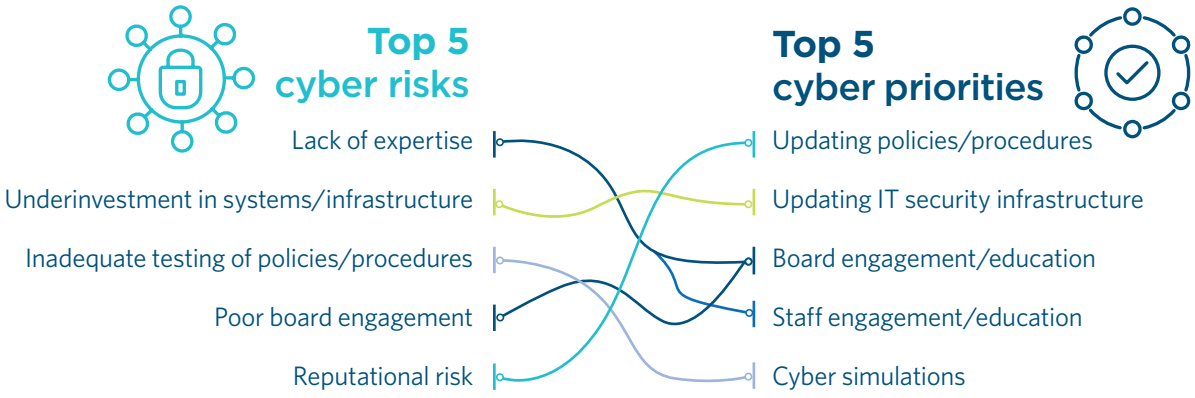
50%

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

Cyber risks and priorities

Respondents were asked to identify the cyber-related risks for their organisation, as well as their organisation's cyber risk priorities in the past 12 months.

The top five risks and top five priorities identified by respondents were:



The need for cyber specific expertise

ONLY **36%** have a **board member with specific cyber expertise**

ONLY **30%** have a **legal resource dedicated to cyber risks**

Lack of expertise is an aspect of cyber risk giving rise to great concern among survey respondents across Asia. Only 36% of respondents stated that they had a board member with specific cyber expertise and only 30% of the respondents have a legal resource dedicated to cyber risks.

This concern may be misplaced. At the board level, there is a risk that complacency can stem from appointing a dedicated or uniquely qualified individual. Cyber is like any area of business risk, and all directors should be armed with the skills to interrogate and actively participate in discussions. It is also entirely appropriate for a board to have the ability to directly interrogate cyber experts brought in to assist the organisation.

Engaging trusted external advisers supports a more efficient and effective incident response, particularly where their expertise comes from deep experience across a broad range of incidents and industries.

Data footprint

ONLY **29%** are satisfied with their organisation's **data collection and retention practices**

69% consider **it would take a cyber attack** to meaningfully improve their **organisation's focus on data risk management**

Too many organisations are still only turning their attention to the risks posed by poor data governance when an attack occurs: 69% of respondents consider it would take a cyber attack to meaningfully improve their organisation's focus on data risk management.

According to survey participants, aged data was the aspect of cyber risk causing least concern. Indeed, fewer than 40% of respondents were concerned with their organisation's data collection and retention practices. But in our practice, we observe that cyber criminals attack the digital assets you have, not the digital assets you think you have. In this context, getting a handle on your data footprint ahead of an incident is a critical part of cyber resilience, particularly in those jurisdictions with regulatory obligations to notify stakeholders and affected individuals.

Getting a handle on your data footprint ahead of an incident is a critical part of cyber resilience.

PEGGY CHOW, OF COUNSEL, CYBER AND DATA SECURITY

Underinvestment in systems and infrastructure

Survey respondents from Asia also reported concern with, and a focus on investment in, updating cyber-related policies and procedures and IT security infrastructure – proportionately more so than their peers in other jurisdictions. This may be a reflection on the relative immaturity of the Asia Pacific region when it comes to cyber preparedness.

The flurry of new cyber security legislation introduced across Asia that is designed to bolster the protection and resilience of critical infrastructure suggests a growing recognition in the region of the need to safeguard essential systems against cyber incidents. Specific legislation requiring entities to implement baseline protections in their data and information systems suggest that governments are focussing on mitigating infrastructure vulnerabilities in an era of heightened digital interconnectivity and geopolitical tensions.

The results of our survey mirror the results of cyber security preparedness surveys conducted by authorities in the region. For example:

- The Hong Kong Office of the Privacy Commissioner for Personal Data and the Hong Kong Productivity Council jointly released the results of the "Hong Kong Enterprise Cyber Security Readiness Index and AI Security" in November 2024. The results indicate that most Hong Kong enterprises' cyber security readiness fall in the 'basic' category (the five levels from high to low being 'anticipated', 'managed', 'basic', 'ad hoc' and 'unaware') and that there is still significant room for improvement.
- The Cyber Security Agency of Singapore reported in March 2024 that organisations cited a lack of knowledge and experience as a top challenge, and the perceived unlikelihood of being a target of cyber attacks being a close second.

These results suggest businesses are primarily managing cyber risk through a technical, IT security lens. But cyber risk is a whole-of-business risk. Boards, executives and legal leaders need to understand the risk, including the language each other use to discuss the risk, so they can fully participate in planning and decision-making.

SIMONE HUI, OF COUNSEL, CYBER AND DATA SECURITY

OVER 60%

believe **cyber risk management sits with Chief Information Officers or IT**

Third party risk

The vulnerability of organisations to third party risk has become topical worldwide following the global outage of the endpoint detection and response service provided by US-based cyber security software provider CrowdStrike in July 2024.

The incident reportedly had a smaller impact on the Asian market, because proportionately fewer organisations based in Asia use the CrowdStrike product.

Elsewhere in the world, however, the outage served as a useful wake-up call for organisations that had not adequately invested in their crisis response systems and business continuity planning. It will be interesting to see if this was a missed 'opportunity' for businesses in Asia.

Indeed, when we speak to our clients in Asia, managing third-party risk is a key concern for them. While organisations may seek to allocate the risk through contractual arrangements with their suppliers, organisations are still the 'controllers' of the personal data collected in their businesses and bear the regulatory burden in relation to personal data. Conducting sufficient due diligence before onboarding a supplier may be a way to mitigate this risk, and regulators do expect organisations with outsourcing arrangements to audit their suppliers through the contract term to ensure their compliance with data protection law obligations to protect personal data in their control and possession.

OVER 75%

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

Board and governance

Boards remain unprepared

Limited or no testing of policies and procedures is another area of great concern.

There is still a lot of work to do to bring boards up to speed, in particular. While more than half of boards have been educated about cyber risk, more than 44% of boards have not participated in a cyber incident simulation exercise and 35% have not even formed a view on whether it would be open to paying a ransom in the context of a cyber attack.

Cyber simulations give participants a risk-free opportunity to clarify roles and responsibilities, and to practice delegations and decision-making. They can shine a light on weaknesses in an organisation's policies, procedures and cyber resilience programmes, leading to a renewed focus and investment in systems and processes, in advance of a real-life crisis.

A clear delineation of roles and responsibilities between management and the board during a cyber crisis is critical to an effective response. Boards must also have confidence in management's ability to respond. Indeed, in our practice, we observe that experienced boards bring a welcome sense of calm and strategic clarity to cyber incident response.

The role of legal in incident response

Historically, the task of coordinating cyber incident response fell to an organisation's IT security team. Indeed, over 60% of survey respondents believe cyber risk management sits with Chief Information Officers or IT.

The survey results suggest that lawyers are downplaying, or unaware of, their relevance to cyber incident response. Less than half of respondents consider legal to be key member of the incident response team in a cyber crisis.

In this context it is not surprising that legal teams are underinvesting in their own preparedness. Over 75% of respondents do not have a cyber risk budget, only 38% of respondents have participated in a cyber simulation exercise, and most do not have a legal cyber incident response plan.

Lawyers play a key role in incident response. Lawyers may be intimately involved in reviewing compromised data, engaging with regulators, drafting communications for staff, customers and suppliers, assessing compliance risk and operational impacts, responding to contractual claims, and engaging with insurers. But the role often goes much further, given their level of visibility and engagement: in the complex aftermath of an incident, legal teams are uniquely positioned within an organisation to coordinate the overarching response and ultimately play the role of 'breach coach'.

Effective incident response is multi-disciplinary. Relying on an individual or taking comfort in a particular individual's expertise can lead to a false sense of security. Cyber is like any area of business risk, and all directors should be armed with the skills to interrogate and actively participate in discussions. It is also entirely appropriate for a board to have the ability to directly interrogate cyber experts brought in to assist the organisation.

CAMERON WHITTFIELD, PARTNER, HEAD OF CYBER SECURITY – ASIA PACIFIC

MORE THAN
44%
of **boards** have not participated in a **cyber incident simulation exercise**

LESS THAN
50%
of respondents **consider legal to be key member of the incident response team** in a cyber crisis

52%
of **legal teams** have never participated in a **cyber simulation exercise**

35%
of **boards** have not formed a view on whether they would be **open to paying a ransom**

58%
do not have a **legal cyber incident response plan**

Nuances across Asia regulations

One of the key challenges in Asia is that there is no uniform regulation on data privacy and cyber security. Unlike the EU General Data Protection Regulation (GDPR) or Digital Operational Resilience Act (DORA) in Europe, each Asian jurisdiction has its own data and cyber laws, and sector-specific requirements.

Further, companies in Asia Pacific are facing an increased regulatory burden across the region, as regulators enhance legislation and step up enforcement against organisations.

Data privacy laws

Mandatory breach notification obligations under data privacy laws is the norm across Asia, with exceptions in the Hong Kong SAR and Malaysia. However, Malaysia has issued draft rules for data breach notification obligations for public consultation and is expected to introduce them soon. In the Hong Kong SAR, mandatory breach reporting is one of the proposed reforms to data privacy laws advocated by the privacy regulator.

Notification requirements across Asia vary in several key aspects, including thresholds for reporting, the stakeholders that must be notified, notification timeframes, the definition of a personal data breach, and whether data subjects must be informed. These differences make data breach responses across jurisdictions in Asia particularly challenging.

Given these complexities, understanding the nature and extent of compromised data is critical in jurisdictions with regulatory obligations to notify stakeholders and affected individuals. Personal data is governed by data privacy laws and, in many cases, organisations are required to report breaches to privacy supervisory authorities or impacted individuals. For example, in Singapore the requirement to report a data breach depends on factors such as the nature of the compromised data and the number of affected individuals.

Cyber security laws for critical infrastructure operators

In addition to data privacy laws, designated critical information infrastructure operators in Asia are also required under cyber security laws to report data and cyber incidents to relevant stakeholders and are subject to enhanced supervisor and audit requirements to enhance their cyber resilience.

New cyber security laws to enhance the protection of critical infrastructures (CIs) have either been enacted or proposed across Asia Pacific. The objectives of these new laws are to strengthen the security of the computer systems of CIs and minimise the chance of essential services being disrupted or compromised in connection with a cyber attack.

Designated critical infrastructure operators (CIOs) are subject to enhanced reporting and audit obligations in respect of their computer systems, including reporting any change in ownership of the systems, regular audits and vulnerabilities scans, and notification of cyber incidents. Sectors providing essential services to the public (for example, energy, IT, banking and finance, transport, healthcare, utilities, and telecommunications) are often named as critical sectors with selected players in these sectors being designated as CIOs.

For a long time, privacy regulation was a proxy for cyber regulation. This has started to change, as governments appreciate the broader risks posed by poor cyber resilience. We are starting to see more scrutiny and regulation, particularly in relation to critical infrastructure.

HANNAH CASSIDY, PARTNER, HEAD OF FINANCIAL SERVICES REGULATORY, ASIA

57%

say **more could be done to support cyber resilience** in their jurisdiction.

Across 12 Asia-Pacific jurisdictions, nine jurisdictions have cyber security laws in place to identify CIOs and impose obligations on such CIOs to enhance cyber security resilience of the country. They are:

- **Singapore**: *Cybersecurity Act 2018*
- **Malaysia**: *Cybersecurity Act 2024*
- **Thailand**: *Cybersecurity Act 2019*
- **Indonesia**: *Presidential Regulation No. 47 of 2023 regarding National Cyber Security Strategy and Cyber Crisis Management*
- **China**: *Cyber Security Law 2017*
- **Taiwan**: *Cyber Security Management Act 2019*
- **Australia**: *Security of Critical Infrastructure Act 2018*
- **Japan**: *Basic Act on Cybersecurity 2020*
- **Korea**: *Critical Information Infrastructure Protection Act 2001.*

Further, the three jurisdictions below have proposed enactment of cyber security laws:

- **Hong Kong**: *Protection of Critical Infrastructure (Computer System) Bill*
- **The Philippines**: pending enactment of the *Critical Information Infrastructure Protection* law
- **India**: *Critical Infrastructure Protection Act* has been advocated.

Sector-specific requirements – financial services

Financial services regulators across Asia typically require financial institutions that sustain significant cyber incidents to report within a tight timeframe.

For example, the Monetary Authority of Singapore (MAS) should be notified no later than one hour upon discovery of a system malfunction or IT security incident, that has a severe and widespread impact on the financial institution's operations or materially impacts the financial institution's service to its customers. MAS also needs to be notified as soon as possible if a bank's critical system has failed or a distributed denial-of-service (DDOS) attack occurs.

In the Hong Kong SAR, a licensed corporation (LC) should report to the Securities and Futures Commission (SFC) immediately upon any material cyber security incident, including a ransomware attack. The SFC has not provided guidance on what it considers to be a "material" cyber security incident. An authorised institution (AI) is also required to report to the Hong Kong Monetary Authority (HKMA) immediately that an AI becomes aware that a significant incident, an IT-related fraud or a major security breach has occurred. However, the HKMA has not provided guidance on which incidents it considers should be reportable.

How we can help you

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

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

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

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

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

Our cyber offering

Cyber risk management and advisory

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

Post-incident response

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

Incident response

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

Our team

Hong Kong SAR

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

Simone Hui
Of Counsel
T +852 2101 4106
M +852 6020 9031
simone.hui@hsf.com

Leanette Ko
Associate
T +852 2101 4159
M +852 6711 1710
leanette.ko@hsf.com

Singapore

Harry Evans
Partner
T +65 6868 8079
M +65 9137 1472
harry.evans@hsf.com

Peggy Chow
Of Counsel
T +65 6868 8054
M +65 9757 7966
peggy.chow@hsf.com

Kenji Lee
Associate
T +65 6812 1356
M +65 9738 2557
kenji.lee@hsf.com

Indonesia

Cellia Cognard
Partner
T +62 21 3973 6125
cellia.cognard
@hbtlaw.com*

Dessy Arisanti
Associate
T +62 21 3973 6211
dessy.arisanti
@hbtlaw.com*

Naila Amatullah
Junior Associate
T +62 21 3973 6145
naila.amatullah
@hbtlaw.com*

Mainland China

Justina Zhang
Partner
T +86 10 6535 5158
M +86 135 2084 0636
justina.zhang
@hsfkewei.com*

Nanda Lau
Partner
T +86 21 2322 2117
M +861 3681 917366
nanda.lau@hsf.com

Tracy Chen
Associate
T +86 10 6535 5167
tracy.chen
@hsfkewei.com*

Thailand

Nonnabhat (Niab) Paiboon
Partner
T +66 2 857 3834
M +666 3681 0222
niab.paiboon@hsf.com

Supadith Palungteapin
Associate
T +66 2 857 3826
supadith.palungteapin
@hsf.com

Australia

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

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

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

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

** In Shanghai, the firm is part of a joint operation with Kewei, allowing access to China legal services alongside Herbert Smith Freehills' international expertise. In Jakarta, Herbert Smith Freehills' international counsel practise on secondment at its longstanding affiliate firm, Hiswara Bunjamin & Tandjung, one of Indonesia's leading commercial and corporate law firms.*

Notes

HERBERT
SMITH
FREEHILLS

CYBER