Cybersecurity Awareness Month Report

Asia Pacific, October 2024

Kennedys

Cybersecurity Awareness Month Report

October is Cybersecurity Awareness Month – an annual global initiative to promote awareness and education about the importance of cybersecurity practices. It serves as a timely reminder of the need to stay secure in our digital world in the face of increased cyber risks and a rapidly evolving global regulatory landscape.

To acknowledge Cybersecurity Awareness Month, Kennedys' APAC Cyber and Data Privacy team prepared a series of short updates on issues and major regulatory developments across the region as outlined in this brief report.

We looked at recently introduced regulatory reforms, including Australia's Cyber Security Bill 2024, Hong Kong's implementation of a legal framework to enhance protection of computer systems in critical infrastructure, Singapore's voluntary scheme for rating medical devices, and how APAC regulators are addressing guidelines for the responsible use of AI.

We also hosted cyber networking lunches in Singapore and Hong Kong, along with a session on handling international cyber incidents as part of our annual Hong Kong CPD day. These well attended events provided the opportunity to bring our key clients and local cyber experts together to share observations on the major issues influencing cyber and data risk mitigation, incident response, cyber claims, and the impact of regulatory and legal reforms on businesses and the insurance industry.

We hope you find our report useful. Please reach out to any of our APAC cyber contacts if you would like to discuss any of the topics covered.

Joanie Ko
Partner, APAC Head of Cyber & Data Privacy

t: +852 2848 6318
e: Joanie.Ko@kennedyslaw.com

Kennedys

Cybersecurity issues and developments

Enhanced protection of computer systems in critical infrastructure

Hong Kong will implement a legal framework to enhance the protection of computer systems in critical infrastructure. There will be two categories of critical infrastructure, with one covering those that provide infrastructure for delivering essential services in Hong Kong in these eight sectors: Energy, Information Technology, Banking and Financial Services, Land Transport, Air Transport, Maritime, Healthcare Services, and Communications and Broadcasting.

We expect to see improved security of not only the systems of critical infrastructure, but also those of the supply chain vendors that they rely upon.

Supply chain attacks are on the rise, with initial entry via leaked credentials of a vendor account being one of the major causes of network breaches. Companies must ensure that they limit privileges to vendor accounts on a needs basis and implement multi-factor authentication.

Joanie Ko, Partner (Hong Kong)

Australian Cyber Security Bill 2024

Following the Australian Government's recent proposed amendments to the Privacy Act 1988 (view our article here), another significant regulatory development was tabled on 9 October with the Cyber Security Bill 2024 designed to strengthen cybersecurity across the whole of the Australian public and private sectors.

Many of the proposed new laws are novel by international standards, and include the mandatory requirement for entities to report ransomware payments within 72 hours to the Australian Signals Directorate, introduction of security standards for smart devices, and the establishment of the Cyber Incident Review Board (CIRB) tasked with conducting reviews of significant cyber security incidents.

The Bill is part of a wider cyber security legislative reform package that has involved considerable industry consultation and puts Australia at the forefront of cyber security regulation globally. You can read our full update on the new Bill here.

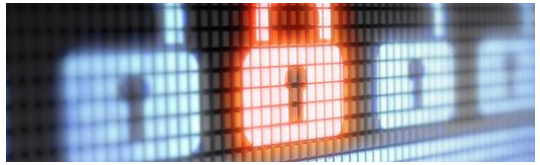
Nicholas Blackmore, Partner (Melbourne)

The importance of cybersecurity awareness with SMEs

SMEs (up to 50 employees) make up 97% of New Zealand businesses and a significant cyber incident can have a major impact. The National Cyber Security Centre's recent study showed that while awareness of cyber threats has increased in New Zealand SMEs, the majority still do not know how to get prepared or what to do if they experience an incident.

The constant juggling of time and cost priorities within SME businesses adds to the challenge. Cybersecurity incidents do not discriminate and can impact any profession or industry. Demystifying cybersecurity and ensuring easy access to help in an incident is crucial for this demographic. It is up to all of us to normalise conversations around cybersecurity.

Jess Keating, Partner (Auckland)



Legal professional privilege in cyber incident reports

The Australian class action against Optus in respect of its 2022 data breach continues to be full of important developments. At the recent PLUS Singapore Conference, we discussed the latest development from that case – the court's decision that the report of the forensic investigation commissioned by Optus was not protected by legal professional privilege.

The decision serves as a stark reminder of the importance of adhering to incident response protocols to protect legitimate claims for legal professional privilege. In particular, it is critical that when a forensic investigator is engaged for the purposes of obtaining legal advice or preparing for litigation, everyone involved in that engagement understands that those legal purposes must be the dominant purpose for the investigation, and that all aspects of the investigation, including internal and external discussion of the investigation, must be consistent with that. You can access a recording of our recent webinar on the case here.

Pippa Austin, Legal Director (Singapore)

Cybersecurity issues and developments

Voluntary scheme to rate medical device cybersecurity provisions

On 16 October 2024, Singapore introduced a voluntary scheme where medical devices can be rated according to their levels of cybersecurity provisions. It will require a minimum level of cybersecurity provisions for any medical product to be sold in Singapore. Given the growing number of medical devices that collect sensitive medical data and the interconnectedness of devices, this development is welcomed.

Medical data, unlike financial data, cannot be changed. You can easily change your bank account number or credit card, but you cannot change your medical diagnosis or results. This is why medical data is so much more valuable in the black market.

Joshua Chan, Senior Associate (Singapore)

Evolving regulatory frameworks for the responsible use of AI

The landscape of artificial intelligence continues to evolve. New guidelines and regulations have been issued by APAC regulators, including the Office of the Privacy Commissioner for Personal Data, the Hong Kong Monetary Authority, and the Cyberspace Administration of China. These frameworks include several common key principles, which are essential for responsible AI use – Governance and Accountability, Transparency and Disclosure, Fairness, and Data Privacy and Protection.

As AI becomes integral across all sectors, organisations must stay informed and be proactive in their compliance efforts.

Jeffy Ho, Associate (Hong Kong)

Coverage for BI and third party claims costs in cyber insurance policies

While cyber policies are most well-known for providing indemnification for cyber incident response costs and extortion payments, they do also provide coverage for business interruption losses as well as coverage for the costs of defending any third party claims that might arise out of an incident. A cyber incident can be extremely disruptive to certain industries like manufacturing and transport and can result in significant business interruption losses.

While largely limited to Australia for the moment, we foresee that there will be an increasing number of third-party claims for breach of privacy in other parts of Asia in the coming years.

Wanda Ng, Associate (Hong Kong)

> Supply chain attacks are on the rise; initial entry via leaked credentials of a vendor account is one of the major causes of breaches handled by Kennedys in APAC.
>
> **Joanie Ko, Partner**

> The constant juggling of time and cost priorities within SME businesses adds to the challenge. Demystifying cybersecurity and ensuring easy access to help in an incident is crucial for this demographic.
>
> **Jess Keating, Partner**


Kennedys
Legal Solutions
We think
ahead


THE REFINERY


Kennedys

Key cyber contacts - APAC

Joanie Ko
Partner, Hong Kong
t: +852 2848 6318
e: Joanie.Ko@kennedyslaw.com

Nicholas Blackmore
Partner, Melbourne
t: +61 405 627 472
e: Nicholas.Blackmore@kennedyslaw.com

James Melvin
Partner, Sydney
t: +61 2 8215 5903
e: James.Melvin@kennedyslaw.com

Julian Wallace
Partner, Singapore
t: +65 9369 6835
e: Julian.Wallace@kennedyslaw.com

Jess Keating
Partner, Auckland
t: +64 9 379 9011
e: Jess.Keating@kennedyslaw.com

Pippa Austin
Legal Director, Singapore
t: +65 6436 4381
e: Pippa.Austin@kennedyslaw.com

Vincent Chow
Of Counsel, Hong Kong
t: +852 2848 6316
e: Vincent.Chow@kennedyslaw.com

Joshua Chan
Senior Associate, Singapore
t: +65 6436 4344
e: Joshua.Chan@kennedyslaw.com

Joshua Tong
Senior Associate, Hong Kong
t: +852 2848 6313
e: Joshua.Tong@kennedyslaw.com

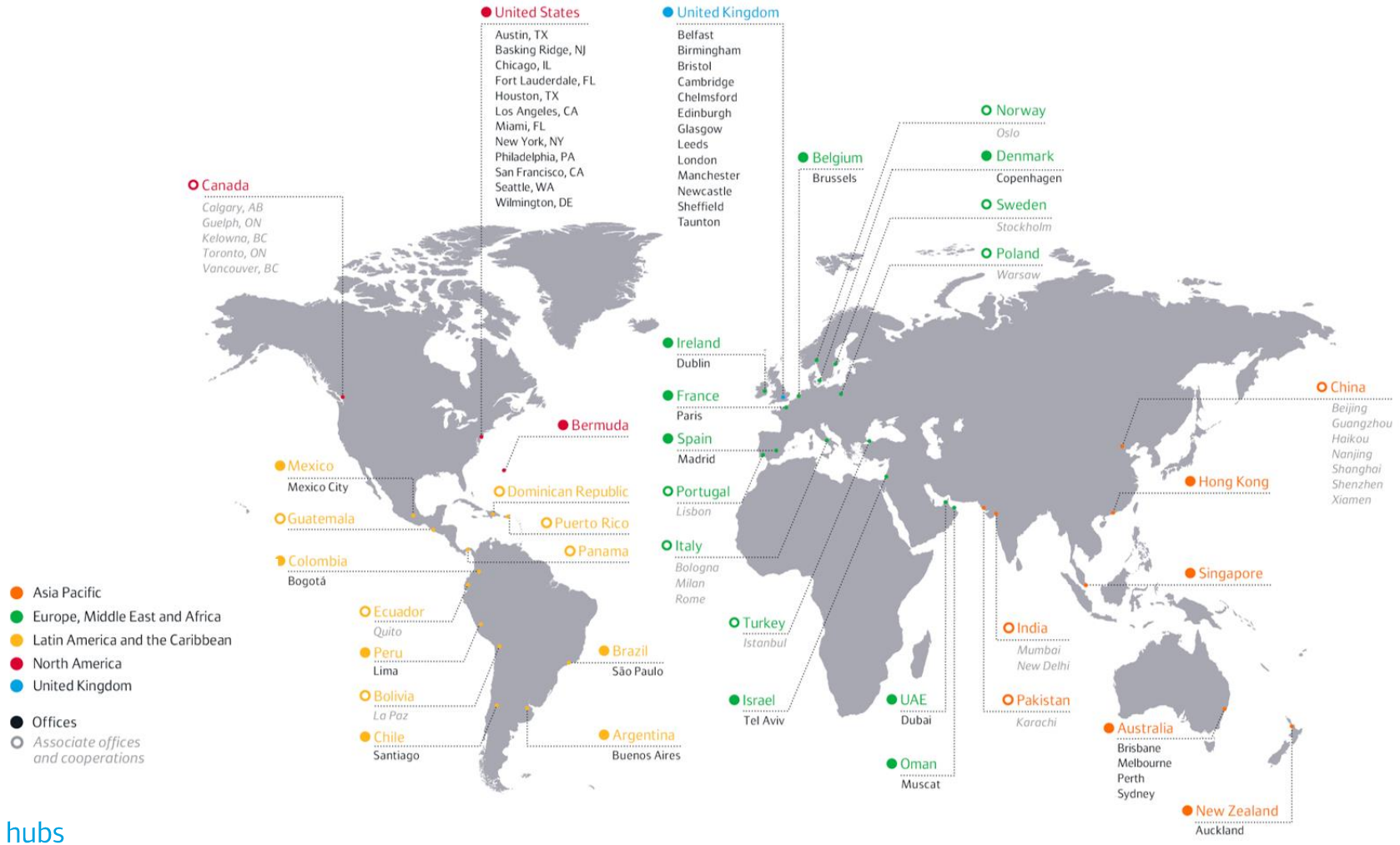
Daniel Cook
Senior Associate, Auckland
t: +64 21 964 267
e: Daniel.Cook@kennedyslaw.com

Our global footprint

Kennedys' global Cyber & Data Privacy team offers a complete 360-degree cyber service, supported by the experience of dealing with cyber incidents across multiple jurisdictions.

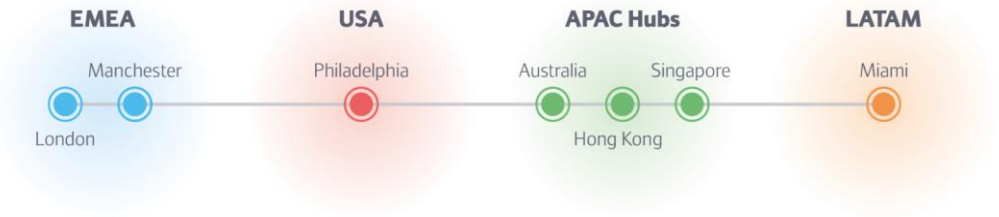
Our global network spans across 78 locations, comprised of Kennedys' own offices or associate/co-operation offices. Our Asia Cyber & Data Privacy team comprises 17 lawyers, who are part of a global strong growing team of around 90 members. We handled over 1,500 cyber instructions for SMEs and large corporates across the globe in the last 3 years.

We are widely recognised for our global, specialist expertise. Kennedys won Cyber Law Firm of the Year at the Intelligent Insurer Cyber Insurance Awards Europe 2024 and has been a finalist in the 'Cyber Law Firm of the Year' category at the Zywave Cyber Risk Awards from 2022-2024.



Global response capability from our regional hubs

One team take ownership of the response to the incident and can leverage our regional cyber team hubs to coordinate a local response as needed. Each hub has a regional network of Kennedys offices and partner firms, which they will manage and oversee. Our approach helps us to streamline the response to global incidents and ultimately save money for our clients.



Kennedys

Kennedys

Kennedys

KennedysLaw

KennedysLaw

kennedyslaw.com