CYBERSIGHT 360

A legal perspective on cyber security and cyber insurance

2025

LANDER & ROGERS

Welcome to CyberSight 360 - a legal perspective on cyber security and cyber insurance

2024 was a pivotal year for cyber security, both in offensive law enforcement and efforts made to close the gap in cyber security law.

In this guide we explore the cyber trends, legislative reforms and regulatory changes that defined 2024, and the developments we are likely to see in the year ahead and beyond. We also identify areas of growing priority – such as the need to tackle the ransomware problem with lasting impact without penalising the victim organisation, and the need to strike a balance between innovation and regulation in the development and use of AI within the cyber security context.

2024: the year strategy turned into action

If 2023 was the year of cyber security strategies, in 2024 these strategies were turned into action. An increase in joint global law enforcement efforts disrupted the operations of major cyber criminal organisations, and a quick succession of cyber security and privacy laws were passed to close identified gaps.

Australia imposed cyber sanctions for the first time in 2024, on three occasions against Revil, Lockbit and Evil Corp personnel. Large-scale data breaches continued to colour the landscape, including some of the largest breaches ever reported in Australia and the US. Whilst joint global law enforcement efforts were commendable, a string of new ransomware groups popped up in the aftermath of each takedown – a clear reminder that in this cat and mouse game, cyber criminals often remain one step ahead and are very much able to reinvent themselves and continue operations.

Australia's much anticipated first tranche of cyber security and privacy law reforms were introduced and passed in a matter of months, with the Cyber Security Legislative Package notably introducing mandatory ransomware payment reporting requirements, which take effect shortly.

Globally, with the arrival of the new Trump Administration, the survival of a suite of cyber security initiatives implemented by the Biden Administration has been thrown into question. Meanwhile, the EU has marched forward with further cyber security regulations commencing application, including the *Digital Operational Resilience Act* (DORA).

What is on the horizon in 2025?

The rapid evolution of artificial intelligence (AI) has dominated global headlines and will continue to do so in the cyber security context. We predict a shift towards new covert, AI-powered attacks, in particular a resurgence in the use of steganography in cyber attacks, and a commensurate increase in incorporating cyber threat intelligence and threat hunting as part of everyday cyber defence.

In this guide, we also take a deep dive into the evolution of ransomware and provide our perspective on how the ransomware problem may be tackled such that the disruption of ransomware groups has a lasting impact – perhaps more lasting than simply imposing a ban on ransomware payments.

We also provide a perspective on AI within the cyber security context, discussing the so-called "good, bad and ugly" that AI brings. In a world where only state actors and large tech AI companies currently have the resources, infrastructure and talent to significantly advance AI for the purposes of cyber security defence, we suggest that developing robust regulations and guidelines for the development and use of AI will be critical in ensuring that AI technologies are deployed responsibly and ethically.

Finally, we also cover the key cyber insurance trends we will likely see in 2025 and beyond, which we anticipate will include all lines of insurance tackling "silent AI" coverage issues, and a shift towards proactive breach preparation by insureds, increasingly in conjunction with insurers.

We hope you find this guide valuable and informative.

Melissa Tan
Partner and Head of Cyber Insurance
Insurance Law & Litigation

Contents

Key cyber incidents and developments in 2024 3

Key developments and offensive measures 5

Key global cyber and privacy reforms and the regulatory landscape in 2024 9

Cyber trends that will define 2025 and beyond 10

Cyber insurance trends shaping 2025 and beyond 14

Ransomware player snapshot 17

How do we tackle the ransomware problem? 19

Cyber risk and AI 24

Appendix 28

Key contacts 30

KEY CYBER INCIDENTS AND DEVELOPMENTS IN 2024

Authors: Melissa Tan and Rebekah Maxton

Global outlook

2024 saw an escalation in joint global law enforcement efforts to take down cyber criminal organisations and their supply chains. In the US, the Federal Bureau of Investigation (FBI) spearheaded a collaborative international operation to dismantle BreachForums, a notorious hacking forum that trafficked in stolen corporate data, which saw the ringleaders apprehended. Operation Cronos, a collaborative operation between the US, UK and Australia, led to the takedown of cyber criminal group Lockbit's critical infrastructure. The Australian Government used its autonomous cyber sanctions framework for the first time in 2024, employing it three times throughout the year.

However, with each successful effort emerged a new ransomware group, seemingly unfazed by enforcement action. New entrants include SafePay, FunkSec and Play, each exhibiting a "catch me if you can" attitude and reinforcing the importance of targeted and sustained global law enforcement.

Several incidents, notably the CrowdStrike outage, served as a reminder that cyber-related interruptions to business aren't always the result of malicious attacks; they can arise from an over-reliance on one dominant technology supplier to create a single point of failure in a complex, global IT supply chain. Non-malicious incidents can lead to litigation risks, such as the Meta Pixel data privacy class action, which involves allegations of misuse of a tracking pixel by Meta and violations of the Video Privacy Protection Act. With globalisation, class actions such as these have also started to impact Australian organisations.

In the last 12 months we've also witnessed an increasing number of large-scale and high-profile cyber incidents impacting the personal information of millions of individuals. In Australia, the MediSecure data breach remains the largest data breach notified to the OAIC to date, with 12.9 million Australians impacted. In the US, the UnitedHealth Group breach is the largest data breach ever reported, with the data of approximately 190 million individuals affected – breaking the previous data breach record set by Anthem Inc. in 2015, in which 78.8 million people were impacted. A number of consumer data breach class actions have been filed in the aftermath of these cyber incidents, particularly in the US. This includes class actions against Prudential Financial and Ticketmaster/Live Nation.

Following is a summary of key cyber incidents, developments and offensive measures globally in 2024.

INCIDENTS AND DEVELOPMENTS

Select a month

January

February

March

April

May

June

July

August

September

October

November

December

KEY DEVELOPMENTS AND OFFENSIVE MEASURES

22 January 2024

Country
Australia

Key developments
Cyber sanctions (first time used), offensive measures

Theat actor
REvil

Key details
Australia has imposed a cyber sanction under the Autonomous Sanctions Act 2011 on Russian national Aleksandr Ermakov for his role in the compromise of Medibank Private in 2022. This is the first time a sanction has been imposed under the Act.

Financial sanctions now make it a criminal offence, punishable by up to 10 years' imprisonment and heavy fines, to provide assets to Ermakov or to use or deal with his assets, including through cryptocurrency wallets or ransomware payments. Ermakov is also banned from travelling to, or remaining in, Australia.

20 February 2024

Target
LockBit

Development
Take down, offensive measures

Sector
Law enforcement sector

Key details
On 20 February 2024, in a Europol-led sting operation titled "Operation Cronos" that involved Australia, the United States, United Kingdom, Canada and Germany, LockBit's main darknet platform was taken down, as well as 34 global servers. LockBit's members were arrested, with warrants out for the arrest of other involved parties.

In May 2024, Dmitry Yuryevich Khoroshev was unmasked as the leader and alleged primary creator, developer and administrator of LockBit, with a warrant still out for his arrest. An indictment against Khoroshev unsealed in May alleges that he began developing LockBit as early as September 2019 and continued acting as the group's administrator throughout 2024, a role in which he recruited new affiliate members, spoke for the group publicly under the alias "LockBitSupp", and developed and maintained the infrastructure used by affiliates to deploy LockBit attacks. Khoroshev is currently the subject of a reward of up to US$10 million through the U.S. Department of State's Transnational Organized Crime (TOC) Rewards Program.

Law enforcement was still arresting members of LockBit in October 2024, with four members detained. Law enforcers resurrected LockBit's website to mock LockBit by using their own platform to tease the development.

In August 2024, Rostislav Panev, a dual Russian and Israeli national, was arrested in Israel pursuant to a US provisional arrest request with a view towards extradition to the United States, for being a developer of the LockBit ransomware group. Panev allegedly acted as a developer of the LockBit ransomware group from its inception in or around 2019 until at least February 2024. During that time, Panev and his LockBit co-conspirators grew LockBit into what was, at times, the most active and destructive ransomware group in the world. The LockBit group attacked more than 2,500 victims in at least 120 countries around the world, including 1,800 in the United States. Their victims ranged from individuals and small businesses to multinational corporations, including hospitals, schools, nonprofit organisations, critical infrastructure, and government and law-enforcement agencies. LockBit's members extracted at least US$500 million in ransom payments from their victims and caused billions of dollars in other losses, including lost revenue and costs from incident response and recovery.

LockBit's members comprised "developers", like Panev, who designed the LockBit malware code and maintained the infrastructure on which LockBit operated. LockBit's other members, called "affiliates", carried out LockBit attacks and extorted ransom payments from LockBit victims. LockBit's developers and affiliates would then split ransom payments extorted from victims.

A total of seven LockBit members have now been charged in the District of New Jersey.

INCIDENTS AND DEVELOPMENTS

8 May 2024

Country

Australia

Developments

Cyber sanctions (second time used), offensive measures

Theat actor

Lockbit

Key details

Australia imposed a targeted financial sanction and travel ban on Russian citizen Dmitry Yuryevich Khoroshev for his senior leadership role in the LockBit ransomware group.

This is the second use of Australia's autonomous cyber sanctions framework and part of ongoing coordinated international law enforcement action.

The new sanction under the cyber sanctions framework makes it a criminal offence to provide assets to Khoroshev, or to use or deal with his assets.

The framework is intended to disrupt and deter the perpetrators of malicious cyber activity, such as ransomware.

15 May 2024

Target

BreachForums

Development

Take down, offensive measures

Sector

Law enforcement sector

Key details

The FBI led a global law enforcement operation to take down BreachForums, a hacking forum where users exchanged stolen data, sold access to corporate networks, and offered various cyber criminal services.

The BreachForums website posted an official announcement indicating that the FBI had assumed control of the site and its backend data. Nevertheless, two weeks after the shut-down, the leak site came back online and appeared to have been hawking personal and payment card data purportedly belonging to more than 500 million Live Nation/ Ticketmaster customers.

1 August 2024

Target

Cryptonator

Development

Take down, offensive measures

Sector

Law enforcement

Key details

Law enforcement agencies from the United States and Germany (IRS-Criminal Investigation, the US Department of Justice, and the Federal Bureau of Investigation in coordination with the German Federal Criminal Police Office (BKA) and the Attorney General's Office in Frankfurt) successfully seized the domain of the cryptocurrency wallet platform, Cryptonator, for failing to have appropriate anti-money laundering controls in place and facilitating illicit activity.

Cryptonator, launched in 2014, was an online cryptocurrency wallet that enabled direct transactions and instant exchange between different cryptocurrencies in one personal account, essentially acting as a personal cryptocurrency exchange.

This platform was reportedly utilised by ransomware gangs, darknet marketplaces, and various other illicit services.

Additionally, an indictment was issued by prosecutors for the Justice Department in the Middle District of Florida against Cryptonator's operator, Roman Boss, who was charged with money laundering and running an unlicensed money service business operation that processed more than US$235 million in illicit funds.

20 August 2024

Target

Fox Sports, AFL, NRL

Development

Meta Pixel lawsuit, privacy class actions

Sector

Technology

Key details

Two class actions were launched in the United States District Court in California against the NRL, AFL, and Fox Sports, including its subsidiary Fox Sports Stream Co, over allegations of breaching the Video Privacy Protection Act through the use of a Meta tracking pixel on subscription services to stream NRL and AFL games outside of Australia.

Meta's tracking pixel is a piece of code that other companies can incorporate into their websites. The pixel tracks users' browsing data and feeds this back to Meta (the owner of Facebook) to deliver targeted advertising.

This stored data helps advertisers to target users on Facebook who have visited the Fox Sports website, as well as find "lookalike" audiences to serve advertising to new users who share similar traits.

In recent years, we have seen a proliferation of such privacy class actions commenced by consumers in the US, with Meta facing at least 50 Meta Pixel class action lawsuits in 2023.

12 September 2024

Target

23andMe

Country

United States

Development

Class action settlement

Sector

Private sector, personal genomics and biotechnology company

Key details

Following a class action filed in a San Francisco federal court, 23andMe agreed to pay US$30 million and provide three years of security monitoring to settle a lawsuit after a 2023 data breach exposed the personal information of 6.4 million customers.

Approximately US$25 million of the cost is expected to be covered by cyber insurance coverage.

The settlement also resolves accusations that 23andMe did not tell customers with Chinese and Ashkenazi Jewish ancestry that the hacker appeared to have specifically targeted them and posted their information for sale on the dark web.

In October 2023, 23andMe revealed that unauthorised access to customer profiles occurred through compromised accounts. Hackers exploited credentials stolen from other breaches to access 23andMe accounts.

The breach originally began around April 2023 and lasted about five months, affecting nearly half of the 14.1 million customers in 23andMe's database at the time.

18 September 2024

Target

Ghost

Development

Take down, offensive measures

Sector

Law enforcement sector

Key details

Led by Europol's Operational Taskforce and nine other countries, the United States, Canada, France, Italy, Ireland, Australia, Sweden, and the Netherlands successfully dismantled the Ghost encrypted communications platform used by crime groups.

Ghost was used by thousands of people worldwide for criminal activities such as drug trafficking and money laundering.

Authorities examined the evidence and coordinated raids in multiple countries, resulting in 51 arrests: 38 in Australia, 11 in Ireland, one in Canada, and one in Italy.

The Australian Federal Police (**AFP**) announced in September 2024 that its Operation Kraken had charged a NSW man, aged 32, for creating and administering Ghost, which the AFP alleges was built solely for the criminal underworld.

2 October 2024

Country

Australia

Developments

Cyber sanctions (third time used), offensive measures

Theat actor

Evil Corp

Key details

Australia has imposed targeted financial sanctions and travel bans on three Russian citizens for their involvement in the Evil Corp cyber crime group: Maksim Viktorovich Yakubets, Igor Olegovich Turashev and Aleksandr Viktorovich Ryzhenkov, all of whom hold senior roles in Evil Corp.

For more than a decade, Evil Corp has been responsible for significant cyber incidents, including ransomware attacks across Europe, the United Kingdom and the United States, resulting in millions of dollars of losses and disruptions to critical health systems, national infrastructure and government sectors.

The sanctions make it a criminal offence to provide assets to these individuals, or to use or deal with their assets. The sanctions also ban them from entering Australia.

CASE STUDY

20 December 2024

Case

Mobius Group Pty Ltd v Inoteq Pty Ltd [2024] WADC 114

Country

Australia

Development

Australian case law on BEC and payment redirection scam

Country

Australia (District Court of Western Australia)

Sector

Legal

Key details

Mobius Group is an electrical instrumentation and control systems engineering consultant and installation contractor. Mobius Group entered into an agreement with Inoteq to perform electrical works on the Rio Tinto managed aquifer reinjection scheme project for Inoteq.

Mobius Group did the work and in March and April 2022, Mobius Group issued invoices totalling $235,400 to Inoteq.

Without the knowledge of either Mobius Group or Inoteq, an unknown third party gained access to Mobius Group 's email account. On 28 April 2022 the scammer sent an email from Mobius Group's email account to Inoteq instructing it to correct the details of its bank address in the earlier invoices, as it said Mobius Group's bank details had changed. That email attached an invoice with the purported new bank details.

Inoteq attempted to verify the new account details by contacting Mobius Group via telephone, but was unsuccessful as the line was bad and the Inoteq employee could not hear Mobius Group's answer over the phone. Consequently, Inoteq sent a follow-up email requesting proof of the account change, to which the scammer responded.

In a typical payment redirection scam, Inoteq then paid the invoices to the account nominated by the scammer.

Upon the fraud being discovered, the police was notified and the bank contacted. The bank was able to recover the sum of $43,541.13. Mobius Group did not receive payment of the sum of $191,859.16 and sued Inoteq for payment of that outstanding amount.

Decision

On 20 December 2024, the Western Australian District Court held that Mobius Group was entitled to payment for the work performed, and Inoteq was liable for the outstanding amount of $191,859.16.

Inoteq's efforts to argue against paying the owed amount, including citing an indemnity clause in the contract and claiming Mobius Group had failed its duty of care by not taking additional measures to secure its email accounts, were ultimately unsuccessful.

The Court placed some emphasis on the issue that Inoteq did not make a follow-up call despite not being able to hear the answer during the verification phone call. The Court said that "ultimately only the defendant was in a position to be able to take measures to stop itself from being the victim of a fraud".

Those measures included the telephone call and making a follow-up call if they could not hear the other person due to the line. This is because "the defendant clearly had Mr Harrington's telephone number, and it would have taken little effort to make another telephone call and receive a clear answer to the question posed. That telephone call could have meant that the loss was avoided, these proceedings never occurred, and the fraudsters left unfulfilled".

The court held that the alleged duty of care does not apply to the circumstances of this case. While Inoteq may have been vulnerable to loss if Mobius Group's email account was compromised, it had the ability to protect itself against that vulnerability. It failed to do so.

Further, any loss by Inoteq constituted pure economic loss. Therefore, reasonable foreseeability of its loss was not sufficient to create a duty.

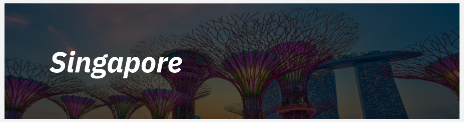
Having found there was no duty of care, the Court did not decide on the point of concurrent wrongdoers and apportionment of liability between Mobius Group, Inoteq and the scammer.

As such, whilst the actions of the scammer are reprehensible, ultimately the defendant was in the best position to protect itself against the fraud.

REFORMS AND REGULATORY

Authors: Melissa Tan, Rebekah Maxton and Jeffrey Chung

SELECT A REGION



CYBER TRENDS THAT WILL DEFINE 2025 AND BEYOND

Authors: Melissa Tan and Jeffrey Chung

The cyber risk landscape continues to shift as threat actors tap into emerging technologies, geopolitical tensions heighten, and enforcement action increases.

The cyber threats and trends that will define 2025 and beyond include:

- a shift towards new **covert**, AI-powered attacks
- an increase in **threat hunting**
- greater clarity on cyber and privacy **regulatory action**
- increased measures to counter threats of technology-enabled espionage, **foreign interference** and sabotage.

1 New methods: A shift towards covert, AI-powered attacks

Cyber criminals are an innovative bunch. They continuously find new and creative ways to launch cyber attacks, making them more difficult to detect and harder to prevent. As AI evolves, cyber criminals are leveraging these tools to streamline their processes and combine them with common forms of cyber attacks (such as phishing and social engineering) to launch increasingly sophisticated attacks that are often able to bypass conventional security measures.

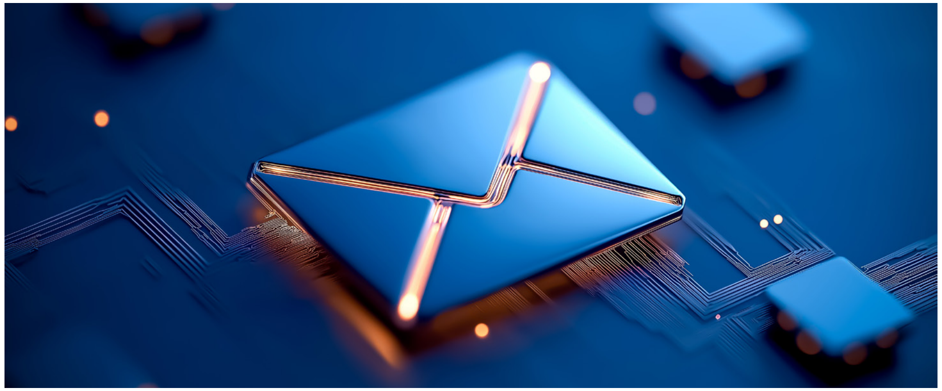
In particular, the growing prevalence of AI has led to a resurgence in the use of steganography in cyber attacks. This involves hiding malicious or sensitive data within what would otherwise appear to be benign files in the form of images, videos and audio.

Cyber criminals have taken advantage of AI to elevate their cyber attacks by crafting more convincing messages to entice users to interact with the content and to automate the process of generating a cover object, and hiding and extracting information through layers of training. As a result, the process of distinguishing a legitimate email from one that has been tampered with has become even more challenging.

In the case of a cyber criminal using an image as a payload (the part of malware that causes harm), a user receives an email that appears legitimate and seemingly harmless; however, once the email is opened, it exploits known vulnerabilities to initiate the download of the image file hosted on a public platform. Concealed within the file is a malicious code that is invisible to the eye. The encoded payload is then extracted and decoded into a fully functional executable file. Once the executable file is activated, malware is deployed, which enables cyber criminals to gain unauthorised access to systems and exfiltrate data. Cyber criminals can also use steganography to hide tools that can communicate with, and control, compromised devices within a network as part of a cyber attack.

This technique allows cyber attacks to evade traditional detection methods, such as antivirus software or scanning technology that typically overlook non-executable files. This presents significant cyber security risks:

- From a user standpoint, the subtlety of the attack and the seemingly innocuous nature of the files attached means that users, and even some security teams, are unlikely to suspect malicious intent. The impact of these types of attacks, however, can be devastating in circumstances where systems are compromised and sensitive data is exfiltrated whilst remaining undetected for a period of time.
- From a forensics standpoint, this technique presents a novel set of challenges as it is becoming increasingly difficult to detect whether information has been exfiltrated through the concealment of information within the code of a file that requires advanced tools to detect.



As such, protecting against the use of steganography is a complex exercise and requires ongoing mitigation tactics, such as:

- advanced Content Disarm and Reconstruction (**CDR**) technologies to sanitise files at the point of entry. CDR works by deconstructing even non-executable files, by analysing them and dissecting their metadata and content, with a focus on safe elements rather than threats. As CDR only rebuilds from the items that are certain to be safe, it prevents payload execution by neutralising malicious scripts or encoded data embedded within files and stopping them from entering the environment.
- using endpoint protection software that extends beyond static checks, basic signatures and other outdated components, and instead focussing on the use of behavioural engines, which work by monitoring the execution of processes on a system for potentially malicious actions.
- ongoing cyber security training for all employees within organisations (not just security teams) to raise awareness of emerging risks and the importance of exercising caution when interacting with any emails or files from unknown sources.

2 An increase in threat hunting

Threat hunting and the use of cyber threat intelligence (**CTI**) will increase as organisations increasingly shift from taking a reactive approach, to incorporating a proactive approach to identify unknown and ongoing threats in their network.

Since threats evolve faster than our defences can adapt, and the attack surface is constantly expanding, it is no longer sufficient to rely solely on technology that generates alerts when threats are detected – particularly as cyber criminals lodge increasingly sophisticated attacks that can evade traditional detection methods.

Threat hunting and CTI are proactive processes that, together, can help organisations gather insights on the threats they are facing and assess their risks. This allows organisations to prioritise resources and budgets to ensure adequate protections from a more informed standpoint. This proactive strategy involves:

- using threat hunting to actively search for, identify, and isolate advanced threats that evade existing security solutions. In this way, organisations are not simply waiting to receive alerts and they have significantly more visibility of the threats within their systems. Having greater awareness helps organisations to deal with and remove threats before they can be exploited, rather than being on the back foot.
- using CTI as a profile-building exercise to obtain knowledge about the enemy, which allows an organisation to better understand who and what it is dealing with in order to prevent and mitigate cyber threats. This involves understanding who the threat actors are, what their motivations may be, and the techniques they are known to use.

These methods will be an integral part of an organisation's comprehensive cyber security program.

3 Greater clarity on cyber and privacy regulatory action

As Australian regulators increasingly use their powers to conduct investigations and undertake enforcement action in relation to cyber attacks, we will likely see greater clarity on the scope and consequences of cyber and privacy regulatory action.

In the past few years, the Office of the Australian Information Commissioner (**OAIC**) has shifted its focus to a more risk-based, enforcement and education-focused posture. This has led to an increase in regulatory action against entities, as demonstrated by the OAIC civil penalty proceedings currently on foot.

Similarly, cyber resilience has remained an enforcement priority of the Australian Securities and Investments Commission (**ASIC**) since its action against RI Advice, in which RI Advice was found to have breached its licence obligations to act efficiently and fairly when it failed to have adequate risk management systems to manage its cyber security risks after experiencing multiple cyber incidents and was ordered to pay $750,000 towards ASIC's costs. ASIC also recently commenced enforcement action against FIIG for "systemic and prolonged cybersecurity failures". ASIC has warned that it would bring charges against directors who fail to adequately prepare for hacks, with ASIC Commissioner Simone Constant confirming the process was under way, although ASIC declined to name the companies.

Speaking at a 2023 Cyber Summit, ASIC Chairman Joe Longo made this clear: "If things go wrong, ASIC will be looking for the right case where company directors and boards failed to take reasonable steps, or make reasonable investments proportionate to the risks that their business poses."

The Australian Prudential Regulation Authority (**APRA**) has also, in the last year, written to all regulated entities to provide further insights and guidance on common cyber control weaknesses, as well as emphasising the critical role of data backups in protecting cyber resilience. This is part of APRA's ongoing commitment to supervising cyber resilience across industry.

The Australian Communications and Media Authority (**ACMA**) has a memorandum of understanding with the Australian Cyber Security Centre (**ACSC**) that allows for the exchange of information about enforcing protections to keep Australians safe from mobile number fraud and scams. In recent years, ACMA has also increased its efforts to investigate and take enforcement action against regulated entities following cyber attacks.

Australian regulators have demonstrated a distinct focus on the cyber resilience of organisations and are exercising their powers to investigate any failings or suspected contraventions falling within their remit. As they continue to develop their investigative capabilities in relation to cyber security, we anticipate that regulators will keep cyber risks firmly on their agenda and be increasingly willing to exercise their enforcement powers, which will bring more clarity to the scope and consequences of cyber and privacy regulatory action.

We say this because at this stage, much of the legislation in question is untested and yet to be judicially determined. Uncertainty remains as to how some of the cyber and privacy regulatory action may pan out, including its potential consequences. One common unresolved issue is whether a cyber attack that affects multiple individuals will give rise to a single breach, or multiple breaches of the relevant legislation (including section 13G of the *Privacy Act 1988* (Cth)). This is an important issue as it determines the potential penalties that may apply. In 2025 and beyond, we foresee that the increase in regulatory activity across cyber and privacy will shed light on such matters as enforcement actions develop and reach their conclusion.

4 Increased measures to counter threats of technology-enabled espionage, foreign interference and sabotage

At a time when geopolitical tensions increasingly shape the digital landscape, threats posed by nation-state actors are an ongoing risk to Australia. For example, sophisticated campaigns undertaken by groups such as APT40 have repeatedly targeted Australian networks, as well as government and private sectors in the region with a focus on critical infrastructure including energy, healthcare and telecommunications sectors.

As outlined in the Australian Security Intelligence Organisation's (**ASIO**) Director-General's Annual Threat Assessment 2025, threats posed by espionage and foreign interference continue to intensify and are aided by advancements in technology, with AI enabling disinformation and eroding trust in institutions, and deeper pools of personal data being vulnerable to collection, exploitation and analysis by foreign intelligence services. Cyber units from nation states routinely try to explore and exploit Australia's critical infrastructure networks, mapping systems to lay down malware or maintain access in the future. If tensions continue to escalate, foreign regimes may become more determined to pre-position cyber access vectors that they can then exploit.

Threats like these demand a proactive approach to resilience and adaptability. In Australia, there are various measures in place that address these ongoing risks.

The Australian Signals Directorate (**ASD**) has an offensive cyber capability, which it uses against adversaries to protect Australians and Australia's national interests. These include a broad range of offshore activities to deter, disrupt, degrade and deny adversaries. In addition, the Australian Federal Police (**AFP**) leads the investigation of serious and organised cyber crime activity that impacts the government, systems of national significance, or the wider Australian economy. The AFP and ASIO also lead the Counter Foreign Interference Taskforce for tactical and operational responses to cases of foreign espionage and interference, identifying them, investigating them, disrupting them and prosecuting those responsible.

In addition to these cyber offensive capabilities, we have seen a growing focus on defensive capabilities that adopt shared responsibility to mitigate threats. On 14 January 2025, the Department of Home Affairs announced the launch of an initiative called "Countering Foreign Interference in Australia: Working Together Towards a More Secure Australia" which outlines measures to identify, mitigate and prevent foreign interference. This initiative was introduced to combat sophisticated and persistent foreign interference activities from a range of countries, which have cyber security implications particularly for the technology and critical infrastructure sectors. The strategy seeks to increase Australia's collective resilience against foreign interference, stressing that it is a shared responsibility. As part of this, individuals and organisations have been urged to report any signs of interference activities and to bolster cyber security controls.

While there are measures in place to address the risks of technology-enabled foreign interference, as AI and other technologies gain sophistication, laws will need to address how these technologies are used to gather information for espionage or for the purpose of generating misinformation for foreign interference. We anticipate ongoing enhancements to measures that counter these risks in the years ahead.

CYBER INSURANCE TRENDS SHAPING 2025 AND BEYOND

Authors: Melissa Tan and Jack Boydell

As we look to 2025 and beyond, four key themes will impact the cyber insurance industry.

1 Coverage for AI risks

Artificial Intelligence (**AI**) technology continues to evolve rapidly, transforming nearly every industry. While AI presents significant opportunities, it also introduces new challenges for businesses. Businesses leveraging AI must proactively assess and manage these unique risks, ensuring their insurance programs adequately cover both current and emerging AI-related risks.

Insurers are slowly starting to respond to the use of AI by businesses and addressing potential coverage gaps for policyholders. While AI risks are potentially caught within current cyber coverage, insurers are increasingly addressing the "silent AI" issue by introducing affirmative AI insurance cover within cyber insurance policies to provide clarity on how incidents are covered when AI is involved, or creating a new insurance product to specifically address AI-related risks. For example, AXA XL has added a Generative AI models endorsement to its global cyber insurance coverage;[1] Coalition has added a new *Affirmative Artificial Intelligence (AI) Endorsement* to clarify what is covered by its US Surplus and Canada Cyber Insurance policies,[2] whilst Armilla Assurance has created a new *Armilla Guaranteed* product that provides warranty coverage for AI products[3]. New insurance products and affirmative AI cover will continue to emerge in 2025 and beyond as the industry moves to address evolving AI-related risks faced by businesses utilising AI.

As stated above, even where AI risks are not explicitly covered, "traditional" policies such as property and liability policies (e.g. professional indemnity (**PI**) or directors and officers (**D&O**) policies) may respond to AI risks or provide "silent" coverage through the absence of AI-specific exclusions. The biggest risk for insurers here is to provide cover for unforeseen losses and claims where the risks have not been assessed or priced. In their efforts to address the silent AI issue, some insurers may also decide to include AI exclusions in policy wordings as AI risks become more defined or claims arising from AI-related risks increase. However, to date, we have generally not seen explicit AI exclusions in liability policies, at least in Australia. However, the dynamic and ongoing development of AI presents challenges for insurers in drafting exclusions that are able to strike the balance between precisely defining AI while not significantly reducing coverage – which impacts demand for the insurance product. We anticipate that insurers will seek to evaluate their suite of products to identify "silent AI" issues and whether any changes need to be made to clarify the scope of cover relevant to AI risks.

Before considering AI-specific insurance policies or endorsements, businesses should evaluate their use of AI ("*In what processes do we utilise AI?*"), their current "traditional" policies to understand the scope of coverage currently available (*"Which liability insurance that we currently hold may respond to AI-related risks?"*), including any applicable exclusions related to AI-related risks, and whether they need AI-specific coverage. In particular, policyholders should consult their brokers to review existing coverage and ensure that future coverage is designed to protect against and mitigate new risks associated with leveraging AI in their business.

---

1 https://axaxl.com/press-releases/axa-xl-unveils-new-cyber-insurance-extending-coverage-to-help-businesses-manage-emerging-gen-ai-risks

2 https://www.coalitioninc.com/au/announcements/coalition-adds-new-affirmative-ai-endorsement-to-cyber-policies

3 https://www.armilla.ai/resources/armilla-assurance-launches-armilla-guaranteed-tm-warranty-coverage-for-ai-products-in-partnership-with-leading-insurance-companies

2 Proactive breach preparation

As businesses uplift their cyber resilience and become more aware of evolving cyber risks, we expect to see more businesses undertaking proactive breach preparation.

A key benefit of cyber insurance is the provision of incident response management services by experts on the cyber insurer's panel, often without an excess applicable. However, for years, insureds have not been familiar with the insurer's incident response management services until an incident occurs, and it can be challenging to establish and maintain a good working relationship with an unfamiliar individual or team in the midst of a crisis.

As such, we have increasingly seen insureds reach out to the insurer's incident response management services panel to request pre-breach training, table-top exercises and/or to enhance their cyber incident response plan with that particular incident response management services expert in mind. If and when an incident does occur, the business is then already familiar with that expert, and can work seamlessly with them to manage the incident. Proactive breach preparation will enhance insureds' preparation and reduce any delays in the management of an incident. This is a positive development for the cyber insurance industry.

3 Increasing identity and access management requirements for cyber coverage

Cyber insurers typically impose certain baseline security requirements on businesses to qualify for cyber insurance coverage. These requirements often include preventative controls such as employee training, data backups and recovery policies, enabling multifactor authentication (**MFA**) and implementing Privileged Access Management (**PAM**). Insurers use these security requirements and risk assessments to evaluate and mitigate risks and quote coverage and premiums before providing cyber insurance coverage.

Globally, and in Australia, a growing proportion of cyber attacks and resulting claims are linked to identity and privilege compromises.[4] For instance, Delinia's 2024 Cyber Insurance Research Report revealed that identity and privilege compromises account for 47% of cyber attacks leading to insurance claims.[5] This trend underscores the growing vulnerability of business accounts and credentials in cyber attacks, reflecting threat actors' heightened focus on exploiting valid accounts and credentials to gain access to business systems.

In response, cyber insurers are and will continue to place greater emphasis on identity and access management within businesses and their associated risks. Consequently, we are witnessing an increase in the scope and extent of security requirements for privileged access and other identity security controls by cyber insurers. This trend is expected to continue in 2025 and beyond.

4 Growing importance of Contingent or Dependent Business Interruption cover

In 2024, a seemingly simple software update by cloud-based cyber security platform CrowdStrike caused a global crisis. The update sent 8.5 million Windows devices into chaos, crashing Microsoft Azure systems. Additionally, a ransomware attack on Change Healthcare, a provider of revenue and payment cycle management within the US healthcare system, resulted in file encryption and the theft of protected health information of an estimated 190 million individuals. This attack led to an outage that lasted for several weeks, severely hampering claims processing and causing massive disruption to the revenue cycles of providers such as physician practices, hospitals, and pharmacies.

These unprecedented events disrupted services to thousands of businesses, in both cases due to a single point of failure or interruption linked to a single third-party service provider. The CrowdStrike and Change Healthcare incidents (among others) highlight the systemic risk presented by third-party technology providers that may have thousands or even millions of users or customers. This systemic risk is caused by businesses being increasingly reliant on technology, creating a growing vulnerability to cyber risks arising from their third-party technology supply chains. Minor disruptions or interruptions can have widespread and cascading effects, bringing millions of businesses and entire industries to a standstill and potentially causing significant financial losses.

Contingent or Dependent Business Interruption (DBI) coverage refers to coverage for an insured's loss of income as a result of a disruption or outage of a third-party service provider, which in turn disrupts the insured business's operations. DBI coverage provides a solution to businesses looking to manage cyber risks arising from their third-party technology supply chains. In light of the recent CrowdStrike and Change Healthcare incidents and their widespread effects, we anticipate that DBI cover will become an increasingly important part of the risk management strategy of businesses in 2025 and beyond, with businesses seeking specific coverage for DBI to manage risks connected with third-party technology supply chains. This is already becoming more common in cyber insurance policies.

Businesses should evaluate their exposure to the risk of disruption or interruption to their third-party technology supply chains and consider whether their current insurance program or standalone cyber insurance policies include coverage for DBI. Businesses should also check that their cyber insurance policy has a "system failure trigger" or similar for DBI, which provides cover for disruptions caused by system failures, such as those seen in the CrowdStrike incident, which are not necessarily the result of a cyber attack. While some cyber policies provide standard business interruption cover, this cover is generally limited to the insured business's own network and may not provide coverage for losses arising from a failure of a third party's network.

---

4 https://cybermagazine.com/articles/delineas-2024-cyber-insurance-research-report; https://itbrief.com.au/story/unmasking-cyber-criminals-the-power-of-privileged-identities

5 Identity Security is Critical to Obtaining and Maintaining Cyber Insurance 2024 State of Cyber Insurance Research Report

6 https://www.crcgroup.com/Tools-and-Intel/post/potential-insurance-impacts-of-the-crowdstrike-outage

7 https://jamanetwork.com/journals/jama-health-forum/fullarticle/2823757

8 https://costerobrokers.com/protect-your-clients-against-supply-chain-cyber-risk-with-dependent-business-interruption-coverage/

9 https://www.insurancebusinessmag.com/au/news/cyber/lockton-unveils-cyber-disruption-guide-amid-rising-threats-in-australia-508632.aspx

RANSOMWARE PLAYER SNAPSHOT

Authors: Melissa Tan, Rebekah Maxton and Jeffrey Chung

BlackSuit: A Royal rebranding

Name

BlackSuit Ransomware

First appearance

2023

Extortion methods

Encrypting and exfiltrating data, public data leak sites

Notable sectors attacked

Healthcare, private sector, critical industries

Claimed victims overall

175

Claimed victims in 2024

156

Biggest attack to date

CDK Global, with US$25 million ransom reportedly paid

Total money extorted

Over US$500 million in demands

BlackSuit, which emerged in May 2023, has garnered notoriety as a sophisticated ransomware group adept at encrypting and exfiltrating data from its targets. The group maintains public leak sites to expose the data of victims who do not meet their demands. BlackSuit's operations have significantly impacted various sectors worldwide, including healthcare, education, and other critical industries.

Cyber analysts were quick to link this threat actor to the infamous Royal Ransomware, finding strong similarities between the Russian dialects, coding sequences and tactics utilised by both gangs to infiltrate organisations.[1] Royal Ransomware gained notoriety between 2022 and 2023 when it launched attacks against multiple sectors and organisations worldwide, including Australia. Royal was also linked to existing ransomware groups, including Zeon and Conti. After comparing ransomware samples used by Royal and BlackSuit, researchers found there to be 98% similarities in functions, 99.5% similarities in blocks, and 98.9% similarities in jumps based on BinDiff, a comparison tool for binary files.[2]

Although the malware shares similarities, BlackSuit is regarded as the successor to Royal. This is due to BlackSuit's use of enhanced encryption methods, higher ransom demands (typically ranging from US$1 million to US$10 million demanded in bitcoin), more aggressive ransom collection tactics, and expanded capabilities through the addition of IP verification to improve targeting accuracy.

BlackSuit utilises four main strategies to infiltrate its targets:[3]

1. **Phishing:** The most common tactic used by BlackSuit actors to access victim networks is via phishing emails. When recipients engage with these emails, which contain malicious PDF documents, they unknowingly install malware. This malware subsequently facilitates the deployment of BlackSuit ransomware.
2. **Remote Desktop Protocol (RDP):** The second most prevalent route for initial access utilised by BlackSuit actors, accounting for approximately 13.3% of incidents, is the compromise of RDP.
3. **Public-facing applications:** BlackSuit actors sometimes gain initial access to victims' systems by exploiting vulnerable public-facing applications that are misconfigured or unpatched.
4. **Brokers:** BlackSuit actors may leverage initial access brokers to gain access and source traffic by harvesting virtual private network (VPN) credentials from stealer logs.

Once BlackSuit gains access, it employs a remote access trojan (**RAT**) that enables the threat actors to establish command-and-control capabilities through an anonymous proxy connection. With control secured, BlackSuit then escalates its privileges and initiates lateral movement across the victim's systems. When the preparations are complete, data exfiltration commences.

BlackSuit has targeted various industries since late 2023, demonstrating a high level of sophistication and adaptability. The group's ability to evolve and employ new tactics positions it as a formidable threat in the cyber security landscape.

BlackSuit's most notable 2024 incident occurred in June, when it launched a cyber attack on CDK Global, a major car dealership software company. CDK makes software that is commonly used by car dealerships to process sales and other transactions. This attack led to a multi-day system shutdown, highlighting BlackSuit's capability to cause widespread disruption. Many dealerships started processing transactions manually, according to local press reports.[4] It has been widely reported/speculated that CDK would likely have paid the US$25 million ransom to BlackSuit to have its systems back online.[5]

Another significant incident involved an attack on Kadokawa Corporation and its subsidiary, Niconico, between 8 June 2024 and 5 August 2024. This attack led to the leak of personal information belonging to 254,241 individuals and the theft of 1.5 TB of data. The Japanese publisher reportedly paid BlackSuit US$3 million in ransom to protect its data.[6]

Australia is not excluded from BlackSuit's cyber attacks, with the ransomware gang targeting two notable Australian companies in 2024. Australian property firm Herron Todd White lost more than 300 GB of data to BlackSuit on 27 April 2024. Herron Todd White did not confirm whether a ransom was paid. The second major attack was on Australian hospitality and catering firm Reward Hospitality on 20 July 2024, where BlackSuit claimed to have stolen large amounts of data from the organisation. The company declined to comment on the incident.

The emergence and rise of BlackSuit, which leverages the ransomware of other groups to scale up, underscores the evolution of ransomware threats and the difficulties in eradicating them.

---

1 https://www.trendmicro.com/en_au/research/23/e/investigating-blacksuit-ransomwares-similarities-to-royal.html

2 Ibid

3 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

4 https://www.reuters.com/technology/cybersecurity/blacksuit-hacker-behind-cdk-global-attack-hitting-us-car-dealers-2024-06-27/

5 https://edition.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html

6 https://english.kyodonews.net/news/2024/12/fffebe5585f1-japanese-publisher-paid-3-million-to-hacker-group-after-cyberattack.html

HOW DO WE TACKLE THE RANSOMWARE PROBLEM?

The answer might just be "us"

Authors: Melissa Tan, Rebekah Maxton and Jeffrey Chung

From "humble" beginnings, ransomware has evolved rapidly in tactics, scale and organisational structure. It is now a billion-dollar enterprise and predicted to cost US$265 billion annually by 2031.[1]

But how did ransomware evolve to the sophisticated system we see today? And more importantly, how can we fundamentally address the ransomware problem so that disrupting ransomware groups has a lasting impact?

The answer might just lie in our own ability to safeguard our networks by preventing initial access by threat actors.

How did we get here?

1989

The first documented case of ransomware,[2] dubbed the "AIDS Trojan Incident". The "hacker" mailed floppy disks to attendees of the World Health Organization's international AIDS conference in Stockholm, claiming to contain software that could help determine whether someone was at risk of developing AIDS. The floppy disks were infected with a virus which, once loaded onto a computer, hid file directories, locked file names, and informed victims they could only restore access to their files by sending money (via cashier's check) to a P.O. Box.

2007

Emergence of the first locker ransomware variants. These versions "locked" machines and prevented users from using basic functions like the keyboard and mouse, then displayed unsolicited images on infected computers. A ransom demand would then follow.

2010

As cryptocurrency gained popularity, cyber criminals found a new way to collect untraceable digital payments. Transactions were difficult to track and enabled cyber criminals to evade law enforcement. This was also the start of ransomware becoming more mainstream.

2012

The first instance of Ransomware-as-a-Service (**RaaS**) occurred with Reventon ransomware, which impersonated local law enforcement and threatened victims with arrest or criminal charges if they did not pay a ransom. These cyber criminals sold their malware to third parties as a service, contributing to the widespread nature of ransomware as we know it today.

2013

Emergence of the CryptoLocker ransomware variant, which employed phishing emails containing malicious attachments to restrict access to infected computers. Cyber criminals then demanded payment to decrypt and recover victims' files. The FBI estimated that victims had paid approximately US$27 million to CryptoLocker's operators by the end of 2015.[3]

2018

Cybercriminals adopt a more targeted and sophisticated approach to ransomware attacks, mainly targeting the government, healthcare, industrial and transportation sectors.

2019

Emergence of "double extortion" techniques. As well as encrypting files, cyber criminals began sending samples of files or "proof of life" from organisations to substantiate their claims of having stolen data. In this way, cyber criminals gained additional leverage over organisations with a data backup strategy; even if the organisations could restore their systems from a previous backup, they would not be able to reverse the data exfiltration. LockBit emerges in the same year, initially known as "ABCD" ransomware due to its ".acbd" file extension).

2020

The ABCD ransomware group begins using the name "LockBit" in cyber crime forums and attacks the education, finance, healthcare, internet software and professional service sectors. LockBit becomes one of the most well-known "ransomware groups", with other cyber criminals using LockBit ransomware to conduct their own cyber attacks.[4] Cyber criminals also increasingly adopt "triple extortion" techniques, which involve stealing data, encrypting systems and then threatening additional exploitation.

2021

Global organisations become targets of complex ransomware operation (also known as RansomOps) attacks targeting high-value organisations or those providing critical services.[5] The thinking behind this is the bigger or more severe the disruption, the more likely that the ransom will be paid.

2022

Ransomware groups continue to adopt new tactics. Initial access brokers play a greater role in ransomware attacks, gaining access to networks and then selling that access to other cyber criminals. The Scattered Spider group emerges, relying on techniques like push bombing to bypass multi-factor authentication (**MFA**) and gain initial access. This technique involves a cyber criminal sending endless MFA push requests to the account owner's device,

1 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

2 https://www.cybereason.com/blog/a-brief-history-of-ransomware-evolution

3 https://www.justice.gov/archives/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-georgetown-cybersecurity

4 https://flashpoint.io/blog/LockBit/

5 https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a

with the goal of having the user accept the prompt.[6] The Play ransomware group also emerges this year (named after the .play file extension it uses to encrypt data), launching more than 300 attacks worldwide since its inception.[7] Play malware is particularly dangerous as it makes detecting and preventing malware more difficult.

2023

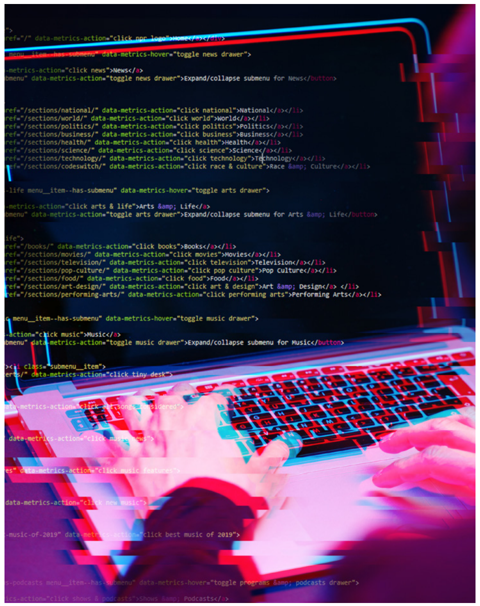
Ransomware groups such as CLOP begin shifting their techniques to increasingly target zero-day vulnerabilities, which reportedly leads to a 143% increase in victims from Q1 2022 to Q1 2023.[8] This technique involves abusing security vulnerabilities before a vendor is notified about it or before the vulnerability is publicly known. Because these vulnerabilities are difficult to identify, they are highly sought after and sold on the black market at high costs.

2024

Malware-as-a-Service (**MaaS**) becomes an integral part of the ransomware ecosystem, with cyber criminals using infostealer malware to steal user credentials and system information for further exploitation, primarily for financial gain. For instance, mobile malware such as GoldPickaxe is an infostealer malware that is capable of stealing facial recognition data to create deepfake videos in order to authenticate fraudulent financial transactions. This type of malware is typically offered on cyber criminal marketplaces on a MaaS basis where the malware developers will sell a subscription to the software. This is appealing for entry-level cyber criminals without extensive technical skills.

2025

New ransomware techniques continue to emerge, with an apparent focus on remote access and increasing efficiency. Cyber criminals employ mailbombing to send large amounts of emails (either through an automated program or by subscribing the target inbox to various sources) to spam a target inbox to conceal legitimate warnings about things like password changes, or as a social engineering tactic to make the user more vulnerable to fake IT calls to allow the cyber criminal to install remote access software to their device to then deliver malware.[9] Cyber criminals also begin to spend less time on a network before stealing data, made possible by remote ransomware techniques where ransomware is deployed from a remote desktop connection that spreads across the network.



Addressing the ransomware problem

In the last few years, two key responses have been implemented globally to address ransomware:

- More offensive measures involving international collaboration; and
- Legislative measures, with countries introducing mandatory ransomware payment reporting obligations and continuing to float the idea of banning ransom payments.

Disruption of ransomware groups

Ransomware groups have always adapted their tactics to respond to law enforcement activity, government regulation and enhanced user awareness.

In the past year, however, we have seen various multinational coordinated operations against cyber criminals, with a particular focus on disrupting and dismantling criminal infrastructures responsible for cyber crimes worldwide. Many of these operations were the first of their kind, including a pivot in focus towards ransomware-as-a-service models, which reflects the trend of ransomware groups relying on affiliates to carry out cyber attacks.

Operation Cronos: disruption of LockBit

The most noteworthy law enforcement actions in the last year involved the disruption of LockBit and ALPHV, which have been behind some of the most harmful ransomware attacks in the past.

LockBit has been described as "the world's most harmful ransomware",[10] operating as a RaaS provider that provides the platform, infrastructure and tools for other threat actors or affiliates to carry out ransomware attacks. According to Zscaler's Ransomware Report, LockBit accounted for 22.1% of ransomware attacks in 2023 to 2024.

In 2024, LockBit was the subject of an international investigation led by Europol, Operation Cronos, involving law enforcement agencies from 10 countries.

Despite this, LockBit has proven more defiant and resilient. Within days, LockBit was attempting to make a comeback by restoring its servers with new domains – highlighting the difficulty of permanently ending ransomware infrastructure and operation.

However, this does not mean that the takedown was ineffective. Operation Cronos provided the National Crime Agency (**NCA**) and the FBI with valuable insight into LockBit's network and affiliates, revealing that 194 affiliates had used LockBit's services until February 2024.[11] Such intelligence is critical in the continued fight against ransomware operators. Nevertheless, these measures are unlikely to permanently stem the growth of ransomware.

6 https://abnormalsecurity.com/glossary/mfa-fatigue-attacks

7 https://www.forbes.com/sites/daveywinder/2025/01/11/ongoing-play-ransomware-attack-what-you-need-to-know/

8 https://www.akamai.com/blog/security-research/ransomware-on-the-move-evolving-exploitation-techniques

9 https://thehackernews.com/2024/12/black-basta-ransomware-evolves-with.html

10 https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

11 https://www.nationalcrimeagency.gov.uk/news/LockBit-leader-unmasked-and-sanctioned

Filling the void: the rise of other ransomware groups

While Operation Cronos sent a clear message to the cyber criminals that even the biggest cyber crime perpetrators can be unmasked and dismantled, the gap left by LockBit (being only one of a number of ransomware groups) has already been filled by other players. Ransomware groups such as RansomHub, Play, and Cl0p have all noticeably incorporated elements of LockBit's playbook into their own, including a widely observed decrease in dwell times.[12]

Notably, RansomHub (operating as a RaaS) was first observed following the FBI's takedown of ALPHV/BlackCat in December 2023, and capitalised on the disruption to LockBit's activities in February 2024. By the third quarter of 2024, RansomHub had become one of the most prominent ransomware groups, which can be attributed to its aggressive recruitment on underground forums, which led to its absorption of ex-ALPHV and ex-LockBit affiliates.

This shift of power from ransomware operators to affiliates demonstrates how these ransomware groups can pivot and rebound despite significant pressure from law enforcement and major disruptions to their operations. According to Zscaler's 2024 Ransomware Report, ransomware attacks unsurprisingly remain a persistent threat. Australia experienced a 5.8% increase in ransomware attacks from 2023 to 2024, and currently ranks seventh among the nations targeted by ransomware, which accounts for approximately 2% of global attacks.[13]

This begs the question of whether dissolution of ransomware groups is an effective enforcement method and whether a different approach should be considered.

Operation Endgame

On 30 May 2024 the FBI announced Operation Endgame, "a multinational coordinated cyber operation by the United States, Denmark, France, Germany, the Netherlands, and the United Kingdom, with assistance from Europol and Eurojust, to dismantle criminal infrastructure responsible for hundreds of millions of dollars in damages worldwide".[14] This operation focuses on disrupting "dropper" criminal services by arresting high-value targets, taking down infrastructure and freezing illegal proceeds, resulting in the takedown of dropper malware infrastructure that facilitated attacks with ransomware and other malicious software, including IcedID, SystemBC, Pikabot, Smokeloader and Bumblebee.

As ransomware remains an ongoing threat, collaboration between international law enforcement agencies will continue, with agencies building on their learnings from previous efforts to continue disrupting and taking down ransomware groups. From observing Operation Endgame, it appears law enforcement is also targeting malware-as-a-service models. The long-term effectiveness of these enforcement methods, however, remain to be seen.

Legislative measures: mandatory ransomware payment reporting and banning ransom payments

Whilst Australia is yet to ban ransomware payments, this has been considered by the Australian Government and a number of other countries.

Australia's Cyber Security Legislative Package 2024 introduced and passed into law a mandatory reporting obligation requiring entities that meet a specified threshold (annual turnover over AU$3 million, and most responsible entities of critical infrastructure, but excluding State and Commonwealth government entities) to report to the Department of Home Affairs if they make a ransomware or cyber extortion payment of money, or an in-kind benefit, in connection with a cyber security incident. The reporting requirement extends only to instances where the ransomware payment is made (not including instances where only a demand is made and no payment is made), and was introduced specifically to enhance the Australian Government's understanding of ransomware threat and how much is being extorted from Australian businesses through ransomware attacks, so as to enhance law enforcement measures. A failure to comply with this reporting obligation, however, can result in penalties being imposed on the ransomware victim entity.

The UK Government also recently held a public consultation process (from 14 January to 8 April 2025) on three proposals in relation to ransomware:[15]

- **Proposal 1:** Targeted ban on ransomware payments for all public sector bodies, including local government, and for owners and operators of Critical National Infrastructure, that are regulated, or that have competent authorities.
- **Proposal 2:** Ransomware payment prevention regime which would require any victim of ransomware (organisations and/ or individuals not covered by the proposed ban set out in Proposal 1), to engage with authorities and report their intention to make a ransomware payment before paying any money to the criminals responsible.
- **Proposal 3:** Ransomware incident reporting regime that could include a threshold-based mandatory reporting requirement for suspected victims of ransomware.

The UK Government is considering a targeted ban on ransomware payments for the public sector and critical infrastructure owners and operators only, which may not apply to individuals and some in the private sector (non-critical infrastructure). It has said: *"We* [the UK Government] *believe that one of the most effective ways of preventing ransomware attacks is to ensure that the criminal gangs looking to target our essential agencies and infrastructure know they will make no money from doing so."*

We have previously written on the issue of criminalising cyber extortion payments and remain of the view that a decision to criminalise or ban the payment of ransoms should not be taken lightly. The current assumption that banning ransom payments will disincentivise cyber crime, striking at the heart of the criminal enterprises, severely undermines the resilience and innovation of cyber criminals. Time and again, when a victim doesn't pay, cyber criminals simply move on to the next big or easy target – proceeding from victim to victim until a payment is procured, while evolving their tactics to be more sophisticated and the disruption more devastating, thereby increasing the pressure for payment.

12 https://www.computerweekly.com/news/366619310/A-landscape-forever-altered-The-LockBit-takedown-one-year-on

13 https://www.zscaler.com/resources/industry-reports/threatlabz-ransomware-report.pdf

14 https://www.fbi.gov/news/press-releases/operation-endgame-coordinated-worldwide-law-enforcement-action-against-network-of-cybercriminals

15 https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible

The public sector and critical infrastructure owners and operators manage the essential services of a country. Of all sectors, we anticipate that these would require the option of making a ransom or cyber extortion payment in the unfortunate event that a cyber attack gives rise to devastating consequences that justify payment, such as physical injury or loss, or even death.

For this reason, legislative measures may unintentionally punish victims of ransomware and cyber extortion.

What is the fundamental solution to the ransomware problem?

The principal way to fundamentally tackle the ransomware problem and ensure lasting disruption to ransomware groups is to address the enablers of initial access – us.

We cannot prevent ransomware attacks. There will always be opportunistic cyber criminals developing malware and employing it for their financial gain. But the ransomware requires initial access to cause damage, which is often the result of human error or human failure to fix technical vulnerabilities. By blocking initial access through multiple layers – locking the door and keeping it sealed across several layers, with effective tools such that even if one layer is breached the other layers remain in place to prevent initial access – we can keep the malware out of our systems and prevent it from gaining a foothold to enable cyber extortion.

Fortunately, this is within our control with the help of the following measures:

1. **Education, training, and more training.** Social engineering and phishing attacks are a common method by which ransomware groups gain entry to our systems and networks. Ransomware attacks will continue to evolve and increasingly employ generative AI to exploit human error, for example through voice-based phishing using AI voice cloning. Enhancing education and training to minimise or eliminate human error and prevent initial access will therefore be key. This means addressing the psychological element of these attacks – for example, teaching users to be wary of unfamiliar emails; encouraging users to check that emails are legitimate, and if unsure, reporting them to IT to be scanned for malicious software; not saving passwords on a web browser; and not using a personal computer for work purposes. Exercising caution with the electronic communication we receive may create delays due to the extra checks and verifications required, but if these measures can reduce, minimise or eliminate initial access for malware to be executed, it will be well worth the effort.
2. **Uplifting cyber resilience by investing in the right tools**: As well as addressing the human factor, preventing initial access will require investing in the right technology tools. Organisations will need to strengthen vendor risk management, continuously update and patch firmware, enforce endpoint detection and response, enforce MFA effectively at all entry points, and continuously monitor their systems to safeguard interconnected networks and ensure operational resilience. They will also need to monitor the threat landscape and be aware of new ransomware groups and their known tactics, which will require investment in cyber threat intelligence and threat hunting. It's not a set and forget; it's a set and continue to learn and upgrade. Of course, not every organisation is able to afford these measures, particularly small businesses – which is where the role of government will be integral. If governments are serious about taking action against ransomware, more cyber legislation is not necessarily going to resolve the issue; rather, investing in helping every organisation, particularly the more vulnerable or small businesses, to uplift their cyber resilience and prevent initial access by threat actors will be far more effective. Investment might come in the form of grants, or technical assistance to organisations at a discounted rate. Incentivising small businesses to invest in cyber security measures by providing tax relief or tax incentives is another solution worth exploring.

By closing off initial access to our networks at the point of entry by cyber threat actors, we have the potential to shift the balance of power away from ransomware gangs – thereby eliminating the question of whether a cyber ransom can or should be paid.

CYBER RISK AND AI

The good, the bad and the ugly

Author: Melissa Tan

Artificial intelligence (**AI**) dominated global headlines in 2024 as generative AI capabilities continued to grow at a rapid pace. Adoption of the technology will no doubt increase in 2025 and beyond as it continues to evolve and advance, with Agentic AI[1] emerging as a highly adaptable, autonomous agent that will open up new possibilities to automation and tap into unchartered territories of personalisation.

At the global level, the AI arms race is already heating up between the United States and China as both countries invest heavily to build advanced AI infrastructure, cultivate AI talent and compete to make the next breakthrough. At the local level, we are seeing businesses increasingly adopt and incorporate AI technology within their system architecture and work processes, to improve efficiency and productivity. Even lawyers, who are traditionally slow at adopting new technology, have started to incorporate generative AI in their work, which recently prompted the Supreme Court of New South Wales to issue Practice Note SC GEN 23 to provide direction on where the use of generative AI is acceptable.

In both its current and future form(s), AI certainly has a huge role to play within the cyber security context as well. However, as with every new technology, the good often brings with it the bad, with malicious actors leveraging the same technology to perpetrate crime and widespread disruption.

Focusing our lens on AI within the cyber security context – how can it be used, what challenges does it bring, and why is robust regulation key for the safe development and use of AI?

Malicious use of AI

AI has opened up a number of opportunities for bad actors to lodge cyber attacks using novel methods that are becoming harder to detect. Threat actors have used AI to varying degrees, regardless of the amount of resources available to them and their level of sophistication. This is the result of the increasing democratisation of cyber attacks through “franchise models” that provide even amateur bad actors, who have limited resources or experience, with the malicious tools they need to lodge their own cyber attacks, including generative AI tools that can be purchased on the dark web.[2]

Threat actors have maliciously utilised AI to perpetrate cyber crime by:

1. leveraging AI to enhance the scale and effectiveness of cyber attacks; and
2. attacking the AI technology itself, for example through data poisoning, whereby the training data is corrupted or compromised, which leads to biased, inaccurate or malicious outputs.

Bad actors have particularly leveraged AI by:

- using natural language processing to create convincing phishing emails and enabling social engineering attacks to be done at scale. AI provides the tools to automate cyber attacks, scan attack surfaces, and even to tailor phishing emails to a particular culture or context to make them more convincing. Traditionally, spelling and grammatical errors have been prominent red flags in potential phishing emails. However, the use of generative AI in phishing attacks eliminates such signs and makes detection even harder. In a recent example, when security researchers tested WormGPT to design a phishing email, WormGPT demonstrated it was capable of creating a phishing email with correct spelling and grammar.[3]

- using AI-generated synthetic media to create fake images, video or audio recordings to impersonate a legitimate person and thereby convince victims to either transfer money or volunteer sensitive information (i.e. deepfake attacks).
- automating code generation, which enables rapid creation of new malware variants.
- analysing exfiltrated data more quickly and in a more targeted fashion, in order to undertake triple extortion or perpetrate further attacks with the information found.

While the advanced use of AI by bad actors is likely to be limited to those with access to significant resources, quality training data and significant expertise both in AI and cyber, the cyber criminal community can be collegiate, commercial and innovative. With a subscription model no different to the Ransomware-as-a-Service model, the more sophisticated bad actors with resources and capability to invest in AI technology can lower barriers to entry by offering subscriptions to amateurs to utilise their AI tools or products to launch AI-powered attacks. For example, it was reported that a bad actor was offering to sell WormGPT with a subscription model ranging from approximately US$112 to US$5,621. [4]

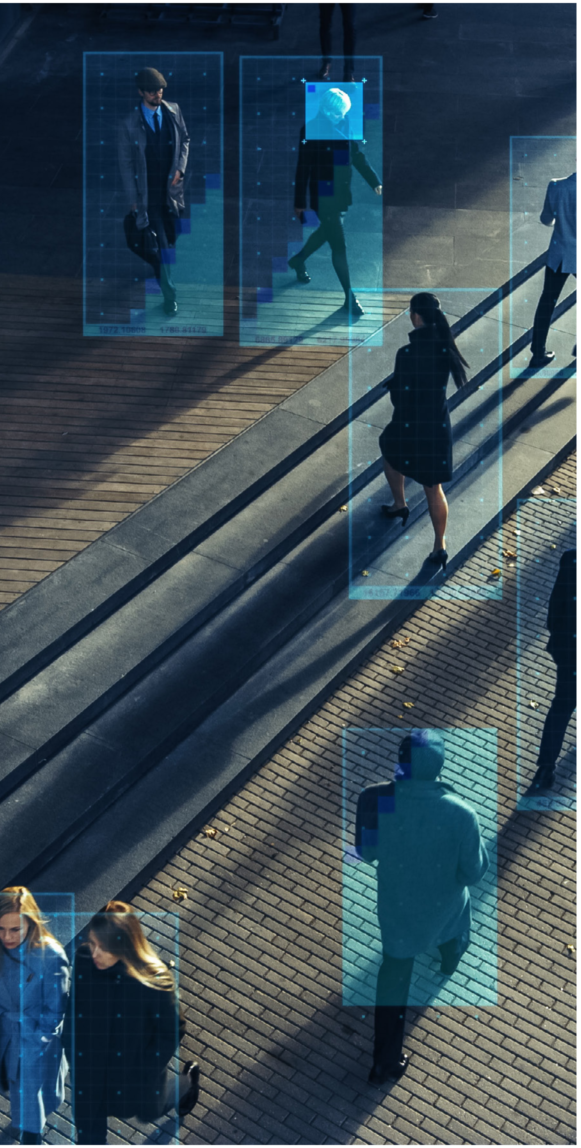
As AI continues to evolve and become more powerful, so will its malicious application. This is unlikely to be prevented even with strict regulation, particularly as it becomes easier for bad actors to gain access to a number of malicious resources on the dark web. However, AI-powered cyber defence systems can play an important role in levelling the playing field.

1 https://www.wired.com/sponsored/story/the-rise-of-agentic-ai-the-next-evolution-of-personalization/

2 https://thehackernews.com/expert-insights/2024/06/the-democratization-of-cyberattacks-how.html

3 https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-design-ai-threat-report-v2.pdf

4 https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-design-ai-threat-report-v2.pdf



AI-powered cyber defence: uplifting cyber resilience

While bad actors are able to leverage AI for malicious purposes, cyber security defenders can also utilise AI-driven cyber security tools to improve threat detection and identify new attack vectors.

There are a number of use cases where AI can play an integral part in a defensive strategy against cyber attacks:

- One of the top advantages of AI is its ability to quickly sieve through large datasets. AI can enhance threat intelligence by analysing large datasets in real time, further training the AI model and providing predictive insights that enable cyber security defenders to anticipate attacks and be proactive in mitigating them.
- AI can improve incident response times by automating threat detection, containment, analysis and mitigation.
- AI can also help automate the patch management process and enable faster identification of critical vulnerabilities, reducing the time gap between release of a patch and deployment.

There is much potential in integrating AI into cyber security tools and using AI to power cyber defences. Applying Agentic AI allows automated threat detection that autonomously identifies malware, phishing attempts and network intrusions by analysing real-time data and recognising unusual patterns of behaviour. Critically, Agentic AI can engage in predictive analysis by identifying trends and vulnerabilities that can be exploited in future attacks.[5] This proactive approach will be key in ensuring that security teams implement countermeasures ahead of any potential cyber attack.

That said, it is likely that in the near future, only state actors and large tech AI organisations will have the ability to further develop and harness the full potential of AI in advancing AI-powered cyber defences. This is because advancing AI-powered cyber defences requires significant resources, infrastructure, expertise and time.

Governments may need to consider how the benefits of advancements in the development of AI-powered cyber defences can be shared and distributed as a public good, particularly with small businesses who cannot afford large budgets for cyber uplift and sophisticated cyber security tools.

A strong commitment to harnessing and developing AI-powered cyber defences would go a long way in tipping the balance against mounting cyber threats.

Ethical, legal and regulatory challenges: robust regulation needed

Despite its many benefits, the use of AI in cyber security also presents ethical, legal and regulatory challenges. As is the case with any form of innovation, measures must be put in place to ensure there are appropriate checks and balances governing the development and use of AI.

If only state actors and large tech AI organisations have the ability to advance AI-powered cyber defences in the short to medium term, having concentration of power over a significant piece of technology in the hands of a few raises ethical concerns over potential misuse by authorities or large tech AI companies.

We have already seen OpenAI request that the Trump Administration helps to shield AI companies from a growing number of proposed state regulations if they voluntarily share their models with the federal government.[6] The premise for this is that the hundreds of AI-related bills currently proposed across the US risk impeding the US's technological progress at a time when competition from China has renewed, particularly following recent news surrounding the DeepSeek platform. This request was in the context of the administration calling for public input in drafting a new policy to ensure US dominance in AI.

The Trump Administration has generally indicated that it will take a deregulation approach to AI technology, and to date, there has been no federal legislation governing the AI sector.

Privacy and intellectual property concerns have always been raised in relation to AI technology and the use of training data, but OpenAI has called for:

- the US government to take steps to support AI infrastructure investments and requested copyright reform, arguing that America's fair use doctrine is critical to maintaining AI leadership;[7] and
- AI companies to get access to government-held data, which could include health-care information, on the basis that such information would help "boost AI development".

If the US government agrees and accepts OpenAI's submissions, this will largely leave the US government and US-based AI companies above the law, with no checks and balances in place and little protection for the data sets they want access to for data training to develop their AI projects.

5 https://www.cybersecuritytribe.com/articles/an-introduction-agentic-ai-in-cybersecurity

6 https://www.insurancejournal.com/news/national/2025/03/13/815448.htm

7 https://www.insurancejournal.com/news/national/2025/03/13/815448.htm

However, fundamental guiding standards and regulations are critical to innovation and the development and use of AI. They enable AI developers to build with confidence, and provide the public with trust in the security of the technology, particularly as emerging forms of independent, autonomous AI (which require minimal human supervision) increasingly raise questions about reliability, accountability and data security.

In Australia, we currently have the first iteration of the Voluntary AI Safety Standard which consists of 10 voluntary AI guardrails and seeks to support and promote best-practice governance to help more businesses adopt AI in a safe and responsible way. As the name suggests, it is "voluntary", although it was proposed in September 2024 that mandatory guardrails be introduced, which largely mirror the voluntary standards. One of the guardrails requires that AI developers have appropriate data governance, privacy and cyber security measures in place to appropriately protect AI systems.

While these standards and guardrails are a start, they represent the minimum requirement to regulate the development and use of a powerful technology with significant potential. Clarity on AI-related risks, the legal boundaries of AI liability, and legal consequences for any potential misuse of AI technology is needed now, before more advanced forms of AI develop. Regulators must develop clear and comprehensive guidelines that define AI-related risks and standardise practices across the industry. This includes setting benchmarks for AI system performance, transparency, and accountability, to ensure AI technologies are deployed responsibly and ethically. Otherwise, we risk descending into a lawless sphere, with the unfettered development and use of AI benefiting and playing into the agendas of bad actors.

Summary of amendments to Cyber Security Legislative Package when passed

Bill	Amendment made by Government	PJCIS Recommendation
Cyber Security Bill	Amend existing provisions to ensure broader categories of information that are obtained under the Act are subject to existing admissibility protections relating to criminal or civil proceedings in: a. Section 32 (information in ransomware payment report); b. Section 42 (information voluntarily given by impacted entity in relation to significant cyber security incidents); and c. Section 58 (information given by an entity as requested or required by Cyber Incident Review Board).	**Recommendation 7** 6.48 The Committee recommends the protections conferred by the 'limited use' provisions be more clearly expressed in the Cyber Security Bill 2024 and the Intelligence Services and Other Legislation Amendments (Cyber Security) Bill 2024 and associated explanatory memoranda, and that the Department of Home Affairs develop guidance to ensure they are well understood by industry.
	Adding a new provision (section 88) to allow the PJCIS to: a. commence a review of the operation, effectiveness and implications of the Act and b. report the PJCIS's comments and recommendations to each House of Parliament as long as the PJCIS begins the review as soon as practicable after 1 December 2027.	**Recommendation 10** 6.60 The Committee recommends that the Cyber Security Bill 2024 be amended to provide that the Comittee may (if it resolves to do so), commence a review of the operation, effectiveness and implications of the Cyber Security Act 2024 as soon as practicable after 1 December 2027.
Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024	Clarifications on the information obtained under the Act that are subject to existing admissibility protections.	**Recommendation 7** 6.48 The Committee recommends the protections conferred by the 'limited use' provisions be more clearly expressed in the Cyber Security Bill 2024 and the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024 and associated explanatory memoranda, and that the Department of Home Affairs develop guidance to ensure they are well understood by industry.
Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024	A new Schedule 7 — Notification of certain critical infrastructure or telecommunications security assessments inserted. Confirmation of application of section 38 of the *Australian Security Intelligence Organisation Act 1979* in relation to an adverse or qualified security assessment (a relevant assessment) to (**notification of security assessments**) certain critical infrastructure or telecommunications assessments.	N/A. In addition to the response to the PJCIS's advisory report, the Government amendments to this bill include a technical amendment to the *Australian Security Intelligence Organisation Act 1979* to clarify provisions relating to the ministerial responsibility for protecting ASIO information and giving notice of an adverse or qualified security assessment in respect of an assessed person in connection with certain provisions of the Telecommunications Act 1997 and the SOCI Act.

Bill	Amendment made by Government	PJCIS Recommendation
Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 *(continued)*	Section 60AAA (the requirement for regular reports about consultation) repealed.	**Recommendation 13** 6.73 The Committee recommends that the Security of Critical Infrastructure Act 2018 be amended to repeal the requirement in section 60AAA for the Department of Home Affairs to provide six-monthly consultation reports to the Committee.
	The PJCIS is able to review the SOCI Act and report on its comments and recommendations to each House of Parliament as long as the review is begun before 2 December 2026 (it was previously 2 December 2024 and has been extended out).	**Recommendation 12** 6.70 The Committee recommends that existing section 60B of the Security of Critical Infrastructure Act 2018 (SOCI Act) be amended to provide that the Parlimentary Joint Committee on Intelligence and Security may (if it resolves to do so) review the operation, effectiveness and implications of the SOCI Act, so long as the Committee begins its review by no later than 2 December 2026.

KEY CONTACTS

Insurance Law & Litigation

Melissa Tan
Partner and Head of Cyber Insurance
Insurance Law & Litigation

D +61 2 8020 7889
M +61 438 742 770
E mtan@landers.com.au

Jack Boydell
Lawyer
Insurance Law & Litigation

D +61 2 8020 7724
M +61 439 499 417
E jboydell@landers.com.au

Jeffrey Chung
Lawyer
Insurance Law & Litigation

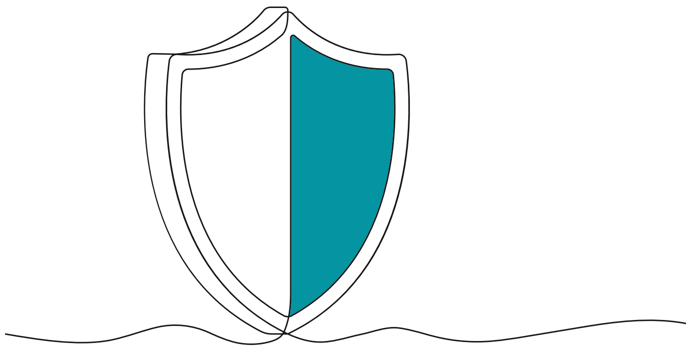
D +61 2 8020 7763
M +61 460 423 748
E jchung@landers.com.au

Rebekah Maxton
Lawyer
Insurance Law & Litigation

D +61 2 8020 7929
E rmaxton@landers.com.au

Annie Weng
Lawyer
Insurance Law & Litigation

D +61 2 8020 7665
E aweng@landers.com.au



ABOUT US

Lander & Rogers is a leading independent Australian law firm, comprising over 650 people including 100 partners.

We have grown organically, resulting in a highly cohesive firm sharing a strong work and client service ethic, as well as high staff and partner retention rates. We believe that legal services involve more than just the law – practical, commercial advice and exceptional client experience are equally important to our clients and to us.

Our firm is global in its approach, but we remain fiercely independent and truly Australian. We work closely with international firms that do not have an Australian presence, and we are the exclusive Australian member of the largest global network of independent law firms, TerraLex.

Consistent with our values and culture, we are strongly committed to pro bono & community work and supporting our environment. We also established Australia's first LawTech Hubs in Melbourne and Sydney. Our key sectors are Government, Insurance & Financial Services, Real Estate, Retail & Supply Chain and Technology.

Brisbane

Level 11 Waterfront Place
1 Eagle Street
Brisbane QLD 4000

T +61 7 3456 5000
F +61 7 3456 5001

Melbourne

Level 15 Olderfleet
477 Collins Street
Melbourne VIC 3000

T +61 3 9269 9000
F +61 3 9269 9001

Sydney

Level 19 Angel Place
123 Pitt Street
Sydney NSW 2000

T +61 2 8020 7700
F +61 2 8020 7701

landers.com.au