CYBERSIGHT 360

A legal perspective on cyber security and cyber insurance

2022/23

LANDER
& ROGERS

FOREWORD

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

Ever-evolving cyber security threats continue to escalate in both volume and severity of attacks.

A review of 2022

In 2022, the world saw new attack methods emerge and artificial intelligence (AI) pose an increasingly real threat as cyber criminals became more targeted and sophisticated in their methods.

Among the worst affected, Australia was subject to more cyber attacks in the final quarter of 2022 than any other nation, giving governments cause to reflect and act. One proposed action was to make it illegal for companies to pay ransoms to cyber criminals while simultaneously increasing penalties for data breaches – a move that critics argue will punish victims of the crime, rather than the perpetrators.

Australia is not alone, with countries around the globe racing to address the rapidly evolving situation amid geopolitical tensions including the Russia-Ukraine war and new cyber warfare threats targeting governmental departments and critical infrastructure.

Globally, the heightened threat environment has increased the risk of large losses and increased demand for cyber insurance, resulting in higher premiums and growing concerns about the sustainability of this type of insurance product. In response, insurers have and are expected to continue to tighten policy language and underwriting standards, which includes the implementation of more stringent limits or sub-limits, higher deductibles and bespoke exclusion endorsements.

Looking ahead

The use of AI in cyber attacks is predicted to increase in 2023 and beyond, representing a new age of cyber warfare. Amid the new threat, the development of AI governance frameworks needs to be a priority for lawmakers, and businesses are also urged to enhance cloud security as part of risk mitigation.

As regulators, investors and customers increasingly demand transparency and reporting from companies in relation to ESG, high-profile cyber attacks have many arguing the importance of cyber risk management as part of an integrated ESG framework that goes beyond compliance requirements.

This guide explores the trends that dominated the cyber security space in the year 2022, and illuminates the risks to organisations in 2023 and beyond.

We hope you find it both valuable and informative.

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

Contents

DISCLAIMER | This guide cannot be regarded as legal advice. Although all care has been taken in preparing this information, readers must not alter their position or refrain from doing so in reliance on this guide. Where necessary, advice must be sought from competent legal practitioners. The author does not accept or undertake any duty of care relating to any part of this guide.

TIMELINE OF CYBER INCIDENTS

If 2021 was a big year for cyber incidents – with the exploitation of zero-day vulnerabilities leading to significant ransomware attacks affecting critical infrastructure and supply chains – cyber threats to businesses and organisations intensified in 2022, particularly in Australia.

Australia was affected by two high-profile data breaches – the largest the country has ever seen, earning it the unenviable title of the most hacked nation in the final quarter of 2022. During this period Australia had the highest data breach density in the world, with 7,387 user accounts per 100,000 being hacked, data breaches surging by 1,550% between October and November 2022, and an average of 22 Australian accounts being breached every minute, which was a 1,000% increase from the previous quarter.[1]

The key cyber incidents of 2022 reflected the extent of the impact of the Russia-Ukraine war on the cyber world, with ransomware and data breaches continuing to dominate and target governmental departments and critical infrastructure. 2022 also saw an increase in the use of application programming interfaces (APIs) as a primary attack vector.[2]

Authors: Melissa Tan and Louisa Henderson

Select a month

January
February
March
April
May
June
July
August
September
October
November
December

JANUARY

14 January 2022

Victim
Government of Ukraine

Country
Ukraine

Threat actor
Russia (suspected)

What happened?

Amid significant tensions between Russia and Ukraine, various Ukrainian government agencies were hacked and their websites compromised, displaying the message: "Ukrainians! ... All information about you has become public. Be afraid and expect worse. It's your past, present and future." The attack caused more than a dozen government websites to be shut down.

20 January 2022

Victim
International Committee of the Red Cross (ICRC)

Country
Switzerland

Type of attack
Data breach - TTPs unknown

Threat actor
Unknown

What happened?

On 20 January 2022, the ICRC made an appeal to hackers who stole the private data of more than 510,000 vulnerable people from at least 60 Red Cross and Red Crescent societies.

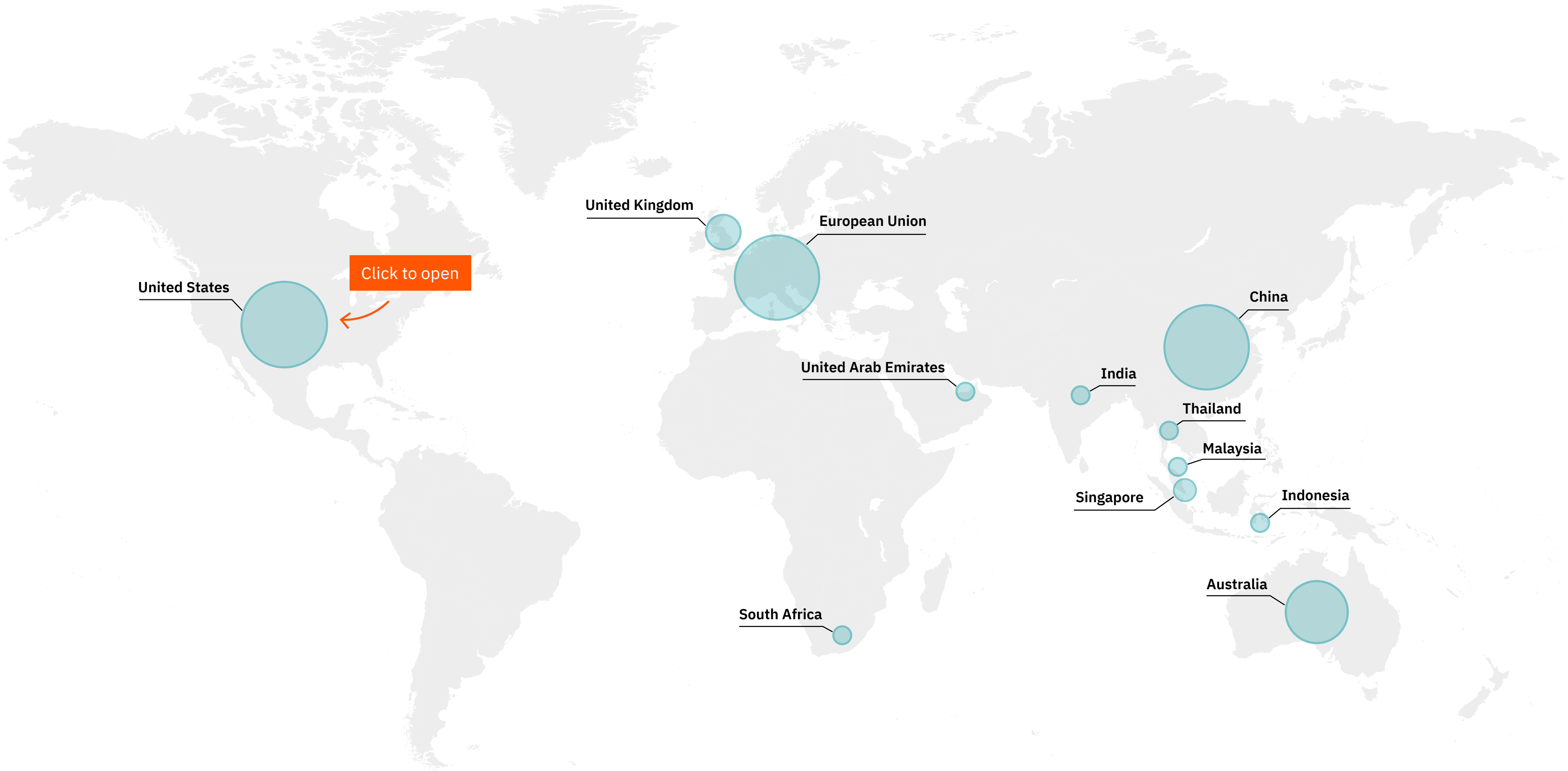
The ICRC noted the information included records of people separated from their families due to conflict, migration and disaster, missing persons and their families, and people in detention.

There was no evidence the data was leaked, and the perpetrators were never identified.

[1] Source: Figures published by Surfshark VPN.
[2] *Info Security Magazine*. 28 October 2022.

GLOBAL VIEW OF THE CYBER LANDSCAPE

As cyber and ransomware attacks continued to escalate in 2022, countries around the world continued to focus on cyber security as a national priority and ramped up efforts enacting or proposing regulations to strengthen their defences against threat actors. Select a country below to view the major initiatives implemented or proposed in 2022 to manage cyber risk.



Authors: Melissa Tan and Louisa Henderson

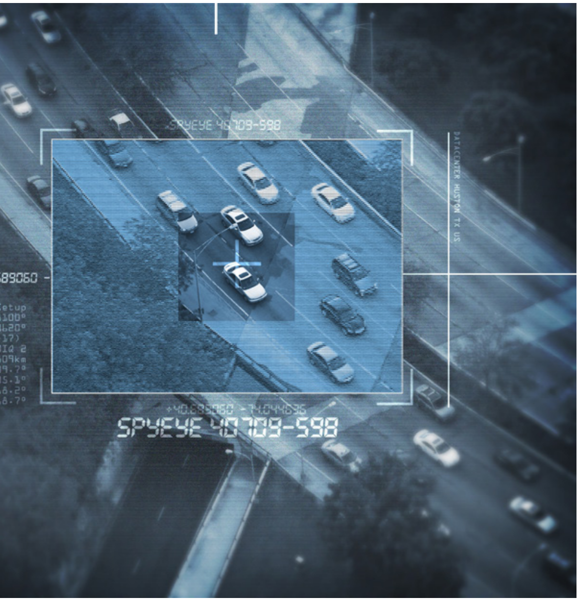
TRENDS

THE CYBER TRENDS THAT SHAPED 2022

Authors: Melissa Tan and Louisa Henderson

The cyber threat landscape is constantly evolving as threat actors and cyber security providers try to outsmart each other. In 2022, well-known attack methods remained popular and new techniques grew in frequency as perpetrators responded to developing defence mechanisms.

There were also a number of motivational factors influencing cyber attacks globally in 2022. For example, multiple high-profile incidents highlighted the value of data, whilst other high-impact attacks demonstrated the role cyber can play in political conflict.



Supply chain attacks

Much of the legislative reform implemented in 2022 aimed to address the risks posed by an organisation's supply chain. This was likely in response to an increase in supply chain attacks in 2021, and a growing body of research revealing a lack of preparedness amongst organisations. A report by software platform Anchore indicated that in 2022, attacks originating from the supply chain increased by 62%.[1]

The way in which businesses operate today makes it extremely difficult, if not impossible, to avoid interacting with and relying on other companies, facilities and services. Whilst software providers are an obvious example, the link does not have to be technological. An integral part of a manufacturer's supply chain could be the third-party company it engages to deliver its products to retailers. Each third-party provider has its own third-party providers, creating a vast interaction of interlinking supply chains.

In engaging third-party providers that are essential to a business, organisations often fail to inquire about the level of cyber maturity of these providers or assume that these providers have cyber security measures in place, which may not be the case. It is likely that a provider will have adequate security measures in place at the highest level, but lack robust systems further down the supply chain. Smaller companies often do not appreciate their links to large organisations several levels removed, or lack the resources to put strong measures in place.

This explains why supply chain attacks are so appealing to threat actors. A threat actor who can successfully infiltrate one weak link in a supply chain has the ability to compromise the entire chain. After all, a chain is only as strong as its weakest link.

Companies of varying sizes were exposed in this manner in 2022. The exploitation of a vulnerability affecting Apache Log4j, an extremely popular open-source logging library in the Java ecosystem, created a large attack surface which the US Cybersecurity and Infrastructure Security Agency labelled an "endemic vulnerability" that will linger for years. In April, an incident on GitHub revealed a supply chain attack in which threat actors stole user authentication tokens issued to third-party integrators and leveraged them to download data from GitHub's customers, raising concerns regarding reliance on external repositories.

Supply chain attacks are also appealing as they are diverse in nature. A threat actor can use various attack methods (such as brute force, malware and vulnerabilities) to attack numerous suppliers (such as hardware, configurations, and open-source code) and achieve various different outcomes (access to personal information, business data, financial information, software and processes).

In 2023 and beyond, supply chain attacks will likely continue to be popular. This is a systemic cyber risk which the insurance industry will continue to grapple with.

Cyber warfare

Geopolitical tensions, particularly the Russian invasion of Ukraine, strongly influenced cyber threats in 2022.

Shortly before the invasion, it is believed that Russian state-sponsored threat actors launched a broad cyber campaign that intended to create disorder and overwhelm Ukrainian defences, targeting government agencies and critical infrastructure. It is also believed that Russia was responsible for a hack on American satellite company Viasat, shortly before Russia physically invaded Ukraine. The effect of the attack was that the Ukrainian military, which relied on Viasat's services for command and control of the country's armed forces, was unable to communicate.

This "hybrid" war strategy seemingly adopted by Russia is one of the first real-world examples of how cyber attacks can be deployed to support physical attacks. It also reiterates one of the major trends from 2021, being the importance of critical infrastructure assets and the potentially fatal consequences an attack on these assets can have on national security.

This increase in cyber warfare also led to a dramatic increase in hacktivism, from newly-formed pro-Ukrainian and pro-Russian cyber legions to well-established groups such as Anonymous. Often using distributed denial of

[1] Anchore 2022 Software Supply Chain Security Report.

service (DDoS) attacks, these groups aimed to cause disruption and use cyber attacks to send politically motivated messages. For example, our **timeline** shows that during the televising of a speech by Vladimir Putin, Anonymous hacked Russian TV channels to air uncensored footage of the war in Ukraine and display a message stating that the country has “blood on [its] hands”.

Similar types of attacks and hybrid strategies were also seen in other conflicts globally, including the Israeli-Palestinian conflict and the China-Taiwan conflict. It is evident that the cyber realm is now a battlefield of its own during times of war, and these tactics will increasingly form an integral part of the defence strategies of certain countries.

Distributed denial-of-service (DDoS) attacks

DDoS attacks are a prime example of the role cyber can play in political conflict. These attacks increased in popularity as a method to cause disruption and send political messages during the Russia-Ukraine conflict. In fact, it is believed that observed DDoS attacks focusing on Russian targets increased by 236% between February and March 2022.[2] Further reports at the end of 2022 recorded that throughout the year, 21.5 million DDoS attacks were aimed at roughly 600 Russian organisations and DDoS attacks accounted for approximately 80% of all cyber attacks on Russian entities that year.

However, it was not just pro-Ukrainian attackers deploying DDoS attacks. Russian-aligned hacktivist group Killnet gained notoriety during the first month of the Russia-Ukraine conflict when it began a widespread campaign of DDoS attacks. Whilst the attacks were described as unsophisticated, their targets included multiple hospitals, government websites and other critical infrastructure assets of NATO countries.

Other geopolitical conflicts also saw DDoS attacks employed to send political messages. For example, a DDoS attack occurred on the Taiwan presidential office’s website and several other government websites in August 2022. It is believed that these attacks coincided with the visit of US House Speaker Nancy Pelosi, following threats from the Chinese government to take action to respond to Ms Pelosi’s trip. Reports also showed some websites and television screens at government facilities defaced with messages criticising Ms Pelosi’s visit in an effort to spread disinformation.

DDoS attacks were frequent in 2022, and not just in cyber warfare. The volume of DDoS attacks targeting financial firms increased 22% year-on-year as of November, with reports that financial services in Europe were most affected, experiencing a 73% increase in attacks.[3] Whilst attacks on financial services can be politically motivated, threat actors also use DDoS as an extortion technique, demanding money in order for the traffic to cease.

In 2022, numerous bank websites and apps experienced significant downtime due to DDoS attacks, creating an extreme amount of disruption and customer dissatisfaction. The ability of threat actors to leverage this for significant ransom payments has seen an increase in a DDoS-for-hire model, where anyone with access to the internet and the dark web can be given access to a botnet to carry out an attack for as little as $10 per hour.[4]

The rise of the DDoS-for-hire industry will be one to watch in 2023.

Large-scale data breaches

Whilst data breaches were prevalent throughout 2022, they experienced a sharp increase in frequency and scale in Q3 2022. According to a report by Surfshark[5], a total of 108.9 million accounts were breached globally in Q3 2022, a 70% increase compared to the previous quarter.

```
        mirror_mod.use_x = False
        mirror_mod.use_y = True
        mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
        mirror_mod.use_x = False
        mirror_mod.use_y = False
        mirror_mod.use_z = True

        #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
        #mirror_ob.select = 0
```

In Australia, Q4 2022 saw major data breaches that targeted some of Australia’s most prominent critical infrastructure organisations, affected millions of Australians and fuelled legislative reform. Although ranked 16th in the world by total data breach count, Australia had the highest “data breach density” globally in Q4 2022, which was 24 times more than the global average. In October and November 2022, an average of 7,387 user counts were leaked per 100,000 Australians.[6]

These attacks shone a spotlight on the sheer value of data available online. As they say, data is the new currency. In many of these large-scale data breaches, threat actors moved away from the encryption of files to a data theft-only approach. Ransomware-as-a-Service gang LockBit, for example, issued guidelines for affiliates including that file encryption was not to be used against certain industries, such as healthcare. Many threat actors are no longer bothering with the technicalities of encryption or using the disruption of services as a bargaining tool. The many ways in which the data itself can provide financial gain is often sufficient.

When a threat actor compromises an organisation’s network and exfiltrates data, they have several options. Firstly, they can demand a ransom from the organisation to prevent the release of the data. This, however, is usually not their main motivator. By exfiltrating personal and sensitive data, the threat actor uses the information of the organisation’s customers and employees to extort each of those individuals. Alternatively, and often in addition to these methods, the threat actor will also sell the data to allow others to use the information for their financial gain, including by extortion, scams, credential theft and identity theft.

Data will continue to be currency, power and opportunity for threat actors.

[2] ASERT Team. DDoS Threat Landscape - Russia. 23 March 2022.

[3] Martin, Andrew. Denial-of-Service Attacks Rise, Raising Concerns for Banks. *Insurance Journal*. 1 February 2023.

[4] Nesbo, Elliot. What is DDoS-for-Hire and Why is it a Problem? *MUO*. 26 November 2021.

[5] Source: Figures published by Surfshark VPN.

[6] Ibid.

Ransomware

A summary of 2022 cyber trends would not be complete without ransomware. The Australian Cyber Security Centre identified that in the 2021-22 financial year, ransomware was the most destructive cyber crime.

As organisations have become more cyber aware, extortion methods have become multifaceted. Ransomware no longer involves simply locking down data and demanding money for its release. Labelled by cyber security company Mandiant as "extortion accelerators", threat actors now engage in a number of practices to more effectively extract payment from victims. Such tactics include:

- exfiltrating and stealing the data
- threatening to publish the data
- publishing parts of the stolen data on name-and-shame websites to prove possession of the data
- carrying out DDoS attacks on the victim's network during ransom negotiations
- disclosing the breach, subsequent details of the incident and any negotiations to media outlets
- amplifying stories of victims in the media to increase public pressure
- notifying business partners and other stakeholders to increase pressure to pay the ransom.

These multifaceted attacks often have the effect of:

- requiring more involvement from various employees, including an organisation's IT department, legal, public relations and management functions
- preventing customers from accessing websites
- preventing employees from accessing software required for day-to-day business operations
- increasing the risk of regulatory fines for data breaches
- creating relationship friction with key stakeholders
- reputational damage and customer loss.

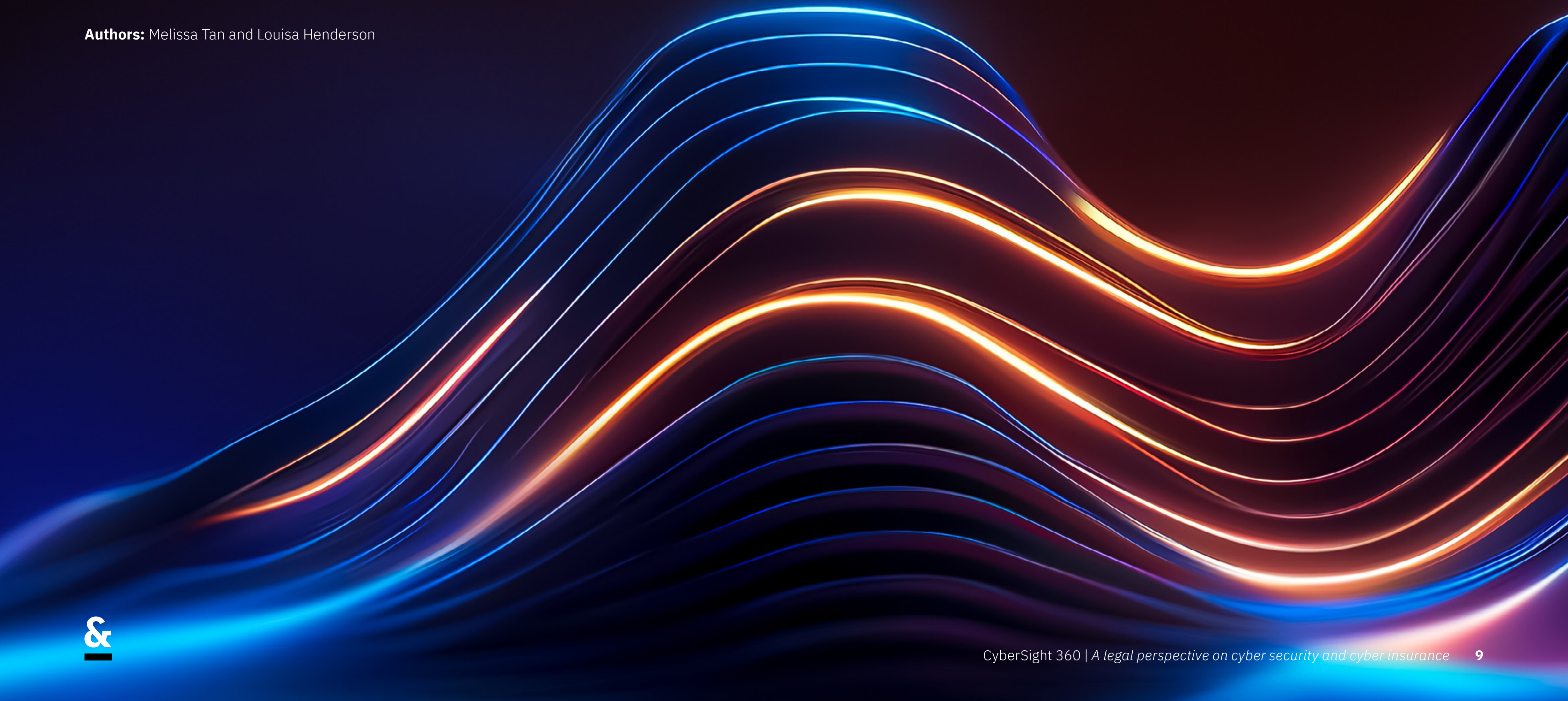
What these effects have in common is that they all cost the business money and pose a risk to its reputation. In a study by GetApp, only 11% of ransomware victims said that the ransom payment itself was the most consequential aspect of the attack. The ongoing reputational damage and financial loss that the threat actors then used to gain leverage to demand higher payouts proved far more impactful.

The changing face of ransomware will be one to watch and prepare for in 2023 and beyond.

TRENDS

CYBER TRENDS THAT WILL DEFINE 2023 AND BEYOND

Authors: Melissa Tan and Louisa Henderson



As threat actors become more sophisticated and leverage new technology to achieve their goals, these are the cyber trends that businesses should be aware of and prepare for in the year ahead.

1. AI-powered cyber attacks

Threat actors will increasingly leverage artificial intelligence (AI) in 2023 and beyond to automate their attacks and launch AI-powered cyber attacks. AI-powered cyber security threats allow threat actors to launch sophisticated attacks that can evade traditional security measures.

Whilst AI can be used in a number of ways, including to avoid detection in a compromised network, we predict that AI will be employed by threat actors to overcome improved cyber awareness among the general public. AI-powered cyber security threats include the following.

Deepfake technology

Deepfake technology uses AI to fabricate synthetic media, such as videos or images, to impersonate a real person and carry out fraud. Historically, deepfake has been most frequently used to spread disinformation, particularly during geopolitical conflicts and political campaigns.

However, deepfake is increasingly being employed to trick users into making unauthorised payments or volunteering sensitive information. For example, an employee may be aware of a requirement from their CEO to provide oral approval before payment can be made for certain large transactions. If confronted with a payment redirection scam conducted through a business email compromise attack, a cyber savvy employee would call the CEO and the CEO would confirm that the payment was never requested – thus thwarting the attack.

But what if the employee called the CEO and the purported "CEO" gave oral approval and directed the payment? Surely it is not possible to impersonate the CEO's voice?

This was in fact possible with AI-based software in 2019, when audio spoofing was used by cyber criminals to impersonate a CEO's voice to trick a UK-based energy firm to transfer USD$243,000 to the threat actor (and purported supplier).[1]

This new spin on impersonation tactics allows attackers to call victims sounding exactly like someone they speak to every day in real time, creating a much more convincing scam. These tactics also bypass the traditionally effective authentication method of oral verification.

Applying machine-learning technology to spoof voices and replicate people's likenesses makes cybercrime easier, and AI technology is only going to evolve and become more sophisticated.

Phishing

Businesses have been grappling with phishing attacks for a number of years. Most recently there has been a dramatic shift from bulk spam emails to targeted phishing campaigns, which use information specific to the recipient to convince them that the communication is legitimate. Whilst phishing attacks continue to be successful, businesses have responded. Education around phishing has increased significantly and there are many resources available on how to spot a fake email.

[1] Stupp, Catherine. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. *The Wall Street Journal*. 30 August 2019.

Common examples include reviewing the malicious link before clicking on it, reviewing the domain name of the sender, and looking out for spelling and grammatical errors.

Always looking for new ways to attack, threat actors have turned to AI to improve their spear phishing campaigns. GPT-3 language models such as ChatGPT have been a hot topic in the media recently for their ability to write university essays, however these models can also do far more. Natural language processing (NLP) and machine learning allow threat actors to compose more convincing phishing emails, free from grammatical and spelling errors. By combining AI and information leaked on the dark web, these programs can also tailor a phishing email to its recipient's interests and traits, in the same way that we receive targeted ads based on our social media and browsing history.

AI does require some level of expertise and it can be very expensive to train a really good model, particularly one focussed on personality analysis, to predict a person's proclivities and mentality based on behavioural inputs. However, AI-as-a-service may play a critical role in phishing and spear phishing campaigns by lowering the barriers to entry.

A team from Singapore's Government Technology Agency recently presented an experiment in which it crafted and sent targeted phishing emails generated by an AI-as-a-service platform to 200 of its colleagues.[2] Surprisingly, the team found that the AI-generated messages were "weirdly human" and more recipients clicked the links in the AI-generated messages than the human-written ones. The platform also automatically supplied surprising specifics, including mentioning a Singaporean law when instructed to generate a phishing email for people living in Singapore.[3]

As recently as December 2022 and January 2023, it was still possible and easy to use the ChatGPT web user interface to generate malware and phishing emails. [4] Since then, the anti-abuse mechanisms at ChatGPT have been significantly improved and it is now not possible to generate malware and phishing emails, with the service replying instead that such content is "illegal, unethical, and harmful".[5] That said, this has not stopped cyber criminals. Hackers have found a simple way to bypass those restrictions by using the application programming interface (API) for one of OpenAI's GPT-3 models known as text-davinci-003, instead of ChatGPT, which is a variant of the GPT-3 models specifically designed for chatbot applications. It appears that the API versions do not enforce restrictions on malicious content and have very few, if any, anti-abuse measures in place.[6] There is now even a user in a forum selling a service that combines the API and the Telegram messaging app to allow malicious content creation, such as phishing emails and malware code, without the limitations or barriers that ChatGPT has set on its user interface (the first 20 queries are free; users are then charged $5.50 for every 100 queries).[7]

Clearly, AI poses serious concerns about its potential abuse and the misuse of language models. It is therefore important that AI governance frameworks are put in place as soon as practicable.

To this end, Singapore released the first edition of its Model AI Governance Framework on 23 January 2019 and the second edition on 21 January 2020. On 25 May 2022, A.I. Verify was launched in Singapore – the world's first AI governance testing framework and toolkit for companies that wish to demonstrate responsible AI in an objective and verifiable manner.[8] There is also a European proposal for a legal framework on AI.[9]

[2] Newman, Lily Hay. AI Wrote Better Phishing Emails Than Humans in a Recent Test. *Wired*. 7 August 2021.

[3] Ibid.

[4] Check Point Research demonstrated in December 2022 how ChatGPT successfully conducted a full infection flow, from creating a convincing spear-phishing email to running a reverse shell, which can accept commands in English.

[5] Goodin, Dan. Hackers are selling a service that bypasses ChatGPT restrictions on malware. Ars Technica. 9 February 2023.

[6] Barreiro Jr, Victor. Cybercriminals bypass ChatGPT restrictions to make malware worse, phishing emails better. Rappler. 11 February 2023.

[7] Goodin, Dan (n5).

[8] Personal Data Protection Commission Sinapore: Singapore's Approach to AI Governance.

[9] European Commission: A European approach to artificial intelligence.

2. Cloud-native attacks

The shift towards cloud-based programs and software has been attractive to many organisations and was accelerated by the COVID-19 pandemic and the adoption of hybrid working. Gartner predicts that by 2025, over half of IT spending within the application software, infrastructure software, business process services and system infrastructure markets will have shifted from traditional solutions to the cloud.[10]

Moving to a cloud-based system, however, poses various challenges and numerous opportunities for threat actors to take advantage. These include the following.

Misconfiguration

Misconfiguration refers to any gaps, errors or glitches that can expose an environment to risk during cloud adoption. The sheer complexity of cloud-native platforms, as well as the rush to move to the cloud, has made misconfigurations more common in recent years. Examples include overly permissive access, default credentials, unrestricted ports and unsecured backups. These misconfigurations can provide unauthorised access to a system and its data, leaving a business vulnerable to various attack methods such as ransomware and major data breaches.

Observability

Observing cloud-based systems' performance is vital when a network utilises open-source platforms such as AWS, Microsoft Azure or Google Cloud Platform. It not only measures performance but can also provide real-time monitoring and alerting for potential security breaches and other threats. However, a recent study found that only 27% of organisations have full-stack observability. Whilst the study reported that observability is high on the priority list of many organisations, we expect that threat actors will exploit this before organisations have been able to invest in and implement observability tools across their whole cloud network.[11]

Insecure application programming interfaces (APIs)

APIs are intended to streamline cloud computing processes by allowing programs to "talk to each other". However, when left unsecured, they can open lines of communication that allow threat actors to gain unauthorised access to data. APIs can become insecure for various reasons; however, we expect to see an increase in the exploitation of APIs with inadequate authentication and vulnerabilities due to outdated components.

Organisations in 2023 will need to pay close attention to the visibility of their cloud environments, reliance on third parties and gaps in their cloud security.

[10] Gartner: Press release, 9 February 2022.

[11] VB Staff. Report: Only 27% of orgs have observability over their full stack. *Venture Beat*. 14 September 2022.

3. A rethink of multi-factor authentication (MFA)

When breaching corporate networks, threat actors commonly use stolen credentials obtained through phishing attacks, malware and data leaks. To combat this, in recent years organisations have relied heavily on MFA as a security measure. Whilst this has provided a useful layer of cyber security, many organisations wrongfully assume that it is foolproof and overlook the many ways in which threat actors can bypass MFA.

In fact, threat actors have used this pressure for MFA implementation to exploit "MFA fatigue" among users. We know that MFA is configured to use "push" notifications to ask a user to verify a login attempt. An MFA fatigue attack occurs when a threat actor runs a script that constantly attempts to log in with the stolen credentials, sending repeated MFA requests to a user's device. The threat actor continues to do this for an extended period of time and often combines it with malicious messages impersonating IT support in an attempt to convince the user to accept the prompt.

Ultimately, the user becomes so overwhelmed or frustrated by the notifications that they either accept the request to stop the notifications, or accidentally click approve when reviewing or attempting to deny the request. They may also suspect a bug within the MFA application and change their configuration to disable MFA. Successful attacks on large organisations including Cisco, Uber and Microsoft demonstrated the effectiveness of this tactic in 2022.

This threat intelligence report prepared by Lander & Rogers with Forensic IT provides valuable insights and recommendations for mitigating a newly identified method of MFA bypass.

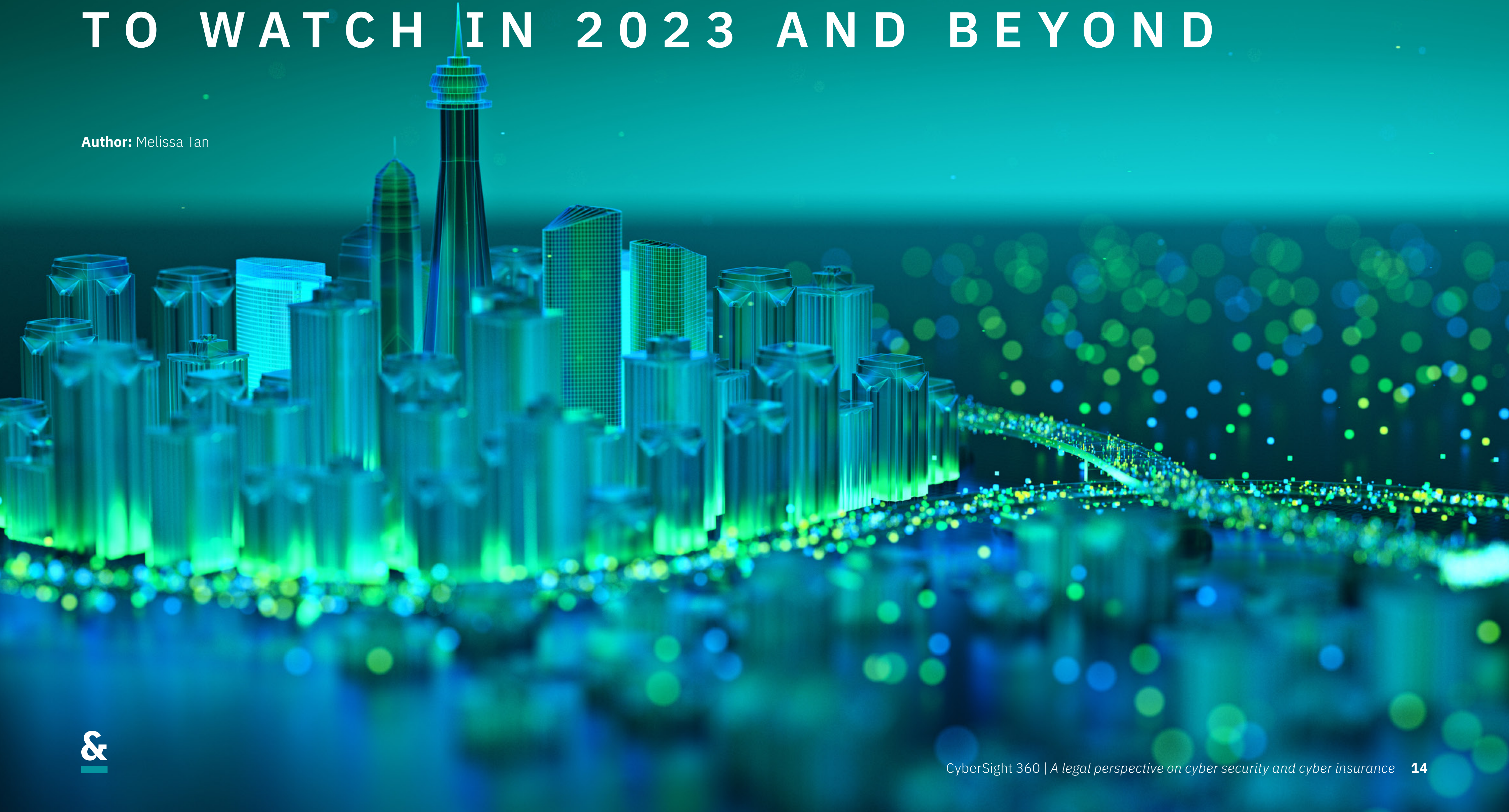
Attacks of this nature are expected to increase in frequency in 2023. As a result, organisations will need to educate their employees on the ways in which MFA can potentially be bypassed, and the malicious tactics to look out for.

Looking forward

Recent patterns and new developments in cyber attacks suggest that threat actors and cyber security threats will not remain static. They will continue to evolve, improve, and leverage new technology to achieve their goals, often at a rate quicker than we can anticipate or react. It is therefore imperative that governments, organisations and individuals stay vigilant, adapt and respond quickly to existing and emerging cyber security threats and risks.

CYBER INSURANCE MARKET TRENDS TO WATCH IN 2023 AND BEYOND

Author: Melissa Tan



As cyber attacks continue to rise, cyber awareness increases and cyber security and privacy laws and regulations strengthen globally, demand for cyber insurance has increased even as premiums soar.

Demand means opportunities; but it can also mean greater risk and exposure. As a result, concerns about the sustainability of cyber insurance are growing, even leading Mario Greco, chief executive officer at insurer Zurich, to claim that cyber attacks are set to become "uninsurable".[1]

Individual insurers will need to decide how to balance the commercial decision of growing their cyber insurance portfolio with their capacity and risk appetite for absorbing potential large losses.

In 2023 and beyond, the focus of the cyber insurance market will likely continue to be on measures to ensure its sustainability in the face of rapidly evolving cyber risks.

But what does this quest for sustainability mean in the short and long term for the cyber insurance market?

IN THE SHORT TERM

1. Tighter underwriting will continue

In the short term, the cyber insurance market will continue to tighten policy language and flush out "silent" cyber exposure.

This will primarily be done through greater clarity on affirmative and non-affirmative cyber cover in policies; greater clarity in relation to exclusions imposed; bespoke exclusion endorsements relevant to any new and emerging threats; more stringent limits or sub-limits, and higher deductibles.

For example, in the last few years, the insurance market has been confronted with the issues of war exclusions and insuring hostile cyber activity. At the end of 2021 the Lloyd's Market Association drafted four model war, cyber war and cyber operations exclusion clauses, which provide Lloyd's syndicates and their (re)insureds (and brokers) with options:

- for a war exclusion they can include in standalone cyber insurance policies; and
- in respect of the level of cover provided for cyber operations between states that are not excluded by the definition of war, cyber war or cyber operations that have a major detrimental impact on a state.

Subsequently on 16 August 2022, Lloyd's issued a market bulletin titled "State-backed cyber attack exclusions" requiring, from 31 March 2023, that all standalone cyber policies must include, at the inception or on renewal of each policy, a suitable exclusion clause excluding liability for losses arising from any state-backed cyber attack with the following minimum requirements:

1. Exclude losses arising from a war (whether declared or not), where the policy does not have a separate war exclusion.
2. (Subject to 3) Exclude losses arising from state-backed cyber attacks that
   a. significantly impair the ability of a state to function; or
   b. significantly impair the security capabilities of a state.
3. Be clear as to whether cover excludes computer systems that are located outside any state affected in the manner outlined in 2(a) & (b) above, by the state-backed cyber attack.
4. Set out a robust basis by which the parties agree on how any state-backed cyber attack will be attributed to one or more states.
5. Ensure all key terms are clearly defined.

Lloyd's has around 20% of the global cyber market. It is hoped that having such exclusions for potentially catastrophic events with robust wordings can provide the parties with clarity of cover, so that risks can be properly priced and reduce the risk of coverage disputes.

In 2023 and in the short term, insurers globally are expected to continue to tighten policy language and underwriting standards in a bid to ensure the sustainability of the cyber insurance market, whilst they work on either increasing capacity or developing more innovative approaches towards underwriting cyber risks.

2. Third-party claims will rise

In the short term, the cyber insurance market is expected to grapple with an increase in third-party claims.

Standalone cyber insurance policies cover a range of losses related to cyber incidents and are typically classified as first-party or third-party coverage. The bulk of indemnity payments under cyber insurance policies to date has been for first-party losses such as forensic investigation costs, legal costs, public relations costs, costs related to the loss of or damage to data, content-related claims related to data, privacy notification costs or costs associated with cyber extortion reimbursement.

However, with:

- regulators' increased interest in cyber security and an uptick in enforcement activities around cyber security (eg. the *ASIC v RI Advice* [2022] FCA 496 case);

[1] "Cyber attacks set to become uninsurable, says Zurich chief". *Financial Times*. 26 December 2022.

- the increasing scale of data breaches; and
- growing prioritisation by consumers of their individual rights to privacy and increased expectations around companies' data protection measures following large-scale data breaches in 2022

insurers can expect an increase in claims made under cyber insurance policies for third-party coverage in the short and medium term. This includes fines and penalties imposed by regulators and compensation to third parties for failure to protect their data.

IN THE LONG TERM

1. Defining and tackling systemic cyber risks

In the longer term, the cyber insurance market will continue to prioritise tackling systemic cyber risks. However, in order to find a sustainable solution to this problem, there first needs to be a common understanding of what the problem entails.

There is no single, widely accepted definition of systemic cyber risk, and most definitions are vague.[2] In a 2017 report, AIG defined systemic cyber risk as "capable of impacting many companies at the same time".[3]

Whatever the definition, the concept of systemic cyber risk boils down to the possibility that a single event or development might trigger widespread failures and catastrophic consequences spanning multiple organisations, sectors or nations, particularly due to various forms of interdependency, whether financial, biological, logistical or digital.[4]

Notably, supply chain attacks and disruptions are a well-known systemic risk with global consequences which the insurance industry has, and will continue, to address to ensure cyber insurance remains sustainable.

In light of the frequency of supply chain attacks on organisations, it is more important than ever for the cyber insurance industry to define what is meant by "digital supply chain" and better understand the potential losses that may arise from a third-party cyber attack. Insurers have begun to do this in a number of ways.

Following the Solar Winds compromise, insurers began reviewing their overall exposure to systemic, aggregated and correlated risks related to the software supply chain.

As a precondition to writing or renewing cover or determining a premium, insurers are increasingly looking at an organisation's third-party arrangements. This requires not just visibility around the supply chain, but also evidence that the organisation has considered the known risks of its supply chain, is actively managing these risks and has persistent monitoring in place. In particular, insurers appear to be looking closely at managing known risks through supply contracts with limits of liability, assurances regarding cyber security posture and rights such as right of audit.

Insureds are also expected to have considered the unknown risks to the supply chain and be able to provide evidence that these risks are being mitigated through strong cyber defences and a risk-aware culture.

Whilst focusing on ways to minimise cyber risk, insurers continue to face difficulties in finding a market-leading but pragmatic approach to quantifying and managing supply chain risk. A report by PwC notes that while 85% of respondents claim to have loss estimation methodology in place, the majority use simplistic exposure and factor-based methods, which have in the past shown to underestimate the risk.

Quantifying and tackling systemic cyber risks like supply chain attacks will likely continue to be a focus for the insurance industry in 2023 and beyond.

2. Innovative insurance solutions

In the long term, insurers will need to devise innovative solutions to address their cyber risk exposure and capacity issues to ensure the cyber insurance market remains sustainable.

This can already be witnessed in the insurer Beazley's unveiling in January 2023 of a US$45M catastrophe bond (CAT) for major cyber events.[5] The Beazley bond provides Beazley with indemnity against catastrophic events that exceed US$300M. CAT is essentially a method used by insurance companies to reduce their risk by transferring the financial risk on investors, who in return receive attractive investment rates. It is said to be the first insurance-linked securities (ILS) instrument established in the cyber insurance market. The CAT offers an alternative for the insurance industry to spread coverage risks and provides insurers with a new source of capital.

There are two other possible avenues that will likely be developed further by insurers in the long term.

Parametric cyber insurance

Parametric insurance provides cover based on a pre-defined trigger. It has commonly been used in situations where it is difficult to

[2] Systemic Cyber Risk: A Primer. Carnegie Endowment for International Peace. 7 March 2022.

[3] Is Cyber Risk Systemic? AIG. February 2017.

[4] Systemic Cyber Risk: A Primer (n2).

[5] Croft, David. "World's first cyber catastrophe bond launched by UK insurer." Cybersecurity Connect. 11 January 2023.

quantify the exact loss that would result from a particular event, such as natural catastrophes or agriculture.

In the context of cyber, the trigger could be a physical trigger such as the number of hacked computers or the cost of damage and repair to the computers. Compared to traditional indemnity-based coverage products, which often require time-intensive damage and loss assessments, parametric insurance has the benefit of providing quick payouts following the trigger event.

In the context of cyber risk, in December 2019 reinsurer Chaucer partnered with InsurTech Qomplx to launch the first dedicated cyber parametric multi-peril insurance (WonderCover). The policy provides protection against operational losses arising from data breaches, IT interruption and non-property terrorism damage. In particular, payouts of a pre-determined amount are made if any of the following trigger event occurs:

- A GDPR breach that requires notification;
- An IT outage with services interrupted; or
- Terrorism non-damage business interruption.

Whilst WonderCover has smaller limits of between GBP5,000 and GBP100,000 and primarily targets UK small businesses, parametric insurance may potentially provide a viable alternative for the insurance industry to address certain large-scale cyber events.

Insurance industry playing a leading role in boosting the public-private partnership

Catastrophic cyber events and systemic cyber risks give rise to large aggregate losses, which the private insurance market may not be able to carry on its own. Government-backed solutions would therefore likely come to the fore, with the insurance industry taking the leading role in enhancing the public-private partnership to tackle the issue of large cyber loss aggregations and ensure its sustainability.

A well-designed public-private partnership could increase risk-absorbing capacity, which takes some pressure off the private insurance market, and yet enable and encourage cyber market innovations to extend cover further for catastrophic cyber events and systemic cyber risks.[6]

Ultimately, some form of government backstop or public-private partnership to finance catastrophic cyber events and systemic cyber risks will likely be needed to ensure a sustainable private cyber insurance market and boost economy-wide resilience. This will be a complex task, but we expect the insurance industry will take the lead in driving this collaboration with governments.

[6] Insuring Hostile Cyber Activity: In search of sustainable solutions. The Geneva Association. January 2022.

OPINION

CRIMINALISING CYBER EXTORTION PAYMENTS

Are we punishing the wrong party?

Author: Melissa Tan

In November 2022, the Australian government announced it was considering new laws to make it illegal for companies to pay ransoms to cyber criminals[1], and that it would increase penalties for data breaches.[2] The announcement comes in the wake of high-profile cyber attacks in Australia in 2022, with discussions about Australia's cyber security strategy expected to ramp up this year.

The renewed focus is welcomed by cyber security experts as a further step towards fortifying Australia's cyber security protections, alongside the international community.

However, a critical question remains unanswered. Will the ban on ransom payments be effected through civil or criminal law, and will it be subject to civil penalties or criminal sanctions?

How can the ban be effected?

At this stage, certain US states, including New York and Hawaii, have introduced bills prohibiting governmental, business and health care entities from paying a ransom in the event of a cyber incident or a cyber ransom or ransomware attack, with a civil penalty of up to US$10,000 imposed for any violation of the ban.

The New York law proposes to amend the state's technology law to include the ban, whilst the Hawaiian law proposes to amend Chapter 128A Homeland Security, Hawaii Revised Statutes.

However, the effectiveness of civil penalties of this quantum in deterring the payment of ransom is debatable. When the very survival of a business is at stake, a cost-benefit analysis could reveal it is in the interests of the business to pay the ransom and simply absorb the civil penalty.

Alternatively, governments may decide to criminalise the payment of ransoms through corporate criminal law, making it an offence to pay a cyber ransom. This would mean a company is criminally liable, and directors and officers personally liable if the corporation commits the offence. In this case, the deterrence effect of such laws on the ransom victim may be stronger.

However, in the same way a ban on extortion cover in insurance policies is little deterrent to cyber criminals, many believe that criminalising the payment of ransoms will also fail to discourage cyber crime.

A decision to criminalise the payment of ransoms should not be taken lightly. The current assumption is that banning ransom payments will disincentivise cyber crime, striking at the heart of the criminal enterprises. However, the punitive approach towards the victims of cyber extortion is far more complex.

Below, we explore the facts in more detail.

1. It is not always about financial gain

The main tenet in support of criminalising the payment of ransoms is that it would reduce the financial incentives for criminals because companies would be bound to refuse payment to avoid committing an offence. It is argued that this would in turn reduce the number and severity of cyber attacks, particularly ransomware attacks and attacks involving cyber extortion.

However, cyber criminals are motivated by a variety of factors, including financial gain, ideological reasons, personal or professional revenge, thrill-seeking or simply to teach a company with cyber security vulnerabilities a lesson. These motivations can be overlapping and often change over time.

If the end goal is to reduce the number and severity of cyber attacks, striking at one motivation by extinguishing the source of funds may not necessarily be effective.

Example

Cyber incidents perpetrated by bug bounty hunters are often undertaken to expose the vulnerabilities of using open-source third-party software, with exfiltration of data viewed as a trophy or to confirm the breach. In these instances, extortion demands are typically opportunistic and a sub-motivation, with very few demands suggesting that financial gain was the main motivation for these threat actors.

Such threat actors are unlikely to stop carrying out cyber attacks if ransom payments are made illegal.

In other words, unless the main or sole motivation is financial gain, criminalising the payment of ransoms is unlikely to make a significant dent in the cyber crime enterprise.

[1] https://www.smh.com.au/politics/federal/we-will-hunt-them-down-o-neil-signals-more-action-on-medibank-hack-20221113-p5bxsi.html

[2] https://ministers.ag.gov.au/media-centre/joint-standing-operation-against-cyber-criminal-syndicates-12-11-2022

2. Cyber criminals are resilient, motivated and creative

Assuming for a moment that the main or sole motivation for cyber criminals and ransomware attackers is financial gain, cyber extortion funds are only one source of funding. Cyber criminals have proven themselves to be resilient, motivated and creative in identifying new opportunities.

Despite hurdles and security measures to thwart cyber criminals, they are often able to devise creative bypass measures to achieve their end goal.

Example

In 2019, Microsoft claimed that multi-factor authentication (MFA) can prevent over 99.9% of account compromise attacks.[3] However, in 2022, we saw cyber crime groups escalating attacks on MFA methods globally, launching MFA bypass attacks to compromise accounts.[4]

Closing off the source of extortion funds simply pushes cyber criminals towards other tactics to procure financial gain. It is well known that cyber criminals utilise malware, phishing scams and other tactics to steal personal information or financial data, which they then use to commit identity theft or fraud for financial gain. Cyber criminals have also developed MFA bypass tactics to carry out account-takeover attacks on banks and crypto wallets for financial gain.

In this respect, criminalising the payment of ransoms is unlikely to make a significant dent in the cyber crime enterprise, as it fails to recognise the other avenues for financial gain.

3. Fewer companies are paying ransoms

A 2022 research report found that fewer companies paid extortion payments to cyber criminals in 2022 than in both 2021 and 2020.[5]

In the findings published by Chainalysis Inc on 19 January 2023, ransom payments (which are almost always paid in cryptocurrency) fell to US$456.8M in 2022 from US$765.6M in 2021. The 40% drop was not attributed to attacks reducing, but much of the decline was due to victim organisations refusing to pay ransomware attackers.

The research from Chainalysis is supported by data from the cyber incident response company Coveware, which disclosed that the number of Coveware's clients that have paid a ransom after an attack has steadily decreased since 2019, from 76% to 41% in 2022, according to Chainalysis's research.

There are a few reasons for this:

1. As companies and businesses become increasingly aware of cyber security risks, invest in uplifting their cyber resilience and/or have the financial support of cyber insurance, there are often options other than the payment of ransoms to recover the data. The cyber insurance industry has played an important role in this by requiring organisations to meet a minimum standard of cyber security and backup measures before insuring them for ransomware coverage. Having these requirements has uplifted the cyber resilience of many insured organisations and led to these companies being able to recover from cyber attacks through means other than paying ransom.
2. The payment of ransoms now comes with increasing legal risk, both in Australia and in other jurisdictions like the US, UK and EU. When considering the payment of ransoms, organisations must consider the significant ramifications that may arise under sanctions laws (both domestic, foreign and international), anti-money laundering laws, and counter-terrorism laws. There are also significant reputational ramifications for an organisation that is publicly known to have paid a ransom.
3. The Australian government's position is to never pay a ransom. As Australian organisations become more cyber security aware, they have become more willing to report ransomware attacks and extortion demands to the police, the Australian Cyber Security Centre (ACSC), and the Office of the Australian Information Commissioner (OAIC) if it involves a data breach. This has created an increased public-private collaboration, which often results in the organisation adopting the government's position of not paying the ransom. Such collaboration has contributed to discouraging the payment of ransoms.

Despite this downward trend in organisations making ransom payments, there has been no reduction in the number and frequency of cyber attacks. Today, ransomware remains one of the top threats to organisations, and cyber crime is costing the Australian economy an estimated AU$42B annually.[6] Therefore, it would not only be reasonable but prudent to query whether the criminalisation of ransom payments would indeed be an effective solution to the cyber extortion and ransomware problem facing Australia.

4. Punishing the victims

The most apparent effect of criminalising ransom payments is that it punishes victims of cyber extortion, which is contrary to the very foundation of the criminal justice system.

Criminal law seeks to identify and punish offending conduct and behaviours for the protection of society. The offending conduct here is the cyber crime, and there are already laws in place (sanctions laws, anti-money laundering laws, and counter-terrorism laws) that prevent organisations from paying the ransom if doing so may cause them to fund the criminal enterprise.

However, laws criminalising the payment of ransoms do not punish the cyber crime perpetrators, at least not directly. Instead, they penalise the victim of the cyber crime directly, who very often only contemplates payment of the ransom in exceptional circumstances and as a last resort.

Australia is in a developing phase of uplifting its cyber resilience as a nation. Whilst organisations that have the resources to invest in uplifting their cyber resilience are able to afford a policy of not paying a cyber ransom, small and medium enterprises (SMEs) that are lagging behind often have fewer options when considering ransom payment for recovery and business survival.

[3] https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

[4] https://www.techtarget.com/searchsecurity/news/252525234/Cybercriminals-launching-more-MFA-bypass-attacks; https://its.unc.edu/2022/10/20/mfa-bypass/

[5] Ransomware revenue down as more victims refuse to pay: https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/

[6] https://www.unsw.adfa.edu.au/newsroom/news/cybercrime-estimated-42-billion-cost-australian-economy

Such a law presupposes that all organisations are able to recover without paying a ransom, which is simply not a realistic assumption at this stage of Australia's cyber security maturity. In actual fact, it is perhaps more likely that a ban on ransom payments would hurt these organisations the most, rather than the cyber criminals themselves.

Further, information-sharing and intelligence-gathering is a key part of the fight against cyber crime globally. By criminalising the payment of ransoms, victims of cyber crime may be less willing to trust, report or share information about the cyber extortion threat with law enforcement authorities or the regulators out of fear of punitive or criminal ramifications.

Is there an alternative?

In short, making it illegal for companies to pay ransoms to cyber criminals will not be a panacea to the cyber crime, cyber extortion and ransomware problems facing Australia. It is a blunt tool that is unlikely to impact or stop the cyber criminals.

The resources would arguably be better spent on measures that would directly impact the cyber crime enterprise and reduce Australia's vulnerability to such attacks. For example:

- Improving international governmental and law enforcement cooperation in the fight against cyber crime and ransomware groups.
- Uplifting the cyber resilience and maturity of all Australian government and non-governmental organisations so that if, and when, a ransomware attack or cyber extortion threat is made, the question of paying the ransom does not arise.

Perhaps it is only at that stage that a law criminalising the payment of ransoms to cyber criminals is more justifiable.

Directors' duties provisions

The decision to make a ransom payment often rests with an individual (or a group of individuals), and/or the board of directors. If the goal is simply to reflect the public policy of discouraging the payment of ransoms, rather than personal criminal liability, a more appropriate approach would perhaps be to regulate such conduct through the directors' duties provisions, to ensure that any decision to make a ransom payment is in line with those duties. This would ensure that any decision to pay a ransom would be limited to the most exceptional of circumstances and where it is, on balance, likely to be reasonable or in the interest of the company.

That said, following discussions and consultation, if the decision is made to criminalise the payment of ransoms to cyber criminals, then we consider it is important for lawmakers to include specific defences and exceptions, such as the common law criminal defence of necessity, to accommodate the exceptional circumstances organisations may face. After all, laws are formal rules which society uses to define how people and organisations are expected to behave, but they should not be rigid and fixed, or lack the flexibility to take account of various circumstances.

OPINION

IT'S TIME TO PUT CYBER SECURITY AT THE HEART OF ESG

Author: Melissa Tan

Technology and digitalisation have transformed society and the way we do business, dramatically improving efficiency, quality, productivity and ultimately value. However, with these benefits come new challenges posed by escalating and rapidly changing cyber security and digital risks.

Cyber security threats and cyber crime are evolving faster than society's ability to effectively respond to or prevent them. It is reasonable to say that cyber security risks have become a fundamental challenge to corporate sustainability.

To ensure long-term corporate sustainability and demonstrate value to investors, organisations should see and manage cyber security risk not only as a compliance issue, but as part of their ESG strategy.

It is time to put the **C**(yber security) in **ESG** – not as a separate pillar, but as a foundational element underlying each of the E-S-G considerations.

1. Preserving trust and reputation

Cyber security is relevant to a company's social responsibilities through data protection and privacy. The high-profile data breaches that occurred in Australia in 2022 have brought home the critical responsibility companies have in protecting the personal data of their customers, employees, and other stakeholders. They have also reaffirmed the detrimental effect a data breach can have on public trust in a company, the reputation of a business, and even its survival.

Investing in uplifting cyber resilience and implementing cyber security measures – such as multi-factor authentication, encryption, secure data storage, secure backups and consistent cyber awareness training for employees – is more than a technical safeguard. In adopting these measures, companies demonstrate to stakeholders that they are taking necessary steps to protect the personal and sensitive data they are responsible for; that they are actively tackling the problem of human error, which has been traced to 95% of cyber security issues[1]; and that they are investing in upskilling and training their employees in cyber risk management. This is key to preserving trust and reputation as well as maintaining corporate sustainability.

2. Minimising environmental impact

A robust cyber security strategy plays an important part in reducing a company's environmental impact. Cyber incidents are not confined to the technological world; they may also bring physical consequences, including pollution and environmental damage. Cyber attacks can target industrial control systems, which may result in the loss of control of critical equipment and warning systems as well as potential damage to human health and the environment from catastrophic spills, waste discharges, air emissions and other environmental hazards. These types of attacks can also disrupt manufacturing, transportation and other operations, and cause fires, explosions and hazardous material releases that result in bodily injury, property damage, environmental remediation expense, and significant legal liability claims.[2] In 2021, a hacker made a (thwarted) attempt to poison the water supply of a city in Florida, USA by increasing the amount of sodium hydroxide to extremely dangerous levels. This serves as an important reminder for companies, particularly those in critical infrastructure and other sensitive industries, of the importance of robust cyber security measures to reduce the potential environmental and societal impacts of a cyber attack.

3. Practising good corporate governance

Cyber security is also relevant to corporate governance, particularly risk and crisis management. Good corporate governance and risk management require the consideration and implementation of cyber security measures including incident response, business continuity and disaster recovery planning to minimise the impact of a cyber attack on operations and service delivery.

Stakeholders and regulators increasingly expect and require boards of companies to consider and assess cyber security risks as part of their enterprise risk management. The positive security obligations now in effect as part of the SOCI Act reforms also underlie the link between cyber security risk and governance risk. In addition, cyber attacks – particularly ransomware attacks and cyber extortion threats – often bring up difficult ethical and legal questions, and investors and stakeholders expect companies to have in place internal and external mechanisms to navigate these issues, and to behave ethically and in accordance with company values.

[1] Mee, P. and Brandenburg, R. 2020. "After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk". World Economic Forum Global Agenda. 17 December 2020; The Global Risks Report 2022

[2] AXA XL Environmental White Paper: Environmental risks: cyber security and critical industries

In other words, cyber security risk is not simply a compliance issue or a matter for risk transfer through insurance; it is a fundamental aspect of corporate sustainability. Companies must assess cyber security risks as part of their ESG strategy and focus on uplifting cyber resilience in their efforts to meet ESG goals.

Companies that integrate cyber security into their ESG strategy will improve not only their financial stability, reputation and trust, but also their compliance with regulations, overall risk management strategy, and their impact on the environment and society. Above all, an ESG strategy underpinned by robust cyber security could prove to be a critical factor in ensuring a company's insurability and long-term sustainability.

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

Edward Smith
Special Counsel
Insurance Law & Litigation

D +61 3 9269 9647
M +61 406 790 432
E esmith@landers.com.au

Suzanne Boutsalis
Senior Associate
Insurance Law & Litigation

D +61 2 8020 7896
M +61 418 886 936
E sboutsalis@landers.com.au

Louisa Henderson
Lawyer
Insurance Law & Litigation

D +61 2 8020 7897
M +61 447 312 413
E lhenderson@landers.com.au

Rose Cavanagh
Lawyer
Insurance Law & Litigation

D +61 2 8020 7741
M +61 439 742 299
E rcavanagh@landers.com.au

Angela Knezevic
Lawyer
Insurance Law & Litigation

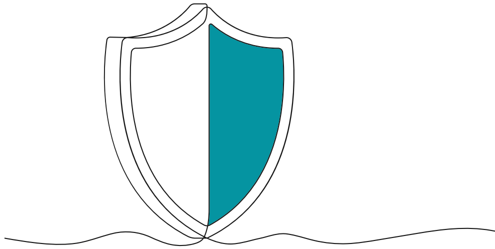
D +61 2 8020 7815
M +61 437 085 753
E aknezevic@landers.com.au

John Zhu
Lawyer
Insurance Law & Litigation

D +61 7 3456 5136
M +61 456 356 729
E jzhu@landers.com.au

Annie Weng
Paralegal
Insurance Law & Litigation

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



ABOUT US

Founded in 1946, Lander & Rogers is one of the few remaining truly independent Australian law firms and a leader in legal tech innovation.

With offices across the eastern seaboard of Australia, Lander & Rogers has grown organically resulting in a unified firm with a strong focus on client and staff care.

We believe legal services involve more than just the law – practical, commercial advice and exceptional client experience are equally important to our clients and to us.

Lander & Rogers advises corporate, government, not-for-profit and private clients in insurance law and litigation, family law, workplace relations & safety, real estate, corporate transactions, digital & technology and commercial disputes.

The firm is global in approach, working closely with a network of leading firms to provide advice to clients, both domestically and abroad. Lander & Rogers is also the exclusive Australian member of the largest worldwide network of independent law firms, TerraLex.

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 St
Melbourne VIC 3000

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

Sydney

Level 19 Angel Place
123 Pitt St
Sydney NSW 2000

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

in

landers.com.au