6

2023 Cyber Predictions and Insurance Implications

Stay ahead: inform, improve and insure with these 6 critical cyber-security risks to look out for.

Reliance on technology, and the associated cyber security risks have been, and will continue to be fundamental to business.

Following the significant events of 2022, we believe 2023 will see its own cyber-security related challenges as new threats arise. Businesses will need to stay ahead of emerging risks and ensure they learn from events of the past.

This report examines various 2023 considerations within the threat environment and regulatory landscape; exploring insurance industry insights and the role and value of risk transfer solutions.

Content

Foreword - Cyber insurance must evolve

2023 presents an opportunity, or perhaps more realistically, a requirement for organisations, directors and officers to properly understand, mitigate and invest in cyber-security risk. This will be achieved through education, mitigation, and risk transfer.

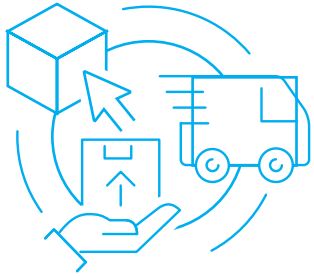
Gone are the days of "being targeted", with the increasing indiscriminate targeting of software and application vulnerabilities, and supply chain/ vendor exposure.

The velocity of change of cyber risks will be ongoing due to the very nature of technology. 2023 will undoubtably bring new developments in this risk landscape. Already it appears as though cyber and technology will settle as the number one Board issue.

Mark Luckin
Cyber Practice Leader

M: +61 433 337 922
E: mark.luckin@lockton.com

1.



Insurer focus on supply chain & third-party vendor exposures

What are third-party and vendor supply chain exposures?

Whilst beneficial, and an essential, undeniable part of doing business in the modern economy, there are risks associated with outsourcing services or products. Unlike the services rendered, the risk and liability cannot be outsourced.

The Australian Cyber Security Centre's (ACSC) most recent annual Cyber Threat report highlights the ways in which threat actors use different tactics for cyber-attacks on supply chains, knowing the disruption it will cause.

According to Blackberry's research, four in five IT security professionals were aware of an attack or vulnerability in their supply chain in the last 12 months. Additionally, 80% of organisations across Australia were notified of a vulnerability or attack within their software supply chain.

> "Compared to the global average, Australia suffered the highest rates of operational compromise and data loss. It proves cyber-security must go far beyond vendor trust."

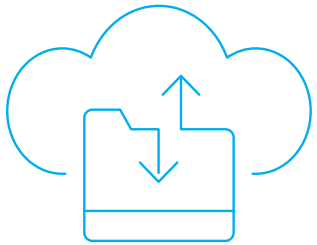
THE RISKS AND IMPACT:

- If a third party fails to deliver, or suffers a breach, **the organisation that utilises the vendor will face the consequences**.
- The impact can be fiscally, operationally, reputationally and **contractually significant**.
- Data shared between external vendors (supplier, vendor, contractor, or service provider) can be **exposed**.
- **Internal operations** can also be affected and vulnerable to **malware** and **ransom threats**.

LOCKTON INSIGHTS

1. Businesses must implement solutions to identify, mitigate and monitor their third party/ vendor exposure from a technology and contractual standpoint.
2. Threat actors across the world use different tactics for cyber-attacks on supply chains and to penetrate, knowing the disruption it will cause.
3. Lockton predict third party/vendor risks and how insureds are mitigating such to be of significant focus from insurers in 2023. Insureds need to review policy response specific to this exposure, as insurers seek to sub-limit, restrict coverage, or remove it in its entirety.

2.



Increased exposures in Cloud and APIs

What are Cloud and API exposures?

Cloud

Cloud services are used by most organisations for data backups, data analytics, and software development.

But with such convenience always comes increased cyber-security risk. How can organisations be sure that their data is securely stored? Do businesses truly know who has access to their data and how it is protected?

APIs

In recent years there has been a significant uptake in Application Programming Interfaces, more commonly known as APIs.

APIs enable applications to exchange data and information quickly, providing more convenience and an enhanced experience to the user on their digital devices. The increased use of APIs will create more opportunities for hackers.

According to a report from Forrester Research, commissioned by Imperva, 78% of organisational decision-makers believe adopting APIs is important for their company to stay competitive, especially for connecting with customers (88%) and improving data ownership and management (83%).

THE RISKS AND IMPACT:

- **Sensitive data** is likely to be **targeted**.
- **Loss of valuable information** from database can be **highly disruptive**.
- **Data leakage** of company and customer/client information is **exposed on the dark web**; cyber criminals sometimes use this as a **means for ransom threats** (note, not all ransoms are monetary).
- **Account hijacking** gives a hacker access to all channels the user has permissions for, enabling them to further **intrude on an organisation's systems and documentations**.
- Cyber-criminals sometimes **recruit individuals in an organisation to gain access to their system**. This is known as **insider actors/threats**.
- **Insecure API's** can be compromised and lead to more **opportunities for bad actors**.

LOCKTON INSIGHTS

1. Organisations should look to ensure they understand their relience on their cloud provider, ensuring they are doing their initial and ongoing due dilligence. Robust contractual arrangements will assist in mitigating exposure.
2. Insureds need to ensure that coverage is not restricted with respect to events arising from cloud service provider events.

3.

High inflation leading to poor decisions

How inflation influences business decision-making on cyber-security risks.

Despite cyber-security being a well-deserved business investment (especially given the increased expectations on organisations from regulators and consumers), the inflationary economic environment is likely to impact the allocation of cyber-security spend, and unfortunately, will affect cyber event and cyber insurance claims costs.

Speaking specifically to D&O Liability, simply noting a reason for not investing in improving an organisation's cyber security posture, or mitigating an identified particular exposure due to the "increased costs" is fraught with danger.

Furthermore, any organisation that faces a significant cyber event, and subsequent regulatory action, will face additional challenges.

Insurers are likely to have an increased focus on assessing an organisation's approach to cyber-security investment from both a cyber insurance and directors and officers liability perspective.

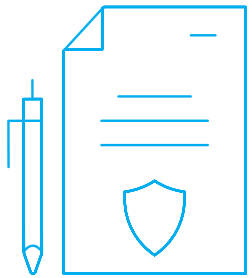
THE RISKS AND IMPACT:

- Inflation should not prevent organisations from **investing in cyber-security**.
- Under the **Business Judgement Rule**, boards and **Directors and Officers** must consider an organisation's best interests - this includes a company's cyber-resilience. **Non-investment due to expense would be a tenuous and likely unsuccessful use of the Business Judgement Rule defence**.
- **Cyber insurance claims costs** and **premiums** are **likely to increase**.

LOCKTON INSIGHTS

1. With cyber information and technology risks already such a broad risk area to attempt to cover, where the velocity of the risk is so significant, CISO's, Heads of Security and equivalents will be faced with some tough decisions in 2023.
2. Ongoing consideration by CISO's and those in executive risk roles (CFOs, CROs, COOs and CEOs) will be crucial to form overall plans.
3. Cyber Insurance should be considered as an essential part of a holistic approach to cyber risk management.

4.



D&O: the stakes are becoming much higher

Businesses have much to learn from history and the incidents of 2022, but in 2023 the stakes are arguably even higher. Boardrooms should be concerned.

Directors, Officers, and C-suite executives can already be held personally liable for the consequences of a cyber event that significantly impacts an organisation. However, new regulatory changes have further increased the potentially significant personal liability exposure and financial implications.

Company Directors have been put on notice...

In an article by the Australian Financial Review, the Australian Securities and Investments Commission Chairman, Joe Longo, said,

> "For all boards, I think cyber resilience has got to be the number one risk facing everyone, and if things go wrong, ASIC will be looking for whether they took reasonable steps and made reasonable investments proportionate to the risks that their business poses to defend themselves from an attack. The major priority has to be to encourage boards, and to remind them of their obligations in this area."

Boards and executives must now step up by asking teams the right questions and supporting clear action. Rather than crossing fingers, having clear, documented steps in place to manage the risk, and investing in impactful cyber-risk management strategies should be a key focus in 2023.

Regulators, shareholders, supply chains, teams and employees are all watching.

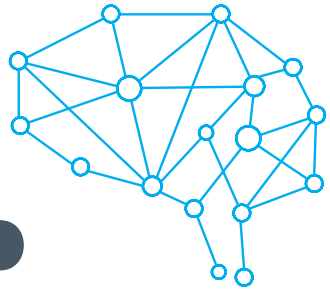
THE RISKS AND IMPACT:

- **Fines and penalties** are likely if reasonable steps are not taken to mitigate risks.
- A **lack of due diligence** can result in **class actions** and even **prosecution**. The duty of **Directors and Officers** under the **Business Judgement Rule** is to make decisions **in good faith** and in the best interests of the company.
- Another consequence of failing to prioritise cyber-security can be **reputational harm**.
- The cyber events in 2022 were a great example of how a cyber-attack can escalate to **loss of revenue and a downturn in share price**.

LOCKTON INSIGHTS

1. Consider methods for collating and holding data and de-identification.
2. The regulatory and socially implied expectations on organisations to be cyber resilient and treat data with the care and respect it deserves is going to be impactful from a regulatory and reputational standpoint.
3. Disconnect between Boards and CISOs - it is important to build a relationship to strengthen cyber-security.

5.



Advancements in Artificial Intelligence

AI is certainly not new, but came in the spotlight at the end of 2022, especially with the popularity of the likes of ChatGPT.

The positives

ChatGPT, the widely popular artificial intelligence tool is from OpenAI. The chatbot responds to questions about topics (e.g. political science, computer programming) with detailed explanations, and its question-and-answer format means users can drill down until they fully understand. This is unlike desktop research which relies upon the user scanning and reaching their own conclusion.

Useful tools could have unforeseen threats...

The concerns

Artificial intelligence and machine learning (AI/ML) models continue to evolve and become more intelligent. Their increased sophistication means threat actors can utilise them, and can be used for more damaging phishing attacks with synthetic profiles and smarter malware.

Malware developers have already explored the use of code generation with AI, with cyber-security researchers concluding that a full attack chain can be achieved, and is a real and likely threat from bad actors.

The unknown

The full extent of the consequences that could arise from data inceptions from AI technology are yet to be seen. Businesses that hold masses of sensitive information and personal details are high targets, and should understand how their AI stores and shares their data.

Many organisations and even governments use AI for assisted business decision-making, or automated decision-making across multiple business areas and realms. However, AI is not always reliable and a 'human insight' should be explored prior to any proceedings.

THE RISKS AND IMPACT:

- On one-hand **AI can help analyse and detect patterns that indiciate cyber-security threats**. They can also respond promptly by **shutting down infected systems or quarantining malicious files**.
- However, **AI can be used for** more **mature and effective cyber-attacks** such as **phishing attacks or AI based malware designed to evade detection**.
- The use of **data analytics** will have to be **carefully managed** to be in accordance with the Office of the Australian Information Commissioner's (OAIC) Guide to **Data Analytics.**

LOCKTON INSIGHTS

1. AI and data science challenges the established norms of privacy. Boards should reflect on these when adopting AI techniques and how it may affect customers/clients, employees, and other stakeholders.
2. Explore AI and OT security to protect exploitation of AI systems from malicious actors. Data encryption and segemented systems to isolate attacks are key.
3. Insureds should give careful consideration to the benefits and exposures associated with AI, ensuring they address both appropriately with insurers.

6.

Cyber-security minimum standards

Will personal passwords be abolished?

More applications, not just the operating system itself, will start using advanced non-password technologies, such as biometrics, either to authenticate directly or leverage biometric technology, like Microsoft Hello, Apple FaceID or TouchID, to authorise access.

The way we store passwords will also have to be closely considered. It is highly likely that a bit breach could occur in browers that save passwords.

Cyber-security standards have shifted...

Multi-factor authentication invincibility fails

In 2023, experts expect a new round of attack vectors that target and successfully bypass MFA strategies.

Inadequate patching

In 2022, Australian organisations, and even individuals, were indiscriminately targeted by malicious cyber actors. Malicious actors persistently scanned for networks with unpatched systems, sometimes seeking to use these as entry points for higher value targets. The majority of significant incidents ACSC responded to in 2021–22 were due to inadequate patching.

Phishing

Typically cyber-criminals use the same or similar basis to design phishing emails and messages or links to compromised landing pages (known as Business Email Compromised - BEC attacks).

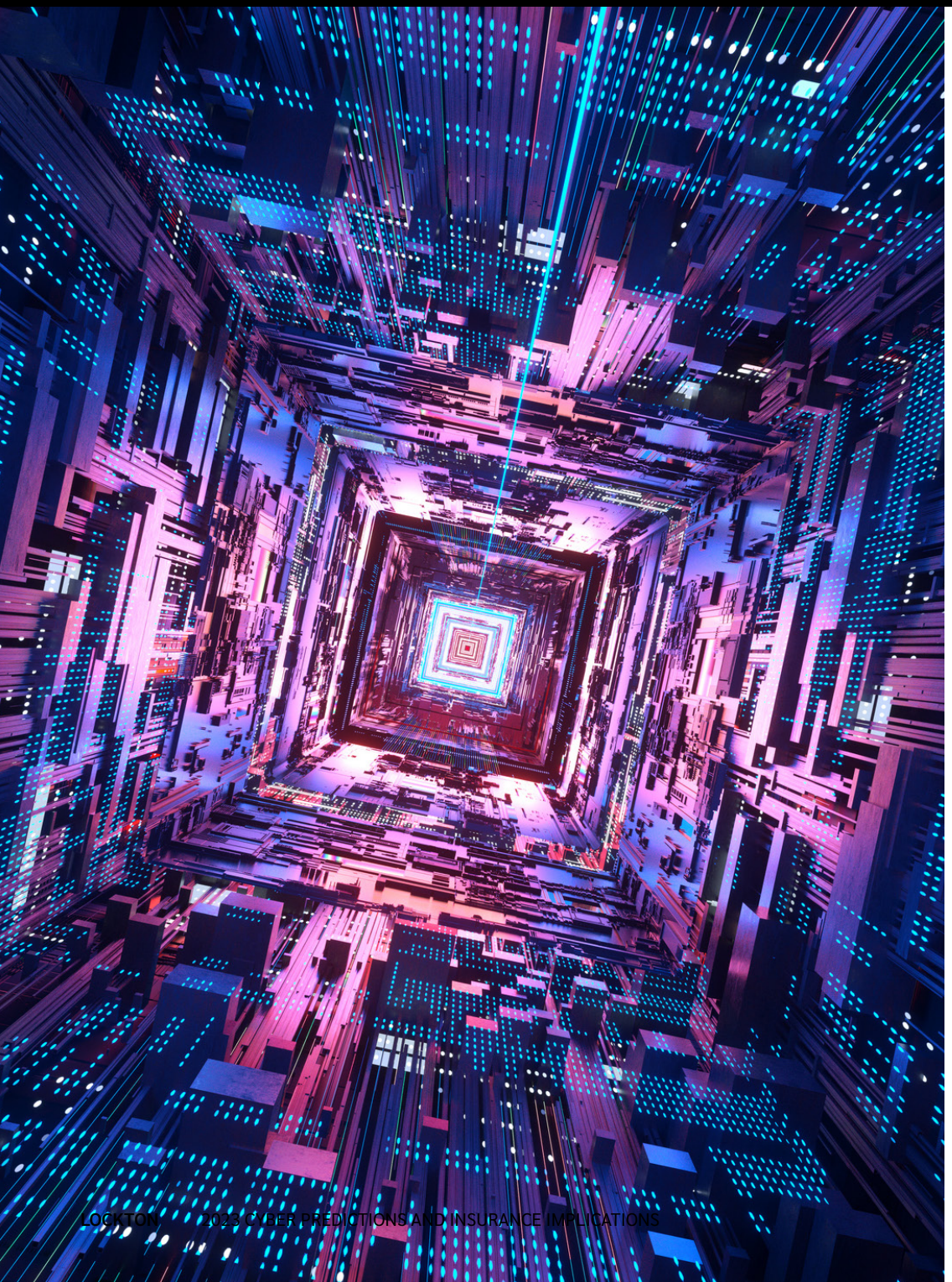
This method can be easily detected by defence systems, so the use of Large Language Models (LLMs) such as ChatGPT can generate varying designs, therefore, being more plausible to appeal to the victim's profile.

THE RISKS AND IMPACT:

- Employee **face-recognition can be hacked/ manipulated** and used for **identity fraud**.
- **Passwords** saved **in browsers are vulnerable**.
- Weaknesses can include **unpatched software or open ports**.
- **Successful attacks** frequently occur in systems where **patches have not yet been applied**.
- **Phishing tricks victims** to open attachments/ **links that contain malicious files**.

LOCKTON INSIGHTS

1. Human error remains one of the biggest cyber-risks, so training and awareness is imperative to an organisation's resilience.
2. Patches should be stress tested frequently.
3. Vulnerability scanning is an automated process that can help identify security flaws that could be exploited.
4. Insured's need to be cognisant of minimum standards of cyber security expected from the cyber insurance market, which may differ from broader industry standards.



Threat actors are recruiting...

Cyber-criminals are establishing their own enterprises.

The cyber-crime business model is underpinned by the same principles as other legal or more traditional business models. One of those principles – perhaps surprisingly to some – is the principle of trust customer experience and engagement. Making engagement, contact, negotiation and payment as easy as possible between victim and threat actor will be an ongoing area of focus for threat actors into 2023.

How will the threat actor customer engagement experience change in 2023?

Grief, a known hacking group, use legitimate research to support their demands for a ransom payment – claiming "the costs incurred from downtime outweigh the average ransom request."

Hackers, such as Grief, are becoming more sophisticated in their approach, using existing PR stategies to either convince victrims to meet their demands, or to attract those within the hacking community to join them.

Will the global Tech/Cyber-Security workforce shortage impact Threat Actors?

There are already advertisements on the dark web calling for 'hacking teams' and 'APT groups' offering attractive and highly competitive packages, inlcuding full-time employment, flexible working arrangements and in some cases, paid sick arrangements and annual leave.

As cyber-crime syndicates operate more like businesses, it is anticipated that more dark web advertisements and recruitment tools will appear, but those tempted by these "gold dusted deals," should be cautious and wary of their employer, as they risk being scammed, framed, and perhaps even prosecution.

Final takeaways...

Despite being around for more than a quarter of a century, cyber insurance continues in a perpetual state of evolution, with rapidly changing underwriting processes, coverage developments, and increased regulatory influence.

A typical update may be in relation to capacity, pricing, supply and demand, and followed by changes to underwriting requirements and some trends in the pure cyber sphere.

But what does this look like for organisations?

Ultimately, organisations need to have an ongoing, focused approach to cyber-risk management.

1. A sound approach should **inform**, **improve** and **insure**.

2. 'Inform' involves, understanding your business operations and aspirations, and is then complimented with the **design of complete enterprise risk strategies** to fit your cyber-security risk management goals.

3. 'Insure' involves **tailored**, **data-driven recommendations** to improve risk posture and build resilience. Finally, and only then, can 'insure' involve **developing an insurance solution** that fits your **individualised risk, potential exposures and targeted goals**. Implement a plan that **protects your balance sheet,** preserves your **reputation** and enables **growth**.

The Cyber Insurance market

In 2023 we foresee;

- Rates stabilising and underwriting discipline continuing.
- Risk transfer demand continuing to increase.
- An ongoing change of underwriting requirements due to an everchanging threat landscape.
- Areas of underwriter focus will be: third party/vendor risk management, staff training, education and culture shifts, and the applicability or war exclusions.

The cyber insurance industry frequently experiences rapid changes within the market, whilst it's still fairly green, it has been around long enough to understand the challenges but not to expect to avoid scrutiny. Insurance has a responsibility within society to protect and address unforeseen events.

Cyber risks are fluid and carry many layers of complexity. The ever-changing developments in technology and software create uncertainty of the risks, and how they might occur. This causes an increasing dependence on key interdependencies. Cyber risk can become a moving target for under prepared (re)insurers.

Cyber insurance now has a proven track record of profitable growth over the long-term and is one of the fastest growing commercial lines of insurance. The reaction to these factors will determine the long-term success of the industry.

Mark Luckin
Cyber Practice Leader

M: +61 433 337 922
E: mark.luckin@lockton.com

global.lockton.com

© 2022 Lockton Companies Australia Pty Ltd. ABN 85 114 565 785 / AFSL 291 954

The contents of this document are provided for general information only. It is not intended to amount to advice on which you should rely and may not necessarily be suitable for you.
You must obtain professional or specialist advice before taking, or refraining from, any action on the basis of the content in this document.