White Paper: A pragmatic approach to Cyber Insurance in 2022

May 2022

Setting the scene

A White Paper is a document that puts forward an argument, grounded in evidence, for a course of action. The desired outcome of a white paper is to challenge or validate the thinking of the reader and ideally this results in action. *Challenge* can initiate new or different actions. *Validation* can enhance confidence in existing actions.

This white paper argues that cyber insurance should only be viewed as a risk management mechanism of last resort in the face of a company ending event.

We build this argument on information from our processes, which are:

- The ongoing conversations and interviews we conduct,
- The collaborative discussions we facilitate within the CISO Lens community, and
- The research we perform to support the decision making of our members.

We submit our argument to you in this white paper for consideration in your organisation's processes and action. Please note that this argument is generic and should be interpreted through the nuances of your organisation's obligations, operations, and policies.

About CISO Lens

For context, CISO Lens exists to support the principal security executives from the largest organisations across Australia and New Zealand. We support these executives through facilitated collaboration with their peers. Our members come from a range of industries, including: banking, electricity generation and distribution, government, healthcare, insurance, logistics, resources, superannuation, technology, and telecommunications. Our listed members represent over 40% of the total market capitalisation of the ASX and NZX.

Importantly for this white paper, data gathered from CISO Lens members is subject to confirmation bias. Our members are only those organisations that consider cyber security to be of sufficient importance that they have a security executive, a security team, and an ongoing security budget. This level of commitment to security is not typical of most companies in the region. Most companies do not have the internal capability to manage cyber security with dedicated resources.

The stunning volume of ransom payments made[1] is a testament to the low capability of most companies in the global market. Many policy holders appear to view cyber insurance as an 'instead of' mechanism to avoid spending on security and take the gamble that they could instead make an insurance claim "if something happens".

[1] "**US Treasury said it tied $5.2 billion in BTC transactions to ransomware payments**", The Record, October 2021. https://therecord.media/treasury-said-it-tied-5-2-billion-in-btc-transactions-to-ransomware-payments/

High level data points on policies

The topic of cyber insurance continues to be of high importance to our members. So, in October 2021, we asked our members for anonymous information on their attitudes toward cyber insurance, and 45 of our members provided information that went into these data points:

- 92% of current policy holders report their premiums increased from the **previous** financial year.
- 85% expect them to increase in the **coming** financial year.
- 55% have already been informed that deductibles in their policy will be increasing in the coming financial year.

Equally as interesting is this observation of the US cyber insurance industry:

> "… in 2021 earned premium growth exceeded the change in incurred losses and the standalone cyber loss ratio improved to 65% from 72% a year earlier."
> - Fitch Ratings [2]

While one better year (65% payouts instead of 72%) does not make a trend, it could be a sign that the insurers are getting closer to a pricing model that is sustainable for them. Or it could be a sign that the exclusions are starting to kick in, and the insurers are proportionately paying out less. (Note that across the global industry, both claims and premiums are *both* increasing. So, more money is coming in, but the insurers had to pay out *proportionately* less in 2021.)

The right answer is likely to be a complex combination of multiple factors, and Fitch Ratings point to the obvious issue with the dynamism of the industry:

> "However, the risk of a systemic cyber incident or several large cyber catastrophes over the near term cannot be discounted, as the frequency and severity of attacks are unlikely to subside and companies continue to expand their digital footprints."

The insurers, looking at their own data on payouts, are unlikely to ease up on premium increases in the near term. Further, the insurers are becoming more discriminating on which companies they will offer policies to.[3] Anecdotally, some of our members report challenges in obtaining a policy, and we hear that some (insurers and/or underwriters) are exiting the cyber insurance market as they do not consider cyber insurance to be good business.

Key point: Both premiums and deductibles are increasing, and will likely continue to increase in the coming years.

---

[2] "**US Cyber Insurance Sees Rapid Premium Growth, Declining Loss Ratios**", Fitch Ratings, April 2022. https://www.fitchratings.com/research/insurance/us-cyber-insurance-sees-rapid-premium-growth-declining-loss-ratios-13-04-2022

[3] "**The ransomware crisis is making cyber insurance harder to buy**", TechMonitor, January 2022. https://techmonitor.ai/technology/cybersecurity/cyber-insurance

Insurers are asking for more data (and, thereby, increasing risk)

Our members report that the questionnaires that insurers provide as part of the policy application process are becoming more granular. This is a mechanism by the insurers to gain a better understanding of the risk they are potentially taking on through offering a policy. Our members tell us that insurers who in the past have sent through dozens of questions are now sending through hundreds of questions.

However, in a perverse twist of incentives, this aggregation of highly sensitive information on policy applicant security postures increases the attractiveness of the insurers as targets for criminals, as well as all the underwriter who may also be provided this sensitive information. [4]

A company's own records may be used against it by the criminals:

> "I've worked cases where they're actually providing a snapshot of your cyber insurance cover page from your own system showing you, 'Hey, you have cyber insurance, so there's no reason not to pay.' "
> - James Turgal [5]

We anticipate that insurers and underwriters will soon need to also provide attestations on their own security posture to provide assurance to their policy applicants and holders.

Key point: Insurers are searching for how best to manage their financial exposure to their customers making policy claims, but despite getting vastly more data the premiums are not plateauing.

Nation states and criminal gangs

The blurry lines between criminal gangs and nation state actors means that the criminals that attack a company may be:

- Employees of a nation state and working with the criminal gang on their own time,
- Under the duress of, and taking directions from, a nation state,
- Working to gather crypto currencies to help a nation state bypass sanctions[6],
- Using stolen technology developed by a different nation state actor[7],

---

[4] "**Insurance giant AON hit by a cyberattack over the weekend**", BleepingComputer.com, February 2022. https://www.bleepingcomputer.com/news/security/insurance-giant-aon-hit-by-a-cyberattack-over-the-weekend/

[5] "**Ransomware claims are roiling an entire segment of the insurance industry**", Washington Post, June 2021. https://www.washingtonpost.com/technology/2021/06/17/ransomware-axa-insurance-attacks/

[6] "**North Korea: Missile programme funded through stolen crypto, UN report says**", BBC, February 2022. https://www.bbc.com/news/world-asia-60281129

[7] "**Exploring the crypt: Analysis of the WannaCrypt ransomware SMB exploit propagation**", Microsoft, June 2017. https://www.microsoft.com/security/blog/2017/06/30/exploring-the-crypt-analysis-of-the-wannacrypt-ransomware-smb-exploit-propagation/

- Themselves under international sanctions. [8]

Any of these scenarios could trigger an act of war or nation state activity policy exemption[9]. You don't know who is attacking you, and the attacker's claims of who they are (or, are not) may not be true.

Key point: There will continue to be a high likelihood that the nature of the criminals behind many attacks will cause nation state and act of war exemptions. If the worst risks a company can face cannot be insured against, it challenges the relevance of cyber insurance. This may drive more companies to self-insure, which will also decrease the amount of customers paying premiums, which decreases the cash reserves of insurers.

Competing forces impacting the cyber insurance market

Cyber security is a 'wicked problem' (a social/cultural problem that is difficult/impossible to solve) largely because it deals with crime (which is, itself, a wicked problem), and crime will endure in the face of evolving technologies.

> "Not only do conventional processes fail to tackle wicked problems, but they may exacerbate situations by generating undesirable consequences."
> - John Camillus [10]

Cyber is a domain where a single security incident can happen simultaneously to one company or thousands, in one region or globally, be immediately obvious in its business impact or only apparent once it is far too late.

Consequently, the cyber insurance industry faces a storm of competing social, cultural and geopolitical motivations which help to create market turbulence.

- The insurance industry has struggled to price its products and manage their own commercial risks through adequate cashflow and reserves.[11]
- The criminals know that many companies will have cyber insurance and, until very recently, cyber insurance would reliably cover ransomware payments[12].

---

[8] "**74% of ransomware revenue goes to Russia-linked hackers**", BBC, February 2022. https://www.bbc.com/news/technology-60378009

[9] "**Cyber War and Cyber Operation Exclusion Clauses**", Lloyd's Market Association, November 2021. https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx

[10] "**Strategy as a Wicked Problem**", John C. Camillus, Harvard Business Review, May 2008. https://hbr.org/2008/05/strategy-as-a-wicked-problem

[11] "**The Cyber Insurance Market Needs More Money**", Tom Johansmeyer, Harvard Business Review, March 2022 https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money

[12] "**Insurers run from ransomware cover as losses mount**", Reuters, November 2021. https://www.reuters.com/markets/europe/insurers-run-ransomware-cover-losses-mount-2021-11-19/

- Further, data is emerging that companies with a cyber insurance policy are twice as likely to pay a ransom as the companies without one[13]. If this metric is further validated, the insurers cannot ignore it and will be compelled to act to further reduce their financial risks.

Many in the cyber security industry argue that payment of ransoms by insurers, as part of a cyber policy, has acted as an additional economic incentive for the criminals and fuelled the ransomware scourge. This was not the intention of the insurers, but it shows the wickedness of this problem and, anecdotally, insurers are now starting to carveout ransomware costs entirely – not just payments – from their policies.

Several members have noted to us that a ransomware attack is the primary risk their company faces from the cyber domain, and so an insurance policy that does not cover ransomware has minimal real-world value.

Key point: Crime will not go away, and cyber insurers face the significant problems of trying to ameliorate the risks, and associated costs, of a wicked problem which has no solution.

Bringing it all together

Insurers are in their own version of the metaphorical used car 'market for lemons' dilemma. The insurers, like buyers of used cars, are struggling to determine which organisations – metaphorically – are the sellers of well-maintained cars, and which organisations are a risky proposition (the sellers of poorly maintained cars that may be more likely to have an incident).

Insurers are turning down the dial on the level of financial risk they are assuming. Premiums, deductibles, obligations, exclusions, and the number of underwriters in a policy, are all increasing.

These factors are designed to help the insurers determine which customers are serious about covering only the 'black swan' events that the policy holders are working to prevent, and which of these customers are trying to transfer the risk of their organisation's sloppy practices and/or underinvestment to the insurer.

- A customer that only wants cover in case a low probability but high impact catastrophe strikes is likely to be making better risk management choices. These customers are more likely to want to take their fate in their own hands and maintain a policy just in case.
- Whereas, a customer that wants an expansive policy may be tacitly admitting that they think many things could go wrong and want someone else to wear the cost.

There is also a third category of organisation, those that self-insure.

---

[13] "**How Insurers Play a Big Role in Spurring Cybercrime**", Barron's, October 2021. https://www.barrons.com/articles/ransomware-attack-cyber-insurance-industry-51633075202

Self-insurance

Anecdotally, some non-security executives are saying they are considering self-insurance in cyber, but what they really mean is that they want to take the chance that nothing happens. But hope is not a strategy and investors will frown on this approach.

So, self-insurance can be a fancy way of saying 'we'll wing it', but it can also be an informed and conscious decision from highly capable company executives.

Many security executives see what their company treasuries are paying in premiums and wish they could instead put that money to additional prevention. This approach has much in its favour, as prevention is likely to be vastly cheaper (in terms of: money, opportunity cost, business interruption, stress, staff turnover, additional regulatory attention, public goodwill, being used as a case study of what not to do) than recovery.

In that vein, the two quotes below are from executives who have run the numbers and chosen to self-insure.

> "We (myself and the Chief Risk Officer) pushed the self-insurance option … we put aside the money and invested it for growth. I'd argue that due to the cost and exemptions coupled with the coverage of other insurances, self-insurance is not a bad commercial/risk option."
> - CISO Lens member

Another member commented,

> "Pricing for insurance to be palatable must be lower than the equilibrium point between the marginal value of the insurance and the marginal value of a relevant preventative measure. At or above this point clearly it is better to place money on some combination of self-insurance and additional prevention."
> - CISO Lens member

These two executives are helping their respective organisations make the conscious and financially pragmatic decision to self-insure, and they are not alone.

It's also worth noting that self-insurance is common for government. Can you imagine the kinds of premiums needed for a policy that could provide the recovery costs of a key public service - such as a nation's tax or social services – rebuilding after a bad cyber incident?

So, clearly, there are organisations with significant capability and operational maturity that run the numbers and know that the cost of cyber insurance does not stack up against their own need – and fiduciary duty – to take responsibility for their own security and resilience.

Conclusion

We argue that the ideal position is to self-insure as much as possible, by consciously committing to a strategy of prevention and resilience in a manner commensurate with the risks your company faces.

The journey toward genuine self-insurance is the path toward operational maturity and better risk management. By genuine self-insurance, we mean; informed, conscious, accompanied by a strategy of prevention and resilience and, potentially, even reserving funds in a Captive Insurance Company[14] for a future rainy day.

As we wait and see how the viability of the cyber insurance market plays out in the coming years, it may make sense to have a policy as your last line defence, in case the absolute worst happens. But *relying* on cyber insurance is not pragmatic. As the cyber insurance industry stand now, there's a chance that your claim:

- May be excluded due to the nature of the criminals (notably, ransomware).
- Will not cover the full cost of the incident.
- May result in your insurer suing you to avoid payment[15].
- May require you suing your insurer to get payment[16].
- May be too late, as a major industry wide incident has already emptied the coffers of your insurer and their reinsurers (an extreme possibility, but one alluded to by Fitch Ratings[17]).

Given the points covered above, we consider that the most pragmatic path forward in this market is to view cyber insurance as a safety net of last resort. Lift your own deductibles as high as practical (in order to minimise premiums), and then only seek to make a claim against your cyber policy in the eventuation of a company ending incident. Pay as little as you can, and plan to use it only once.

The hard truth is that being able to make an insurance claim is a Pyrrhic victory. Your life, and the lives of your staff, your customers, and the myriad of stakeholders in the complex ecosystem that your company receives value from, and delivers value to, would all be easier if the incident that you could make a claim for was, instead, avoided in the first place.

We advocate for a risk-driven approach to allocate commensurate resources to reduce the frequency, duration and business impact of any incidents.

---

[14] "**What Is a Captive Insurance Company?**", Investopedia, December 2020. https://www.investopedia.com/terms/c/captive-insurance-company.asp

[15] "**Sony insurer sues to deny data breach coverage**", IT News, July 2011. https://www.itnews.com.au/news/sony-insurer-sues-to-deny-data-breach-coverage-264430

[16] "**Merck's $1.4 Billion Insurance Win Splits Cyber From 'Act of War'**", Bloomberg Law, January 2022. https://news.bloomberglaw.com/privacy-and-data-security/mercks-1-4-billion-insurance-win-splits-cyber-from-act-of-war

[17] "**US Cyber Insurance Sees Rapid Premium Growth, Declining Loss Ratios"**, Fitch Ratings, April 2022. https://www.fitchratings.com/research/insurance/us-cyber-insurance-sees-rapid-premium-growth-declining-loss-ratios-13-04-2022

About CISO Lens

We collaborate. Peer driven research for cyber security governance

CISO Lens is the peak body for cyber security executives from the largest organisations in Australia and New Zealand.

Our mission is to support the cyber resilience of Australia and New Zealand. We work toward this mission through:

- Peer networking,
- Structured collaboration,
- Information sharing, and
- Benchmarking.

A key driver for the creation of CISO Lens was the recognition that cyber risk is a business issue that can be most effectively addressed through collaboration across organisations and industries.

The structures, set out above, enable evidence-based decision making around strategy and resource allocation. The goal is to support governance and informed decision making, resulting in a commensurate response to cyber risks.

www.cisolens.com