THE AUGUSTA GROUP

# **Cyber insurance:** Thought leadership. Stabilizing the oversight and assurance of cyber-risk for the purposes of insurance and reinsurance underwriting.

## Bringing stability to insurance oversight and assurance.

January 2022

## Why do companies need to manage cybersecurity?

Cyber is the biggest non-financial risk faced by nation states and their governments outside of climate change and global systemic risks such as COVID 19. The World Economic Forum (WEF) report on 'Global Risks 2021 16th Edition[1]' identifies cybersecurity failure as a top 7 global risk. The WEF March 2021 report on 'Principles of Board Governance of Cyber-risk[2]', identified cybersecurity failure as a top 4 short term (0–2 years) risk behind infectious disease, livelihood crisis and extreme weather events for the board room. The political and economic impact of cyber-attacks can be broad and deep when targeted at Critical National Infrastructure (CNI). Cyber-attacks have become a geopolitical weapon that can impact the security of nations, their critical infrastructure and weapon systems. Cyber-attacks result in the loss of Intellectual Property (IP), the destruction of digital assets, damage to brand and reputation, impact competitive advantage and national security.

There is an increased blurring between cyber criminals, nation-state threats, state sponsored actors, hacktivist, and script kiddies. The well documented 2010 Stuxnet attack was the first visible demonstration of a nation-state led cyber-attack on Iranian nuclear facilities, targeting operations technology and repeated in 2021. The Sony pictures hack in 2014, Not-Petya in 2017, several significant hacks against US municipalities, the 2020 SolarWinds hack, the 2021 Microsoft Exchange, Colonial pipeline, JBS meat and the more recent Kaseya hack demonstrate the challenges which nation states and their companies face with respect to cyber. As attacks aimed at governments spill over to impact the private sector and attacks aimed at the private sector spill over into society.

Cyber-attacks can be highly orchestrated using scripting, leveraging AI and machine learning, indiscriminate or targeted. The result of a cyber-attack can be as broad as the organisations supply chains, data, assets, processes, products, services, markets, cyber maturity, and environment of operation (on-premises, cloud, hybrid-cloud). The impact of a cyber-attack can be unique to each organisation, being dependent upon:

- The organizations physical and digital perimeter.
- The complexity of the products and services an organization manufactures and services.
- The number of people a company employs and the number of IT assets they use.
- The organization's dependence on digital products and services.
- The maturity of the cyber threat the organization faces, which can be a nation-state, cybercriminal, hacktivist, or script kiddie.
- The size of the balance sheet.
- The maturity of its cyber-risk and cybersecurity program.
- The reconnaissance a hacker has undertaken on the organization.
- The regulatory environment in which the organization operates.
- The environments of operation and transnational data flows.

Traditional rules of engagement do not apply to cyber. The cyber adversary is not usually seen and is rarely identified and the geographic location of a cyber attacker is difficult to identify. Their target can be indiscriminate or specific and the attacker can range from well-funded nation states to school kids buying hacking as a service (HaaS) attack from their bedroom. In July 2016 NATO formally recognised cyberspace as a domain of operation, reaffirming in April 2021 that cyber defence is part of NATOs core task of collective defence[3]. With conventional offensive and defensive fields of operation, skirmishes are localised between nations and geographies. Cyberspace has no physical national boundaries and geographies are created by communications equipment. A nation state can launch a cyber-attack on an adversary 10,000 miles from their physical location, without spending the fuel bill of a single F35 mission. Nation states can use their own offensive capabilities or those of proxies, and an attacker can be in the office for 9am, home by 5pm, or be at work at 3am. Cyber tools developed by nation states can fall into the hands of cyber criminals and be used to launch attacks on commercial enterprises. Commercial enterprises that include CNI, retailers, construction, pharmaceuticals, defence contractors and manufacturers that are invariably private sector companies. Where governments have little influence over their security posture, that is managed by market forces.

Society relies upon states to protect it and manage conventional offensive and defensive capabilities. Spending significant amounts of money on physical deterrents such as Armies, Navies, and Air forces. Cyber is a new domain of operation and nation states are building up their offensive cybersecurity capabilities, with little regard to effective national defensive cyber strategies. As a global community we depend upon cyberspace to

provide the goods and services that we use daily, and currently governments lack the capability of managing and enforcing the appropriate level of defensive cyber protection across the public and private sector.

## Cyber is no longer a 1 in 100-year event.

The cyber-risk paradigm has changed significantly over the past 5 years. Cyber-related incidents could be considered 100-year, 'black swan' or *extreme loss* events, they are now a regular occurrence. Over the past 5 years cyber-attacks have increased in frequency, complexity, and severity[4]. The likelihood of a cyber-attack is much closer to '1' than '0' (probability of 1, it will happen). Cyber is a risk that companies cannot ignore, and following recent announcements by the insurance industry, cyber maybe a risk that will become increasingly difficult to mitigate through insurance alone. Forcing the cyber-risk mitigation pendulum to swing towards the risk owner and away from cyber insurance and reinsurance companies that are finding it difficult to economically underwrite the risk.

Recent developments in cyber-attacks and ransomware create complex challenges for the insurance industry, and the public and private sector organisations that own cyber-risk. For many organisations cyber-attacks have moved from an *extreme loss event*, with low probability and high impact to an *unexpected loss* and closer to an *expected loss event*. Creating challenges for organisations and insurance companies[5,6].

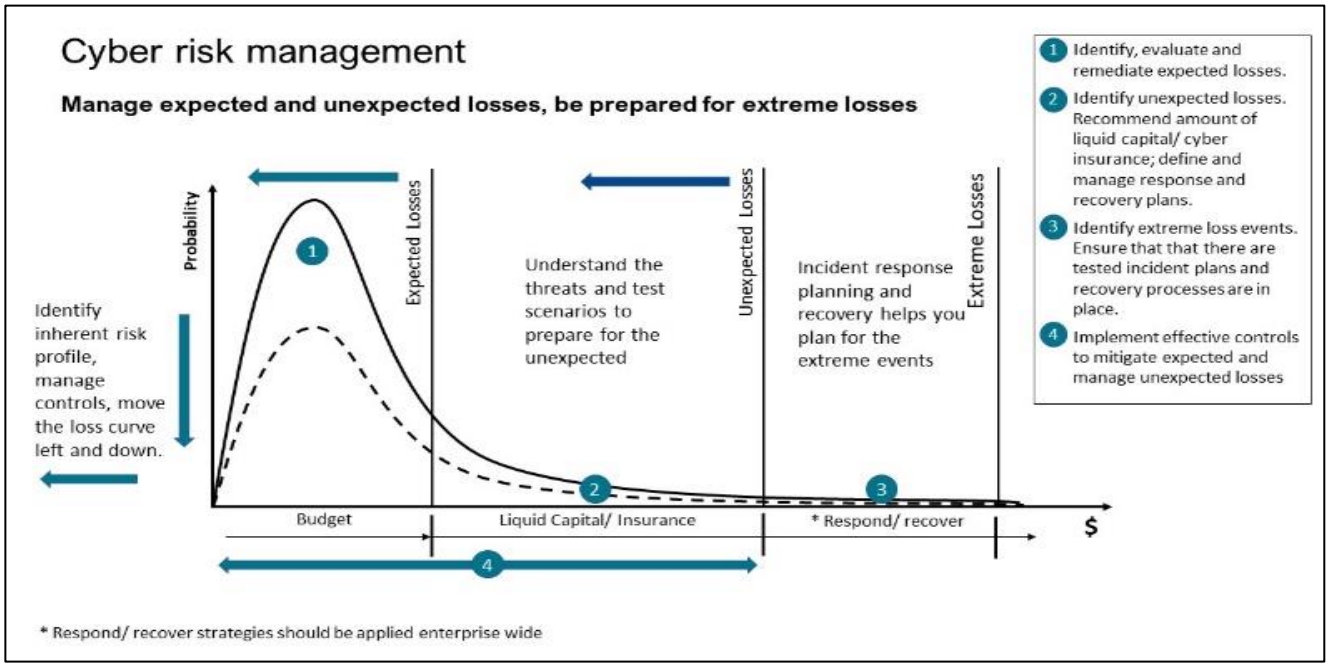


**Figure 1:** Expected, unexpected and extreme losses.

Organisations should have a view of their expected, unexpected, and extreme losses, and manage them accordingly. Pricing in *expected losses*, mitigating *unexpected losses* through additional capital or insurance, and using incident response and where appropriate government intervention to manage *extreme losses*.

However,

- Cyber is no longer an *extreme loss* event. Cyber-attacks are increasing in frequency, complexity, and severity. The volume of ransomware attacks has quadrupled during the pandemic, from around 15 million attempts a month in 2019 to over 75 Million a month by quarter 2, 2021[7]. With an average global increase in cyber-attacks of 29%, in the first half of 2021 year on year[8].
- The cost of ransomware has increased. The average payment made by US companies that decided to pay a ransom in the first quarter of 2021, was up more than 400% from FY2019. The average cost of remediation rose to $1.85 million in 2021 from US$700,000 in 2020[5].
- Cyber insurance premiums rose between June 2020 and June 2021, spiking by 32% higher[5].
- Financial markets are paying close attention to cybersecurity risk following recent high profile cyber-attacks, felt through brand reputation and shareprice[9].
- The US is legislating cybersecurity and setting the groundwork for cyber regulatory enforcement[10,11].

To understand cybersecurity risk management, it is important to understand risk management principles. The risk equation requires an understanding of an organization's inherent risk profile, an assessment of control

design and effectiveness, and an understanding of residual risk in line with an organisations risk appetite. Inherent risk is an assessment of the worst case untreated risk that an organisation faces. For example, in the event of a ransomware attack, what is the worst-case impact to an organisation without doing anything to reduce the likelihood or mitigate the severity of an attack.

Control design, implementation and effectiveness testing is a critical component of organisational risk management. An organisations controls detect, prevent and correct external and internal cyber threats and vulnerabilities. Before they have a significant and costly impact to an organisation. That requires additional capital, cyber insurance, and an incident response plan to mitigate. Control design, effectiveness testing and on-going control management is the largest cost for managing cyber-risk. As an example the NIST SP 800-171 cybersecurity control standard, required by the DoD under DFARS 252.204-7012, regulates the implementation of 110 cybersecurity controls across 17 security domains. Cyber control implementation is now a focus of US regulators that reference the management of cybersecurity frameworks such as NIST SP 800-53[12] or NIST SP 800-171[13] as requirements for Federal regulations including the Federal Information Security Modernization Act (FISMA), Office of Management and Budget (OMB-A130) and DoD DFARS procurement regulations.

Residual risk is a measure of an organisations risk when it accounts for the effectiveness of its controls for the management of inherent risk. Risk management aims to effectively manage the residual risk profile of the organisation through an understanding of inherent risk, and the effective application of appropriate controls (Figure 1). To manage residual risk to a level that an organisation accepts, in line with its appetite for risk. Risk appetite is the level of risk an organisation is willing to accept. The lower the risk appetite the more complex and expensive it is to manage cyber-risk.

## Market forces are not working to manage public or private sector cyber risk.

The impact of cyber-attacks on the public and private sector has increased in line with our consumption of data and reliance on technology. The public and private sector has increasingly relied on market forces and cybersecurity products and services to manage cyber-risk. The cybersecurity market is expected to reach $150Billion globally in 2021 and could reach $400Billion by 2027[14]. However the impact of cyber-attacks does not show any signs of reducing despite the cyber spend. While many of the measures are difficult to quantify precisely, the impact of cyber-attacks is difficult to ignore.

- Ransomware is the predominant cyber threat confronting businesses of all sizes today, and cyber-attacks are increasing year on year[4,5].
- The AV-test Institute registered 1.13 Billion new Malicious and potentially unwanted applications (PUA) in 2020, an 11% increase on 2019 and 240% on 2015[15].
- In 2019, 93.6% of malware observed was polymorphic, meaning it has the ability to constantly change its code to evade detection[16].
- Malware increased 400% and ransomware 435% in 2020 compared to 2019[17].
- Bad Botnets accounted for 25% of all internet traffic in 2020[18].
- Lloyds of London is rumoured to have recommended that its syndicate members reduce their cyber insurance exposure 2022[6].

Cyber spend is increasing and the frequency, severity, complexity, and cost of attacks is also increasing. The impact of the increase in cyber-attacks is demonstrated by the many examples of reported incidents. With notable supply chain attacks reported in 2020 and 2021, with many more attacks on critical national infrastructure, manufacturing, retail, defence, and healthcare providers (www.hackmageddon.com[4]). While cybersecurity has been left to market forces to manage, it is clear that this approach is no longer working. Regulators in the US are focusing on cyber regulatory enforcement and legislation[10] to address identified failures in the public and private sector to manage cybersecurity. With Federal government adopting regulatory enforcement programs for cybersecurity through the Department of Justice (DoJ)[20] and Treasury (DoT)[21]. The DoD DFARS and CMMC cybersecurity program mandate cybersecurity practices are implemented for the protection of controlled unclassified information (CUI) before contract award. FISMA requires all Federal Agencies to implement a risk-based approach to the management of cybersecurity, with legislative proposals put forward in 2021, to align Federal cybersecurity oversight and assurance under the Department of Homeland Security (DHS).

## Cyber is a dynamic risk, making it a difficult risk to insure

Most organisations do not understand cyber-risk, and have not been prepared to address the impact of a cyber-attack, the adage that 'it won't happen to me' remains true. Cyber is a very profitable business for cyber criminals, the 90%-plus profit margin from ransomware attacks in 2021 has been likened to the gains Colombian cocaine cartels made in 1992[6]. Cyber is an expensive risk to manage, and rightly boards look for a 'Return of Investment (RoI)' that invariably does not exist or is palatable for a board table. While it is fair to say that only significant cyber events make the media, a simple review of major cyber-attacks reported over the past 10 years, demonstrates that the ROI becomes a meaningful conversation after the event, rather than before. When the costs of the incident quite clearly demonstrate that it is far cheaper to manage the risk prior to the attack, than deal with its fallout. (Norsk Hydro, Maersk, Merck and Equifax).

The 2017 Equifax data breach resulted in up to $700Mn in fines, $380Mn to settle class action lawsuits and a further $1Bn in court imposed incident remediation costs. The credit rating agency Moody's downgraded Equifax in 2019 due to concerns relating to the longer-term cash flow impact of the hack. The impact of the 2019 Norsk hydro ransomware attack was at least $52Mn. The global cost of the 2017 Not Petya cyber-attack has been estimated between $4Bn and $8Bn, and companies that included Maersk reported losses of around $300Mn and Merck of over $800Mn.

Cyber has proven to be a dynamic and agile risk, adapting to global economic conditions. It has been considered a 'black swan' event when the reality is it is not, and is a risk that is much closer to an 'expected' event and should be managed as such. Cyber-risks and their impact are unique to every organisation. All organisations are impacted by unique factors that include the products, services, geographic locations, operations, technology, people, processes, regulatory environments, controls with varying degrees of effectiveness and threats. Managing cyber-risk requires an understanding of these factors, how external and internal threats impact vulnerabilities within the organisation, and how these create risks to the organisation that need to be managed. Cyber-risk management is a dynamic process that changes as an organisation's strategy, products and services, operations, processes, technology, and external threats change.

A review of international cybersecurity standards such as ISO 27001, NIST SP 800-53 or NIST SP 800-171, detail the complexity of cyber-risk management. Table 1 outlines the cybersecurity domains documented by NIST SP 800-171 and required by affected global defence contractors for contract award under DFARS 252.204-7012. In this case NIST SP 800-171 requires the implementation of 110 cybersecurity practices, across the 17 domains.

| NIST SP 800-171 cybersecurity domains | | | | |
|---|---|---|---|---|
| Access Control (AC) | Asset Management (AM) | Audit and Accountability (AU) | Awareness and Training (AT) | Configuration Management (CM) |
| Identification and Authentication (IA) | Incident response (IR) | Maintenance (MA) | Media Protection (MP) | Personnel Security (PS) |
| Physical Protection (PE) | Recovery (RE) | Risk Management (RM) | Security Assessment (CA) | Situational Awareness (SA) |

**Table 1:** NIST SP 800-171 cybersecurity domains[13]

## Cyber is poorly regulated, but further legislation and enforcement is planned in the US

The increase in cyber-attacks in the US is now the focus of cyber legislation and regulatory enforcement. The US President signed Executive Order 14017 (Americas Supply Chains, February 2021)[21] initiating reviews of current Supply Chain Risk Management (SCRM) and cyber capabilities across Federal Agencies. Executive Order 14028 (Improving the Nation's Cybersecurity)[22] was signed in May 2021 and sets out a range of activities for the Federal Government to assess, recommend, and improve the protection of US National Security. Quarter 3 and 4 2021 has seen a significant drive in the US to develop and pass cybersecurity legislation and implement regulatory enforcement, including.

### Regulation.

- The US adopted the Federal Information Security Modernization Act (FISMA) in 2002, updated in 2014 and legislation has been proposed to update it in 2021.
- DFARS 252.204 - 7012 was regulated by the DoD in 2017 requiring cybersecurity to be implemented by their Defence Industry Based (DIB) Globally. Updated in 2020 (DFARS 252.204-7019 and 7020).

**Legislation introduced across the US House of Representatives and Senate – 2021.**

In process.

- Cybersecurity Maturity Model Certification (CMMC).
- FISMA (2021).
- H.R 3684 - Infrastructure Investment and Jobs Act.
- H.R. 5440 - Cyber Incident Reporting for Critical Infrastructure Act.
- S. 2407, Cyber Incident Notification Act – NB Requires the reporting of cyber incidents to CISA. (S. 2875, Cyber Incident Reporting Act – NB Sets-up Cyber incident review office in CISA)
- S. 2943, Ransom Disclosure Act.

Planned.

- Security and Exchange Commission (SEC) – Cyber-risk Governance

**Cyber Enforcement.**

- Department of Justice (DoJ).
  Civil fraud Initiative (October 2021) and the utilization of the False Claims Act (FCA) to pursue companies, that are government contractors who receive federal funds, when they fail to follow required cybersecurity standards.
- Department of Treasury (DoT).
  Cyber Ransomware payments and OFAC (Office of Foreign Asset Control – October 2021) – requiring the reporting of Ransomware attacks to Federal Agencies and OFAC.
- Securities and Exchange Commission (SEC).
  Existing market regulation requires the reporting of material risks to the SEC.

Changes in US cyber regulatory enforcement and proposed legislative updates in 2021, are setting a new direction for cybersecurity risk management across US Federal, State, Local and Tribal Government. The November 2021 Infrastructure Bill signed $1Trn, for improvements across several critical national infrastructure domains including road, rail, energy, water, and telecommunications. The bill sets out deliverables for cybersecurity to secure US supply chains, and initiating a clear agenda for the regulation of cybersecurity across the public and private sector. The Security and Exchange Commission (SEC) is planning 'Cyber-Risk Governance' legislation, that is expected to complement their program of cybersecurity oversight and assurance of public companies. That started in 2017 with the establishment of their cyber enforcement unit.

## Underwriting cyber insurance requires certainty and stability

It is often referenced that there is not enough historical data to price cyber insurance appropriately. As is the case with categories including life, health, car, or house insurance, where the insurer and insured can clearly articulate the risk that is being mitigated by insurance, in a well-defined and manageable envelope. Supported by historical data for example associated with age, location, crime statistics and accident rates. Using specific and clearly articulated standards such as an MoT certificate, type of door locks and health certificates to validate compliance.

Even with all of the data available to an underwriter, cyber is a difficult risk to price. Cyber is dynamic, evolving and unstable, it is not predictable and is difficult to assess and manage. Cyber is a risk that is influenced by many factors within the control of the insured and many that are not. While an organisations inherent risk is straight forward to calculate, the challenge for both the insurer and insured is the evaluation of an organisations control design, and effectiveness. That is used to reduce the inherent risk to an appropriate level for pricing that is fair for the insured and insurer.

For cyber insurance to be an effective proposition for both the insured and insurer, there needs to be certainty that cybersecurity is, and can be managed. Certainty for the insured in terms of their ability to understand and manage cyber-risk, and its impact on financial statements and shareholder value. By implementing the appropriate number of cybersecurity controls, as defined by an agreed cybersecurity standard or framework. Certainty for the insurer who needs to be able to place an acceptable level of oversight and assurance over the insured. For example assessing the insured's compliance to internationally agreed standards, following a similar approach to existing insurance products. Collecting independent attestation to cybersecurity compliance, and in some cases evaluating real time compliance in line with the dynamic nature of cyber-risk management.

Cyber-risk can be managed so that insurers can have confidence that organisations understand and are managing their cyber-risks. This can be delivered using existing standards such as ISO 27001, NIST SP 800-53 or NIST SP 800-171. Enabling both insurers and the insured to assess cybersecurity compliance to an agreed acceptable level. The insurance industry can implement a road map over a number of years, to build up cybersecurity maturity, oversight, and assurance (Figure 2). That includes self-attestation, certified oversight, and assurance and continuous diagnostic monitoring (CDM).

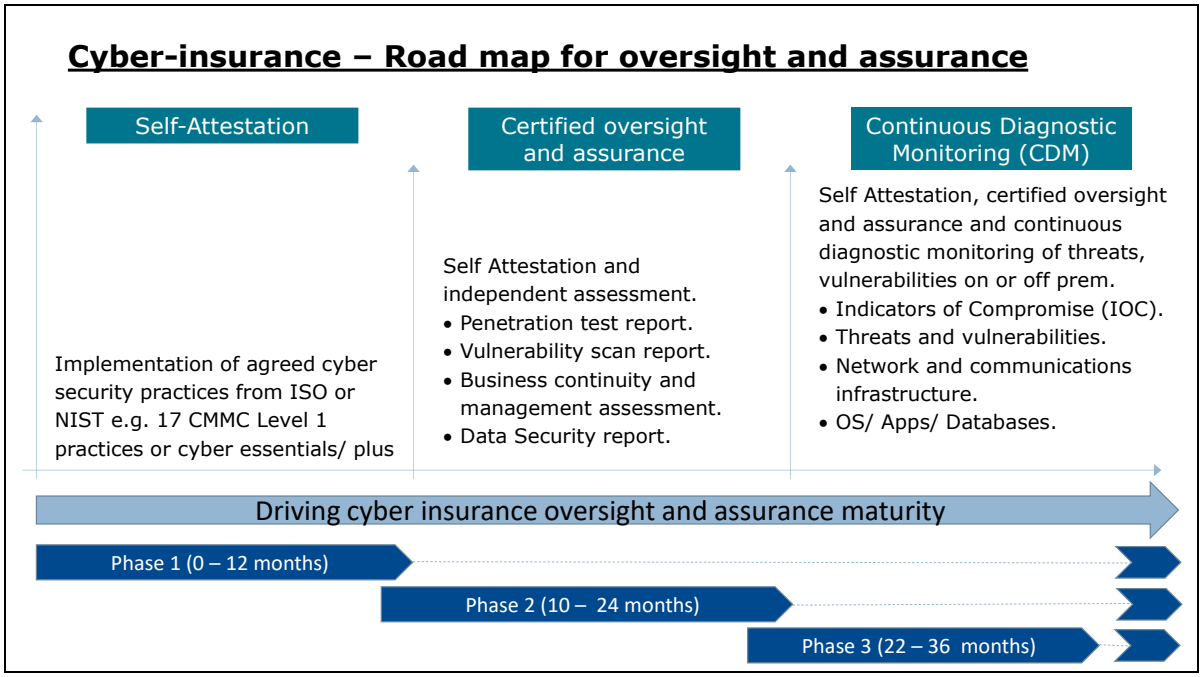


**Figure 2:** Road map to improve cyber insurance certainty, stability oversight and assurance

### Self – Attestation

Assessment of cyber-risk management to an agreed international cybersecurity standard.

- The insurance industry identifies cyber-security practices, in line with local, regional or international cybersecurity standards, setting the expected controls for cyber compliance. Adopting the model that is used by the US Department of Defence, requiring global defence contractors to self-attest to their compliance to NIST SP 800-171 cybersecurity requirements, under DFARS 252.204-7012.
- The use of smart contracts for the delivery of cyber insurance, and the submission of compliance assessments. To provide integrity over the self-attestation process.

### Certified oversight and assurance, (plus Self - Attestation)

Approved certification of critical cybersecurity assessments based upon potential financial exposure. That could include.

- Penetration test.
- Vulnerability scans.
- SoC reports.
- ISO 27001 or NIST SP 800-171/ 53 assessments.
- Cybersecurity risk assessments in line with industry sector threats.

### Continuous Diagnostic Monitoring (CDM), (Certified oversight and assurance)

Real-time situational awareness data to validate control effectiveness. Intended to reduce the inherent risk to an acceptable residual level.

- An agreed suit of appropriate controls data to be identified, collected, and analysed by an agreed third party.
- Real time monitoring of critical infrastructure including networks and communications endpoints, applications, databases, mobile technology.
- On-site monitoring and reporting of Indicators of Compromise (IoC).
- Data consolidated by a consortium of insurance companies. Allow for the movement of organisations between insurance providers and the opportunity for insurers to evaluate potential customers. i.e. a FICO score, anonymised to protect client confidentiality.

- Adoption of smart contracts for the delivery of cyber contracts and submission of compliance assessments to provide integrity over the self-insurance process.

Implementing a road map to provide oversight and assurance, and creates both certainty and stability for the cyber insurance industry and those insured. It sets clear expectations for compliance in line with regulation, legislation, and enforcement. Using the oversight and assurance of cyber-risk being adopted by legislators as a tool to enable more effective cyber insurance. Balancing the relationship between the insurer and insured, and enabling greater accountability of cyber-risk management by boards.

## Conclusion

Cyber is a complex, dynamic, and unstable risk, making it a difficult risk to manage for many organisations and a difficult risk to insure. This is demonstrated by the number of successful cyber-attacks that have been publicised over the past 12 months, including SolarWinds, Colonial Pipeline, Kaseya and JBS meat. The development of cybersecurity as a Nation state weapon has made cyber an effective tool used by Nations, their proxy's, and cyber criminals to target both public and private sector organisations.

Market forces alone have failed to meet the challenge of managing cybersecurity, best demonstrated by both the increase in the cybersecurity spend and the failure to decrease the number of successful cyber-attacks, despite the sums of money spent. With cybersecurity spend and the number of successful attacks increasing at a similar pace, the solution that seems to be adopted by US government and other governments is one of regulation. Since 2002 Federal risk management for government departments and their contractors has been regulated under FISMA. The DoD is regulating DIB contractors under DFARS, requiring the implementation of NIST SP 800-171, and the Securities and Exchange Commission (SEC) plan to regulate 'Cyber-risk Governance'.

Other potential influences on the direction of cybersecurity came in the form of Executive orders signed in February and May 2021, focusing on Supply Chain Risk Management (SCRM) and the Nations Cybersecurity. Proposed legislative modifications to FISMA (2021) aim to give the US Department of Homeland Security (DHS) greater control over Federal cybersecurity, standards and increase incident reporting requirements.

Compliance to these existing regulations is taking shape through increased enforcement by the Department of Justice (DoJ). That announced its intention to develop a Cyber Enforcement regime, focusing on the compliance to cyber standards by Federal contractors, enforced under the False Claims Act (FCA). The Department of Treasury (DoT) is enforcing oversight of ransomware payments under OFAC (Office of Foreign Asset Control), that has severe penalties including $1m per breach and up to 30 years in prison.

Cyber is a very complex risk to manage impacting an organisation's financial statements, both 'top' and 'bottom' line. The bottom-line costs including implementation, remediation, on-going maintenance, requirements for monitoring and potential legal ramifications of a cyber event, that include regulatory fines or civil action. Top line figures that include lost sales during the attack and the potential brand and reputation damage post incident. Yet unknown in light of what could be developed by the SEC for cyber-risk governance, are impacts associated with material risk misrepresentation, restatement of financial reports and close regulatory oversight of cyber-risk governance.

All of these factors make it challenging for insurers to properly price, insure and reinsure cyber-risk. Demonstrated by the losses incurred by insurers between 2019 and 2020, as ransomware attacks have increased in frequency, complexity, and severity. Resulting in insurance companies re-evaluating their participation in the cyber insurance marketplace. Unfortunately for many companies, cyber insurance is the only mechanism available to manage *unexpected losses* from events such as ransomware. An absence of this risk treatment will have long term ramifications on the balance sheets of companies with high levels of exposure to cyber threats. Requiring companies to self-insure, that in turn reduces the capital available to manage and implement the controls that will reduce the impact of a cyber-attack.

Cyber insurance will become viable again if the insurance industry can stabilise the risk, and its exposure to loss. This can be accomplished by establishing a baseline of performance through the adoption of cybersecurity controls by organisations, and having the necessary oversight and assurance of compliance. There are other examples of insurance classes where requirements for coverage are set including house, car, commercial

property that require compliance to set standards for insurance. There are numerous cyber standards the insurance industry may choose to apply.

Pricing of insurance could function dependant upon the level of oversight provided to the insurance companies, similar to that adopted for young drivers and their driving habits. The more data that the insured provides regarding the effectiveness of controls the greater the premium discount. Adopting a phased approach through self-attestation, certification, and continuous diagnostic monitoring (CDM) of cybersecurity oversight and assurance. The insurance industry can incrementally adopt a standard in line with Government and industry to manage cyber-risk, as is the case for other risk categories.

The insurance industry has an opportunity to influence cybersecurity in a manner that governments are not able to do without regulation. Using market forces to improve compliance through recognised cybersecurity standards, or newly defined benchmarks for cybersecurity established by the insurance industry. This is a moment for the insurance industry to demonstrate leadership and leverage its knowledge and experience in managing risk to help solve some of the issues around protection of critical national infrastructure.

## References

1. World Economic Forum: The Global Risks Report 2021(Jan 2021) http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
2. World Economic Forum: Principles for Board Governance of Cyber-risk (March 2021) http://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021.pdf
3. NATO recognises Cyber domain: https://www.nato.int/cps/en/natohq/topics_78170.htm
4. Hackmageddon global cyber incidents: https://www.hackmageddon.com/2021/11/02/q3-2021-cyber-attacks-statistics/
5. The cost of a cyber-attack: https://www.insurancebusinessmag.com/us/news/cyber/global-cyber-insurance-pricing-spikes-32--report-259795.aspx
6. Lloyds cyber-insurance: https://www.reuters.com/markets/europe/insurers-run-ransomware-cover-losses-mount-2021-11-19/
7. Ransomware attacks rise (FT July 2021): https://www.ft.com/content/c8c7630f-86f8-453f-a664-3fb5401bcb2a
8. Rise in ransomware in 2021: https://www.computerweekly.com/news/252504676/Ransomware-attacks-increase-dramatically-during-2021
9. SEC focus on cyber: https://corpgov.law.harvard.edu/2021/07/25/sec-increasingly-turns-focus-toward-strength-of-cyber-risk-disclosures/
10. Bloomberg law – Advancing US cyber legislation: https://news.bloomberglaw.com/privacy-and-data-security/cyber-agency-resists-regulator-role-as-bills-aim-to-expand-power
11. DOJ Civil Fraud initiative: https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative
12. NIST SP 800-53: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
13. NIST SP 800-171: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
14. The forecast size of the cybersecurity market: https://www.cepro.com/security/cybersecurity-market-forecasted-worth-403-billion-by-2027/
15. AV-Test (malicious programs) : https://www.av-test.org/en/statistics/malware/
16. Webroot 2020 threat report https://mypage.webroot.com/rs/557-FSI-195/images/2020%20Webroot%20Threat%20Report_US_FINAL.pdf
17. Malware increase 2019 – 2020: https://www.helpnetsecurity.com/2021/02/17/malware-2020/
18. Bad Botnet traffic: https://www.imperva.com/blog/bad-bot-report-2021-the-pandemic-of-the-internet/
19. The cost of a cyber-attack: https://www.insurancebusinessmag.com/us/news/cyber/global-cyber-insurance-pricing-spikes-32--report-259795.aspx
20. Department of Justice: https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative
21. Department of Tressure OFAC: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf
22. Executive Order - Americas Supply Chain: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/
23. Executive Order - Nation's cybersecurity: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/