MARSH

The 10 cyber trends Australian businesses must consider in 2019

The ever evolving cyber risk landscape has led to an increasing awareness at senior management and board level of cyber exposures, and the need for it to be treated not only as a technology exposure but an overall enterprise risk.

The 2019 Global Risks Report[1] confirmed that technological instabilities remain an elevated concern for businesses across the globe. Utilising data collated from 1,000 multi-stakeholder members who responded to the World Economic Forum 'Global Risks Perceptions Survey', this year's Global Risks Report showed that "massive data fraud and theft" was ranked the number four global risk by likelihood over a 10-year horizon, with "cyber-attacks" at number five.

With this as our starting point, we're pleased to be able to share with you our list of Top 10 cyber considerations and predictions for Australian businesses in 2019.

The Top 10 Trends:

1. Creating a Strong Cyber Security Culture
2. Cyber Coverage Under Traditional Insurance Policies
3. Data Encryption Legislation
4. Contractual Requirements to Purchase Cyber Insurance
5. Cyber and Business Interruption
6. Blockchain
7. IoT Devices Increase the Risk of Security Incidents
8. Social Engineering Fraud
9. Government Incentives: grants for micro/ small business to conduct a health check
10. Less about security, More about resiliency

MARSH & McLENNAN COMPANIES

1 Creating a Strong Cyber Security Culture

An organisation's culture regarding online security and data management can have a material impact on their overall cyber risk.

Throughout 2019 it will become increasingly essential for organisations to foster a strong culture of cyber security within their workforce.

A strong cyber security culture should not only focus on the training of employees to build awareness of common forms of threats (phishing emails, social engineering scams) but should also empower individuals to understand their responsibility and the critical role they play in the success of their company's cyber risk management framework. It should become normal practice to report cyber risks to responsible managers as soon as they present, or to exercise caution if a peculiar email has been received; uncomplicated changes such as these will greatly assist in mitigating potential issues before they cause wider damage.

Aside from engaging with employees, a strong cyber security culture should be reflected in an organisation's policies and procedures. These include policies that set-out: the correct management of sensitive data, how network administrative access rights are granted, and proper engagement with third party service providers.

Increased focus on an organisation's cyber risk culture is also being seen in the insurance space; insurers require details on an insured's training programs, approach to data management, and how executive oversight of cyber risk is implemented, before offering terms for a cyber insurance policy. As insurers develop a greater understanding of cyber risk and how it interacts with other, more traditional forms of risk, these types of questions are also being asked by underwriters of other lines of business - especially directors and officers insurance.

2 Cyber Coverage Under Traditional Insurance Policies

A key discussion point amongst risk managers, insurance buyers and cyber security teams this year has been whether there is existing coverage for a cyber event under a traditional (non-cyber) insurance policy.

There is growing attention from insurers regarding the provision of unintended 'silent cyber' coverage within non-cyber insurance policies. We are at a point in time where these policy wordings are being closely reviewed with a view to adding affirmative/ non-affirmative language that clarifies instances where cover will/ won't be provided for a cyber event.

INTO 2019 WE EXPECT THAT:

1. The insurance market will closely examine the inclusion of unintended coverage for cyber events, and look to either completely exclude cover under non-cyber insurance policies or provide write-backs that have been specifically negotiated on a case by case basis

2. A good number of cyber attacks will be cyber warfare threats from nation states. This reflects the growing shift from physical to online attacks in a bid to cause widespread societal disruption or to achieve certain political objectives. As cyber-attacks and cyber terrorism continue to grow in severity, insurers and insurance buyers will revisit the issue of including a war exclusion on Cyber insurance policies. Greater clarification should be sought, and policy wordings reformed, to clearly articulate the thresholds for triggering war exclusions. This includes pushing for increased clarity on the use of terminology like "warlike", what this encompasses, and the circumstances required to trigger its application.

3 Data Encryption Legislation

In the event of a cyber-attack that causes widespread disruption to business networks, software applications that are traditionally intended for personal use can become invaluable. This is certainly what one multinational law firm found when impacted by the NotPetya malware in 2017, relying on messaging application WhatsApp for several week to keep their business running[2]. What happens however when the encrypted communications within these messaging applications lose their encryption protections?

In early December 2018, the Australian Senate passed new laws aimed at providing law enforcement agencies access to encrypted communications. Encrypted communications are used in popular applications like iMessage and WhatsApp, and have previously evaded scrutiny by these agencies due to security protocols present in these forms of software.

This encryption law seeks to circumvent the hurdles established by such protocols by compelling technology companies like Apple, Google and Facebook to assist law enforcement agencies,

---

[1] The Global Risks Report 2019, World Economic Forum in Partnership with Marsh & McClennan Companies and Zurich Insurance Group [pg 16] www.weforum.org/reports/the-global-risks-report-2019

[2] www.thelawyer.com/dla-piper-cyber-attack-one-year-on/

via the provision of access to encrypted communications of individual(s), where they are the subject of a law enforcement enquiry. While the legislation has seemingly built in safeguards to ensure encryption is not weakened for both the individual(s) in question and other wider users (i.e. avoiding the creation of a systemic weakness), the question remains: what if a weakness is stolen or leaked and applied to unintended users of these applications?

Globally the regulatory landscape continues to transform at a rapid pace and it remains to be seen how perceived extreme legislative changes such as this will impact on changing privacy laws that enshrine new rights for consumers and provide individuals with greater control over how their data is collected, used and retained.

4 Contractual Requirements to Purchase Cyber Insurance

There has been notable growth in the caution displayed by companies on how their business partners and suppliers handle sensitive and confidential information. Organisations, especially government associated entities are seeking to include in their contracts a requirement for a contractor or supplier to hold cyber risk and data breach related insurance.

The insurance purchasing requirements within these clauses can often be confusingly written, requiring some analysis to determine exactly what form of insurance is necessary and to ensure that the relevant insuring clauses will respond appropriately. The required policy limits within these clauses can often be surprisingly high, meaning that purchasing the required insurance may not always be straightforward, especially when there is a limited timeframe to do so, which can often be the case in contract negotiation.

We expect that organisations will continue to take steps to ensure their systems and data are protected through the imposition of minimum data management insurance purchasing requirements within their standard contracts with key service providers.

5 Cyber and Business Interruption

Cyber security has traditionally been a key focus for organisations that maintain large volumes of personal or confidential data on their networks. The 2017 WannaCry and NotPetya attacks resulted in significant financial harm to companies operating in non-privacy industries by causing widespread disruption of technology networks, severely hampering an organisations ability to operate at normal business levels.

All types of organisations, even if they do not hold large volumes of sensitive or valuable data, need to consider and account for potential risk associated with a cyber event rendering operating systems ineffective or inaccessible. Interestingly, from late 2017 and into 2018, Marsh saw a notable growth in the take-up of Cyber insurance by companies in industries such as manufacturing and utilities, sectors that do not typically hold large amounts of sensitive personal data. This growth reflects the increased realisation that cyber risk extends well beyond just data breach and privacy issues, and we expect that interest in Cyber from non-privacy industries will continue to grow in 2019.

6 Blockchain

Blockchain is attracting large amounts of attention, particularly around its more well-known use – cryptocurrencies. Blockchain is a digital payment that does not require an intermediary party; it is a peer-to-peer transaction.

Whether you are a financial institution or professional services firm, the use of Blockchain technology and/or digital assets is here to stay. While there has been no consensus to date on how to regulate the use of cryptocurrency, we anticipate that there will be a greater global coordination amongst government bodies. In the United States, members of congress are seeking to introduce legislation to regulate cryptocurrencies. In the European Union regulators are considering creation of a bespoke regime to cover crypto-assets that are not currently subject to any existing laws. When considering that these forms of digital assets cross the traditional boundaries of currencies, commodities, and securities[3], the potential for the use of this dynamic technology in the corporate world is vast.

Within the insurance industry, insurers have traditionally been reluctant to provide coverage to this newer risk class, due, in part to media coverage about the instability and volatility of Blockchain technology and digital assets. There are some niche insurance companies who can currently consider providing coverage, but their appetite remains limited. As the use of Blockchain and digital asset currencies grows, and governments establish protocols for regulating their use, we anticipate the insurance market will rapidly evolve to provide alternate risk transfer solutions to the corporate world.

---

[3] Crypto-Assets and Blockchain Technology On the Brink of Legitimacy? January 2019 www.marsh.com/my/insights/research/blockchain-technology-brink-of-legitimacy.html

7 IoT Devices Increase the Risk of Security Incidents

Can you envision 50 billion devices connected to the internet by 2020? That's the number of Internet of Things devices Oliver Wyman predicts could in operation by 2050[4]. While these devices have brought about significant technological advancements, they greatly increase the potential attack surface areas available to cyber threat actors. This is due to the myriad of connection points and weak security protocols often present in IoT devices, as well as their connections to wider operational networks where confidential data is contained.

The vulnerabilities that exist in IoT devices are substantial, and there is certainly heightened awareness that cyber criminals will continue to target IoT devices as a gateway to larger computer networks. Despite these exposures organisations can successfully position themselves to take advantage of powerful new technologies made available using IoT devices. This can be achieved by proactively identifying the potential risks exposures of using these machines, and implementing robust security policies, procedures and a strong cyber risk culture to counter the potential cyber risks they carry.

8 Social Engineering Fraud

There is no doubt that social engineering scams remain a lucrative trade for cyber hackers. As well as providing potentially substantial financial gains, they also present a relatively straightforward method of gaining unauthorised access to otherwise secure systems. Fraud reports collated by the FBI's Internet Complaint Center over the period October 2013 to May 2018 show that globally social engineering fraud losses, also known as business email compromise or CEO fraud, have exceeded USD12.5 billion[5].

Interpol defines social engineering fraud as "scams used by criminals to trick, deceive and manipulate their victims into giving out confidential information and funds. Criminals exploit a person's trust in order to find out their banking details, passwords or other personal data."[6]

This type of fraud doesn't require sophisticated software or a high level of technical knowledge. It only takes a basic understanding of a company's organisational structure and key employees, which can be found through a quick internet search, to launch this fraud. Social engineering fraud is a relatively low cost crime that can bring about significant benefits (via monetary or sensitive data gains) for criminals. Given the relative ease of conducting social engineering fraud when compared to carrying out a sophisticated hack or targeted ransomware attack, it should come as no surprise that this form of cybercrime is expected to continue, and even escalate, this year. In conjunction with implementing mitigation procedures and awareness training, organisations should work with their insurance advisors to assess the potential exposures to social engineering, and undertake a review of the current insurance policies to ensure the insurance risk transfer solution is fit for purpose based on the organisations needs.

9 Government Incentives: grants for micro/small business to conduct a health check

In late 2018 the Australian Government announced that applications were open for its Cyber Security Small Business Program[7]. This initiative is targeted at small businesses with 19 or fewer employees to cover up to 50% (to a maximum of $2,100) of the cost of a micro, small or standard certified small business cyber security health check. Applications remain open until 30 June 2020 but may close earlier if funding is fully committed.

This initiative underscores growing recognition from Government bodies that clearer and more stringent privacy protection legislation can only be effective if companies are taking an active role in the management of their cyber risk. It is not only larger companies that can be significantly impaired by a cyber event; organisations of any size are at risk. Building of cyber resiliency, and awareness of cyber security health, is paramount for any company.

---

4 www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/jun/Internet-of-Things_Report.pdf [pg 2]

5 www.ic3.gov/media/2018/180712.aspx

6 www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud

7 www.business.gov.au/assistance/cyber-security-small-business-program

8 www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

9 www.mcafee.com/enterprise/en-au/solutions/lp/economics-cybercrime.html

10 Less About Security, More About Resiliency

According to research and advisory company Gartner, Inc the global spend on cyber security in 2018 was more than USD114 billion; for 2019 this figure is forecast to reach US124 billion[8]. Yet cyber-attacks are estimated to cost the world economy USD600 billion each year[9]. The disparity between expenditure to improve cyber security, and the cost to the economy of cyber-attacks, highlights that as companies adopt new advances in digital technologies such as Artificial Intelligence, Blockchain and Internet of Things devices, attackers are also innovating and utilising these same technologies for nefarious reasons.

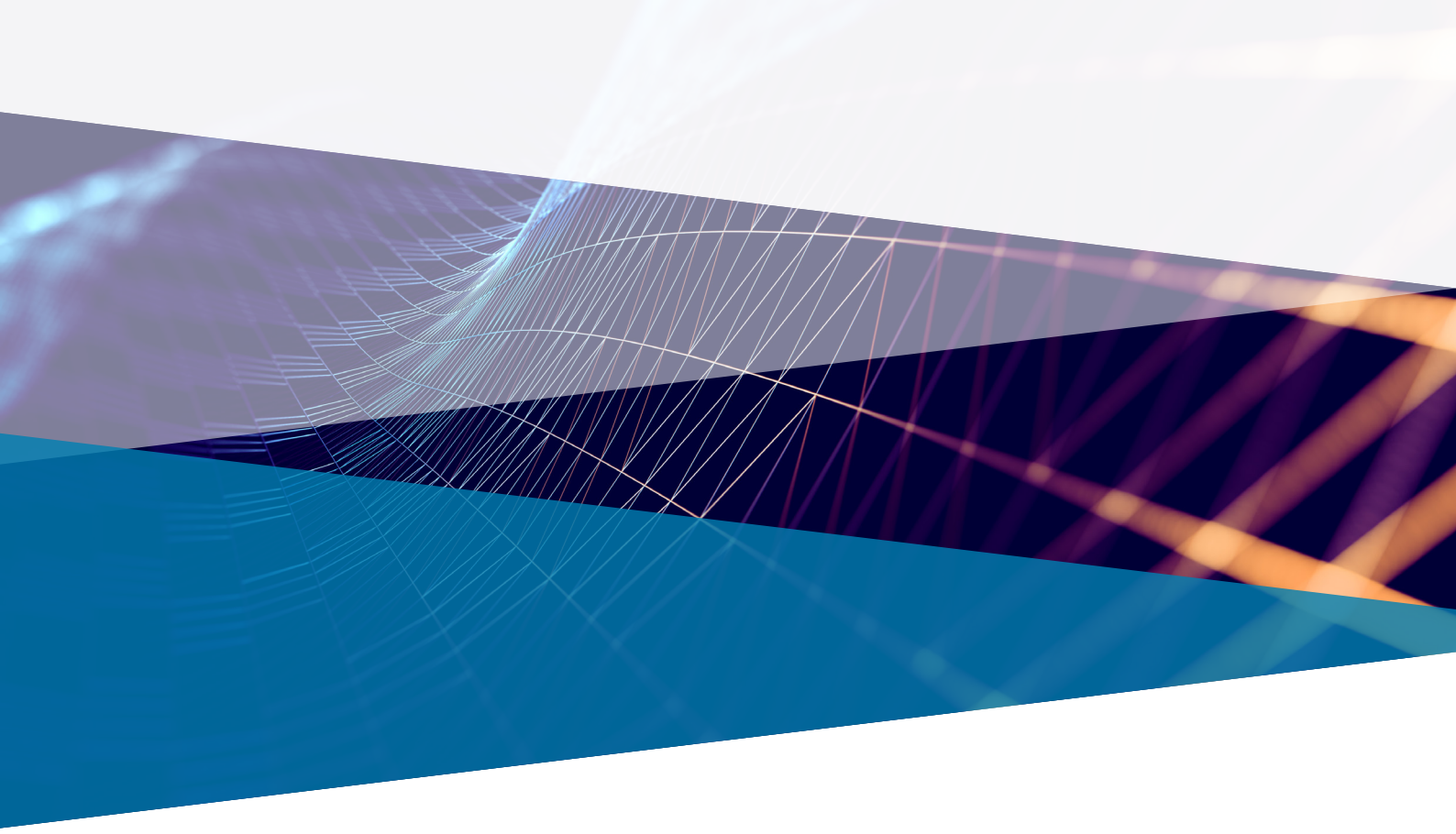
Every company has an ongoing digital transformation plan that seeks to improve the way in which business is conducted. While decisions can be made to invest money in preventing cyber events from occurring, the nature of operating a company in today's highly technological and connected world means that cyber risks will always be there. Therefore, the cyber security conversation should also include a focus on resiliency, which ASIC defines as the "ability to prepare for, respond to and recover from a cyber attack"[10]. It is a holistic approach to protecting your company, considering factors to both prevent an attack as well ensuring that the organisation can respond to and recover from one.

Technology continues to play a profound role in shaping the global risks landscape for individuals, governments and businesses[11]. Technological advancement should be embraced, and companies should take a proactive approach to managing the cyber risk it brings. Cyber risk should be treated like any other strategic risk. Enterprise-level governance should be in place to create accountability, holistic risk management framework's should be implemented and reviewed regularly, and management should lead by example in creating a workplace that promotes a strong cyber security culture.

---

[10] asic.gov.au/regulatory-resources/find-a-document/reports/rep-429-cyber-resilience-health-check/ [pg 4]

[11] The Global Risks Report 2019, World Economic Forum in Partnership with Marsh & McClennan Companies and Zurich Insurance Group www.weforum.org/reports/the-global-risks-report-2019



Next Steps

To further understand your organisation's cyber exposures and which potential risk management and insurance solutions may assist, please contact your Marsh representative, or speak to one of our cyber risk and insurance specialists:

KELLY BUTLER
Cyber Leader – Pacific
+61 3 9603 2194
kelly.butler@marsh.com

KRISTINE SALGADO
Managing Principal – Cyber
+61 3 9603 2871
kristine.salgado@marsh.com

NICOLE PALLAVICINI
Principal – Cyber
+61 2 8864 8323
nicole.pallavicini@marsh.com

SAMUEL ROGERS
Managing Principal – Cyber
+61 3 9603 2381
samuel.rogers@marsh.com