

# The 10 cyber trends New Zealand businesses must consider in 2019

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

The 2019 Global Risks Report<sup>1</sup> 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 want to share with you our list of Top 10 cyber considerations and predictions for New Zealand businesses in 2019.

<sup>1</sup> The Global Risks Report 2019, World Economic Forum in Partnership with Marsh & McLennan Companies and Zurich Insurance Group [pg 16]  
[www.weforum.org/reports/the-global-risks-report-2019](http://www.weforum.org/reports/the-global-risks-report-2019)

## The Top 10 Trends:

1. Creating a Strong Cyber Security Culture
2. Cyber Coverage Under Traditional Insurance Policies
3. Increased Regulatory Requirements
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. Changing Attitudes and Awareness
10. Less about security, More about resiliency

## 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 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/will not be provided for a cyber event.

### IN 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 cyberattacks 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 Increased Regulatory Requirements

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 changing privacy laws that enshrine new rights for consumers and provide individuals with greater control over how their data is collected, used and retained.

In mid-March 2019, the Privacy Bill moved through New Zealand Parliaments' Justice Select Committee, recommending that the Bill be passed. The purpose of the Bill is to promote and protect individual privacy by repealing and replacing the Privacy Act 1993 – which was created in an era in which most New Zealand households did not have access to the internet. The Bill would keep the principles-based framework of the current Privacy Act, while updating the law to reflect the requirements of the digital age.

Expected changes include mandatory reporting of privacy breaches, new offences and penalties and issuance of compliance notices from the Privacy Commissioner. This local regulatory framework will align New Zealand with the rest of the developed world with regard to data protection.

## 4

## Contractual Requirements to Purchase Cyber Insurance

There has been increasing 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 a requirement for a contractor or supplier to hold cyber risk and data breach related insurance in their contracts. US-based companies are also increasingly asking for cyber insurance as a contractual requirement for overseas suppliers, including suppliers based in NZ.

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 organisations' abilities 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 uptake 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 a wider range of 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 such as a traditional bank; it is a peer-to-peer transaction involving real-time updating of a universal ledger or record.

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 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. Considering that these forms of digital assets cross the traditional boundaries of currencies, commodities, and securities<sup>2</sup>, the potential for the misuse of this dynamic technology in the corporate world continues to grow

Within the insurance industry, insurers have traditionally been reluctant to provide coverage for 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 are considering providing coverage, but their appetite remains limited. As the use of Blockchain and digital asset currencies grow, 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.

<sup>2</sup> Crypto-Assets and Blockchain Technology On the Brink of Legitimacy? January 2019  
[www.marsh.com/my/insights/research/blockchain-technology-brink-of-legitimacy.html](http://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 be in operation by next year<sup>3</sup>. 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 mitigate 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<sup>4</sup>.

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."<sup>5</sup>

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 with 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 current insurance policies to ensure the insurance risk transfer solution is fit for purpose based on the organisations' needs.

## 9 Changing Attitudes and Awareness

There has been a slow but changing attitude in the New Zealand business community that cyber risk is a real and serious issue. The geographic isolation that has long protected us from other global threats is a safety net that is no longer an excuse to hide behind when it comes to cyber risk. As such, Boards are starting to be more concerned about the issue and are increasingly tabling it as an agenda item.

NZ business leaders are now actively tackling cyber risk and cyber security as an organisational issue as opposed to relegating this responsibility as solely an 'IT matter.' The Government organisation, CERT (Computer Emergency Response Team) NZ, was set up in 2017 to focus on improving cyber security in New Zealand. Having this centralised government-led resource has improved the awareness of cyber risk overall around the country. The Q4 2018 report from CERT NZ evidenced that 3445 cyber incidents were reported to CERT in 2018, more than triple the number (1131) received in 2017.<sup>6</sup> This not only shows cyber incidents on the rise, but that businesses are understanding how and who to report this to.

Despite NZ's cyber maturity not being at the same level as overseas counterparts, our business community is demonstrating that it is taking steps in the right direction.

<sup>3</sup> [www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/jun/Internet-of-Things\\_Report.pdf](http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/jun/Internet-of-Things_Report.pdf) [pg 2]

<sup>4</sup> [www.ic3.gov/media/2018/180712.aspx](http://www.ic3.gov/media/2018/180712.aspx)

<sup>5</sup> [www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud](http://www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud)

<sup>6</sup> CERT NZ Quarterly Report: Data Landscape Q4 1 October-31 December 2018 <https://www.cert.govt.nz/about/quarterly-report/quarter-four-report-2018/>

## 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<sup>7</sup>. Yet cyber-attacks are estimated to cost the world economy USD600 billion each year<sup>8</sup>. 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 be here to stay. 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"<sup>9</sup>. It is a holistic approach to protecting your company, considering factors to both prevent an attack and 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<sup>10</sup>. Technological advancement should be embraced, and companies should take a proactive approach to managing the cyber risks 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 frameworks should be implemented and reviewed regularly, and management should lead by example in creating a workplace that promotes a strong cyber security culture.

<sup>7</sup> [www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019](http://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019)

<sup>8</sup> [www.mcafee.com/enterprise/en-au/solutions/lp/economics-cybercrime.html](http://www.mcafee.com/enterprise/en-au/solutions/lp/economics-cybercrime.html)

<sup>9</sup> [asic.gov.au/regulatory-resources/find-a-document/reports/rep-429-cyber-resilience-health-check/](http://asic.gov.au/regulatory-resources/find-a-document/reports/rep-429-cyber-resilience-health-check/) [pg 4]

<sup>10</sup> The Global Risks Report 2019, World Economic Forum in Partnership with Marsh & McLennan Companies and Zurich Insurance Group [www.weforum.org/reports/the-global-risks-report-2019](http://www.weforum.org/reports/the-global-risks-report-2019)



## Next Steps

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

### **JONO SOO**

Head of Cyber Specialty – New Zealand

+64 (0)9 928 3092

[jono.soo@marsh.com](mailto:jono.soo@marsh.com)

### **KELLY BUTLER**

Cyber Leader – Pacific

+61 (0)3 9603 2194

[kelly.butler@marsh.com](mailto:kelly.butler@marsh.com)

About Marsh: Marsh is the world's leading insurance broker and risk adviser. With over 35,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data driven risk solutions and advisory services. Marsh is a wholly owned subsidiary of [Marsh & McLennan Companies](#) (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With annual revenue over US\$15 billion and 75,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market-leading firms: [Marsh](#), [Guy Carpenter](#), [Mercer](#), and [Oliver Wyman](#). Follow Marsh on Twitter [@MarshGlobal](#); [LinkedIn](#); [Facebook](#); and [YouTube](#), or subscribe to [BRINK](#).

Disclaimer: The information contained in this publication provides only a general overview of subjects covered, is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Insureds should consult their insurance and legal advisors regarding specific coverage issues. All insurance coverage is subject to the terms, conditions, and exclusions of the applicable individual policies. Marsh cannot provide any assurance that insurance can be obtained for any particular client or for any particular risk.

Copyright © 2019 Marsh Ltd. All rights reserved. S19-0517