2018 PREDICTIONS: TRENDS IN CYBERSECURITY

The 2018 Cybersecurity Predictions by Aon's Cyber Solutions team outline the top trends in cybersecurity and cyber risk that are likely to impact organisations in the next 12 months.

Since issuing our 2017 Predictions, we've seen a dramatic rise in the sophistication, scale, and impact of cyber-attacks. As companies strive to enrich their customer experience through a spectrum of endpoints, ranging from mobile devices to automobiles, the attack surface has increased dramatically.

With this ever-growing threat landscape comes a proportionate increase in the impact that cyber-attacks have on enterprises, and the customers they serve.

This report draws on our experience working with boards and C-suites, as well as security and risk professionals to plan for, mitigate, and manage the expanding impact of cyber risk across the enterprise.

The following predictions are outlined in the report with local commentary below from Aon Australia's National Cyber Risk Practice Leader, Fergus Brooks.

Businesses adopt standalone cyber insurance policies as boards and executives wake up to cyber liability.

As boards and executives witness the material impact of cyber-attacks, including reduced earnings, operational disruption, and claims brought against directors and officers, businesses will turn to tailored enterprise cyber insurance policies. At the same time, insurers will limit coverage of cyber-related losses in traditional property, casualty, and other business policies.

Local view

Whilst still behind the US in terms of the penetration of standalone cyber policies, Australia has seen significant year-on-year growth in terms of new policies and increased limits. We are yet to see a large scale data breach locally where executives have "retired" following an incident, however solid media coverage of the impacts of these events has driven awareness at all levels of business management.

As the physical and cyber worlds collide, chief risk officers take centre stage to manage cyber as an enterprise risk.

As sophisticated cyber-attacks generate real-world consequences that impact business operations at increasing scale, C-suites will be rudely awoken to the enterprise nature of cyber risk. Chief risk officers (CROs) will take centre stage, working with information security teams, treasurers, chief financial officers (CFOs), and general counsels (GCs) to improve risk modelling and paint a more holistic picture of the business' exposure.

Local view

Cyber risks to Australian business are still largely considered to be Information Technology risks, rather than Operational Technology risks. This has been changing over the last few years and 2018 should see a shift to cyber risk being a key operational risk with Audit & Risk Committees and board taking a more active role. Certainly awareness around cyber issues that can impact supply chain and autonomous equipment are driving the awareness.

Regulatory spotlight widens and becomes more complex, provoking calls for harmonization.

The EU holds global company to account over GDPR violation; big data aggregators come under scrutiny in the US. In 2018, regulators at the international, national, and local levels will more strictly enforce existing cybersecurity regulations and increase compliance pressures by introducing new ones. Companies burdened by multiple rules and regulations will mount a campaign to harmonize the complex cybersecurity regulatory landscape.

Local view

Australia's Amendment to the Data Privacy Principles regarding mandatory data breach notification comes into effect on the 22nd February 2018. Australian companies may also be impacted by the GDPR described above. The Office of the Australian Information Commissioner has issued guidelines for organisations in terms of preparing for potential privacy incidents through having a cyber incident response plan.

Criminals look to attack businesses embracing the IoT, in particular targeting a small to mid-sized company providing services to a global organization.

In 2018, global organizations will need to factor into third-party risk management the increased complexities in how their business partners are using the IoT. However, we will not see this happen, and as a result we predict a large company will be brought down by an attack on a small vendor or contractor that targets the IoT as a way into their network. This will be a wake-up call for large organizations to update their approach to third-party risk management, and for small and midsized businesses (SMBs) to implement better security measures or risk losing business.

Local view

Australia is seeing the same concerning increase as the US & EU in terms of a growth in criminally-backed cyber incidents. This has not extended into the Industrial Internet of Things, such as Industrial Control Systems including SCADA that are used extensively in Australia's mining, resources and utilities sectors. These types of systems have often been protected by being on separate private networks. These are increasingly being connected to IT networks without the same level of security rigor as office and internet-facing systems.

As passwords continue to be hacked, and attackers circumvent physical biometrics, multi-factor authentication (MFA) becomes more important than ever before.

While passwords alone do not provide adequate levels of security, their convenience means that they are still widely deployed. Although they will be phased out as the primary method of authentication on mobile and IoT devices in 2018, they are unlikely to disappear completely. As companies implement biometrics to authenticate identity, criminals will advance their attacks to override these new technologies. In 2018, as more credentials are compromised, and biometrics are hacked, we will see the rise of MFA.

Local view

Australian organisations tend to be early adopters of IT security solutions such as MFA and we will see continued implementation in Australia of advanced authentication solutions and completion of exercises of data classification.

Criminals will target transactions that use points as currency, spurring mainstream adoption of bug bounty programs.

In 2018, companies beyond the technology, government, automotive and financial services sectors will introduce bug bounty platforms into their security programs. Businesses with loyalty, gift, and rewards programs, such as airlines, retailers, and hospitality providers, will be the next wave of adopters as criminals target transactions that use points as currency.

Local view

In its Cyber Security strategy, the Australian federal government outlined a key initiative in innovation for Australian companies in the development of security tools and services. In 2017 we saw at least one large Australian company launch a bug bounty program and as these technologies mature, we will continue to see the rise of bug bounty programs.

Ransomware attackers get targeted; cryptocurrencies help ransomware industry flourish.

By the end of 2017, the global cost for organizations of ransomware attacks is estimated to reach $5 billion, up 400 percent from 2016. The WannaCry ransomware attack impacted more than 300,000 people across 150 countries in less than two days. In 2018, criminals will evolve their tactics, including launching well-researched, targeted attacks intended to infect specific high-value assets known to hold critical data.

Local view

Whilst Australian organisations were relatively un-impacted by Wannacry in 2017, this was mostly down to:

- timing as it was released on a Friday evening Australian time when the majority of businesses were already closed, and
- a reasonably good culture concerning patch management.

Australian companies should maintain their vigilance with regards to patching and back-ups as ransomware attached will continue in 2018.

Insider risks plague organizations as they underestimate their critical vulnerability and liability, and major attacks continue to fly under the radar.

Since we predicted the rise of the "insider" in 2016, we have seen organizations severely impacted by actions taken by malicious, careless, negligent, and unaware employees, contractors, leavers, consultants, and others with access to information, systems, and networks. Despite this, in 2017 we saw businesses underinvest in proactive insider risk mitigation strategies and 2018 will be no different. With a continued lack of security training and technical controls, coupled with the changing dynamics of the modern workforce, the full extent of cyber-attacks and incidents caused by insiders will not even become fully public.

Local view

Many Australian companies consider themselves to be too small to attract a cyber-attack, however smaller business don't tend to have the dedicated cyber security resources which larger organisations have in place, making them a softer target. Further, many attacks are opportunistic, as opposed to specifically tailored and dedicated. Criminals will typically use the most cost effective attacks to improve their profits.

Contact:

Fergus Brooks

Cyber Risk Practice Leader
Aon Risk Solutions
+61 2 9253 7835
fergus.brooks@aon.com

Joerg Schmitz

Cyber Risk Profiling Expert
Aon Risk Solutions
+61 2 9253 8030
joerg.schmitz@aon.com

ARS0303 0118

Empower Results®