Cyber security lessons — Risks and resilience

CONTRIBUTORS:

MARK HAWKSWORTH
Technology Specialist Practice Group Leader, Sedgwick, United Kingdom

TIM OVER
SVP Specialty Operations, Sedgwick, United States

ANTHONY SMIT
Manager Cyber Specialist Group, Sedgwick, Australia

According to the latest World Economic Forum Global Risks Report 2018, cyber attacks are perceived as the global risk of highest concern to business leaders in advanced economies and are viewed by the wider risk community as the risk most likely to intensify. While companies often have rigorously developed response plans for extreme weather events, the same level of advance planning consideration is not always given for cyber attacks. The Forum's research suggests that only one third of companies have prepared a pre-incident response plan for a major cyber attack. Sedgwick has found time and time again that policyholders in the midst of a cyber event do not have a plan in place to assist with management of the cyber issues they face.

As businesses become ever more dependent on technology in order to function, companies' exposure to cyber risks is also heightened. Similarly to how we prepare for natural disasters and other catastrophes, we must also focus on crisis response planning for cyber threats. Businesses must not only continue to anticipate cyber attackers' objectives and implement prevention measures; they also must shift focus toward cyber resilience and respond to protect their firms and their customers from the impact of malicious cyber attacks.

AN EMERGING GLOBAL MARKET...AND THREAT

The cost of cyber exposures to the global economy is more than $400 billion a year and continues to grow.[1] Cyber insurance products have been around since the late 1990s. Still considered to be in the early stages of the market, we face emerging needs and evolving products. It is estimated that premiums for the global cyber insurance market will grow to $14 billion by 2022.[2]

The projected growth of cyber insurance policies is further corroborated in the recent 2017 Aon Global Risk Management Survey, where it is reported that 67% of businesses in North America, Europe and Australia have not purchased or are planning to purchase cyber insurance.

We have seen evidence of this need firsthand in Australia, where the Sedgwick cyber team has seen a marked increase in cyber-related claims over the past few years – from the more common email phishing, social engineering fraud attempts and malware infections, to more serious denial of service attacks, ransomware and other attacks. The majority of claims are malware-related, which aligns with the results published by AV-TEST GmbH, an independent research institute for information technology (IT) security, which registers over 350,000 new malicious programs every day.

The focus of corporate and individual cyber security has recently been brought to bear on the hijacking of data using ransomware. Although this form of extortion, albeit at a much less sophisticated level, has been around since the late 1980s, it really gained widespread attention after the recent "WannaCry" attacks (known as "WanaCrypt0r 2.0") hit the headlines. This worldwide cyber attack took advantage of vulnerability in computers running the Microsoft Windows operating system where the necessary security updates had not been applied. WannaCry ransomware attacks affected the operations of major companies and government agencies worldwide. For example, NHS computers in the UK were affected across the whole organization's internal network; the impact of the attack lasted for six days and resulted in a cost of £92 million to the cash-strapped health service.

Even more recently, Sedgwick has seen claims where a new type of ransomware attack has been identified. Traditional models have incorporated delivery of malware using mass mailing spam campaigns or exploit kits. In the latest incidents, criminal groups use targeted malware in attacks designed specifically to disrupt high turnover small to medium enterprise (SME) businesses by locking up crucial digital assets. Initially, a network is compromised and the hackers spend time researching, mapping and collecting credentials from the SME. Once the target network infrastructure is fully understood, the criminals execute their ransomware to cause maximum impact. Ever-increasing ransom payments, recently in excess of £100,000,

have been demanded to unlock the affected data.

In 2016, Microsoft reported that ransomware cost approximately $325 million in damages and it is predicted to rise to $11.5 billion in 2019 with a ransomware attack taking place every 14 seconds, according to Cybersecurity Ventures.

To address this scenario, an increasing number of insurance companies are launching cyber risk policies to the market that include coverage such as third party liability, technical assistance and research expenses, repair and restoration costs, loss of profit, legal defense, crisis communication and incident management, etc. Some also offer additional services such as adaptation to data protection regulations, prevention measures and help lines. At Sedgwick, our incident management team incorporates in-house technical experts who can assist in the initial stages of a ransomware hack, identifying the mitigating factors to help prevent large turnover losses or loss of customers.

In addition to considering cyber risk insurance policies and response measures for their own operations, it is important for businesses to discuss cyber practices with upstream and downstream partners. Reviewing contracts and building in specific language can help ensure the right protections and plans are in place throughout a connected supply chain.

CYBER LOSS MANAGEMENT

With the increasing frequency of cyber attacks, it is crucial for cyber loss management to be expeditious, restoring the company's normal activity as soon as possible through robust coordination among all the parties involved: loss adjusters, IT forensic experts, lawyers and communication agencies. To achieve this, it is essential to have identified all those involved before the attack and loss occurs.

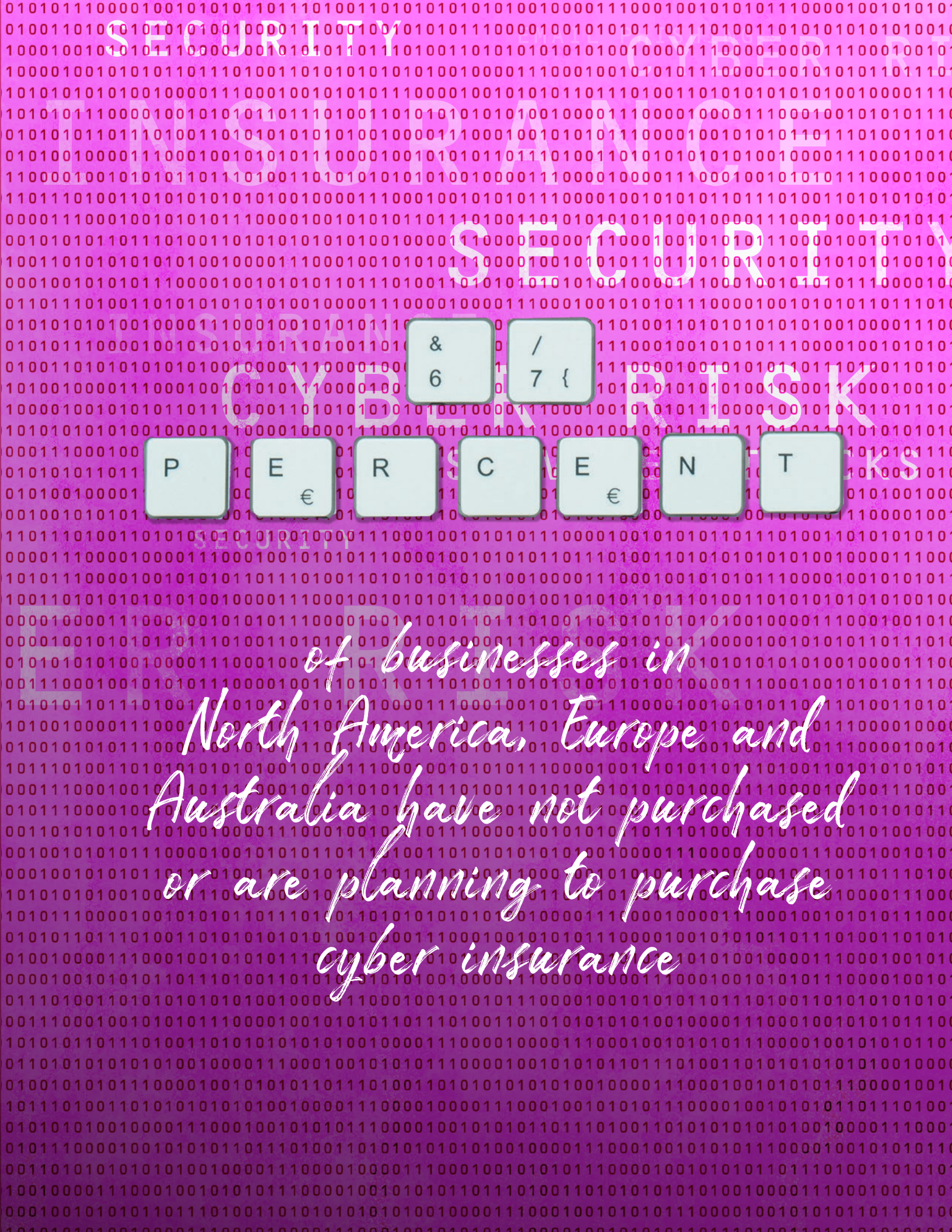
As the saying goes, it's better to be safe than sorry, and in this case, prevention is our main ally against a cyber attack. The best way to protect your data is to create "off-network" backup copies, stored remote from the network, where they cannot be accessed during an attack. The remote data can then be used to overwrite any encrypted (locked) data following an attack. That can make the difference between a few days of lost network functionality or a major disruption event.

Other measures can also be implemented, such as providing staff training to avoid classic phishing traps, keeping operating systems updated and using good enterprise-level antivirus software.

We know that 100% cyber security is a myth which exists only in the minds of those who are not computer savvy. Even if all of the correct prevention measures are taken (creating daily verified off-network backups, making employees aware of the techniques used and having a robust data protection policy), vulnerabilities always exist. Knowing where weaknesses lie and taking positive action to prevent an attack can potentially be the difference between a quick recovery and business failure.

PREPARING FOR ACTION

Businesses that are prepared from a technical standpoint are minimizing their exposure, but what about the impact of even the smallest of cyber breaches? What is your plan of action if faced with a notifiable data breach? While the cyber world offers plenty of territory still to explore, there are sound risk management pathways to tread. Businesses can prepare themselves by having a thoughtful, immediate



of businesses in North America, Europe and Australia have not purchased or are planning to purchase cyber insurance

response plan that puts key measures in place to mitigate damages if faced with cyber exposure.

1) First notice of loss management – The identities of each affected person or organization must be determined, and appropriate notification provided. Notification must be timely, accurate and provide details sufficient to alert those involved of the breach and the steps to be taken. Failure to do so opens up the potential for third-party actions, penalties or even class action litigation.

2) Reputational management – Your reputation as a trusted fiduciary of client confidentiality is a cornerstone of your success; quickly managing the reputational impact of a cyber breach can make or break your business. Reputation and brand impact management may include outbound and inbound communication, possible setup of call center resources, and public relations support for appropriately engaging the media.

3) Forensic IT expertise and accounting – Upon notice of a breach, forensic action must be immediately undertaken to determine the source of the breach, stop the loss of additional data and fix the original source. Forensic accountants and IT specialists can undertake a cause and impact analysis, with investigations detailing what was lost, how it was lost, replacement costs, whether the company is still at risk, the necessary steps to improve security, and potential damages due to the loss.

4) Claims support – Regardless of the number of records exposed, the direct and indirect costs are real and instantaneous and may include expenses for data recovery and restoration, business interruption costs, cyber extortion costs, crisis management costs and more. The right claims resources can help with exposure and coverage interpretation, final claim adjustments, and ongoing activity such as credit- or identity-monitoring solutions.

5) Legal support – Skilled legal experts can help you understand the intricacies of the liability picture in the evolving cyber world. It is important to align with appropriate legal counsel, who must be retained for defending litigated claims, as well as addressing potential regulatory investigations and fines.

With evolving products, a swiftly changing market and a constantly growing knowledge base, cyber is guaranteed to remain a hot topic throughout 2019. We will continue to see questions of coverage vs. indemnity, explore policy language and limits, and prepare ourselves for known and unknown risks.

REFERENCES

1) World Economic Forum. Our Shared Digital Future Report. December 10, 2018.
http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf

2) Property Casualty 360. 2022 cyber event could result in major losses of policyholder surplus. September 4, 2018.
https://www.propertycasualty360.com/2018/09/04/2022-cyber-event-could-result-in-major-losses-of-policyholder-surplus/

RESOURCES

World Economic Forum Global Risks Report 2018.
https://www.weforum.org/reports/the-global-risks-report-2018

Cyber attack claims: Stick or twist? Sedgwick Connection blog. June 2, 2018.
https://www.sedgwick.com/blog/2018/06/02/cyber-attack-claims-stick-or-twist


$11.5 billion
predicted cost of damages from ransomware in 2019