# The CYBER THREAT – It's only a question of when

Written by:
ALEXANDRA BRETSCHNEIDER
**(Johnson, Kendall & Johnson)**
and ED VENTHAM (**Paragon Brokers**)

**It seems like every day there is news of another major cyber incident in the press, followed by the latest statistics on the rise in ransomware attacks and extortion demands.**

Then every couple of months there is a new Cybersecurity or Privacy law passed by a government body requiring a new wave of compliance. Some law makers are also beginning to debate whether they should outlaw the right to pay a ransom to a criminal at all (see article: https://insights.paragonbrokers.com/post/102gqpe/paying-a-ransom-is-inadvertently-funding-cyber-crime), but cybercrime which is often perpetrated by nation-state actors, will continue to flourish despite the regulatory and legal action taken against the 'bad actors'.

And long gone are the days when only the big companies were the targets for their money or information. In today's world, no business is immune to being the target of an attack as hackers seek the easiest and most economical means to earn quick cash. Although the 'spray and pray' techniques are perhaps not as successful as they once were (the level of company security is undoubtedly rising to counter such obvious cyber threats through the use of antivirus, firewalls and Multi-Factor Authentication), the sophistication and frequency of cyber attacks and incidents has demonstrated clearly that no one is 100% safe.

What was once considered an "IT issue" – now has the attention of the C-Suite and shareholders/board members – it is a companywide problem, from the most senior leader down to the most junior employee.

## Is there a solution for this dynamic risk?

Cyber risk management requires a broader and holistic focus; it is not solved with only the purchase of the latest and greatest technology, or only a cyber insurance policy. It requires investment in talent, education, training, and a review of internal processes and operations on a regular basis. Cyber risk management is ultimately accomplished through a combination of People, Processes, and Technology.

## People

Employees are the gatekeepers to our organisation. The responsibility for data security should be written into our employees' job description and understood as part of their duties. Furthermore, organisations should invest time and money into frequent and engaging training tools. Conducting phishing tests periodically can assess the efficacy of a training programme and identify users in

need of a refresher course. Consider assigning an in-house cybersecurity director, responsible for the data security oversight of the organisation.

## Process

A business should start with a self-assessment, going through the process of identifying what type of data and information you have, and who should vs. does have access to it. Developing solid processes around managing access, deploying patches, acting on alerts and notifications of a potential incident should be consistent practice. Businesses should spend time to develop a cyber-specific incident response policy as a subset of their broader business continuity/disaster recovery planning, and these plans should be tested via tabletop exercises. Process should include supply chain/vendor management: taking a look at vendors and partners to question what type of access to or information they have about your organisation, and how it is managed. Ultimately, what is your 'vendor management protocol' – how do you choose them and what due diligence do you do to ensure your reliance on their support is not crippled in the event of an incident which is indirectly going to affect your company's integrity and operation?

This is critically important if you are reliant on a managed-service provider for your IT infrastructure and support, but still applies to non-IT/operational vendors.

## Technology

Of course – when we think of cyber we often think of technology. The technologies of today that a business should be considering include Intrusion Detection Systems, sophisticated spam filters and firewalls, next-generation antivirus software, Endpoint Detection and Response systems. Multi-factor authentication has become a must-have tool in the eyes of insurance companies for them to consider offering coverage, which can be centralised through a password management software.

But, to err is human. And as much as we invest in the prevention of a cyber attack, human error still leads to the majority of cyber incidents today. The goal of your cyber risk management programme is not to reach a state of being entirely cyber secure (because no such state exists). Instead, your goal is to reach a state of cyber resilience in which your organisation can sustain and recover from an attack.

## Cyber insurance

Once a luxury purchase, Cyber insurance has become a must-have for businesses everywhere to ensure the survival of your organisation after an attack. Insurance is a form of risk transfer, and is meant to provide a backstop when the preventative controls of an organisation have failed or proven inadequate.

Cyber insurance provides the key components of incident response, in the form of attorneys/lawyers, IT forensics, criminal negotiators, public relations, and compliance with the various privacy laws. Coverage is designed to respond to and provide the defence during a regulatory investigation, and cover fines and penalties assessed to you, as long as they are insurable by law.

Cyber-crime coverage offers indemnification for insureds who have suffered social engineering, funds transfer fraud, and phishing attacks. With the explosion of ransomware during the global pandemic, the coverage for the extortion demands offered by standard cyber insurance policies proved critical to the recovery process.

Coverage for revenue loss related to a cyber incident can be found in a comprehensive cyber insurance policy, both during the time your network is down, and/or after you are back up and operable but have then lost prospective revenue as a result of an adverse media event.

As quickly as the cyber risk evolves and grows, cyber insurance carriers are constantly trying to keep up. With the increase in both frequency and severity of attacks, profitability on insurance premiums historically has waned and the insurance markets are being forced to increase rates in order to keep up with the increased losses. In order to minimise their exposures, insurance markets are modifying policy terms and conditions, restricting coverages that were once broadly written, like extortion, with sublimits and coinsurance penalties. Ensuring you have a comprehensive cyber policy is just one issue – but obtaining coverage at all is becoming problematic for organisations that are falling behind the curve in their cybersecurity controls. Without multi-factor authentication on email access, administrator accounts, and remote access are becoming a pre-requisite to obtaining coverage. Segregated backups, encryption, firewalls, incident response planning, employee training and more are becoming preferred controls securing a better premium rating.

Businesses should start the conversation now with their broker partner about what is needed to be insurable and to obtain optimal insurance terms. With cyber insurance continuing to serve as the lifeblood for organisations to recover from cyber attacks, obtaining and retaining coverage is crucial as part of broader cyber risk management and resilience programming.

UNIBA