The Unpredictability Series

Cyber, a tough risk to pin down

By Simon Hoejmark
Underwriter

Fast changing technical and regulatory factors make cyber an unpredictable risk, but with more experience and better tools, the threat can be made more manageable.

Overview

Cyber is one of the biggest threats shaping today's risk landscape. Surveys [1] of global executives have ranked cyber risks highly, up there with geopolitical volatility and climate change, while a poll of European risk managers cited cyber as the top risk of concern.

800 million

current jobs could be eliminated by automation by 2030

Technology is an important driver of political and economic change, the two biggest causes of growing unpredictability for business, as revealed by QBE's Unpredictability Index. Social media is changing the political debate while new technologies, like driverless cars, robotics and artificial intelligence, are expected to have huge impact on people's lives. According to McKinsey, around 60% of occupations will be in some way impacted by automation, while up to 800 million current jobs could be eliminated by 2030.

Technology is now at the heart of most organisations, driving their operations, supply chains and distribution. However, the pace of technology adoption appears to be outstripping the technical and cyber security capabilities of most users and companies. Many do not fully understand what cyber means for them, nor do they anticipate the impact on their business when something goes wrong.

With hindsight, many cyber incidents seem predictable, even preventable. Yet compared with risks like natural catastrophes or fire, which are well understood and can be modelled using historical loss data, cyber risk is particularly tricky to pin-down. When, where and how a cyber event will unfold is very difficult to predict. Even where likely scenarios can be identified, the likely impact and potential financial loss can be hard to anticipate and calculate.

[1] World Economic Forum Global Risks, 2019 PwC survey, https://www.ferma.eu/2018-european-risk-manager-report

Myriad unknowns

Technology and cyber events mean dealing with a lot of unknowns. Cyber incidents come from a diverse range of sources and triggers, such as malicious cyber attacks, technical glitches, via the supply chain or a rogue employee.

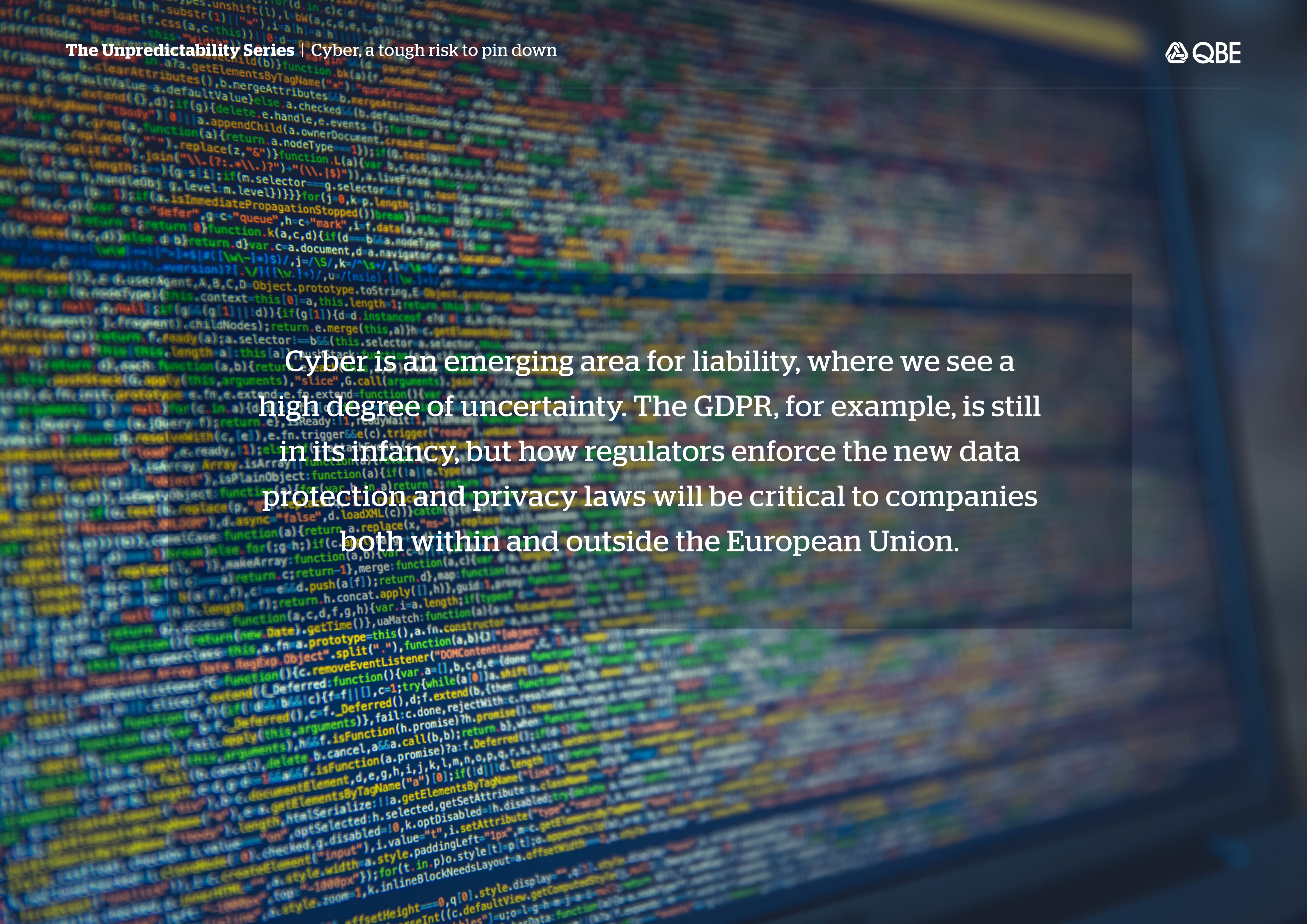
Organisations will not know where on the spectrum they will get hit or the degree of impact. And, as each business has its own IT set-up, it is hard to learn from the experience of peers.

> Cyber is a never-ending race where hackers are always one step ahead and new vulnerabilities can come from unexpected quarters.

Keeping on top of cyber risk is also a challenge. Cyber is a never-ending race where hackers are always one step ahead and new vulnerabilities can come from unexpected quarters. Emerging threats include the exploitation of IoT devices and hardware vulnerabilities (such as the 2018 Meltdown and Spectre threats), while attention is now turning to cyber attacks powered by artificial intelligence. However robust an organisation's cyber security defences are, it will never be immune.

Predicting the impact of a cyber incident is particularly difficult and will vary widely by company, even for the same incident. For example, the 2017 NotPetya malware attack caused massive disruption for a number of companies, while others in the same sector were unscathed.

Scale and interconnectivity also drive unpredictability, last year's Marriott hotel data breach affected 500 million people, while the 2017 WannaCry ransomware outbreak affected an estimated 300,000 computers in 150 countries. According to recent Lloyd's of London research, a large global contagious malware attack could affect more than 600,000 businesses worldwide and cost US$193 billion; as large as a major natural catastrophe event.



Cyber is an emerging area for liability, where we see a high degree of uncertainty. The GDPR, for example, is still in its infancy, but how regulators enforce the new data protection and privacy laws will be critical to companies both within and outside the European Union.

Business interruption

Events like WannaCry and NotPetya highlight the potential for cyber-related business interruption and contingent business interruption losses, which are particularly tricky to predict and quantify, given the complexity and concentrations of risk within physical and digital supply chains.

For example, a manufacturer suffering an IT systems outage might be able to make up for lost production, but would face the additional cost of workarounds and potentially loss of business. Last year, semi-conductor manufacturer TSMC was hit by malware, resulting in an estimated 3% loss of revenue and additional costs. Business interruption losses and additional expenses arising from the NotPetya attack cost shipping group Maersk and logistics company FedEx US$300 million apiece while food manufacturer Mondelez reported losses from the attack in excess of US$100 million.

As insurers of cyber risk, we see many incidents where companies have not fully understood the knock-on effects of a cyber incident. Even where a company prepares for possible cyber scenarios, the performance of business continuity plans in practice is difficult to predict. Restarting systems in a controlled environment, for example, is very different to the reality of rebooting following an outage or a ransomware attack.

> **“As insurers of cyber risk, we see many incidents where companies have not fully understood the knock-on effects of a cyber incident.”**

Regulatory uncertainty

The fast pace of technology change is such that regulatory and legal frameworks are continually evolving. This is particularly true for privacy and data protection laws, but also with cyber security requirements and liability regimes, for example, the introduction of autonomous cars, IoT and artificial intelligence all raise regulatory and legal questions.

New regulations and untested laws create uncertainty for companies, from the size of fines to the compensation sought by affected individuals. This can already be seen with the EU's General Data Protection Regulation (GDPR), which introduced tough data protection and privacy rules in May 2018. The GDPR gives regulators greater powers and consumers enhanced rights, but it will take several years before the implications of the GDPR are fully understood.

Cyber is an emerging area for liability, where we see a high degree of uncertainty. The GDPR, for example, is still in its infancy, but how regulators enforce the new data protection and privacy laws will be critical to companies both within and outside the European Union. The GDPR applies to companies processing EU data anywhere in the world, while a growing number of countries are now looking to introduce similar requirements.

Litigation is also an emerging area for cyber. As yet, we have not seen a large volume of litigation, but there is clearly potential far greater third party liability going forward. Laws like the GDPR make it easier for individuals to claim compensation following a cyber incident, including for non-financial damages, like emotional distress. Attitudes to privacy and service disruption are changing, and a growing number of cyber incidents are leading to collective actions as investors and consumers seek compensation for damages suffered.

Prevention

Cyber risk is clearly not about to go away. However, robust risk management and insurance arrangements can shift the odds and help organisations better cope with the effects. Well established risk management techniques, for example, can assist organisations and their boards as they adopt technology and embrace digitalisation.

> Experience has shown that good preparation can significantly reduce the impact of a data breach, and by building overall resilience, an organisation should be able to respond to any cyber event, however unexpected.

93%

of risk managers are now working closely with their IT and cyber security colleagues

37%

identify and assess risks prior to the adoption of new technologies by the business

A survey of risk managers by the Federation of Risk Management Associations (FERMA) found 93% of risk managers are now working closely with their IT and cyber security colleagues while 37% already identify and assess risks prior to the adoption of new technologies by the business. It is still early days for digitalisation. But through experience, companies will get better at understanding cyber risk and prevention. And in the meantime, there are steps that companies can take now to reduce the risk. For example, in addition to basic cyber security hygiene, such as penetration testing, patching and training, planning for a cyber event like an outage or data breach can significantly reduce the impact.

At a high level, companies should think through the what-ifs of a data breach or outage, identifying data, services and third parties that are critical to their business. It pays to spend time working through scenarios ahead of time, preparing crisis response and business continuity plans. Experience has shown that good preparation can significantly reduce the impact of a data breach, and by building overall resilience, an organisation should be able to respond to any cyber event, however unexpected.

Technology could also come to the aid of companies, providing tools to help assess and quantify cyber risk. Cyber risk assessment platforms can already assess and benchmark an organisation's cyber risk and cyber security, as well as help quantify losses or map supply chains. Such tools are in their early stages of development but are likely to become indispensable in coming years.

Companies can also transfer risk to the insurance industry, as well as access their services and expertise. Cyber insurance products are improving all the time and can bring additional comfort as organisations invest in new technology and digital business models.

Steps you can take to reduce cyber risk and the impact of an event:

Basic cyber security hygiene:

- ✓ penetration testing
- ✓ patching
- ✓ training

Planning for a cyber event:

- ✓ an outage
- ✓ data breach

Keep in touch

If you haven't already signed-up to receive the Unpredictability Series you can do so at

qbe.se

Published April 2019

QBE Insurance (Europe) Ltd, filial Sverige
Sveavägen 13
111 57
Stockholm

Tfn: +46 (0) 8 587 514 00
infoqbesweden@se.qbe.com