Sponsored by

TOKIO MARINE HCC

CIR
CONTINUITY INSURANCE & RISK

The good, the bad and the ugly *- Cyber attacks and data security have long been a growing issue for organisations and society as a whole, and with the pace of technological change, it's a problem that's about to get a great deal bigger. Deborah Ritchie reports* *p26*

Cyber readiness, key to survival *- So much is said and written about cyber risks and how to prepare for them, but, as ever, the devil is in the detail. In this in-depth analysis, Xavier Marguinaud offers a framework for companies looking to achieve comprehensive 'cyber readiness'* *p28*

Cyber risk

TOKIO MARINE HCC

Sponsored by

The good, the bad and the ugly

Cyber attacks and data security have long been a growing issue for organisations and society as a whole, and with the pace of technological change, it's a problem that's about to get a great deal bigger. Deborah Ritchie reports

Digital connectivity is now crucial both for business innovation and individual prosperity, but each creation, each step towards positive change is met with a corresponding cyber threat – that now ever-present, inescapable obstacle to doing business in the vast majority of sectors.

From data breaches and identity theft to the disruption of operations and critical infrastructure, the threats are varied and many, presenting organisations with an ongoing challenge when it comes to prevention or recovery.

Indeed, 2019 was the year the public "woke up" to the potential of its personal data, according to Information Commissioner Elizabeth Denham, hailing an "unprecedented" year for the authority, with record-setting fines and a record number of people raising data protection concerns.

In data management and security, the biggest moment of the year was as we are all painfully aware, the arrival of the General Data Protection Regulation. This, she said, saw people realise the potential of their personal data, leading to greater awareness of the role of the regulator when their data rights aren't being respected. "The doubling of concerns raised with our office reflects that," Denham said.

Since May 2018, all the European data protection authorities received a combined 90,000 breach notifications. The ten most serious GDPR breaches in the UK this year led to a total £345 million in fines, with the three highest penalties making up almost 90 per cent of the total. British Airways, Marriott International and Google were among the high-profile companies to be caught out.

Since then, Dixons Carphone has been hit with the maximum possible fine after malicious software was installed on 5,390 tills in branches of its Currys PC World and Dixons Travel chains in an event that affected at least 14 million people. And, just as its staff were returning to their desks early in the New Year, Travelex was forced to take down its website after a suspected ransomware attack. In this instance, it seems that no customer data was compromised, but the company's website had been taken offline for some time before BAU was restored.

"A civil liberties group plans to submit a legal complaint on behalf of over 1,000 people, which may set the stage for proposals contained with the Representative Action Directive"

The problems plaguing the foreign exchange firm reflect a trend among cyber criminals to deploy ransomware attacks, according to cyber analytics firm, CyberCube, which warns that such attacks could become so widespread they may stifle economic growth. Client services manager at the firm, Nick Beecroft said: "What's happened to Travelex is part of a rapidly growing trend. Ransomware has become more than a cottage industry with ransomware developers and hackers teaming up to attack companies and then divide the spoils. There are also so-called 'big game hunters' who work alone and target firms able to pay large ransoms." Beecroft also points to a movement towards the publication of 'shaming sites', with companies infected being listed.

This increasingly prevalent form of malware joins a host of other threat vectors such as phishing, denial of service attacks and session hijacking, that will keep information security professionals in business for some time to come, with new strains, such as the recent trojan malware Emotet, evolving all the time.

The World Economic Forum's *Global Risks Report 2020,* ranks cyber attacks as the second most concerning risk for doing business globally over the next 10 years. Published at the beginning of this year, the WEF report goes on to cite "information infrastructure breakdown" as the sixth most impactful risk in the years until 2030.

Both sets of respondents to the organisation's *Global Risks Perception Survey* (the multistakeholder community and the Global Shapers) identify cyber-related issues, such as cyber attacks and data fraud or theft, within the list of top 10 long-term risks.

The possibilities are endless

Already, technology is ushering in a new era of possibilities, as what was once just science fiction is quickly becoming reality. Quantum computing, AI and 5G networks are creating as many threats as they are opportunities, and lack of a global governance framework for technology risks could deter economic growth and aggravate geopolitical rivalries.

The WEF points to the need for coordination amongst stakeholders in developing solutions to this growing challenge – a challenge that will manifest substantially in AI in particular.

According to the UN's International Telecommunication Union, it will take "massive interdisciplinary collaboration" to unlock AI's potential. Security, verification, deepfake videos (the modification of images, video and audio recordings through AI so that they appear genuine), mass surveillance and advanced weaponry present problems of an as yet undefined magnitude.

Law firm DAC Beachcroft goes as far as to say AI is about to usher in a new era of offensive cyber attacks as well as defensive cyber security measures, in what may quickly become a new arms race.

"Deepfakes...could pave the way for more personalised scams and frauds," says partner and head of cyber and data risk at the firm, Hans Allnutt.

"Many cyber attacks begin with a phishing email – maliciously fooling individuals into disclosing credentials or authorising payments through emails that are surprisingly convincing. If hackers are able to utilise the sophisticated technology behind deepfakes, it is conceivable that they could mimic human voice commands by telephone so they appear to come from a trusted source."

Those companies with the impetus and resources to access this technology may fare best in this new arms race, he adds; those that do not, risk becoming the new "low hanging fruit" for attackers.

The firm's *Informed Insurance* report also foresees further and more significant enforcement action – with big name IT providers possibly in the firing line.

"The GDPR introduces direct obligations on data processors (the party who processes personal data only on the instructions of the data controller). Although fewer and fewer companies' operations fall under processor activity, due to the narrow definition applied by the ICO in the UK and more and more sophisticated uses of data by service providers, the new liability which attaches directly to data processors means that in certain circumstances they can be sued directly by data subjects and fined directly by the ICO for data breaches.

"Data regulators across Europe may soon bear their teeth and impose monetary penalties for a full range of breaches"

"With many IT providers having much deeper pockets than their clients, we consider it possible that we will see a big name IT provider at the forefront of an enforcement action very soon," Allnutt adds.

Staying with GDPR, it says data regulators across Europe may soon bear their teeth and impose monetary penalties for a full range of breaches under the relatively new regulation, not just those associated with security.

Meanwhile, a significant development in Ireland is raising awareness of multiparty actions due to breaches of data protection rights. A civil liberties group plans to submit a legal complaint on behalf of over 1,000 people, which may set the stage for proposals contained with the Representative Action Directive.

"The Irish Government introduced a Public Services Card which the Data Protection Commissioner considered was in breach of the GDPR," Allnutt explains. "The DPC concluded that the manner of information collection and retention on millions of citizens was unlawful and is planning to launch enforcement against the relevant government department."

A shift in approach

Embracing technological change and all the opportunities it presents means identifying and embracing the threats and accelerating and incentivising solutions through an ongoing commitment to investment and cooperation.

To this end, the World Economic Forum is working on a project focused on increasing global cooperation between the public and private sectors in addressing key challenges to security and trust in the digital landscape. The aim of its *Future Series* project is to understand how the key technology waves of the near term will impact the threat and risk landscape in the future, how these technologies will change the cyber security landscape and the subsequent security and response implications for countering these developments.

That cyber as a top risk issue is widely acknowledged, and never refuted, but the risk persists as technologies evolve, and as new doors are opened up – both in terms of new and exciting developments and in terms of the vulnerabilities, as cyber criminals seek new ways to exploit each new door opened.

And while the last few years have seen dramatic technological change, it's nothing compared with what's in store.

Cyber readiness, key to survival

So much is said and written about cyber risks and how to prepare for them, but, as ever, the devil is in the detail. In this in-depth analysis, Xavier Marguinaud offers a framework for companies looking to achieve comprehensive 'cyber readiness'

Lately, we are hearing more and more new cyber-related terms such as cyber index, cyber institute, cyber program, cyber review, and cyber readiness, to name a few. The latter is one that is trending right now. Unfortunately, as this is a relatively new term, most explanations surrounding the concept often only provide a high-level overview without going into detail. So, what is cyber readiness exactly?

If 'readiness' is the state of being fully prepared for something, we could easily define 'cyber readiness' as having everything programmed and in place to minimise any possible effects stemming from a potential cyber incident. If that is so, then we understand that the goals of cyber readiness are to detect, contain and mitigate these consequences. Therefore, cyber readiness would imply that any potential impacts of a cyber incident are envisaged and will be limited so that a company can return to business quickly.

There are several ways of describing the cyber readiness framework and all its components. For the purposes of this article we will reference the one provided by the Cyber security & Infrastructure Security Agency. In 2019, this US governmental entity linked to the department of Homeland Security released a set of recommendations about cyber readiness to help companies implement organisational cyber security practices. This approach, in particular, stands out for being original in its communication yet consistent with the NIST Cybersecurity Framework and other cyber security standards.

CISA's approach

There are six essential elements in CISA's approach:

1. **Yourself – the leaders** emphasises governance and the importance of having board members and top executive management involved in designing, investing and driving the company's cyber security strategy. Cyber security should be handled as a business risk and companies should understand that it takes time and money to define and implement a relevant strategy.

2. **Your staff – the users** focusses on encouraging the development of a cyber security culture among employees and external stakeholders (service providers, customers, etc.), improving everyone's vigilance. Awareness of your staff, which can only be achieved through training and education, is key. Remember that they might become your first line of defence!

3. **Your systems – what makes you operational** highlights that protecting critical systems is one of the most important actions to take in cyber security. It is crucial to know what your critical systems are and where your most valuable information resides. Companies should build security into and around these assets. Therefore, drawing up a risk map and performing a data/system classification are two unavoidable exercises.

"Cyber readiness would imply that any potential impacts of a cyber incident are envisaged and will be limited so that a company can return to business quickly"

4. **Your surroundings – the digital workplace** recommends companies ensure that only those who belong to their digital workplace have access to it. Granting appropriate access and setting up relevant rights should be a priority. Any digital environment needs limits.

5. **Your data – what the business is built on** sets out to convey that making back-ups and avoiding loss of information is essential to the company's operations. It may seem obvious to most of us, but I think it is worth repeating over and over again. The CISA guide recommends establishing regular data backups and redundancies for key systems along with protecting backups using encryption and offline copies.

6. Finally, one of the main goals in cyber security for any company should be to limit damage and speed up the time it takes to resume normal operations. The final step, **Your actions under stress – what to do?**

puts the onus on companies to make their reaction to cyber attacks and systems failures an extension of their other business contingency plans. It is highly advisable to plan and prepare drills for cyber attacks as you would for fire drills or any other tangible threats.

The CISA document itself also encompasses some guidance for IT professionals. It is a single and common document that gathers information for both leaders and IT teams working for the same company. This is a brilliant idea!

Although all six of CISA's steps are relevant and imperative for a company's survival in the face of one or more cyber threats, the sixth is of particular importance. The business continuity plan can only be prepared if all other steps have been completed. To complete the BCP, several stakeholders within the company, who may not normally interact with each other, need to come together on an ultimate common goal: survival.

If the BCP has been correctly prepared, then the company can bounce back. The incident response plan, which forms part of the BCP, plays an essential role in ensuring cyber readiness.

The incident response plan structure

A relevant incident response plan is usually made of three key elements: plan, team and tools.

Firstly, the plan addresses the question: what are we going to do to deal with the threats? Here, we must consider concepts such as containment, eradication, and escalation.

Secondly, the (centralised) team addresses the questions: what kind of expertise do we need? what would the team members' responsibilities and authorities be? Ideally, any incident response team should be made of the following seven people: response manager, security analyst, lead investigator, threat researcher, communication leader, documentation leader, HR/legal representative.

Thirdly, having the (adequate) tools addresses the question: how will we be handling the incident? The company needs a set of analytical, alerting and remediation tools: cold/warm/hot sites, SIEM, IDS/IPS, NetFlow analysers, and so on.

When addressing all three elements in the Incident Response Plan, one must keep in mind the three ultimate goals of any incident response strategy: analyse, report, respond.

So, this explains how the plan is structured and why. However, from my point of view, as a cyber insurance underwriter, a comprehensive cyber incident response plan needs to be elaborated.

The incident response plan – Contents

From experience, we like to see the following six elements in the incident response plan:

Preparation: Define policies, conduct risk assessment, develop communication plan, outline roles/responsibilities/procedures/authorities, recruit and train team members, set up appropriate tools.

Identification: Decide what criteria calls the team to action, identify and assess the incident, gather evidence, establish the severity scale, use the escalation protocol.

Containment: Isolate the security incident (the aim is to stop further damage), short-term containment, systems backups (take a forensic picture before wiping affected systems!), long-term containment.

Eradication: Isolate the root cause of the attack, identify and mitigate vulnerabilities to stop further attacks (this might change the configuration of the organisation, so the aim is to minimise the effect on operations).

Recovery: Bring affected (and therefore decontaminated) systems back into their production/working environment.

Lessons learned: Improve both the production/work environment and the Incident Response Plan.

A cyber essential

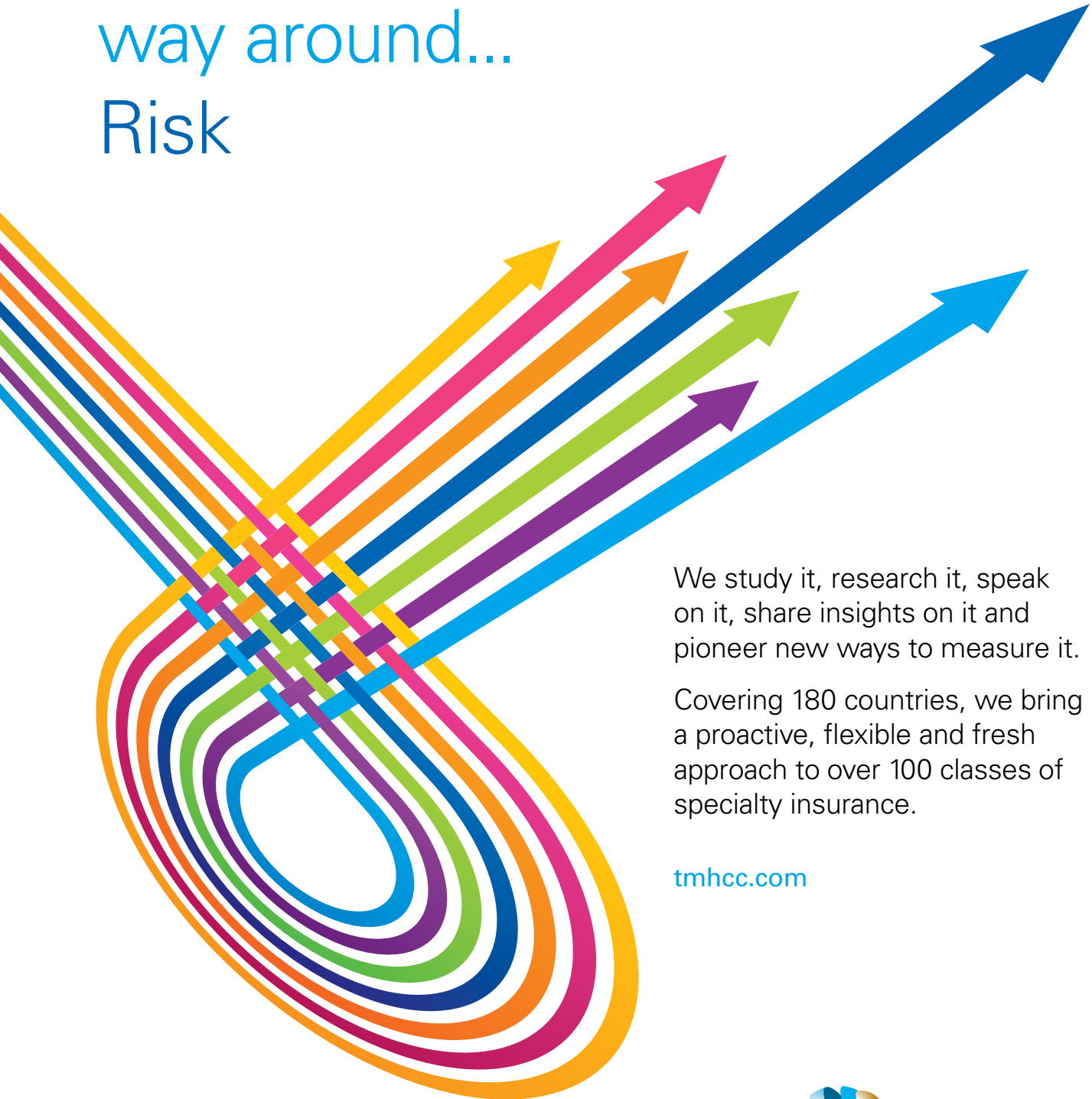
So, to recap, I hope to have given sufficient detail to provide a good understanding as well as some much-needed depth to the concept of cyber readiness – this term that we seem to hear all too often nowadays without knowing what it really means in practice. I also hope to have emphasised just how essential cyber readiness is as part of any company's strategy, and which can help unite company stakeholders in preparation and readiness to confront the inevitability and reality of cyber threats today and tomorrow.

In essence, companies should be asking themselves just how cyber-ready they actually are. When they seek appropriate insurance, this is one of the first questions that will be on the table.

Xavier Marguinaud,
Cyber Underwriting Manager
Tokio Marine HCC
xmarguinaud@tmhcc.com

Tel: +34 93 530 7439

We know our way around... Risk



We study it, research it, speak on it, share insights on it and pioneer new ways to measure it.

Covering 180 countries, we bring a proactive, flexible and fresh approach to over 100 classes of specialty insurance.

tmhcc.com

TOKIO MARINE HCC