CYBER SECURITY & DATA MANAGEMENT

in the Modern Digital Age

A FINANCIER WORLDWIDE EBOOK

IN ASSOCIATION WITH

RAPID7

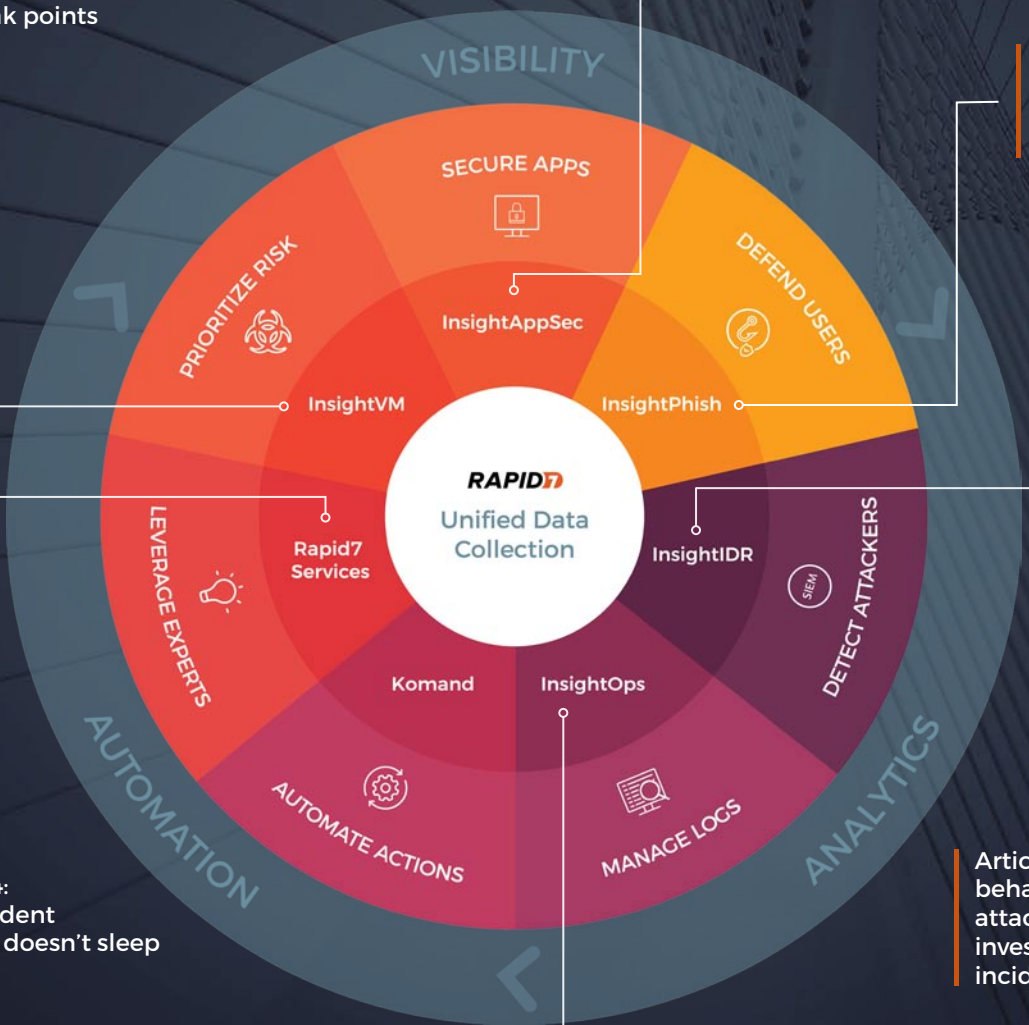
Tackle GPDR with Rapid7 Insight

The Rapid7 Insight platform is an essential resource for your GDPR compliance challenges. Get the visibility, analytics, and automation you need to unite your teams and work smarter and faster toward compliance.

Article 32: Assess applications for vulnerabilities

Article 32: Know your network and identify weak points

Article 32: Test effectiveness of your security and empower your users



Articles 33 & 34: Outsource Incident Response that doesn't sleep

Articles 33 & 34: Monitor behavior, detect attackers earlier, and investigate security incidents faster

Articles 32, 33 & 34: Quickly search your data and logs to investigate availability issues

READY TO TACKLE GDPR WITH INSIGHT?

Start your free trial at www.rapid7.com/try/insight

Learn about all of Rapid7's GDPR solutions and services at www.rapid7.com/gdpr

CYBER SECURITY & DATA MANAGEMENT

in the Modern Digital Age

A FINANCIER WORLDWIDE EBOOK

Published by
Financier Worldwide
23rd Floor, Alpha Tower
Suffolk Street, Queensway
Birmingham B1 1TT
United Kingdom

Telephone: +44 (0)845 345 0456
Fax: +44 (0)121 600 5911
Email: info@financierworldwide.com

www.financierworldwide.com

Ebook • May 2018

Cyber Security & Data Management in the Modern Digital Age

A FINANCIER WORLDWIDE EBOOK

in association with **Rapid7**

with contributions from

Advent IM

AstraZeneca China

Baker Hughes, a GE company

Browne Jacobson LLP

Brown Rudnick LLP

Capital One

Credit Suisse

De Montfort University

Edison Electric Institute

Good Harbor Security Risk Management

McAfee

Microsoft Corporation

Nokia

Norton Rose Fulbright LLP

Oxford Internet Institute

Simmons & Simmons

Skadden, Arps, Slate, Meager & Flom, LLP

Tannenbaum Helpern Syracuse & Hirschtritt LLP

Venable LLP

Contents

Foreword

IN THE NOT-TOO-DISTANT PAST, cyber security and data privacy were infrequent topics for the boardroom. If the subject of data breaches was mentioned, a few big names were referenced in sentences starting "we do not want to be the next 'insert name here'", and it was assumed or hoped that the chief information security officer (CISO) was capable of preventing such an event from occurring. Fast forward to today, and the next 'insert name here' name seems to change on an almost weekly basis. 'When, not if' has become the mantra of the breach conversation. Data breaches have gained significantly more publicity, in part due to the frequency of incidents, but also due to changes in regulatory reporting requirements.

Unquestionably, the most drastic and widespread changes to security and data privacy compliance are those brought in by the General Data Protection Regulation (GDPR). The GDPR is a lengthy legal text that seeks to bring consistency across the EU, and has a reach extending way beyond the physical borders of

the 28 EU Member States. The maximum fines under the GDPR for non-compliance are eye-watering, bringing a new sense of urgency to the "we do not want to be the next 'insert name here'" statement.

On the flipside, however, is the importance of keeping your organisation's cyber security and data privacy houses in order. This is the right thing to do for your customers, partners, prospects, employees and shareholders. Practicing good data hygiene, and following security best practices, can help to significantly reduce the risk of impact to your business, and to those whose data you process.

The sophistication and escalating number of threats, the increasing agility of attackers, the complexity of the modern ecosystem, and the need for businesses to innovate at speed, has created a challenging risk landscape for security and privacy teams, as well as executive boards. Personal data no longer resides purely on physical servers, and numbers of connected devices are at an all-time high. As the traditional network perimeter continues to blur, the effectiveness of traditional security methodologies continues to reduce. Visibility is vital to understanding organisational risk, as invisible risk is impossible to

calculate. And, at a time when data protection laws are becoming more stringent than ever before, there is no easy answer.

Regularly discussing these issues at board level is both essential and increasingly common, as the ability to meet compliance regulations requires ongoing investment, ongoing visibility and ongoing commitment, across the entire organisation.

■ *Jen Ellis is vice president of community and public affairs at Rapid7.*

ABOUT RAPID7

Rapid7's mission is to lead the emerging SecOps movement with our multi-product analytics and automation cloud and expertise.

We believe in:

Innovation. We believe it is possible to innovate and push the boundaries of progress while keeping data and assets secure. We are passionate about SecOps, the practice of making security inherent to innovation.

Transformation. We believe that the emerging SecOps movement will transform systems design to make good security a core design principle. We will provide the visibility, analytics and automation needed to succeed.

Collaboration. We believe secure and reliable innovation requires governments, researchers and practitioners to collaborate, share knowledge and educate each other. We will lead in this effort.

Accessibility. We believe that all businesses should have access to great security software and services. We deliver solutions powerful and scalable enough for the largest organisations, but simple and accessible enough for organisations of every size and maturity.

Samantha Humphries
Senior Product Marketing Manager,
Global Markets & Compliance
samantha_humphries@rapid7.com

Samantha Humphries is responsible for ensuring Rapid7's International Markets receive the proper solutions messaging, collateral and information. She also trains sellers (internal and partners) on security concepts and solutions. Ms Humphries has nearly 20 years of employment experience in the information technology field, and has held multiple positions including senior product manager, global threat response manager, and incident response manager. She has spent many years helping hundreds of organisations of all shapes, sizes and geographies recover and learn from cyber attacks. She regularly speaks at industry events.

Jen Ellis
Vice President of Community and
Public Affairs
jen_ellis@rapid7.com

Jen Ellis is Rapid7's vice president of public & community affairs. She believes security practitioners are the guardians of society's trust in technology, and works extensively with security professionals, technology providers/operators and various government entities to promote better collaboration. She believes this is our best path to reduce cyber crime and protect consumers and businesses. To this end, Ms Ellis also provides free skills training to security professionals so they can get greater buy-in and achieve more positive security outcomes. She has testified before Congress and spoken at numerous industry events.

Introduction

BY FRASER TENNANT AND RICHARD SUMMERFIELD

CYBER SECURITY

AS TECHNOLOGY CONTINUES TO EVOLVE at a rapid pace, the likelihood of an organisation falling victim to a cyber attack has never been greater. From small to large organisations and everything in between, cyber hackers do not discriminate as a rule, and almost any entity is a potential target.

Some hackers wish to disrupt systems and take them offline, while others are looking to acquire data and then sell it on or lock organisations out of their systems until a ransom is paid. If these scenarios come to pass, then every facet of a business is likely to experience pronounced consequences.

Whatever the reason for a hack, an attack can have major cost implications for organisations, including thousands or even millions in lost profits, the need to repair systems, as well as numerous other business disruption costs.

Perhaps more alarmingly, in some cases several months may pass before an organisation is even aware its systems have been breached. This of course gives it no opportunity to respond quickly and little chance of limiting the damage – operational, financial and reputational – the attack is likely to have engendered.

When one considers the high-profile breaches that have been reported in the past year alone, the conclusion is unpalatable as well as unavoidable: cyber attacks are now mainstream.

Among the cyber security breaches which have caused particular havoc in recent times are the WannaCry ransomware attack in May 2017 and the NotPetya malware outbreak the following month. The WannaCry attack – described by Europol as "unprecedented and beyond what had been seen before" – crippled parts of government and infrastructure in more than 150 countries, including Germany's railways and the UK's healthcare system. While it was a relatively unsophisticated attack, the WannaCry incident infected hundreds of thousands of computers, causing enormous damage.

For its part, the NotPetya malware, which superficially resembles the Petya ransomware (itself used to disrupt networks across Europe in 2016) and masquerades as such, is particularly

dangerous. First emerging in July 2017, NotPetya infection sites were initially focused in Ukraine but soon spread quickly around the globe, affecting businesses in Spain, France and India. Unlike Petya, NotPetya did not require spam emails or social engineering to gain administrative access to networks.

As far as attributing responsibility for the WannaCry and NotPetya attacks is concerned, the jury is still out to a certain extent. In December 2017, more than six months after the event, the US publicly blamed North Korea for the WannaCry attack, stating that Pyongyang was "directly responsible" for unleashing the virus. The US also named the Lazarus Group, a North Korea-based cyber crime group, as the threat actors involved. When assessing culpability for the NotPetya incident, the National Cyber Security Centre found that the Russian military was almost certainly responsible for the attack – an assertion backed by both the UK and US governments.

The upshot of the WannaCry, NotPetya and Petya cyber attacks is that they left little room for doubt as to the vulnerability of the network systems utilised by organisations operating in a range of sectors across the globe.

Naturally, some sectors are more vulnerable to cyber attacks

than others due to the type of data their servers and networks contain, with healthcare, financial, manufacturing, government agencies and legal typically at risk. Healthcare organisations in the US are certainly in the high-risk bracket – specifically targeted by cyber criminals as they operate privately, for profit and have a high reliance on access to data.

One aspect of the cyber security debate organisations will assuredly be reluctant to examine is the extent to which they themselves are the architects of their own downfall. For many, the bald truth is that even as the number and sophistication of cyber attacks increases, established strategies for protecting data are few and far between. Senior management and boards are often slow to recognise the scope of risks they face and may underestimate the extent of their exposure.

To address weaknesses in cyber security fundamentals, organisations – with clear understanding and guidance from the upper echelons – need to dispense with the notion that cyber security is merely an issue for the IT department, bring it into the strategic risk management framework and implement policies and procedures accordingly.

Another issue for organisations is the difficulty finding per-

sonnel with the requisite skill set, with the demand for cyber security specialists rapidly outpacing supply. According to National Initiative for Cybersecurity Education (NICE) research, the skills shortage is expected to escalate over the next five years. NICE also found that the areas particularly impacted by the skills gap relate to visibility and detection and incident response, with a lack of expertise in both disciplines often resulting in a costly delay in identifying and then responding to a potentially devastating cyber attack.

While the outcome of a cyber attack may indeed be damaging, it should never be defined as a one-off event, and organisations need to be aware that the chances of them being retargeted are high. Evidence suggests that if an organisation has been breached once, there is a strong possibility that it will be targeted again by another, or maybe even the same, attack group. Preparing for this eventuality is therefore key. Among the options is for organisations to implement threat-management platforms that fast-track investigation and prioritise security alerts. At the same time, insurance solutions should be explored.

For the moment, the spectre of a cyber attack remains a potent threat and the landscape is constantly evolving. Year-by-year, new technology risks are emerging and advanced persistent

threat (APT) groups are proliferating. Despite this ominous backdrop, progress is being made, with many organisations now well enough informed to identify breaches internally, rather than unknowingly awaiting notification of a breach by law enforcement agencies or other external sources.

While the ideal is for organisations to adopt a proactive approach to cyber security in order to avoid being compromised, the reality is that in a world of complex and inextricably interconnected systems, falling victim to a cyber attack is now very much the norm, rather than the exception.

DATA PRIVACY

WHILE COMPANIES HAVE BEEN WRESTLING with the task of data protection for decades, in recent years, as a result of technological advancements, the challenge has evolved, growing in both complexity and importance. The volume of data being produced is a key driver of this phenomenon. According to a 2017 MarTech report, 2.7 zetabytes of data exists in the current 'digital universe' and is doubling in size every two years. By 2020, existing data it is

expected to reach 44 zetabytes. This vast cache has obvious value to companies, as well as cyber criminals and other malicious actors. How then, can companies safeguard their data?

First and foremost, it is imperative that the board of directors and C-suite develop a clear understanding of the challenge they face. Companies today run on data, from intellectual property and other intangible assets, to the personal, private information of customers and employees. Collecting and managing data has become central to value creation; as such, data storage must be a priority, within a robust data privacy framework, guided by the C-suite.

One of the most important and logical steps a company can take is to appoint a data protection officer (DPO). The DPO must identify the weak points in the company's data privacy provisions, and demonstrate a strong understanding of the privacy laws in the jurisdictions in which the company operates. The legal risk including penalties for non-compliance can be substantial. For companies in the European Union, appointing a DPO may soon be a legal requirement under the incoming General Data Protection Regulation (GDPR).

A data breach is a very real possibility for almost every or-

ganisation. According to a 2017 Radware report, 45 percent of companies suffered a breach in 2016, and those that have fallen victim are often not even aware. Furthermore, according to Risk Based Security's '2017 Data Breach QuickView Report', there were an unprecedented 5207 breaches recorded in 2017, a 20 percent increase on the previous high seen in 2015.

Recent breaches, including those at Under Armour/MyFitnessPal, FedEx, Yahoo, Equifax and others, have highlighted the difficulties companies face in protecting their data and, when a breach has occurred, responding in a timely manner, communicating the situation to relevant stakeholders and regulators. Historically, companies have failed to adequately respond to these challenges. Due to the frequency of attacks, it is becoming difficult for companies to cope.

In the event of a breach, a company's response is of paramount importance. Not only should stakeholders be informed of the breach, but regulators too. Companies can no longer afford to neglect their breach notification responsibilities, particularly given the impact of the GDPR in Europe and beyond. Through its accountability principle, the GDPR will introduce new breach notification requirements for the first time. It is not the only piece

of legislation to do so. In Australia, the Notifiable Data Breaches (NDB) scheme, which came into force in February 2018, requires Australian government agencies and the various organisations with obligations to secure personal information under the Privacy Act 1988 to notify individuals affected by data breaches that are likely to result in serious harm. California has also enacted data breach notification legislation which stipulates that state agencies and businesses have a duty to protect customer information.

These legislative developments are an important step; however, additional measures will be required. The old system of viewing data-related issues through the prism of existing legal frameworks is increasingly outdated. Global regulation governing data and data breaches must be task-appropriate. Governments must be willing to move with the times and introduce much-needed legislation. In the UK, the government is pursuing a number of short- and long-term initiatives aimed at promoting the cyber security profession and developing skills in the sector. Training is being made available to help develop new cyber security professionals. The National Cyber Security Strategy is an exciting development and a number of other jurisdictions are exploring similar initiatives.

It is important that companies and regulators are on the

same page when it comes to data privacy and cyber security, particularly as consumers are becoming increasingly aware of the importance of their personal data and how it is handled by organisations. Scandals such as the recent Facebook/Cambridge Analytica revelations only serve to draw more attention to the issue.

Increasingly, consumers are demanding transparency from organisations. Establishing and maintaining trust will be crucial in an increasingly data-centric economy. Depending on the nature of a breach, embarrassment and loss of customer trust can be significant. Breaches are far from just a public relations disaster, however, as they can have serious financial consequences. According to a 2014 Semafone survey, 86 percent of customers would shun brands following a data breach.

Companies found to be in violation of the GDPR will also face severe financial penalties. Those that collect data on EU citizens will need to provide a 'reasonable' level of protection for personal data. Failure to comply could see them fined the greater of €20m or 4 percent of annual global turnover. And when the average cost of a data breach is considered – according to the Ponemon Institute, the cost of a breach in 2017 was $3.62m – it is clear that organisations must be proactive.

One weak spot which requires attention is data storage, including the cloud. Cloud storage is expected to account for 40 percent of the digital universe by 2020. There are myriad risks associated with transferring and storing data, particularly for organisations utilising cloud storage systems. Enterprises have to deal with security issues such as a loss of control over sensitive data. By utilising third-party storage solutions, companies are allowing their data to be taken outside of their IT environment. Accordingly, companies should insist that their third-party partners encrypt their files during transit and storage.

Bring your own device policies (BYOD), which allow employees to use their own mobile devices, such as smart phones and tablets, to access business enterprise content or networks, have helped to revolutionise working environments. As more millennials enter the workforce, BYOD policies and remote working will continue to have a bearing on data privacy. While BYOD strategies can improve employee job satisfaction, efficiency and flexibility, as well as provide cost savings from initial device purchase to ongoing usage and IT helpdesk support, they also represent a serious data privacy risk.

Companies must take steps to ensure that employees are

fully aware of the data privacy risks and responsibilities of remote working. Data protection principles should be embedded at the core of companies' business activities. Companies should consider ring-fencing certain data, keeping it contained within a specific app, as well as ensuring that, if a device is lost, the data on it is kept confidential and retained via a backup facility.

Moving forward, compliance with legislation such as the UK's Data Protection Bill, as well as the GDPR, will be crucial. However, according to a Data Privacy Snapshot report released by DLA Piper, many companies are not prepared for GDPR. Among surveyed companies there was an average alignment score with all key international data privacy principles of just 34.4 percent.

As the total cost of data breaches continues to grow, companies must tackle data privacy and security proactively. Increased legislation and regulatory oversight should be viewed as an opportunity for companies to gain a better understanding of the data they hold and ensure that customers are placed at the heart of data protection efforts.

■ *Fraser Tennant and Richard Summerfield are associate editors at Financier Worldwide*

Security-based vs. risk-based approaches to cyber risk

Jen Ellis at Rapid7 looks at how companies can evaluate and address cyber risk.

Q. When implementing a cyber security programme, how important is it to balance business requirements with security needs? What challenges might this present?

ELLIS: The goal of security should be to protect the business and its customers from disruption or harm. In order to achieve this, the security team needs to understand the requirements and priorities of the business and its customers, as well as their standard operating procedures. Designing a stringent security

programme that protects the organisation from all potential threats may sound good, but if it brings the business to a halt, it has failed in its most basic requirement. So the security team must build an understanding of the real risks that relate most compellingly to the business, and balance mitigations for these against the operational needs and goals of the business. Part of this is understanding the business' risk tolerance or appetite, which will vary greatly based on industry, customer profile, operational history, investor and board perspectives, and various other elements.

Q. How would you characterise the level of cyber risk awareness among boards and senior executives? What general tips would you offer to organisations in terms of tailoring cyber risk management to the specific needs of their business?

ELLIS: The level of cyber risk awareness among business leadership teams is improving thanks to the sheer number of high profile breaches occurring today, together with the publicity garnered by the requirements of the GDPR. There is often still a chasm between high level intent and a good understanding of

the work that needs to be done. Effective information security professionals are excellent communicators. They bring the board with them and explain in business terms how information security needs to be improved. Senior executives and board members can play a role by inviting security leadership in to present to them on the security programme, and asking basic questions about the organisation's most critical assets, employee awareness, types of threats the organisation might be subject to, and the security team's needs and plans.

Q. Could you provide an overview of how both security-based and risk-based approaches can improve the effectiveness of an organisation's cyber policies and procedures?

ELLIS: A security-based approach prioritises security practices above all other considerations. While this approach will introduce more cyber security policies and procedures into your business, it will not necessarily make your business more secure. If security requirements are too stringent, the business will start to work around them and communication with the security organisation will break down. Alternatively, a risk-based approach

prioritises decision making, based on making informed decisions that balance security needs with the business' goals, context and risk tolerance. By working with the organisation to understand risk appetite and business implications, the security team can craft security processes that work better for the business and will be more likely to be adopted and maintained over time. Communication and awareness between security and the rest of the business should build over time.

Q. How would you compare and contrast each approach? What advantages and disadvantages do they bring?

ELLIS: Starting with considering security, rather than business, is a common approach which often leads to lack of engagement and board-level commitment. Starting with considering business risk is often more effective, as this is a language that the board natively understands.

Q. Once the extent of its vulnerability to a cyber attack has been identified and assessed, how should an organisation go about implementing a standard operation procedure (SOP)

that reinforces prevention and response measures?

ELLIS: There are a number of tools that organisations can use to build a security programme that works for their own environment. For example, the UK's National Cyber Security Centre (NCSC) offers guidance on building a risk management programme. The US NIST Cybersecurity Framework and the CIS Critical Security Controls are also popular. Generally, most programmes begin with identifying the organisation's critical and sensitive assets that need protecting, understanding the relevant types of threats, and determining the organisation's exposure to these threats. Risk management frameworks will then walk through a variety of measures to protect critical assets, educate employees and leadership on risk, and detect intrusions, attacks or suspicious behaviour. These measures will be a variety of technology, people and processes – all three are needed to work together for effective security. Frameworks should also discuss measures for security incident preparedness and recovery as no one is completely invulnerable, no matter how good your security programme is.

Q. As both ecosystems and attacks grow increasingly complex, what new skills, methodologies and approaches do you foresee being required to adequately defend and protect business operations against cyber attacks?

ELLIS: As complexity increases, it is essential that we embed security in all development and operations of the business, creating greater alignment and building more awareness of security needs. This is the principle driving the practice of SecOps. Security, IT and development teams share data to speak a common language, leverage advanced analytics, and build automation into their tools and workflows. This emphasis on automation is also critical in addressing the increased demand for security. By automating as much tactical, repetitive activity as possible, we can reduce costs and increase productivity, and perhaps more importantly, we can free up skilled employees to apply their expertise to more strategic challenges and opportunities.

Q. How do you expect security-based and risk-based approaches to evolve over the coming years?

ELLIS: We expect to see a greater drive toward the adoption of SecOps practices, embedding security considerations and execution in all functions, and tearing walls down between security, IT and development. As the GDPR pushes security higher up the corporate priority list, organisations will look to adopt pragmatic, industry-recognised best practices more widely. The stigma of a breach will lessen as more disclosures occur and the understanding of how widespread this issue is increases. This will pave the way for an environment of greater information sharing on threats and defensive approaches. We will see vertical sectors organising themselves for this purpose and demanding more from their technology vendors in terms of patchability and transparency around risks. The financial sector has already started down this route and will continue to be a leader in terms of security investments and understanding, but with other verticals such as healthcare, government and energy starting to make strides forward. Further cyber security regulations – either sector specific or broadly applied – may also drive further changes.

Data breaches – preparation, identification and response

Samantha Humphries at Rapid7 looks at how companies can confront the constant threat of a data breach.

Q. How would you characterise the adequacy and robustness of data breach-related procedures generally deployed by organisations?

HUMPHRIES: Many organisations fail to pay enough attention to breach preparedness and planning for recovery. At best, the majority have high-level procedures that have not been tested and lack sufficient detail to be useful in a crisis. More organisations need to properly consider how they will deal with a breach,

as it is a matter of when, not if, they will need to react.

Q. With data breaches essentially a matter of when, not if, how should organisations go about preparing for a breach and implementing an appropriate incident response plan?

HUMPHRIES: Careful consideration ahead of time regarding how to identify, contain and recover from a breach pays dividends during a crisis. Identifying key roles, responsibilities, processes and requirements helps ensure the bases are covered and the core team knows what is expected of them. They still need to be able to react to the specifics of the situation, but being well-prepared will help them work as a team and achieve the optimal outcome with as little disruption as possible to the business. Run regular drills to build trust among core stakeholders and identify weak spots in your plan or response processes. In a live scenario, you may want to call in external technical, legal or communications expertise; it is a good idea to include these experts in your drills or plan reviews. You may also want to identify relevant contacts in law enforcement in case you need them, and it is essential to understand the legal requirements for disclosure in various sce-

narios, particularly in light of GDPR.

Q. What are the initial issues and challenges facing organisations upon discovery of a data breach? How important is it to identify a breach as early as possible and take appropriate action?

HUMPHRIES: The biggest initial challenge is a lack of clarity or certainty over what has happened, and how to move forward. The goal should be to minimise disruption to the business and end-users, but this is not always straightforward when you need to investigate the issue in order to understand the full implications and what recovery action needs to be taken. This is exacerbated by most breaches going undetected for over 100 days. It is critical to have effective monitoring and alerting in place to ensure that breaches are detected as quickly as possible. Steps can then be taken to contain the breach before it spreads, thereby limiting the damage in terms of business disruption and information loss. Having well-managed and searchable logs makes investigation and recovery easier.

Q. What key elements should a data breach response plan possess to ensure fast containment and damage limitation?

HUMPHRIES: First, identify and prioritise key assets. What information or systems are most likely to be targeted or would cause greatest disruption to the organisation and its customers? Second, assign roles and responsibilities. Who is in the core response team and what is expected of them? Who runs the overall response? Third, establish foundational workflows. What are the basics processes that need to be covered? When do they need to be covered? And who is involved? Fourth, understand reporting requirements. Identify both internal and external reporting requirements. When and how should the executive team be informed? When is disclosure mandated for customers? In what scenarios will law enforcement be contacted? What are the SEC reporting requirements? Fifth, document key contact information. Who are your go-to external consultants for technical, legal and communications expertise? How will the core response team communicate if email is compromised? Sixth, evaluate cyber insurance. What are the details of your policy? Does it mandate specific behaviours or external expertise? Finally, prepare

a drill schedule. When and how will you practice to ensure the plan works well and is understood by core stakeholders? Also, make sure you keep updated hard copies of the plan in case you are unable to access online resources during the incident.

Q. Have any recent, high-profile data breaches caught your eye? What lessons can we learn from the nature of the breach and the response of the organisations concerned?

HUMPHRIES: It is rare for a week to pass without there being a report of a data breach. There are a lot of common themes, from which lessons can be learned. Securing web applications is an area where organisations need to improve their focus for sure, as well as ensuring that the right tools are in place to detect potential attackers as early as possible. According to Mandiant's M-Trends report, the average dwell time – essentially the time it takes for an organisation to learn of a breach – is 101 days, which is an incredibly long time frame to investigate. Another area which can make a difference is the way in which crisis communications are handled. Over the last year, we have seen examples of good, bad and exceedingly ugly. How you communicate during and after

the event to your customers, stakeholders and anyone who is impacted, is a vital step in managing the incident.

Q. To what extent will the application of regulations such as the EU General Data Protection Regulation (GDPR) impact data breach planning and procedures?

HUMPHRIES: GDPR mandates that best practices are followed and that organisations notify the authorities within 72 hours of being aware of a breach. Fortunately, there has been some solid clarification from Working Party 29, who are helping to decipher GDPR, as to what 'being aware' actually constitutes. With the aforementioned average dwell time of 101 days, plans need to clearly identify roles and responsibilities, and communications requirements. GDPR also stipulates that organisations have a process in place to test out the efficacy of their security programmes, and arguably this has a knock-on effect to testing the efficacy of data breach response plans.

Q. What advice would you offer to companies on ensuring that they have the right people, processes and technology in place to

manage a data breach?

HUMPHRIES: Be realistic about whether the organisation has the means to effectively detect, contain and recover from a breach. Seek expert external guidance if you are unclear about what is involved in each of these tasks. Build a plan and run regular drills to identify shortcomings or weaknesses in the plan or response capabilities. Few organisations have sufficient people with the available time and right skills and experience to effectively manage breach monitoring, detection and response on their own. Automation via technology can significantly reduce the workload.

Machine learning as cyber defence

BY DOMENIC PUZIO

AS CYBER THREATS BECOME MORE SOPHISTICATED, simple rule-based approaches are no longer sufficient for detecting attacks. From advanced malware to cleverly-crafted phishing campaigns, cyber criminals are finding ways to evade traditional solutions. A more dynamic, proactive and intelligent technique is required to bolster security against these complex problems: machine learning. With machine learning, analysts have the power to learn from existing data, find hidden patterns and generalise knowledge to understand attacks that have not yet been seen. Machine learning will transform every aspect of technology, and cyber security is no exception.

The blacklist is one of cyber security's most prevalent tools,

but it is also one of its most rudimentary. A blacklist is just a series of rules – allow traffic from here, block this type of activity from there. They do a good job of stopping known threats that never change. If a fraudster always uses the same site as part of a phishing campaign, an analyst can simply update the blacklist to block that domain, stopping that threat with a single rule. However, life is rarely this easy. Rule-based defences have two critical failings: (i) they can only prevent or detect known attacks; and (ii) they are static, unable to adapt to even a slight change in an attack pattern.

Many traditional cyber security methods fall into the rule-based paradigm. Most anti-virus and malware detection tools use signatures, known sequences of behaviour, to find and stop malicious code activity. As new malware samples are created by attackers, analysts must first spot and decode them before they can understand their signatures and incorporate them into a detector. This means that the malware could be in a system for weeks or even months before analysts know its signature and update the rules of the system to detect it. Worse still, even after analysts go through the work of reverse-engineering a malware sample and adding its behaviour to a signature-based detector,

a small change to the malware's behaviour is all that is necessary to avoid being spotted by these new rules. Thus, rule-based solutions tend to be outdated, even if a large team is working to maintain them.

When a problem grows beyond the scope of listing rules, we should think about using machine learning, a technique that implicitly learns the relevant rules without instruction from a software engineer or domain expert. Understanding natural language is a good example of such a problem – as you read this, you are not thinking about the grammatical rules in place and how they confer meaning. The human brain stores implicit rules around language that allow us to understand the meaning behind these sequences of shapes that we call letters. Trying to write out all the rules for linguistic understanding would take ages; instead, we can use machine learning to teach our computer the principles of natural language. Instead of spelling out the rules, we pass tons of data to a learning algorithm, allowing it to infer the underlying structure of that data on its own. A key advantage of this learning process is generalisation. When properly trained, a machine learning model can generalise its learnings to new situations that were not present in the original data

that it was shown. To learn natural language, a machine does not need to see every possible sentence; with enough sentences (hundreds of thousands or millions), the model can generalise to understand scenarios that is has not yet seen.

This ability to pick up rules from existing data and generalise knowledge to new situations is what makes machine learning so powerful as a cyber security defence. Unlike a traditional rule-based system, a machine learning system is adaptive and can detect threats before they are known and analysed. Already, there is a huge volume of research that shows machine learning can make an impact on some of the most complex problems faced by security teams, from detecting intelligent malware to picking out expertly-crafted spear-phishing attacks.

Malware detection, which used to be entirely signature-based, can now utilise machine learning to demonstrate greater success. To do any damage, a machine infected with malware has to 'phone home' to the attacker to receive further instructions or send back sensitive information that it has found. The destination maintained by the attacker is called the command-and-control (C&C) hub. In the past, malware samples would have the C&C destination hard-coded, making it straightforward for

an analyst to find and blacklist. However, newer malware makes use of a domain generation algorithm (DGA), which pseudo-randomly creates fresh domains on the fly in order to avoid detection and rule-based blocking. Even if an analyst learns which domain is in use for C&C today, that domain will be irrelevant by tomorrow. Some malware even generates hundreds or thousands of domains to use every day, making it impossible for a blacklist to keep up. Since writing a rule for every new domain created by a DGA is infeasible, this is the perfect case for machine learning.

The algorithmically-generated domains of a DGA (for example, 'www.x4rjqs9.com') look very different from human-curated domains like 'www.linkedin.com' since domains selected by humans tend to be phonetically plausible, contain known words, and have a distribution of characters that mirror natural language. By providing a machine learning algorithm with many examples of legitimate domains and many examples of domains created by a DGA, we can train a model that learns the traits of an algorithmically-generated domain name. Now, instead of relying on a team of humans to pick out malicious domains by hand and blacklist them, a model can do that work, all without

requiring explicit programming.

Detecting malware that leverages DGAs is just one cyber security problem in which machine learning is being used to provide a more effective and dynamic defence. And while this use case certainly demonstrates the value of a machine learning solution, it also highlights the additional resources required to build such a solution. The most significant requirement is data. Data is the fuel that machine learning needs to be successful, so the first step for implementing a machine learning technique is to collect data, instrumenting everything. For a security system, this means capturing and labelling log data from sources like DNS servers and proxies. Machine learning also requires a different skill set from traditional programming; a mathematical background is important for modelling work, even as machine learning frameworks abstract away some of the more complex data science knowledge. Finally, once a machine learning model is built, putting that model into production requires nontrivial data engineering efforts, especially when that model needs to process large-scale information, which is often the case in the cyber security domain.

Machine learning is an ideal fit for defending against a variety of cyber threats because of its power to go beyond a rule-based approach, which can quickly become outdated. By learning the rules of a system rather than requiring that they be explicitly written, machine learning models can generalise to new situations and find previously-unknown attack patterns. However, to be successful, machine learning efforts require large datasets, skilled engineers and strong data engineering practices. Machine learning will empower the next generation of cyber security tools.

■ *Domenic Puzio is a machine learning engineer at Capital One.*

Intelligence gathering and analysis

BY GERALD REDDIG

WITH THE PROLIFERATION OF INTERNET of Things (IoT) devices comes an increased risk of cyber attacks. Last year's massive distributed denial of service (DDoS) attacks that infected IoT devices and services for many companies around the world served as a wakeup call for users, corporations and governments alike. Today, anything connected to the internet is at risk of an attack. In addition, compromised IoT devices can be used as a launch point to carry out attacks against other systems.

This year, more than 10 billion devices will connect to networks around the world, and that number is expected to grow tenfold over the following years. Applying conventional human-centric practices to IoT security management is not practical or sufficient,

as the rate of IoT adoption outpaces many organisations' ability to keep pace. There are simply too many devices to monitor, especially with the growing number of low-cost sensors and the temptation to connect everything to the internet.

Today, security professionals monitoring service provider and critical infrastructure networks often get more than 10,000 cyber security alerts each day. Not all these are security beaches. Many are false alerts and duplicate information. Yet, the sheer number of alerts can overwhelm a company's security team, resulting in incidents that are not investigated. For example, the Cisco 2018 Security Capabilities Benchmark Study found that on average, 44 percent of alerts are not investigated, and of those investigated and deemed legitimate, nearly half (49 percent) go un-remediated. Teams need better ways to automatically prioritise alerts that allow them to focus on the most severe ones first.

With the number of IoT devices today at 10 billion and counting, it is clear that conventional human-based security management is about to be overrun. There are simply too many devices to monitor and too many threats to address. The sheer diversity of IoT devices, from simple sensors to sophisticated devices that connect to the network and with each other, adds further complications.

And even if a device is being monitored, it is all too easy for conventional security systems to miss unwanted activity. For example, an IoT device may be performing its intended function, but still leaking data undetected.

The solution is to replace today's manually-intensive approaches with security systems built on three pillars – intelligence gathering and analysis with machine learning and automation.

Intelligence gathering and analysis correlates data from across the network, devices and cloud layers to spot suspicious anomalies, and provide insight into the nature of the threat, the associated business risk and the recommended response. In the example of a device functioning correctly but leaking data, security analytics could spot trouble by detecting CPU activity spikes or unusual levels of keep-alive signalling.

With machine learning (ML), the effectiveness of such intelligence gathering and analysis would increase continuously. Having access to a massive amount of high quality data is the basis for training an ML system. When using a security product that includes ML, you will want to augment the things you have done in the past, like signature collection and automated malware analysis, and combine them with the machine's capability to

determine new, malicious content. In addition to looking at bad data, you also need to have a large collection of good data, so that when it comes time to train the machine, it can accurately distinguish between what is dangerous and what is benign.

In December 2015, hackers launched an attack on Ukraine's electricity grid, leaving 250,000 people without power. The first outage was the result of the hackers gaining access to the utility's systems and manually switching off circuit breakers. But a 2016 attack on the utility is said to have been caused by sophisticated malware that could automate large-scale power outages on grids around the world. This reveals just how fast hackers are advancing their capabilities.

Automation is an essential component for intelligence gathering and analysis. There is a global shortage of cyber security experts that is forecast to grow to around two million unfulfilled jobs by 2019. Furthermore, current approaches are inefficient, with up to 33 percent of incident response time spent on manual processes, leading to delays in addressing and mitigating security issues. Combined with alert fatigue and time wasted on false alerts, many security breaches can go undetected. Security automation that encompasses business processes, regulations and

security policies are essential to keep pace with the rapid rise in attacks that will inevitably accompany the growth in IoT.

The traditional approach is largely based on manual processes without a centralised management system. This is still a reasonable approach for some organisations, but the increasing sophistication of attacks and growing regulatory complexity means this will not be a tenable approach in the medium term.

In spite of the multiple point products that organisations deploy as part of a defence-in-depth strategy, the volume and velocity of compromises and breaches continue to increase. These layers of protection are largely unintegrated, operate in silos and are difficult to manage, creating gaps in defences. Intelligence gathering and analysis can serve as the glue to integrate these disparate technologies, sharing the right intelligence with the right tools at the right time. Exporting curated intelligence directly to your sensor grid, (firewalls, anti-virus, IPS/IDS, web and email security, endpoint detection and response, NetFlow, etc.) allows these tools to generate and apply updated policies to mitigate risk. You can take a proactive and anticipatory approach to more effectively prevent attacks in the future.

When the time comes to take action, most security opera-

tions or investigations occur amid chaos as teams act independently and inefficiently. A single, shared environment where managers of all security teams can see the analysis unfolding, allows them to coordinate tasks between teams and monitor timelines and results. Threat intelligence analysts, security operations centres (SOCs) and incident responders can work together to take the right actions faster, reducing the time to response and remediation.

An expanded intelligence gathering and analysis solution enables security operations teams to automate and prioritise activities and report data to inform better business decision making. The use of automation leverages vendor APIs and software-defined security methods to rapidly respond to and prevent attacks earlier in the kill chain.

Recent attacks that have had a global impact are a warning call for users, corporations and governments. Yet, with the kinds of security management systems described above, they could have been prevented. It is time to act before further damage is caused.

■ *Gerald Reddig is head of product marketing, security, at Nokia.*

Time to strengthen cyber resiliency and increase investment in IoT security

BY JING DE JONG-CHEN AND ROB SPIGER

THE INTERNET IS A CHAOTIC AND VULNERABLE environment with more and more devices being connected to it. Internet of Things (IoT) devices, in particular, are becoming pervasive with applications across a wide spectrum, including consumer wearables, medical devices, vehicles, smart buildings, industrial control systems and more. The sheer number of IoT devices anticipated in the future may become unmanageable from a cyber security perspective unless technology addresses key aspects of device resiliency and manageability. IoT devices and related software applications are all subject to malware infection, yielding devices impossible for

people to identify or recover, preventing the restoration of functions as originally designed. Most concerningly, the gulf between society's increased dependence on IoT applications that are often lacking built-in security, and the rising sophistication of cyber attacks, if left unaddressed, can have serious and life-threatening consequences.

Traditional interactions between users and technology are often managed in an environment that has a limited number of known devices running known software. If malware infects devices or something else goes wrong, device owners or users have options to replace or restore the devices to a working state. For the future usage of IoT, people will be vastly outnumbered by devices both known and unknown, not fully aware if devices are corrupted or misbehaving at any given time, and not always able to manually identify, validate or restore even a small percentage of them. IoT devices will not be just in the office, by the user's side or in a data centre. Rather, they will be sprinkled throughout business facilities, hospitals, airports, homes and other private and public spaces, often without a direct human interface for recovery.

A wake-up call for both security practitioners and policymakers occurred on 21 October 2016, when hackers deployed malware

through phishing emails and took over many private networks. The attack infected a large number of low-cost consumer devices, such as DVRs, cable set-top boxes, routers and internet-connected surveillance cameras which were harnessed as a part of a botnet. These devices were controlled remotely by the hackers and sent a massive number of messages without owners' knowledge, bringing down the DNS servers operated by DYN, a US-based company that provides critical functions to keep the internet running.

Device infections generally have two stages. The first corrupts the code running on a device and gives malware control, like a burglar breaking into a house. The second persists the malware; even after a device is restarted it is still infected either by updating the stored code or configuration information. This is like a burglar keeping a house key to repeatedly enter at will. This pattern of attack can affect everyone with connected devices, including consumers, enterprises, governments and critical infrastructure operators.

FOUNDATIONAL IOT SECURITY AND RESILIENCY REQUIREMENTS

The ability to recover an infected device and to return it to a functional state is important for 'cyber resiliency', which is defined

by the US Department of Commerce National Institute of Standards and Technology (NIST) as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources". Understanding and enforcing the foundational device requirements of protection, detection, attestation and recovery are critical. These properties, coupled with the cloud management of devices at scale, can help IoT stakeholders address resiliency principles and prevent a digital future of rogue IoT solutions degrading or disrupting the internet, or worse, society at large.

Protection by design for devices means externally generated data is processed carefully by the devices to prevent corruption. Devices only accept code updates to device storage if the update package is cryptographically authenticated based on a valid certificate issued by the device maker. Devices should only accept configuration updates that are sanitised by their specific interfaces before persisting them. These are the same basic protection principles used to reduce infections in more complex systems like PCs and are powerful protection techniques for IoT devices as well.

Infection detection and recovery must be critical components of IoT design. Detection has limited effectiveness when attempted by a device in isolation. A device cannot know about new vulnerabilities or attacks, especially when device exploits are often specifically engineered to evade or degrade local device detection techniques. Devices need a reliable capability that checks for updates or recovery instructions from the device maker or operator over a network using a central management service, ideally in the cloud.

When a device connects to a network, the online service can require the device to pass verification to confirm that it has the latest updates and complies with related network security requirements. This process is called attestation. To achieve device-to-service attestation, each device must be identifiable, based on a unique device identity that cannot be mimicked by another device. This allows the management service to communicate with and interrogate each device individually. Device makers can issue certificates that include a device identity and help verifiers retrieve current information about software patches, other properties and expected behaviour.

Finally, devices need a mechanism to ensure forced recov-

ery when the device is running on outdated software, is infected by malware, or fails to verify itself with its online management services in a timely manner. Recovery and update functionality can be separated from the regular software environment that is more easily corrupted by attacks. Trusted execution environments or key isolation can allow the use of device identity secrets without providing a way for malware to transfer the information to other devices.

CLOUD-BASED MANAGEMENT SOLUTION

From scalability and manageability perspectives, a centralised, cloud-based management service can systematically verify the assets under remote management and confirm each device is updated and running the most current software mitigating against current and past vulnerabilities. With cloud management of devices, forced recovery can be initiated when the device is unresponsive to verification requests or is unable to prove the software version is current on the device. Devices that can prove their health are able to keep functioning without entering recovery. Connecting devices to cloud management allows the operators of devices to have a single account to connect to the

cloud and effectively manage an unlimited number of devices. It can also enhance security. Each device can use its device identity to cryptographically authenticate to the cloud, circumventing the need for device operators to manually maintain passwords based on weak defaults or user input for individual devices.

As a security best practice, device makers and software developers need to have the capacity to manage the entire product lifecycle once the product is released, including issuing security updates and assisting owners, operators and users with continuous security support to bring infected devices back to a functional state. Unfortunately, many IoT hardware suppliers and application providers are newer companies with minimal security and resiliency experience or which belong to traditional industry verticals without substantial security experience in connected technology. Raising awareness and increasing security investment to address the needs of the IoT sector are becoming urgent issues.

INDUSTRY COLLABORATION AND STANDARDISATION

An option to support inexperienced IoT suppliers is to consider the power of virtualisation and cloud. Cloud providers can ef-

fectively provide remote management services at scale. By migrating applications to virtual servers, businesses and IoT device makers can focus on developing and delivering products and services. In other words, less experienced companies can benefit from the collaboration with cloud infrastructure organisations and leverage their implementation of ongoing security policies and controls in the cloud. Cloud providers can benefit from managing diverse business applications and enhance their security expertise and capabilities in return. The result raises the bar for overall cyber security and resiliency.

The good news is that leading technology providers are moving quickly to provide new frameworks that enable small and medium-sized companies to implement their IoT application business ideas, including those sectors whose products historically have not been internet enabled. The frameworks include hardware reference designs, software architectures with manageability, security, resiliency and ways to orchestrate long-term lifecycle product support. This brings strong cyber security benefits. Technology investment can be made to refine capabilities and infrastructures to deliver security updates, verify devices, manage devices at scale, respond to incidents and fulfil

other cyber security activities required to properly operate IoT solutions.

IoT security and resiliency standardisation have become priorities for both public and private sectors. To date, progress has been made to define IoT resiliency design principles and trusted computing-based approaches for protection, detection, attestation and recovery. Examples include the draft NIST Special Publication 800-193 and standards like the Trusted Platform Module (ISO/IEC 11889) and the Device Identifier Composition Engine (DICE) from the Trusted Computing Group. More effort is needed to create standards and ecosystem support for how devices enter forced recovery spontaneously to repair while infected with malware.

CONCLUSION

To summarise, the IoT industry is new and cyber threats are on the rise. While IoT applications are enriching the lives of people in a connected world, they are also pushing the limits of technology. Innovations for IoT must strive to balance computation capabilities, power consumption, persistent storage, network capabilities, manageability, security and resiliency. Continued

partnerships and investment are needed throughout the IoT ecosystem. Stakeholders from both the public and private sectors need to consider how policies and innovations address security, cyber resiliency and device management. As the world experiences rapid digital transformation, it is a prerequisite that IoT devices must be designed and managed with security and resiliency throughout their lifecycle for the benefit of all.

■ *Jing de Jong-Chen is a general manager of global cybersecurity strategy and Rob Spiger is a principal security strategist at Microsoft Corporation.*

Cyber risk and directors' liabilities – the risk landscape and how to navigate it

BY STEVEN HADWIN

IN THE LAST COUPLE OF YEARS, cyber risk in the financial services sector has undergone a surge in prominence. There are several reasons for this.

One reason is an increasing number of high-profile, adverse cyber incidents that have brought the issue of cyber risk to the public's attention. The threats to companies in the financial services sector arising out of cyber risk are now well-known and incidents that have led to loss of profits, reputational damage, regulatory liability and third-party litigation have been reported in various regions.

Another reason is forthcoming legislative change relating to the use of technology and data, which will have a significant impact on the financial services sector, particularly in Europe. Most prominent among these changes is the EU General Data Protection Regulation (GDPR), which imposes enhanced data privacy obligations on organisations that control or process personal data in a European context. Certain incidents affecting personal data will need to be notified to the relevant data privacy regulators within 72 hours, and notifications to affected data subjects may also be required. Penalties for non-compliance with GDPR are severe, with potential fines up to 4 percent of annual global turnover or €20m (whichever is greater) in certain circumstances.

A broader expectation that organisations will safeguard personal data and implement appropriate cyber security is also a key development in this area. This expectation manifests in a number of ways – the English courts, for example, are seeing an increased frequency of claims against companies by individuals for misuse of private information, as well as direct claims brought by individuals who have suffered loss as a result of breaches of data protection legislation. Claims of this nature

can now be brought in respect of distress only – claimants do not need to demonstrate financial loss as the basis of a claim. This expectation is particularly prominent in the financial services sector.

Finally, regulators in the financial services sector are taking an active interest in investigating adverse cyber incidents affecting companies that operate in the sector and in engendering a culture of accountability for cyber incidents. Significant fines have been imposed in a number of jurisdictions where adverse cyber incidents (and the consequences flowing from them) have been deemed to be a breach of rules, regulations or principles applicable to that company.

Companies, therefore, face a more challenging landscape than ever before when it comes to the potential losses and liabilities arising out of cyber risk. Given that those costs are significant (with a recent study suggesting that the average cost of a significant data breach is over $4m), cyber risk management is inevitably high on the agenda of boards in the sector.

However, what is often less well-understood is how a failure by the board to manage the risk appropriately might lead to individual liability on the part of board members. While, to

date, in many jurisdictions personal liability of directors in this context has not been common, it is worth noting the below potential sources of liability in this area which exist, in one form or another, in a range of jurisdictions.

First, liability for breaches of fiduciary duties to the company for failure to manage cyber risk appropriately. This is increasingly common in the US where shareholder derivative actions are often brought following data breaches. Settlements in such cases can be significant. Such claims can also lead to the removal or resignation of key board members, even in circumstances where formal liability is not established.

Second, liability for breaches of regulatory duties imposed on directors or other key individuals of entities that are regulated in the financial services sector, such as under the UK Senior Managers' Regime.

Third, liability for breaches of data protection or cyber security laws, to the extent those laws provide for personal liability of responsible individuals.

Finally, direct claims brought against board members by third parties, such as tort claims for personal negligence in the handling of data or the use of technology.

As expectations continue to grow as to a board's ability to understand and manage cyber risk, these sources of potential liability are likely to become more prominent. This may be an intimidating prospect for individual directors who frequently see cyber risk as a technical challenge which they may not have the necessary skills or knowledge to understand.

However, effective cyber risk management at the board level does not necessarily require a detailed individual understanding of the technical issues on the part of all board members. There are a number of steps which a board can take in order to effectively assess and manage cyber risk in this regard.

The first step should see directors ensure that the company has a full understanding of the technology it uses and the data it holds. Directors should obtain input from internal and external experts in order to understand fully the scope of the cyber risks that the company is facing – establishing a cyber risk committee is often an effective means of ensuring that the board has access to people with the required skills and knowledge for these purposes.

The second step should see directors ensure that investment in cyber security is given appropriate priority within the

company. This would include technical security, as well as the fostering of a good cyber risk management culture by way of regular training and education to employees.

The third step relates to the cyber resilience of the company, which should also be scrutinised by the board. This essentially means assessing the company's ability to continue to do business in the event that it is affected by an adverse cyber incident.

The fourth step should see directors ensure that the company has appropriate policies and procedures in place relating to the use of technology and data, which factor in the full suite of legal and regulatory requirements that the company is facing in this area. This should include a cyber incident response plan, detailing the practical steps to be taken in the event of an adverse cyber incident and the internal and external resources which will be available to assist with a cyber incident response should the need arise.

The final step should see directors guarantee that these policies and procedures have been stress-tested for effectiveness and that they are kept under review in order to reflect the changing cyber risk landscape that the company will inevitably

be facing.

Cyber risk management is not a question of eliminating cyber risk, but of diminishing it. This is true of the risk of individual liability of directors, as well as of the risks to the company. The liability risk can never be eliminated, so board members should always ensure they have adequate protection, ideally by way of an indemnity for the company for liabilities arising out of the conduct of their role and by way of appropriate D&O insurance.

If a board can demonstrate that the above steps have been taken to manage and mitigate the cyber risks that the company is facing, the individual liability risks set out above should themselves also be diminished.

■ *Steven Hadwin is head of operations for risk advisory and cyber security at Norton Rose Fulbright LLP.*

Cyber security in diligence for investments, mergers and acquisitions

BY EMILIAN PAPADOPOULOS

IN JULY OF 2017, AVAST, A GLOBAL anti-malware vendor headquartered in the Czech Republic, acquired the company Piriform and its product CCleaner, a software solution that cleans up unwanted files from personal computers and workstations.

Two months later, researchers at Avast and at Talos, the threat intelligence team of IT giant Cisco, reported that Piriform had suffered a cyber security incident.

Hackers had compromised Piriform's CCleaner product and used it to distribute malware to 2.27 million customer computers between August and September 2017. The malware was

a 'backdoor' that gave hackers remote access to infected computers. Next, the hackers reportedly used this access to target companies such as Intel, Sony, Samsung and VMWare. In a blog post, Avast's chief executive Vince Steckler and chief technology officer Ondrej Vlcek wrote that the attack, which researchers believed was conducted by Chinese hackers, "was targeting select large technology and telecommunication companies in Japan, Taiwan, UK, Germany and the US". To its credit, Avast appeared to respond quickly, once it realised what was happening, to update the software, notify affected customers and work with law enforcement.

The full extent of harm suffered by Avast or its customers may never be fully understood, but whatever the costs, business disruptions and reputational consequences suffered by Avast, they were likely far greater than if they had discovered the problem during diligence, before acquiring Piriform.

Looking back, Avast's CTO, Mr Vlcek, said: "What we didn't know was that before we completed the acquisition, the bad actors were likely already in the process of hacking into the Piriform systems." In a recent interview, he added: "We bought the company while it was being compromised."

For Vlcek, the lesson learned is clear: "When doing M&A, cyber-due diligence is really important... a no-brainer."

The fact that a cyber security company failed to do cyber diligence may be ironic, but it should not be surprising. Many companies, even ones that sell cyber security solutions, do not do adequate cyber security diligence during investments, mergers and acquisitions (IM&A).

The Avast case focuses on hackers targeting big technology and telecommunications companies. So too does the well-known case of Verizon and its acquisition of Yahoo, in which Verizon learned of Yahoo's massive breach of account details with just enough time before the deal closed to negotiate a $350m discount on the purchase price.

It would be wrong to think that hackers always target big companies, or companies with sophisticated intellectual property (IP), or even companies with lots of credit card data, like Target and Home Depot, which have both been hacked in previous years.

Hackers target all kinds of companies. They have targeted companies that make paint, companies that sell ice cream and companies that manufacture electric components. They target

private equity firms and hedge funds. They target universities, think tanks and law firms (a lot). They target big companies and small companies alike. Sometimes, they target smaller companies, like Piriform, to get to bigger companies, like Samsung or Intel. Target was hacked through a vendor that provided its heating, ventilation and air conditioning (HVAC) services. Finally, companies can be disrupted by indiscriminate malware that is not targeted at all, such as ransomware, which locks up computer files until a ransom is paid and often spreads automatically from computer to computer, network to network.

CYBER SECURITY DUE DILIGENCE

Thus, every company that engages in IM&A should be doing cyber security diligence on its target. Unfortunately, cyber security diligence is hard to do and to understand. It is new, having emerged for the most part in the past two years, and it lacks established best practices that exist in other areas of diligence. Cyber security diligence can also be challenging to adopt because it frequently delivers bad news about risks or incidents that are hard to mitigate. Nonetheless, mature companies are endeavouring to integrate it as a routine part of their diligence, since

the benefits of doing it, or the consequences of not doing it, can be so significant.

What are those consequences? Without adequate cyber security diligence, an acquiring entity will absorb unknown risk. It may acquire a company that has already had its IP stolen, harming its competitive prospects. It may acquire a company that is actively compromised, in which case the IT systems of the acquiring entity could be put at risk, too. Or, it may acquire a company that is ill-prepared and at risk, which will require the acquiring entity to spend resources bringing the target's cyber security up to code.

Conversely, a company that does cyber security diligence has options: it can seek representations and warranties from the seller, it can buy additional insurance for the transaction, it can plan ahead to improve the target's cyber security and factor those costs into the transaction or, in the most extreme cases, it can decide to restructure or decline the deal. At minimum, a company that does cyber security diligence enters the transaction with eyes wide open and having signalled to the target that cyber security matters.

GETTING STARTED

Given all this, doing cyber security due diligence should be, as Mr Vlcek said, "a no-brainer".

Companies can adopt the following three practices to help achieve effective cyber security due diligence. First, start early. Cyber security due diligence takes time. Target companies often do not expect to undergo cyber security due diligence, so their relevant records may not be organised as well as records about finance, human resources or customer contracts. Cyber security diligence also requires time on-site that must be scheduled in advance. Without an on-site assessment, companies can put policies on paper or respond to questionnaires in ways that imply they have good cyber security when they actually do not.

One of the most important questions that cyber security diligence tries to answer is, "has this company already been compromised?" The follow-up is, "Would it know?" Most incidents take weeks or months to discover. Answering the first question may require a technical compromise assessment of IT systems to look for indicators of compromise, and this process takes weeks.

Second, recognise that cyber security is a business issue,

and a whole-of-business issue, not just a bits-and-bytes issue. Cyber security is not just about IT. Effective diligence should start by understanding the business. What sector is it in? What is its business model? What sensitive information does it hold? What IT systems does it depend on? What value is the acquiring entity trying to capture? And what are the cyber risks to that value? In short, what could go wrong?

Cyber security risks vary widely across businesses. An easy way to see this is to look at the varying threats facing different sectors, as reflected in Verizon's 'Data Breach Investigations Report'. The 2018 report examined hundreds of incidents and breaches across various sectors. In the accommodation and food services sector, 99 percent of incidents came from external sources. In the healthcare sector, however, only 43 percent of incidents were external, while 56 percent were internal. In accommodation and food services, 99 percent of incidents were financially motivated, whereas in the manufacturing sector, financial motivations explained just 53 percent of incidents, with espionage accounting for another 47 percent of incidents.

Effective cyber security diligence must also examine governance (who is responsible for cyber security and how are they

managing it?), policies and technologies (how well is the company securing its systems?), and crisis management (is the company prepared to handle a cyber security crisis?). Effective cyber security diligence will probe the company's cyber insurance, the composition of the cyber security team and spending. If the companies will incur substantial costs to clean up a compromise or to get the target's cyber security up to the acquiring entity's standards, how will this affect the financial attractiveness of the deal?

Third, use the entire diligence team. Since cyber security is a whole-of-business issue, effective diligence requires a whole-of-team approach on the part of the acquiring entity, too. Technical assessments alone are not enough. For diligence to be effective at identifying and mitigating risks, the acquiring entity must bring its whole team to bear in an integrated approach. Of course, cyber security experts will lead this portion of the diligence, but they must work with the business-oriented team to understand the business context, the finance team to assess spending and financial risks and the legal team to write protections into the terms of the transaction. These teams will not all speak the same language or have the same perspective, and dil-

igence is already a challenging, time-constrained exercise, but starting early can help, and success is possible.

CONCLUSION

Cyber security due diligence can reduce risk and even generate value by improving deal terms, aligning teams and planning ahead for improved cyber security. Cyber security due diligence is also hard, the issue is complex, the IT environment and threats keep changing and best practices are just beginning to emerge, since it is a relatively new discipline. Nonetheless, we can learn from the experiences of others: "it's a no-brainer".

■ *Emilian Papadopoulos is president of Good Harbor Security Risk Management.*

Modern vulnerabilities in high-target industries

BY STEVE POVOLNY

EVOLVE OR DIE. IT IS A SIMPLE MANTRA, reflected in nearly every industry. Take automotive, for example: those who cannot adapt to the pressing demands for innovative technology – such as electric/hybrid energy, autonomous driving or even smart phone integration – will almost certainly finish last in the highly contested race for automotive market share. Another example is transportation and shipping. Consider the nascent technologies currently being tested to improve the speed, efficiency and accuracy of shipping or transporting goods. In the last few years alone we have seen vendors testing drones for delivery, smart sensors for fleet telematics and, in an example that should hit close to home for many, GPS data harvesting for traffic control

and route planning. These are just a few areas in which several vendors have increasingly invested in the 'do or die' mentality of technology adaptation.

With this wonderful, breakneck speed of innovation comes the darker side of security, or to be more accurate, *in*security. As nearly every industry in the world attempts to connect itself more, deploy more code, distribute more systems and manage more technologies, we observe the corresponding negative side effects. The most notable of these is insecure software development. In a rush to get to market, secure coding practices have become of secondary, or perhaps even of tertiary importance. As a result, industries that should prioritise security above all else are subject to the same flaws as their less critical counterparts. Consider industrial controls and, specifically, supervisory control and data acquisition (SCADA) and human-machine interface (HMI) software as some of the best examples of this problem. Although much of the United States' infrastructure may not be directly connected to the internet, there are often gateways to this infrastructure from private and public networks (often including even the internet), controlled or managed by HMI software.

You have only to look at MITRE's Common Vulnerabilities and Exposures (CVE) repository to find the extent of vulnerabilities in this critical software category. A simple regular-expression search returned well over 500 unique vulnerabilities in SCADA or HMI type systems. When reviewing ICS-Cert's vendor vulnerabilities tracking, we come up with nearly 900 unique vulnerabilities. These vendors release products that control key infrastructure in all industries, including the power and energy grid, transportation, robotics and manufacturing, weapons deployment, national infrastructure including water and roadways, and much, much more. You might think the former list of vulnerabilities requires an exceptionally skilled hacker to exploit, but you would be mistaken.

Let us analyse a CVE entry (CVE-2017-14016) in Advantech's SCADA component 'WebAccess', an HMI software used as a front-end interface for deployment and management of SCADA systems, including real-time data, control, alarms and logs. (Imagine being able to remotely enable or disable an alarm system for a nuclear energy facility.) Without diving too deep into the technical analysis of the vulnerability, it is worth examining its relative simplicity. The bug is a standard buffer overflow:

an attacker can provide a larger amount of input data than the software programme expects, causing the memory region that was created to hold this data to overflow with input, and allow the attacker to write arbitrary code into otherwise protected areas of memory. With just a small amount of exploit code, an attacker can gain elevated access and control the operations of the exploited system, in this case enabling or disabling alarm functionality, editing or scrubbing access logs and probably much more. What could make this even easier? One such exploit is currently available in the popular open-source penetration-testing tool Metasploit.

The ease of access to canned exploits, the trivial nature and impact of these exploits, and the ubiquity of deployment for the software make for a perfect storm from an attacker's vantage point. This is not an isolated example. A quick search shows an additional seven exploit modules for various Advantech vulnerabilities in Metasploit alone.

This is just one SCADA vendor in a lengthy line-up of vendors that have been exposed to numerous trivial software flaws in their products. Time will tell if this negative attention results in more secure coding practices; to date, we have not seen sig-

nificant changes from most of them. This vendor has what is considered a relatively 'fast' patch cycle, at a still-comical 131 days on average.

Although a large number of CVE may be a good indicator of the level of interest by attackers, what about the inverse? When we observe certain sectors in which we do not see many CVE reported, could there be a message to draw from this as well? Possibly. In many cases we see the alignment of interest between security researchers and malicious hackers. This is because, like it or not, we are often learning from and reacting to each other. When a new exploit is presented at a major conference or a new paper on a mitigation bypass is produced, attackers quickly look to implement that knowledge and adjust their techniques. However, security teams and technologists share the same benefit from the research and can adapt both products and security solutions to incorporate the same techniques defensively. Should we be concerned if a certain attack surface or industry vertical does not contain a sizeable number of reported vulnerabilities? It is certainly worth further exploration. SCADA is being actively researched and reported on by 'whitehats'. If that industry were being quietly researched only for malicious purposes, it would

leave a large knowledge gap for the security and software development community. These are industries that deserve special attention.

We have learned from the preceding examples that high-profile industries are susceptible to design flaws and software issues which can be easily exploited with devastating impact. Because we are interested here in 'modern vulnerabilities', let us pivot to some of the most popular vulnerabilities in today's threat landscape.

We see many of the familiar vulnerability categories when viewing the OWASP Top 10 Application Security Risks for 2017. These include web-based vulnerabilities such as cross-site scripting, SQL injection and other categories of injection flaws, and authentication failures, among others. Each of these has been a top offender for many years, and will likely continue to be for years to come. Perhaps more interesting is the list of non-traditional vulnerabilities we have observed in the last 12 months. Let us reflect on a few recent but still modern vulnerabilities to predict what we may see in the near future.

First, we have the 'should-have-been-pwny-worthy' infamous Apple root password bypass from late 2017. In an age

with multiple layers of security mitigations, defence in depth and code reviews, this vulnerability allowed any MacOS High Sierra user to log in via an empty password for the root account. Nothing more needs to be said about this one; let us just pretend it never happened.

Last year also demonstrated how closely assimilated the whitehat and blackhat worlds are. After a public dump from the hacking group Shadow Brokers in 2016, security researchers scrambled to understand the stolen hacking tools and exploits, just as malicious actors worked to analyse and weaponise the same set of vulnerabilities. Even with a head start, the entire world felt the impact of the vulnerability EternalBlue as it was propagated in the network worm WannaCry. This simplistic vulnerability was present in the server message block (SMB) protocol, which, for no good reason whatsoever, was still widely in use on a global scale, and in many cases at the network perimeter. The most publicly-exposed industries for the exploit included major companies across healthcare, telecommunications and the energy sector.

Later in the year researchers uncovered a vulnerability in WPA2, a Wi-Fi network encryption standard that allowed hack-

ers to hijack communications between supposedly trusted entities. Until this point, WPA2 was widely considered to be a de facto secure authentication protocol used by nearly every Wi-Fi network in the world.

Last, but certainly not least, come the Spectre and Meltdown vulnerabilities from the first days of 2018. These highlight a different class of vulnerability entirely, being present in both software and even the hardware architecture of major chip manufacturers. These critical bugs allowed extremely sensitive and protected memory in the operating system's kernel to be read, on almost every computing device. (Researchers had discussed theoretical attacks against these chipsets in whitepapers for several years prior to the public disclosure of these two major bugs.)

This sample set of vulnerabilities represents a continuation of well-known security issues that we have been exposed to for decades. Security researchers and malicious hackers are not reinventing the wheel; they are finding and exploiting configuration issues (Apple root bug), classic buffer overflows (EternalBlue SMB), authentication bypasses and man-in-the-middle attacks (Krack WPA2), and even time-of-check, time-of-use (TOCTOU)

memory bugs such as Spectre and Meltdown. These are all variations of vulnerability concepts that are well known

We can learn from these examples as we look to securing the future; there is no industry that is untouched by the reach of security flaws. From banking to retail, from education to industrial controls, from autonomous driving to aviation, and from energy to e-commerce, we need a heightened focus and an intentional investment in secure software development to tip the scales in our favour. Vulnerability research and responsible disclosure will continue to educate vendors and industries on the true cost of breaches. We know that security will always be a journey, not a destination – but if we do not want someone else to drive us off the road, we had better take the wheel.

■ *Steve Povolny is head of Advanced Threat Research at McAfee.*

Recent cyber attacks and high-profile cases: say safety, think security

BY ROBERTO MINICUCCI, MATTEO CAMPRINI AND MASSIMILIANO COPPONI

DURING THE LAST 10 YEARS, ATTACKS against industrial control systems (ICS) have been constantly on the rise. As a consequence of reduced availability and loss of sensitive data, owners of compromised facilities have felt significant financial impacts. Here, we will discuss the increased dependency between security and safety, starting with a recent attack which was specifically designed to compromise a safety instrumented system (SIS). We will first describe the attack steps and mitigations which may have proved effective, then look at the international standards and draw some conclusions.

INTRODUCTION

The focus of the ICS community on security principles sharply increased in 2010 when Stuxnet malware, which was designed to target an Iranian uranium enrichment facility, destroyed or caused physical damage to more than 900 rotating machines, mostly (but not only) within Iran's nuclear centrifuges. After this event, ICS providers and end-users started adopting approaches and techniques from IT and secure software development domains, appropriately tailored to match the peculiarities and priorities of an industrial control network.

In parallel, several factors have contributed to dramatically increase the exposure of ICS to cyber attacks. In order to achieve more aggressive financial targets in terms of production optimisation and reduction of OpEx and CapEx, a shift towards a more collaborative working paradigm based on pervasive connectivity was needed. This resulted in convergence of automation technologies and media towards enterprise or even consumer solutions.

Legacy standalone control systems have progressively evolved to distributed architectures. In several cases, the traditional ICS design approach – which is based on physical or at least logical segregation between control network and plant com-

munication infrastructure – has been replaced by a flattened architecture with safeguarding systems, process control systems, enterprise data collectors and monitoring interfaces located on the same general-purpose network.

Other market trends that have significantly contributed to increase the attack surface are the extensive use of remote monitoring and troubleshooting services. To reduce the need for qualified personnel at site, the adoption of remotely-operated devices (e.g., drones) perform risky operations without the need for human personnel, the expanded footprint of a vendor ecosystem and the introduction of cloud data storage and processing.

CASE STUDY: HATMAN/TRITON ATTACK

On 14 December 2017, a cyber security attack on critical Middle East infrastructure was publicly disclosed by Schneider Electric. The attack was conducted by means of a malware (known as HatMan) explicitly designed to compromise Triconex/Tricon controllers used in plant SIS. Media refer to this malware as both 'Triton' and 'Trisis'.

The SIS was compromised using a two-step strategy. Attacker's first gained remote access into the ICS network via unknown

means, then infected an engineering station running Microsoft Windows. After that, they used the malware framework loaded on the infected workstation to connect to a safety controller and to reconfigure it, leveraging on proprietary OEM protocol.

What is peculiar about this cyber security breach is the use of a malware specifically designed to emulate the protocol and sequence of commands normally used by a development tool designed by the OEM. This result is achievable only by means of an accurate reverse-engineering process which, in turn, requires technical skills and resources that were not commonly observed in previous attacks on ICS systems.

Moreover, the availability of a toolkit capable of reconfiguring a safety controller from any PC connected to the plant control network dramatically increases the attack surface, compared to a more traditional scheme which would require the attacker to compromise the dedicated engineering workstation where the OEM development tools are installed. Despite these unique features, Triton was still affected by two weak points that, most likely, limited the consequences of the attack.

The first weak point represented by the physical security measures implemented by the OEM is that Triconex safety con-

trollers are equipped with a key switch that allows CPUs to be reconfigured only when set to the 'program', i.e., maintenance, position. Attackers must then either wait for someone at site to switch the mode to 'program' or have an accomplice inside the victim company switch it for them.

Also, since the controller is set to 'program mode', there are limitations to the activities that can be performed without rebooting it, which represents a second layer of protection from an attack which aims to cause more severe consequences than a simple plant shutdown. In the event, this happened on 14 December. The layer of protection provided by the key switch was defeated because the selector was in 'program mode' position, for reasons as yet unknown. Fortunately, validation checks performed by the Tricon firmware detected an anomaly caused by a bug in the Triton malware framework, and, consequently, the controller was repeatedly rebooted, therefore triggering operators' attention.

CONCLUSIONS

Although the HatMan/Triton malware is not capable of compromising an industrial facility (safeguarding systems do not

directly control the process, so a degraded system will not cause a correctly-functioning process to misbehave), it could be extremely damaging when combined with a second attack that simultaneously compromises the process controller or when safety and process control functions are tightly integrated.

The security community views Triton as the first part of a two-step attack designed to cause a destructive event, not just interruptions. More concerns are arising due to Tricon being one of the few safety controllers approved by the US Nuclear Regulatory Commission (NRC) and, as such, it is one of the most widely-used platforms within that infrastructure.

Looking at the regulatory framework, industry awareness of the interaction between safety and cyber security has matured over the last few years, as witnessed by the increasing number of standards and initiatives revolving around this topic, such as IEC 62443-2-4, IEC 61511, new revision of IEC 62061 and IEC 61508, IEC TR 63069 (draft) and IEC TR 63074 (draft).

Despite a growing focus on this topic, some challenges are still unaddressed, including legacy SIS controllers which have never undergone a security assessment and have all design and implementation vulnerabilities present in dated control sys-

tems. Moreover, many of the above-mentioned standards are either non-prescriptive or generically refer to high-level risk assessment activities. In some cases, such as API670, IEC 61508-3, and 62443-2-4, there have been attempts to clarify more relevant requirements, but, at present, a common and widely-approved methodology for joint management of safety and security is not available.

This is the direction we think should be pursued: more detailed guidelines on ICS safety-security principles, definition of roles and responsibilities for manufacturer, integrator and end-user, and a set of minimum security requirements that an ICS platform needs to fulfil to achieve functional safety certification.

As hinted above, additional challenges come from an industry trend towards integrated architectures – systems which have components common to process control and safety must trigger a greater focus. This is typical for continuous/high-demand mode scenarios of operation, such as in the automotive sector or manufacturing facilities. We believe it is pointless to counter this approach, but at the same time it should pair with built-in security mechanisms (key switches, protocol authen-

tication, data encryption, network segregation, etc.), and with detailed rules for verification that the actual security measures have been correctly implemented in operations and are properly managed throughout the product lifecycle.

In the absence of such actions, we will prepare for the next Triton, which will come, since attackers now know where (else) to look.

■ *Roberto Minicucci is a senior director and Matteo Camprini is a principal engineer at Baker Hughes, a GE company, and Massimiliano Copponi is a senior engineer at General Electric.*

Protecting the electric power industry from cyber threats

BY SCOTT AARONSON

RECENTLY, THE DEPARTMENT OF HOMELAND Security and the FBI identified Russia as the source of last summer's cyber attack that targeted the business networks of America's electric companies. While the attack did not impact the energy grid, the government's unprecedented public acknowledgement underscores how serious cyber security is to US national security. In the face of evolving cyber and physical threats, cooperation between the electric power industry and government is more important than ever in order to protect the energy grid.

The Trump administration has already taken significant steps to enhance coordination between the electric power industry and the federal government. Earlier this year, secretary of energy Rick

Perry announced the creation of a new Office of Cybersecurity, Energy Security, and Emergency Response (CESER), to help the electric power industry better protect itself from future cyber attacks and to continue to provide a reliable supply of electricity to customers. We value the Department of Energy's (DOE) partnership as the electric power industry's sector-specific agency, and we expect the new CESER office will further advance the role of coordinating government and industry efforts to address evolving threats to the energy grid.

America's electric companies work every day to produce and deliver energy that is reliable, affordable, safe and increasingly clean for their customers. The energy grid powers our economy and our way of life, so providing reliable service is a responsibility electric companies take very seriously.

Threats to that reliability have changed over time and continue to evolve. So, too, has our approach to security. The industry's member companies prepare for all hazards – that means physical and cyber events, naturally occurring or manmade threats and severe weather of every kind. Since companies cannot protect every asset from every threat all the time, we must prioritise based on the likelihood and severity of a threat. We also focus on man-

aging consequences by preparing to restore power quickly and safely, regardless of why an outage occurred.

Companies are taking a 'defence-in-depth' approach with several layers of security strategies, designed to eliminate single points of failure. The three main components are mandatory and enforceable reliability regulations, industry-government partnerships across all levels of government as well as with other independent sectors, and efforts to enhance response and recovery when incidents occur.

First, under the Federal Power Act and Federal Energy Regulatory Commission (FERC) oversight, the electric power industry is subject to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards that include cyber and physical security requirements. Entities found in violation of CIP standards face penalties that can exceed $1m per violation, per day. These mandatory standards continue to evolve using the process created by Congress to allow for input from subject-matter experts across the industry and government.

Second, in an ever-changing threat environment, constant information sharing across the industry and with government

partners is critical to the defence-in-depth approach to cyber threats. We are working in a complex ecosystem where the defence capabilities of one privately-owned business might not be enough to stop nation state actors. That is one reason why grid security is ultimately a shared responsibility between the private sector and government.

To address national-level threats to critical infrastructure, the industry leverages its robust partnership with the federal government through the Electricity Subsector Coordinating Council (ESCC). The executive-led ESCC coordinates with senior officials from across the federal government, including the White House, the Office of the Director of National Intelligence, the Departments of Energy, Homeland Security, and Defense, FERC and the FBI to improve security, improve situational awareness, deploy resources and enhance preparedness.

Coordinating directly with the government allows the industry to take a more comprehensive approach to identifying, assessing and mitigating threats and suspicious activity. The government regularly provides classified briefings to system operators regarding the latest threats to the electric power industry. When companies receive actionable intelligence, they are able to

take action to prevent or mitigate future attacks.

Another information-sharing partnership, the Cybersecurity Risk Information Sharing Program (CRISP), brings together the electric power industry, DOE, Pacific Northwest and Argonne National Laboratories, and the Electricity Information Sharing and Analysis Center (E-ISAC). More than 75 percent of US electric customers are served by a company that has deployed CRISP, and this programme will continue to grow as the information gleaned from its sensors and the associated analyses have proven extremely valuable to identifying and addressing security risks. These long-term partnerships are helping the industry identify cyber security threats before they can cause harm, and they allow industry and government stakeholders to develop the capabilities needed to mitigate any impacts and to address outages quickly and safely.

The third part of the defence-in-depth approach focuses on resiliency and on being prepared to respond in the event of an outage. When outages happen, many key investments help companies restore power safely and as quickly as possible. The industry invests more than $100bn each year to make the energy grid stronger, smarter, cleaner, more dynamic and more secure.

The US public depends on the industry to restore power safely and as quickly as possible, and industry-government exercises regularly test capabilities and responses to outages before they ever need to be put into action. This past November, more than 6000 participants representing more than 400 organisations from across the electric power industry and federal and state governments participated in NERC's grid security and incident response exercise, GridEx IV. This two-day exercise was designed to test coordination among industry and government stakeholders, as well as cyber and physical security incident response protocols. The biennial exercise gives participants from the US, Canada and Mexico the opportunity to self-assess their emergency response and recovery plans through a simulated exercise that takes place across North America.

The defence-in-depth approach to cyber security also can be illustrated through mutual assistance, which is a hallmark of the electric power industry. Because the energy grid itself is so interconnected and because daily life is so dependent on the power it provides, electric companies need to respond quickly to natural disasters. The industry has a longstanding culture of sharing critical personnel and equipment when responding to emergencies.

Even before a storm hits, men and women from across the US are likely travelling to other states to aid in restoration efforts.

When it comes to cyber attacks, there are no warnings from weather reports, and companies may not be able to focus their attention to one geographical area. That is why the electric power industry has developed a Cyber Mutual Assistance (CMA) programme, based upon the effectiveness of traditional mutual assistance networks, to improve the industry's emergency response capabilities. During GridEx III in 2015, several industry executives identified the need for a programme that would help electric companies restore critical computer systems following a major cyber incident. The CMA programme was developed and launched by the ESCC within a year, and it was exercised during GridEx IV.

Participation in the CMA programme is open to all entities that provide or materially support the provision of electricity or natural gas service. When new entities join, they sign a non-disclosure agreement that provides mutual assurance that sensitive security or operational information remains protected. Participants also do not pay anything to join or activate the programme beyond reimbursing any company or entity for operating costs associated with providing emergency cyber assistance.

If a cyber attack occurs and overwhelms an organisation's ability to respond, its CMA coordinator can call upon the CMA programme participants to assist it in responding to the situation. That means tapping into a network of more than 140 entities, representing investor-owned electric companies, municipal utilities, electric cooperatives, natural gas companies, regional transmission organisations and independent system operators and Canadian electric companies. This network covers approximately 80 percent of US electricity customers and roughly 75 percent of US domestic natural gas customers.

In today's dynamic threat environment, programmes like CMA and CRISP are critical tools for the electric power industry to ensure its ability to provide reliable energy to customers. The energy grid is the backbone of the US economy and critical to the life, health and safety of all Americans. In the face of evolving threats, the industry will continue to invest in security, improve information sharing, further develop mutual assistance networks, and strengthen government and cross-sector partnerships.

■ *Scott Aaronson is vice president of security and preparedness for the Edison Electric Institute.*

The outlook for cyber crime

BY VICTORIA BAINES

PREDICTING THE FUTURE WITH ANY KIND of certainty is a fool's errand. Technology is by its very nature disruptive. Its mainstream adoption can have unforeseeable and far-reaching impacts, as the internet itself has demonstrated. But by assessing the risks of emerging technologies against current knowledge of cyber criminal activities and behaviours, organisations can increase their preparedness for emerging threats. This in turn can reduce the time taken to respond to cyber attacks, and the financial cost attached to reputational damage.

It has long been said that it can be difficult to determine whether a cyber crime is financially or politically motivated – at least at first. Historically, if the method of an attack included a means of generating revenue, it was assumed that the motive was chiefly financial. By that same logic, state sponsored cyber

espionage appeared to be in a different class.

But when data is so fundamental to the health of national economies, all cyber attacks are arguably matters of state security. In no other field of operations is the line between civil and military response so blurred. In contrast, offline public order and criminal investigation is largely the remit of civil law enforcement authorities – defence of the realm the responsibility of armed forces by land, sea and air.

In the last few years a number of nation states have made renewed public commitments concerning their cyber defence – and offence – capabilities. This should not be read purely as political posturing, rather as an indicator of governmental priorities and preoccupations in response to major cyber crime campaigns. The world is rapidly coming to terms with the reality of attempted election interference by actors apparently either located in Russia or with Russian connections. Could this have been foreseen? Yes. State propaganda and misinformation is a millennia-old tactic. It is what newspapers and TV stations around the world do to varying degrees. Social media is a very popular format for mass distribution, particularly of targeted advertising. Political parties across the globe already make use of

it. So, it stands to reason that a nation state looking to sow the seeds of discord and spread misinformation would also use this channel. The motivations of the actors involved, however, can be wide-ranging. The group known as APT28 or Fancy Bear, reportedly responsible for leaking Hillary Clinton's hacked emails and for recent attacks on the German government, has been identified essentially as a service provider for the Russian government. Teenagers of the city in Macedonia recently revealed to be a hotbed of fake news distribution are driven as one might expect by a desire for cash.

Meanwhile, tools like ransomware designed to generate revenue by means of extortion result in massive denial of service in essential public services when used on a large scale. The effects of the WannaCry attack in 2017 were felt not only by businesses. In the UK alone, nearly 20,000 hospital appointments and medical procedures were cancelled when the National Health Service (NHS) computers were locked. While the NHS may not have been the intended target, a lack of basic security protections resulted in considerable disruption to healthcare provision in some areas of the country. Subsequent investigation revealed the likely source of the attack to be North Korea.

As the two examples above demonstrate, in a world of hybrid threats and complex motivations it is increasingly challenging for regulators and law enforcement to distinguish cyber crime from nation state activities. Stakeholders in critical national infrastructure, the financial sector included, are reviewing their defences and incident response plans. Multinational corporations are understandably scrutinising more closely their relationships with some governments and their outsourcing arrangements in certain locations.

What is certain is that cyber crime will continue to evolve, mutate and develop resilience to countermeasures. The age-old comparisons with virology are still relevant. And while anti-virus vendors are adept at spotting new malware variants in the wild, this is no longer sufficient to respond to the rapid evolution of the threat. Companies need to complement technical cyber security measures with strategic intelligence on external developments and environmental factors – utilising this just as they would to inform the rest of their business. Only then will they be able to move from reactive 'whack-a-mole' mode to an approach that enables them to get ahead of cyber threats.

Cyber criminals have always exploited legal loopholes and

discrepancies in different jurisdictions. The criminal misuse of dark address space in underused country code top level web domains – for example, the .tk domain for the tiny territory of Tokelau – was an early indicator of this, as was the flourishing of cyber crime in countries perceived to be beyond the reach of international law enforcement. As the remaining 3.5 billion people connect to the internet, discrepancies in cyber security awareness will become more evident, and vulnerable to exploitation by criminals.

Wherever people are connected, cyber crime follows, both in terms of the online spaces they frequent, and their geographical location. Governments of long-connected nation states have the opportunity, and perhaps a responsibility, to share lessons learned with rapidly-connecting countries in order to help them protect their citizens, businesses and critical infrastructure. Global organisations with a presence in these countries should be alert to the risk attached to lower levels of cyber awareness and prepare local service providers accordingly, all the more so as internet technology itself becomes more decentralised and distributed. The market dominance of cloud computing solutions for both storage and processing means that many busi-

nesses can no longer precisely locate their data geographically at any given time. They should assume their assets are only as secure as their most vulnerable location.

Blockchain is the most fêted of distributed systems in 2018. At the time of writing, various claims are being made for its future role as a means of securing financial transactions and document certification. While the prospect of having an unalterable ledger of transactions may make them more efficient, this should not be confused with the aim of making them more secure. It remains the case that all code is hackable and there is no such thing as absolute cyber security, not least because the pace of technological change ensures that existing security measures risk becoming obsolete very quickly. Equally, every new technology becomes particularly desirable to hackers when it gains in popularity, as a series of Bitcoin thefts has demonstrated.

Advances in quantum computing continue apace, with a number of global tech companies, academic labs and governments working on developing their own architecture. At current estimates, quantum processing will crack existing encryption algorithms by the 2030s. By that time, encryption, too, will need to have moved on. The adage that cyber security is an arms race

has never been truer.

The vastly increased processing power promised by quantum will also enable a step change in the development and use of artificially intelligent (AI), autonomous systems. Many companies are already using machine learning (ML), for example to identify anomalies or suspicious activity. In general, human intervention is still required at some point – to manually review transactions flagged by an automated system, to check for false positives, or to take the necessary enforcement action. The smarter and more powerful these systems become, the lesser will be the need for human intervention. The smartest thought leaders in the field are now considering how to assure autonomous systems, and prevent them from taking actions that may be harmful or counterproductive.

Until then, the greatest risk to organisations using ML is the people with access to it. Insider threat has long been on the radar of corporate security departments. Malevolent individuals with access to AI systems can arguably do more damage than those with simple data access. Equally, should cyber criminals gain access to AI it would be natural for them to seek to introduce it into target corporate environments. Organisa-

tions should prepare for attacks on and by intelligent systems by vetting and auditing access to these tools, and by hardening target employees. Since AI is also likely to have a higher value on cyber criminal marketplaces, it will be a desirable target for exfiltration, and therefore perfectly suited to serve as leverage for extortion.

On a shorter horizon, businesses worldwide are already incorporating virtual reality (VR) and the Internet of Things (IoT) into their operations, whether for internal communications and logistics, or for external engagement with customers.

After a number of false starts, VR hardware is now accessible and affordable. Leading tech companies such as HTC, Google, Facebook and Sony all have devices on the market that provide immersive, 360-degree experiences. Integration with social media functionality is ensuring that the future of VR will not be a solo experience. VR will inevitably make its way into the workplace much as personal devices and social media usage have. It is already being used for workplace training purposes – from heart surgeons to tank drivers – and it is doubtless the intention that social VR will replace video conferencing. The time for boards and chief information security officers to draw up plans

for securing assets in VR should not be on the day they experience their first incident.

VR is just one in a long line of emerging technologies coming companies' way very soon. All of these will need to be secured, and it should not be assumed that existing cyber security measures will suffice. Organisations need to become more agile in their threat monitoring now to be fit for the future.

■ *Dr Victoria Baines is a visiting associate of the Oxford Internet Institute.*

UK approaches to cyber crime – a legal perspective

BY PAUL WAINWRIGHT

OUR EXPERIENCE OF CYBER CRIME ISSUES as a law firm operating across commercial, public and health sectors is not unique. The increasing frequency of calls from clients as victims of cyber enabled fraud, for instance, is not an indictment of lax IT security, controls, staff training or risk management. Rather, it is a sign of a growing problem of managing financial risk within a commercial environment driven by online communications and e-commerce.

With each new case, we are seeing increasing levels of sophistication, highlighting the ingenuity of criminals and more organised approaches to targeting commercial enterprises at their weak spots though social engineering, malware and hacking. While we have not yet seen the developments of artificial intelligence (AI)

and machine learning in fraud *per se*, the use of untraceable mobile technology, faceless email accounts, servers in unfriendly jurisdictions and perhaps more surprisingly, mule bank accounts in our High Street banking system mean that once the money has gone, layered through various accounts, particularly offshore, it can be difficult to trace and recover.

And therein lies the rub. Regional or national solutions are often proving inadequate in a globalised world of trade. While notoriously inaccurate as a true measure of offending (largely as a result of underreporting), the September 2017 crime statistics from the Office of National Statistics show 4.7 million incidents of fraud and computer misuse experienced by adults up to September 2017, with banking and credit account fraud making up the majority of offences. The fact that this figure virtually doubled the number for 'conventional' crime overnight should be a stark warning, a fact acknowledged by the launch of the National Cyber Security Centre, and further increased funding as part of the government's National Cyber Security Strategy from 2016. How this impacts on business is very much open to debate, however.

UK businesses are being targeted by actors who sit outside the UK jurisdiction, but who have access to UK bank accounts.

While we cannot rule out the possibility of account takeovers, by far the majority we have identified are linked to non-UK nationals who have had a connection with the UK, as students or on work visas. While they may be the foot-soldiers of larger enterprises, some have incorporated businesses in the UK, though Companies House lending an air of legitimacy, it would appear, to their activities and perhaps allowing them to 'set up' bank accounts (often online) for the purposes of fraud.

This raises questions not only of the UK's AML regime and the level and effectiveness of the suspicious activity reports, but also of Companies House and the banks' own due diligence processes. New checks introduced in January 2018 following an impact study by HM Treasury, the Financial Conduct Authority, the Home Office and the Ministry of Justice in 2015 mean that banks will now check their current accounts (and associated lending) against the CIFAS anti-fraud database. As part of the government's controversial 'hostile environment' policy to identify over-stayers, and illegal foreign nationals, this might have the unintended consequence of cleaning up UK lenders' books from hostile agents of international criminal gangs intent on fraud, whether cyber enabled or otherwise. But it is in no way a panacea for what is a complex

transnational disease.

Banks, in addition, seem reluctant to scrutinise online payments into dormant or infrequently used accounts, but as potential proceeds of crime they should do so; by freezing the account and ensuring the beneficiary is the intended recipient. Banks will, of course, argue that their first duty is to their customer, who may well be a further victim, but if the system were designed to ensure that banks verified transactions over a certain value, checking names as well as account numbers would alleviate some of these concerns. The lack of joined-up thinking in the frontline defence against these crimes leads victims to accept their losses which can, in certain cases, have a devastating effect on their business and livelihood.

At a global or holistic level, there is also an argument for greater regulation and intervention. ISPs (and other platforms, such as social media) should be encouraged to introduce automated methods of policing the web. Such technological solutions would prevent, for instance, the dissemination of spam, which is a social menace and a true cyber crime. Filtering out the harmful noise of spam would not be missed by anyone, and it would prevent or at least limit the delivery of malicious software. Ethical

considerations regarding the inviolability of the internet's 'freedom of movement of information' aside, this would see a step-change in behaviour online.

Despite the imminent arrival of GDPR, in instances where crime is committed, there is a real need for access to information and sharing data, across jurisdictions and with law enforcement. Collaboration is key. Our experience is that through careful use of intelligence, combined with pre-emptive disclosure and litigation tactics, parties have had measurable success in identifying the wrongdoers in the UK, and some overseas – and have then worked closely with the police to ensure their apprehension and prosecution. But this can be time consuming and in all matters which involve a court process potentially costly and bureaucratic.

It can be disappointing that after the obligatory notification to the police and Action Fraud by parties seeking to recover their losses, they are often left with little support by, or follow-up from, law enforcement. Responses to the notifications of cyber fraud through Action Fraud are slow, if they manifest themselves at all, and often the thought process of a referral to a local force (often nowhere near the crime victim's address) is clouded in mystery. As a victim, ultimately, the consumer or customer still bears the

loss and the liability for online fraud, barring exceptional circumstances and the extent to which the police can assist in recovering the financial loss is problematic with only a small percentage of the total losses recovered.

All organisations affected by cyber fraud are keen to ensure their businesses can continue without significant disruption. They want reassurance to be able to recover what they can as quickly as possible.

So perhaps with the regulatory gaps in the banking sector, and the online space, and as traditional policing and policy makers get up to speed with the technological challenges, there is room for cyber insurance. This cannot be a substitute for effective cyber security. The right policy will not only allow restoration of data following attack, but would cover intellectual property, theft, legal advice and defence, incident response and lost business too. It will also allow businesses to deal with the rebuild of their IT systems and meet any regulatory investigations such losses might present.

■ *Paul Wainwright is a partner and head of counter fraud at Browne Jacobson LLP.*

Survival conditions for the UK and Israeli cyber threat intelligence sector: a comparative glance

BY MOIRA CARROLL-MAYER

UK CYBER THREAT INTELLIGENCE PROFESSIONALS operate in an increasingly hostile legal terrain, constrained by domestic and international legislation that threatens their global influence and economic strength. The situation persists in the face of increasingly sophisticated cyber attack methodologies which have the potential to devastate civilian and defence systems infrastructure leading to loss of life and an unsustainable natural environment. As commercially-viable quantum computing capabilities

reach a five-year horizon, the situation is becoming more untenable and urgent than ever. Even RSA, the standard encryption algorithm that protects every day and critical infrastructure is, according to IEEE Spectrum, under threat from quantum computing.

Ciaran Martin, the director of the UK's National Cyber Security Centre, and Sir Nick Carter, chief of the general staff, fear a category 1 attack capable of crippling critical infrastructure within two years unless an adequate response to pending threats is formulated and acted upon. In response to actual and potential threats from hostile threat actors and criminals, the UK government, through the Cyber Security Strategy, has called for increased efforts by public and private entities to protect their cyber systems; failure to do so will result in the imposition of undefined penalties.

Somewhat ironically, however, UK cyber threat intelligence professionals, the people best positioned to support the strategy, find themselves hamstrung by legislation that criminalises activities required to effectively counter cyber threats. In effect, the UK is prevented from fully exercising its influence, through its cyber threat intelligence capabilities, in ensuring civilian and

defence stability nationally and globally. The handicap is felt economically and in terms of global influence since other leading cyber security nations, such as Israel, do not appear to operate under such restrictive regimes.

The NCC, a leading UK cyber threat intelligence enterprise, describes cyber threat intelligence activities as "helping organisations understand who their adversaries are – their motivation, capabilities and skillsets, intents and targets...to better define investment in cyber defences to anticipate, detect and mitigate threats". It is clear, therefore, that the industry, in order to maximise its effectiveness, requires the freedom to covertly peer inside the systems of adversaries which can only be achieved through remote, covert internet access.

The most noted impediment to effective and competitive cyber threat intelligence in the UK is the Computer Misuse Act 1990. Section 1 of the Act criminalises unauthorised access to a computer or hacking, regardless of the reason or motive for doing so. Under S.1 (1) a person is guilty of an offence if: (i) he causes a computer to perform a function with intent to secure access to any programme or data held in any computer or to enable any such access to be secured; (ii) the access he intends

to secure, or enable to be secured, is unauthorised; and (iii) he knows at the time when he causes the computer to perform the function that this is the case.

To remove the danger of criminalising the police and security services, section 44 of the Serious Crime Act 2015 introduces exceptions for them. Those exceptions do not exist for private cyber security operators, so the unauthorised placing of a Trojan on a system, an offence for them under section 3 of the CMA, is not for the police and security services. Other dangerous impediments stem from the Data Protection Act 1990 and the European Data Protection Regulation (GDPR). The Act and the Regulation, even more severely, penalise unlawful monitoring, use or disclosure and recording of information relating to individuals. The GDPR places cyber security and most particularly the cyber threat intelligence sector in jeopardy when it comes to sharing of personal data within Europe and, for example the US where personal data is defined more narrowly. Take, for example, the transfer of an IP address without the owner's knowledge and the linking of identity to it – an everyday event in threat intelligence. In 2016, in *Patrick Breyer v. Germany*, the European Court of Justice found that an IP address could, in

certain circumstances, be personal data; therefore, it could be personal data for the purposes of the GDPR. Despite some hope pinned upon the 'public interest' provision, the ambiguity is still there. Anecdotally, it is said that the police and Crown Prosecution Service are disinterested in the prosecution of cyber intelligence firms that may cross the boundaries of lawful behaviour; cold comfort when the new data protection rules, coupled with unprecedentedly high penalties of up to four time annual income for infringements, make the GDPR the hottest topic in town.

Speak to cyber security professionals about the laws circling their operations and the cases of Andrew Auernheimer and Olivier Laurelli are soon raised. In 2013, Mr Auernheimer was convicted in the US of conspiracy to violate the Computer Fraud and Abuse Act. Mr Auernheimer, through unauthorised access, discovered a flaw in AT&T's systems and emailed the media to alert both the public and AT&T. In France in 2014, Mr Laurelli, the owner of a security business, was convicted of illegally accessing and downloading files belonging to the French National Agency for Food Safety, Environment and Labour. Later acquitted of the charge, Mr Laurelli was nonetheless sued by

the Agency and fined €3000. Even without legislation, courts in most technologically-advanced countries are inclined to reject notions of self-help, including hacking by cyber professionals, into criminal adversaries' systems. Though cases involving cyber security professionals are not numerous, until now European cyber security professionals have taken those meagre lessons in a salutary manner. In 2015, the European Network and Information Security Agency warned of a chilling effect from anti-hacking legislation for cyber security operations across wider Europe and the US post-GDPR. The chill is in danger of becoming a freeze.

The temptations are great. Globally, the scale of intelligence gathering is exponential and boundaries are ill-defined; the difference between offensive action and intelligence gathering is only 'a few lines of code', in the opinion of Professor Sir David Omand of the department of war studies, Kings College London, and former director of GCHQ. From a UK perspective, Sir David was critical of how the scale of intelligence gathering with no agreed norms of good behaviour could be destabilising, provocative and lead to a hacking arms race. Sir David was speaking at an Israel-UK Ambassadors roundtable at the Royal Society in

2017, under the auspices of the Anglo-Israel Association. The prevailing difference in perspectives can be sensed through the contribution at the same conference of Keren Elazari, a prominent Israeli security researcher and industry analyst, who described herself as a 'friendly hacker' and provided a hacker's perspective of the future of tackling cyber crime.

Anti-hacking laws reside in Section 4 of the Israeli Computers Law 5755-1995 and the 1979 Wiretapping Law. Nonetheless, the Israeli model for a private sector cyber security response is attractive as it seems to foster, at least nominally and perhaps increasingly controlled, defensive and offensive capabilities. Israel is perceived as a cyber super power, second only to the US and perhaps outflanking it in terms of cyber intelligence gathering. In 2017, there were 420 active cyber security companies operating in Israel, according to Start-Up Nation Central, an increase from 379 in 2016. The report noted 70 new start-ups founded in 2017, and an increase in firms focused on IoT security.

The root of Israel's success and range of defensive as well as apparently offensive capabilities seems to derive from the unique movement of personnel from the Israel Police, the Israel

Defence Force (IDF), Mossad, the Israel National Cyber Security Directorate and the Israeli Security Agency (Shabak) into the private cyber security industry, under the auspices of the National Cyber Bureau and the Cyber Defence Authority. By bringing together their interdisciplinary methodologies, Israel has created a multidisciplinary, robust cyber security ecosystem. A key moment for the centralisation of Israeli cyber security efforts came about in 2011 with the establishment of the National Cyber Bureau (NCB) under the prime minister's office. According to its website, the NCB is charged with "advancing defence and building national strength in the cyber field...building up Israel's lead in the cyber field [and] advancing processes that support the first two tasks". It is responsible for defending national infrastructure from cyber attack. Since January 2015, the Israeli National Cyber Bureau has published an official list of core professions to be taught at See Cyber Security College, including cyber security practitioner (CSP), cyber security technology professional (CSTP), cyber security methodology professional (CSMP), penetration tester (hacker) and forensics specialist. In addition to the civilian pool, many graduates of the college derive from Mossad, the Shin Bet and elite military intelligence Unit 8200

and from there go into the private sector, taking with them their electronic warfare skills. There is also mandatory military service for young people in the technologically orientated IDF.

In 2016, the National Cyber Defence Authority, pursuant to government Resolution 2444, emerged, focusing on close cooperation among all parts of the civil sector and the establishment of a civilian authority to focus solely on cyber security. Controversially the Authority would assume some roles traditionally performed by the Israel Security Agency (ISA) to defend critical national infrastructures. In 2016, a memorandum of understanding between the Authority and the ISA was drafted in order to regulate activity to assuage the resentment of the ISA, but the inherent tension persisted. In August 2016, the Knesset Foreign Affairs and Defence Committee issued a report on 'Division of Responsibility and Authority for Cyber Defence in Israel'; the report robustly defended the position of the Authority and its head, more or less granting him autonomy from the ISA in making decisions and taking action in the field. There was also controversy regarding the division of responsibilities for cyber security operations between the Cyber Defence Authority and the IDF. If the confusion tells us anything it is that the Cyber

Defence Authority was a force to be reckoned with. As if to underscore the importance of the new Authority for Israeli cyber security, in April 2017 the government announced the Cyber Defence Authority had fielded warnings of a massive planned cyber attack on Israel whereby malicious emails were sent from the servers of an academic institution and a private company to 120 Israeli institutions through a vulnerability in Microsoft Word.

Finally, in December 2017, following a letter of objection from the ISA, the Cyber Defense Authority was merged with the NCB into the National Cyber Directorate and situated within the prime minister's office. The Directorate is responsible for all aspects of civilian cyber defence. The Directorate's activities are extensive and in certain circumstances subject to the direct approval of the prime minister or the minister of defense.

Another crucial difference contributing to the apparently comparative boldness of cyber security efforts in Israel may be the country's less stringent data protection laws. The only protection offered to individuals under the Privacy Law 1981, according to lawyers Belan and Harel in an interview for the Times of Israel in 2016, is their "right to be informed that providing

information is subject to their consent and they have a right to review this information and a right to demand a correction of inaccuracies". Importantly, Belan and Harel said the existing legal framework lacks elements that exist in modern data privacy laws in other countries. There is no requirement to inform the data subject and the relevant authorities in the event of a data breach, or minimum data security standards that a controller of personal data would have to meet. Instead, the Privacy Law simply provides that the owner, controller and manager of a database are responsible for protecting the data stored in such database. Belan and Harel continued: "This law reflects an outdated concept that data privacy may be protected by requiring organisations that store personal data to register their 'databases' with the government…This is a technical process under which the organisation is required to provide a few general details on the database, its intended use and the types of data it contains." The Israeli government strongly disagrees with this assessment.

Any restructuring of UK private sector cyber security training to match that of Israel is likely to take decades and there is little likelihood of replicating its technologically-informed intake pool. One solution to the comparative dilemma of UK cy-

ber threat intelligence professionals is amending the Computer Misuse Act 1990 and the GDPR to create exceptions for accredited cyber security professionals, similar to the exception provided for the police and security services by the Serious Crime Act 2015. Another might be the creation of a memorandum of understanding between the police, Crown Prosecution Service and accredited cyber security professionals. Either of these solutions would provide clarity and enhanced purpose for the UK cyber threat intelligence community.

■ *Dr Moira Carroll-Mayer is a senior lecturer in law and ethics at De Montfort University.*

Achieving multijurisdictional compliance for global companies

BY PAUL LANOIS

AS GLOBALISATION AND EMERGING MARKETS drive businesses to expand their horizons, companies are increasingly challenged by the growing scope of laws and regulations that they have to juggle with. For example, the European Union, Canada, Russia, Australia and a dozen Latin American countries (Argentina, Aruba, Bahamas, Chile, Colombia, Costa Rica, Curacao, Dominican Republic, Mexico, Nicaragua, Peru, Uruguay and Trinidad and Tobago) have comprehensive privacy laws. Other countries, such as the US, Brazil and certain African nations, have broad sectoral data protections. China has also issued laws, regulations

and guidelines focused on privacy and security issues. Other countries are working on data protection laws. Earlier this year, India solicited public comments on principles to be considered for data protection and has constituted a committee to propose a draft data protection law.

While similar concepts and principles can be found across multiple data protection regimes, this is still an area of law with variations and distinctions between jurisdictions. Such sanctions could, for example, be applicable to breaches of requirements relating to consent or international transfers of data. In addition to financial and operational risks, global companies should consider cultural, political and reputational risks. Getting it wrong can be very costly. For example, once the European General Data Protection Regulation (GDPR) enters into effect on 25 May 2018, the data protection authorities in the European Union can impose fines of up to 4 percent of annual worldwide turnover or €20m, whichever is greater. In light of the ever-increasing amount of laws, regulations and other mandatory requirements imposed by each country, what should global companies do to achieve compliance on a multijurisdictional basis?

MAPPING THE APPLICABLE DATA PROTECTION REQUIREMENTS

The first thing to do to understand and rationalise the applicable data protection requirements across jurisdictions is to create a matrix of the applicable sources of data privacy requirements, together with the relevant types of controls. Mapping the requirements in such fashion will provide a better vision of the applicable privacy requirements on a global level and what is done to address those; in other words, drafting a global privacy framework.

The mapping should cover the data protection and cyber security laws in the different countries where the company operates and list what data is covered by those laws, the key obligations imposed under those laws, any restrictions on international or cross-border transfers of data, any security or data breach notification requirements and the applicable sanctions. For example, there are currently no restrictions on transfers of personal data outside of Hong Kong, since the restrictions relating to cross-border data transfers set out in section 33 of the Ordinance have not yet come into force, whereas the Australian Privacy Act requires the transferring entity to ensure that the

recipient of the personal data holds it in accordance with the principles of Australian privacy law.

In relation to data breach notification requirements, the GDPR introduces mandatory data breach reporting for companies which are required to comply with the GDPR. Likewise, in Australia, the Notifiable Data Breaches (NDB) scheme came into effect in February 2018, requiring agencies and organisations that are covered by the Privacy Act to notify individuals whose personal information is involved in a data breach that is likely to result in 'serious harm' as soon as practicable after becoming aware of a breach. In March 2018, Alabama became the final state in the US to enact a data breach notification law, exactly one week after South Dakota enacted its own data breach notification law.

UNDERSTANDING THE CONCEPT OF 'PERSONAL DATA' IN EACH COUNTRY

As a general rule, only personally identifiable information/ personal data is covered by data protection laws, however the definition of what is protected in each country may differ. For example, under the GDPR, 'personal data' is defined as "any in-

formation relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". It does not matter whether the data relates to the individual in their personal or professional capacity. It would still be 'personal data' even if the individual is not identified by name. The scope of 'personal data' therefore goes well beyond the concept of 'personally identifiable information' (PII). For instance, photographs and online identifiers, such as the IP address or the MAC address, are personal data under the GDPR but some countries may not have the same extensive scope for their own data protection laws.

Another example which further demonstrates the need to look in detail at the scope of what is actually covered under each country's data protection laws can be found in Singapore. The country's Personal Data Protection Act (PDPA) provides an exception for business contact information. Thus, under Singapore law, companies are not required to obtain consent before

collecting, using or disclosing any business contact information nor do they have to comply with any other data protection obligation in relation to business contact information. Business contact information is defined in the PDPA as "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes".

DOCUMENTING THE ADOPTED APPROACH IN RELATION TO PRIVACY

It is crucial to document the adopted data privacy approach and some countries do in fact require such documentation. For example, the GDPR in Europe introduces the concept of a Data Protection Impact Assessment (DPIA), a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data.

Carrying out a DPIA is not mandatory under the GDPR

for every processing operation. A DPIA is only required when the processing is "likely to result in a high risk to the rights and freedoms of natural persons", under Article 35(1). For example, any systematic and extensive evaluation of individuals based on automated processing, including profiling, or the processing of sensitive data, or the systematic monitoring of a publicly accessible area on a large scale, require a DPIA under the GDPR. In particular, the DPIA is described in the GDPR as a useful tool that can help organisations understand the risks related to their processing of data and a process for building compliance. In cases where it is not clear whether a DPIA is strictly mandatory under the GDPR, or even in countries where a DPIA is not a legal or a regulatory requirement, carrying out a DPIA is still good practice and a good way to demonstrate that appropriate measures have been taken to ensure compliance with data protection laws.

MINIMISING RISK

Data protection laws tend to be complex and because they often involve or have to interact with new technologies, there are a number of questions on compliance matters which remain un-

resolved. For example, the right to be forgotten or 'right of erasure' of personal data, which can be found under Article 17 of the GDPR, presents a particular challenge for open blockchain technologies since one of the foundations of blockchain technology is the notion of immutability.

In order to minimise risks, it is recommended that companies: (i) consider adopting best practices to limit the amount of personal data collected, processed, transferred and stored; (ii) ensure that access to any personal data within an organisation is restricted to authorised staff on a 'need-to-know' basis in accordance with a defined policy; (iii) make certain that all access to computer systems and networks is password protected with other factors of authentication as appropriate based on the sensitivity of the information; (iv) implement physical security safeguards, such as the use of key cards, in order to restrict access to sensitive areas; (v) provide training to staff who handle personal information in order to make them aware of their responsibilities through appropriate induction training with refresher training; (vi) ensure that third parties, such as consultants and contractors, service providers and others, receiving personal data are subject to and apply appropriate security measures;

(vii) have in place processes and a plan to handle data security breaches since most data breach notification laws impose very strict deadlines for notification – for example, an organisation must report a data breach within 72 hours under the GDPR, leaving little room for improvisation; and (viii) involve personal data monitor developments in data privacy and information security, such as new guidance issued by regulators.

■ *Paul Lanois is vice president and senior legal counsel at Credit Suisse.*

Identifying and preventing insider threats

BY WILLIAM RIDGWAY

AS COMPANIES HAVE STRENGTHENED their cyber security defences against outside hackers, too often they underestimate the threat posed by their own employees. Indeed, despite the headlines about recurring attacks from sophisticated hackers, many, if not most, data breaches arise from employee negligence or misconduct. According to a March 2017 study by IBM Security, in 2016 more than half of the cyber attacks against the financial services and healthcare industries were carried out by employees who maliciously stole or unwittingly distributed sensitive data. Companies in these and other industries find themselves increasingly vulnerable from the inside as the value and volume of their data grows.

To address this threat, companies should take a multidisciplinary approach, relying on a combination of employee policies and training, human resources techniques, and technical measures. The following measures are among those that a company should consider to mitigate the threat of security leaks by both malicious and negligent insiders.

Set clear guidelines in confidentiality agreements. New employees should sign confidentiality or nondisclosure agreements that spell out the circumstances under which an employee may access valuable information, such as customer data or trade secrets. These agreements deserve careful attention because they often become the linchpin in a lawsuit against an insider who makes off with company secrets. It is important to define the technology and proprietary information, describe the scope of authorised use of that information, and provide for the destruction or return of sensitive data.

Conduct background checks regularly. Background checks have become a routine technique for evaluating the risk posed by potential employees, but they should not end at the pre-hire stage. Ongoing monitoring of employees is necessary because the risk posed by an employee can change with a new arrest, lawsuit or

alarming financial behaviour. Indeed, several recent insider threat cases have involved employees whose financial circumstances dramatically changed post-employment.

Set data access restrictions and monitor employees for suspicious activity. Data access restrictions play a critical role in thwarting insider threats. In a 2016 survey of American and European companies, 'Closing Security Gaps to Protect Corporate Data: A Study of US and European Organizations', the Ponemon Institute found that 62 percent of employees reported having access to confidential data that was not necessary for their work. In order to minimise overbreadth of access, employees should be authorised to use only the resources needed to do their jobs, a notion that is often referred to as the principle of 'least privilege'. That principle may be enforced using network segregation or software to log access to confidential documents or databases.

Equally important for an organisation is a security information and event management solution, which aggregates data from a variety of sources – including databases, applications, networks and servers – to continuously monitor employee network activity. Such tools will allow the identification of irregular computer use, such as connections to unusual IP addresses at

unusual times, abnormally large data transfers or unauthorised uses of encryption. Monitors ought to pay special attention to remote access, terminated employees and highly privileged users.

Enforce clear written policies and procedures with signed acknowledgment. Employers should design and enforce all organisational policies and procedures in a clear and consistent manner. Many insider incidents result from misunderstood or poorly communicated policies. In several documented cases, insiders have taken to a new employer proprietary information that they had a hand in creating, unaware that their previous employer owned it. Organisations ought to provide documentation of and reasoning for all policies, and ensure they are consistently enforced. These policies may be reinforced through training that incorporates awareness of both malicious and unintentional insider threats.

Prepare for employee departures with separation agreements and asset collection policies. Exit interviews serve as an invaluable, and often overlooked, method of limiting the security threat of outbound employees, regardless of the circumstances surrounding their departures. The interview allows the employer to re-

inforce confidentiality provisions and procedures and collect all company assets.

A departing employee creates a uniquely risky event for any company. A Symantec study reported that 50 percent of departing employees kept confidential corporate data from their former employer. Companies must protect themselves by asking for a final signed assurance that no confidential information or trade secrets are being removed from the company control. At the same time, the company's information technology team should ensure that departing employees have all privileges and access revoked.

The frequency and cost of attacks from insiders will not subside in the coming years, particularly because an increasing number of companies are encountering an operational need to give employees, partners, suppliers and contractors remote access to their networks. The safeguards discussed above should help put companies in the best position to prevent or mitigate this growing problem.

■ *William Ridgway is a partner at Skadden, Arps, Slate, Meager & Flom, LLP.*

Policies for the bring your own device (BYOD) revolution

BY MIKE GILLESPIE AND ELLIE HURST

THERE ARE MANY QUESTIONS still unanswered when it comes to the bring your own device (BYOD) revolution.

Is it working and is it delivering all we hoped? Does it suit all organisations and is it still considered the best solution for current complex business needs? Have the cost savings materialised and the information risk been reduced? Who is accountable for the success or failure of a BYOD programme?

Research and experience tells us that many businesses have embraced BYOD policies. For instance, the 2016 BYOD report from Syntonic suggests around 60 percent of businesses have a

BYOD policy in place. Some have done so voluntarily, having risk assessed it and subsequently created suitable policies. Others may have had it forced upon them as a requirement of a workforce demanding potentially better (or more frequently upgraded) devices than they were getting from employers or possibly as a recruitment tool. Of course, there is still a group that is participating in a BYOD scheme without knowing it, as policies are variously uneducated or unenforced, ignored or circumnavigated or simply non-existent. This is a complex area as it may involve some firms which fall into the 60 percent with a policy, as well as the 40 percent without one, as naturally every policy and culture will differ.

There are, however, some key themes and expectations for the policy-setting business, and these seem to fall into three broad streams. In no particular order, reduce information risk, boost productivity and efficiency and save money are the overarching drivers to implementation. As the first two actually contribute to cost saving, the cost piece is a clear driver to BYOD culture, but has it delivered?

In terms of ownership and accountability for BYOD, who has it, who wants it and who really understands how it fits into

a broader security strategy and the resulting privacy impact on employees? We know that cyber security, which is a contributory theme to the uptake of BYOD through the information risk theme, is an area that business leaders tend to struggle with. This creates more risk, as we can see from the research which suggests many C-suite members consider themselves responsible for their BYOD programme.

REDUCING INFORMATION RISK

Generally speaking, businesses that have had a bad experience with a data breach and the resulting cost, both financial and reputational, will be first in line to consider BYOD policy as part of the response. The response is likely, therefore, to be quite an evolved one, as some of the pitfalls may have already been unwillingly explored. According to research from Syntonic, 17 percent of respondents have implemented policies because of a security breach. In other words, having no policy in place has meant employees of all levels were able to potentially port data around on unknown devices, with unknown security, in unknown places with unknown levels of third-party access. Those are just some of the known unknowns. Quite naturally, having

lost some information this way, a business will take robust measures to shore up security. If a business that has not experienced a breach is implementing a policy, this a win for information risk management as a proactive behaviour, if it is following a risk assessment in line with organisational risk tolerance and appetite.

There appears to be some confusion over who should have BYOD ownership. The research indicates that the C-suite feels generally responsible, according to 79 percent of respondents to Syntonic. But 73 percent of IT departments feel the same and 51 percent of finance departments also feel responsibility should sit with IT. It is entirely right that a senior management figure should take ownership of such an important programme, but to take into account one of the priorities of a BYOD roll-out, that of reducing information risk, means they need to be fully conversant and aware of their organisational cyber risk tolerance and appetite. In most cases, this is simply not true.

The Intelligence Unit at The Economist conducted extensive C-suite research in 2016 and found that only 17 percent of respondents, who were all senior board members, felt that building a security culture was the most important thing they

could do to support data security. Only 11 percent felt they had oversight of the security programme. Given that culture is set by leaders, a robust security posture and culture is therefore going to have to force its way back up the chain into the boardroom. Therein lies the problem: a lack of oversight and leadership in a crucial area that needs just as much boardroom attention as finance but rarely receives it. And yet they are the majority that wants to own responsibility for BYOD, according to Syntonic.

We need leaders to be far more switched on and involved for reduction of risk to take place. If we are talking about the reduction of information risk, then, according to Osterman research, only 37 percent of security professionals feel that risk is reduced as a result of their conversations and reports to their boards. Sixty-two percent of security professionals said they were reporting to their board on cyber threats quarterly or less frequently. Only 12 percent received weekly updates. Although this is a broad brush, these respondents were on boards of organisations that employed 2000 people or more. Less than monthly reporting on cyber threats in these circumstances seems inadequate. It does, however, explain why IT professionals feel that BYOD responsibility should lie with them.

INCREASED EFFICIENCY AND PRODUCTIVITY BOOST

With more up-to-date devices, businesses were hoping that this would offer significant benefits to productivity. Users may change their technology more frequently than corporate programmes may allow, and so speedier processing, more efficient applications and a user who is comfortable and experienced with the device should, in theory, be more productive. But what seems to happen is that any benefit from any of these changes is swallowed up in the administration of the programme itself. Some of the key organisational concerns identified in recent research include the difficulty in differentiating between business and personal use, inadequate security, IT helpdesks unable to keep up with employee requests for help and the creation of administrative overhead. It seems clear from the kind of concerns being raised that the hopes of individual agility may have been paid for in administration and IT encumbrance. This makes it a top priority to work out, before even approaching policy-writing, whether it is a good organisational and risk appetite fit, because if there are security concerns, and apparently a quarter of those surveyed say there are, then you are not only failing on the increased productivity requirement but on reduction of information risk too.

SAVE MONEY

For most organisations, cost saving is the primary criteria for introducing a BYOD programme. That is not to say that they would forgo security or efficiency, but as they both feed cost saving, this is a real driver. Yet many feel that the promise of BYOD cost savings has not materialised.

Given that 75 percent of businesses have some concerns about their current BYOD programme, it is wise to look at what those concerns are – and the majority fall into the cost bracket. The cost of reimbursing employees is too high or too hard to calculate, expense report processing fees are higher, segregating personal from business use is too challenging, support costs are too high, the return on investment is unclear, it creates too much administrative overhead – these are some of the most common problems.

Reimbursement problems are sometimes addressed by choosing a fixed stipend model, but that is not without issue as it is not immune from overpayment. Nearly 40 percent of CEOs and COOs know they are overpaying employees in BYOD reimbursement, and this is across all repayment methodologies. Those businesses choosing employee-based reimbursement are

troubled with the privacy issues of personal billing information that has to be submitted in order to fulfil this reimbursement.

There are also the hidden costs, such as overburdening IT helpdesks and creating additional administration. These costs contribute to the difficulty in realising real cost savings. Perhaps BYOD should be seen as a recruitment tool if these issues cannot be overcome, assuming it is still within the company's risk appetite to implement.

Leadership in this area is vital. If the process is not risk assessed in the first place, as part of the discovery period, then the practical and security difficulties of trying to reverse a BYOD programme that is not meeting the three objective groups are akin to trying to get toothpaste back into the tube. Ownership and accountability needs to be clear as well, aligned with organisational risk appetite and tolerance, which of course, may vary by role. There is no doubt that BYOD continues to be a popular option for employees and the temptation may be to adopt it, as many have. Perhaps the most important thing an organisation can do is to have a position on BYOD and have a policy for it, even if that policy says it is not allowed. Any area of doubt or lack of clarity can lead to self-adoption, which introduces risk with-

out management being aware. BYOD needs to be part of organisational security posture and employee privacy must be carefully considered. HR therefore needs to be as involved as security to create an effective policy. The next important thing is to enforce that policy.

■ *Mike Gillespie is a director and Ellie Hurst is the marketing manager at Advent IM.*

Managing the risks arising from third parties which hold or use your and your clients' data

BY ROBERT ALLEN, PAUL BAKER AND CAMILLE TEWARI

PROTECTING THE COMMERCIAL VALUE of data created and captured is a top priority for right-thinking businesses. Businesses know that they must bolster their cyber security defences and have focused on strengthening their own data controls and security. But what of the data controls and security of the third parties with whom they deal – suppliers, professional advisers, outsourcing partners and those who provide IT infrastructure?

This third-party risk is often overlooked by businesses.

One recent report commissioned by the Department for Culture, Media and Sport in the UK suggests that only 13 percent of businesses require their suppliers to adhere to specific cyber security practices or good practice, despite these suppliers providing a 'potential stepping stone into the networks' of their clients. That oversight is potentially very costly, not only in terms of regulatory fines and civil damages arising from a breach, but also in terms of reputation and goodwill. Customers are not willing to dissociate a company from its chosen business partners and suppliers; the market's response to Facebook's relationship with Cambridge Analytica is a case in point.

The risk to financial institutions is particularly acute, given the nature of the data at the centre of these enterprises. Among other things, as noted by the Financial Conduct Authority (FCA) in its most recent business plan, the advent of PSD2 and the Open Banking initiative has potential to increase cyber attacks and data breaches.

REGULATION

The FCA Business Plan 2018/19 zeros in on the risk presented by third parties having access to data and networks: "Regulated

firms should have appropriate oversight and control over third-party providers and take responsibility for the service they provide. Doing so will reduce the risk of third party failures or weak controls which could lead to operational disruption, unauthorised loss or disclosure of consumer data".

The FCA states that in the coming year one of its focuses will be outsourced services, and the potential harm arising from regulated firms' use of those services, with particular attention paid to outsourcing arrangements where the provider supports many firms. This forms part of the continuing development of the global regulatory efforts to compel businesses to protect their data against cyber security attacks on third-party defences.

From a UK perspective, the businesses that are most heavily regulated are data controllers as defined under the General Data Protection Regulation (GDPR), implemented on 25 May 2018, and firms regulated by the FCA.

GDPR

The GDPR imposes direct obligations on both businesses (as data controllers) and third-party service providers appointed as data processors. However, the data controller remains liable for

ensuring that its business is compliant with the GDPR. To this end, businesses must only appoint data processors that can provide sufficient guarantees that appropriate technical and organisational measures will be implemented such that the requirements of the GDPR will be met.

All processing activities must be governed by a binding contract containing a number of specific provisions required by the GDPR, and must only be performed following documented instructions from the data controller. Both processors and controllers are responsible for implementing appropriate security measures, taking into account factors including the type of data, the nature and purpose of processing, the risks to individual rights associated with any security breach and the cost of implementation, and for regularly testing and evaluating the effectiveness of these measures.

Breaches involving personal data must be notified by data processors to data controllers, and by data controllers to the relevant supervisory authority (in the UK, the ICO) without undue delay. This new regime of obligatory notification will inevitably lead to an increase in enforcement activity by the ICO (and equivalent supervisory authorities in EU member states).

A probable knock-on effect to this will be an uptick in litigation. Where enforcement is pursued, the possible sanction – fines of up to 4 percent of global annual turnover – is severe.

PRINCIPLES FOR BUSINESS AND SYSC RULES

While the FCA's business plan highlights cyber security as one of the FCA's key activities for the coming year, its handbook already provides a regulatory infrastructure where failing to engage with the cyber security risk presented by third parties could lead to a breach. The starting point is Principle 3 (PRIN 2.1.1, FCA Handbook) which requires a firm to "take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems".

A drop into the more detailed provisions of the Handbook takes one to the Senior Management Arrangements, Systems and Controls rules (SYSC). SYSC 6.1.1 is particularly relevant and wide-ranging: "a firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives, with its obligations under the regulatory system and for countering the risk that the firm might be

used to further financial crime".

In July 2016, the FCA produced guidance for regulated firms that outsource data hosting to the cloud and other third-party IT firms. That guidance was designed to assist regulated firms to discharge their oversight obligations and avoid enforcement action pursuant to the SYSC rules. Given the comments in the FCA Business Plan, it is not unreasonable to expect an update to this guidance. Other financial regulators indicate the direction the FCA might take in this area. For example, in August 2017, the New York Department of Financial Services published a new cyber security regulation requiring certain financial services organisations to maintain detailed cyber security plans, and extending this obligation to their unregulated third-party service providers.

LIABILITY

ICO enforcement. The ICO has imposed fines on businesses (as data controllers) for data breaches arising from the action (or inaction) of third-party data processors. A recent example is the 2017 enforcement against HCA International Ltd (HCA). HCA engaged a company in India to transcribe audio recordings con-

taining interviews with fertility patients, transcripts of which appeared online. The ICO found that HCA had failed to encrypt the recordings when transmitting them to the third party. Moreover, HCA had failed to obtain any guarantee or assurance from the third party as to how it would store the data or that it would erase the data after transcription. HCA was fined £200,000 for failing to keep its patients' data secure. It will be interesting to see the level at which fines are set for similar failings in the GDPR era.

FCA enforcement. We have seen the FCA enforce against firms both for weak controls over parties to whom they outsource vital functions (see, for example the October 2016 fine imposed on Aviva), and following critical IT resilience failings (the RBS/Natwest fine in 2014). Given the FCA's focus on cyber security, and its February 2018 joint update with the ICO on GDPR compliance, which emphasised the connection between the GDPR and the SYSC rules, it is only a matter of time before we see a final notice sanctioning a firm for failing properly to oversee a third party's handling of its data.

Civil litigation. Civil claims may be brought against businesses as a result of a cyber attack against one of its third-party

service providers, regardless of regulatory enforcement action. Article 79 of the GDPR confers a right to a judicial remedy for data subjects against any unlawful processing of their personal data by a controller or a processor. Article 82 of the GDPR states that "any person who has suffered material or non-material damage as a result of an infringement of GDPR shall have the right to receive compensation from the data controller or data processor". As set out in the (at the time of writing) Data Protection Bill, this damage can include financial loss, distress or other adverse effects. Follow-on litigation whereby a data controller seeks to recoup losses incurred through litigation with a data subject from a data processor (or vice versa) seems likely.

GDPR-era litigation may well give rise to collective action or group litigation. The 2017 case *Various Claimants v Wm Morrisons Supermarket PLC*, which involved a significant data breach, is a recent example of how claims brought by data subjects (in this case 5518) lend themselves to the structure of a Group Litigation Order (or alternatively a representative action under CPR 19).

Other claims connected with data breaches could include claims for misuse of confidential information, breach of confi-

dence or breach of contract. The latter could arise following non-compliance with data protection clauses or undertakings concerning the robustness of data security. In turn, the business itself should anticipate contractual claims if it has made representations about the robustness of its cyber security systems to customers or other third parties. That could include claims from shareholders seeking to recover losses arising from a fall in the share price of a company as a result of a data breach.

CONCLUSION

While support from third-party service providers may be necessary on the basis of cost, efficiency or specialism, it must be recognised that the sharing of data with a network of third parties magnifies cyber security risk.

In order to manage this risk, businesses should now, as a matter of priority, review their relationships with third parties to ensure that security is maintained to an appropriate standard and that the contracts giving rise to those relationships provide the necessary oversight and control over third-party service providers.

Businesses that do not act quickly to protect their data in

this way may find themselves suffering the potential enforcement, litigation and reputational consequences of a cyber security breach described above, which are all the more likely given the increased regulatory focus in this area.

■ *Robert Allen and Paul Baker are partners and Camille Tewari is a consultant at Simmons & Simmons.*

Borderless data and government search power: the Microsoft case and the CLOUD Act

BY GUILLERMO S. CHRISTENSEN, OLIVIA GONZALEZ AND ANUPREET AMOLE

IN DECEMBER 2013, THE US GOVERNMENT ordered Microsoft to produce emails belonging to a user suspected of trafficking drugs. While the account information was stored in the US, the emails were located on a server in Ireland. Microsoft refused the government's request, arguing that the US had no authority to issue a warrant for information stored outside of the country. This crystallised the question of whether a US company could be forced to retrieve digital communications from its customers

located outside the US. The issue reached the Supreme Court in 2017. Approximately a year later, shortly after the case was argued before the Supreme Court, the US passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Since then, the Supreme Court accepted the position of the parties that the CLOUD Act rendered moot the question posed in the case. Microsoft has subsequently gone on to provide the data requested by the government

The CLOUD Act requires companies to comply with a government request for data relevant to an investigation, even if the data is stored on servers outside the US. In certain respects, this represents a shift in the legal landscape for data sharing between countries. Traditionally, transnational data sharing relied on informal agreements or cumbersome, process-intensive Mutual Legal Assistance Treaties (MLATs). The issues at the heart of the Microsoft case and ancillary issues not directly addressed in the case but dealt with in the CLOUD Act will impact governments, companies and lawyers for years to come.

The changes in US data regulation precipitated by the CLOUD Act will generate new considerations for companies outside the US. Below, we explain the effects of the CLOUD Act

and the implications for non-US entities, paying particular attention to the possibility of reciprocal data-sharing agreements between the US and other countries. Combined with the European Union's General Data Protection Regulation (GDPR) and the newly proposed US legislation regarding electronic evidence, the legal obligations meriting attention by companies now span multiple jurisdictions.

EFFECTS OF THE CLOUD ACT

The CLOUD Act's main objective is to amend existing US law, the Electronic Communications Privacy Act (ECPA), to allow law enforcement to collect data from providers regardless of where that data is stored. The CLOUD Act makes clear that the US government can order production of data in the 'possession, custody or control' of an electronic communication service provider or remote computing service provider, regardless of where in the world the data is stored. In this context, a 'provider' will typically be a company, such as Microsoft, Google, Apple or other commercial entities providing some combination of email, instant messaging or cloud storage services.

While the CLOUD Act requires companies to comply

with requests for data, it does have two built-in exceptions. An electronic communication service provider may challenge the government's order if the 'customer or subscriber' whose data would be supplied is not a US person and does not reside in the US. A 'US person' is defined in the Act as a US citizen, national, permanent resident, US corporation, or unincorporated association with a substantial number of US citizens or residents as members. Additionally, a company can refuse to disclose the data if it would risk violating the laws of a foreign government. Service providers who receive these requests can challenge the orders they receive on the grounds that they conflict with the laws of a qualifying foreign government.

A novel element of the CLOUD Act is the provision for executive agreements between the US and qualifying foreign governments that would expedite the process of requesting information from a US provider. This has major implications for law enforcement activities, such as counterterrorism, money laundering and other complex crimes, because most major providers operating globally are located in the US.

Recognising that these executive agreements would empower foreign governments to secure far more access to data

located in the US, the Act also established a legal framework that is subject to congressional disapproval but not necessarily subject to judicial oversight. The US Attorney General would first have to confirm that foreign governments seeking to enter into executive agreements had legal protections for privacy and human rights that meet US standards. The foreign government will also have to adopt procedures to handle the collection and retention of information on US persons as a result of a request to a US provider. A request for information made under the bilateral agreements must focus on a defined type of underlying investigation issue and relate to a 'serious crime', such as terrorism. The order will also have to identify, with specificity, the person, account, device or other identifier of the subject whose information is being collected, and the foreign requestor will have to provide reasonable justification based on credible facts. Moreover, the foreign requestor can only seek orders for a defined and limited duration and these should only last as long as reasonably necessary. The foreign requestor will have to confirm that the same information could not be obtained through a less intrusive method. Each order will be subject to judicial review during or prior to enforcement proceedings. In addition,

the foreign government will have to agree to undergo an annual compliance review of each agreement that will be conducted by the Attorney General.

However, the nature of these protections will remain unclear until the first qualifying foreign governments enter into reciprocal data-sharing agreements with the US.

IMPLICATIONS FOR NON-US ENTITIES

Another key facet of the CLOUD Act is that it encourages greater international law enforcement cooperation by decreasing reliance on the existing, overburdened channels for data requests. Every six months, Microsoft alone responds to just as many individual requests from Germany, France and the UK as it does from the US. From July to December 2017, of the 22,939 law enforcement requests Microsoft received, only 3984 were from the US. Countries that enter into reciprocal agreements with the US potentially will have an expedited route to accessing data stored by US operators.

In order to enter into a data-sharing agreement with the US under the CLOUD Act, a country will have to satisfy a set of requirements. According to the CLOUD Act, countries must

have adequate laws on cyber crime, demonstrate respect for the rule of law and adhere to applicable human rights obligations. This includes a demonstrated respect for principles of non-discrimination and recognition of rights, such as free expression and fair trial. Additionally, the requesting countries must have sufficient mechanisms to provide accountability and transparency regarding the collection and use of electronic data.

The Act's privacy protections have also been the subject of considerable controversy. One critique is that the US government is not in a position to be able to properly assess the adequacy of a country's human rights and privacy laws, particularly as they are applied in practice. Critics worry that arbitrary enforcement of the CLOUD Act's privacy standards would result in the US sharing data with countries that abuse human rights or inadequately safeguard information. Proponents of the CLOUD Act counter that privacy standards must remain sufficiently broad in order to encourage consensus, otherwise countries would be reluctant to sign executive agreements that may, by implication, force them to adopt US practices.

Overall, the CLOUD Act will have important repercussions for US and non-US entities. Chiefly, there will be a marked in-

crease in the amount of information that law enforcement will be able to quickly collect across borders.

CONCLUSION

Moreover, the changes in the regulatory obligations under the CLOUD Act and European GDPR portend further changes in existing relationships between non-US entities and US providers. International companies hosting data that may be subject to US jurisdiction will need to ensure that they are prepared to comply with a US request for data. For instance, data would need to be organised and accessible such that a provider could comply with a US order if necessary. Notably, the European Union has been considering its own legislation, granting powers similar to those for the US authorities under the CLOUD Act. On 17 April 2018, the European Commission published its own proposal for EU-wide laws "to make it easier and faster for police…to obtain the electronic evidence, such as e-mails or documents located on the cloud, they need" to prosecute serious crimes. Specifically, the European Commission proposes the creation of new production and preservation orders, available to law enforcement in any EU Member State to request data from a service provider offer-

ing services in the EU. As this new proposal begins to make its way through the European Parliament, many observers across Europe will also be watching how the CLOUD Act is used, and eventually interpreted by US courts.

To date the CLOUD Act has been met with the approval of large technology companies like Facebook, Apple, Microsoft and Google. US and non-US companies should nevertheless begin preparing internally to ensure that their IT, compliance and legal teams will be able to assess the immediate impact of the CLOUD Act. This requires companies to examine their obligations and establish a process to determine whether an individual request raises issues that need to be addressed or challenged in the courts.

■ *Guillermo S. Christensen is a partner, Olivia Gonzalez is an associate and Anupreet Amole is counsel at Brown Rudnick LLP.*

Data risk analysis: understanding and prioritising risk based on resources and legal requirements

BY JAMI MILLS VIBBERT AND JOHN F. BANGHART

REGULATION OF A COMPANY'S CYBER security controls is an evolving and growing area of law for which standards are continually being developed by governmental and regulatory bodies, including the Securities and Exchange Commission, the Federal Trade Commission, the European Union and individual US states, as well as through case law, independent agency guidance, self-regulatory standard-setting bodies and industry best

practices. Regardless of the legal complexities that the current landscape presents, companies are expected to comply with applicable standards or face the potential of government enforcement action or liability in civil litigation.

Indeed, several of the regulations are vague in the security controls required, forcing companies to make decisions as to how to protect their sensitive and personal information. For example, the SEC's Regulation S-P requires companies to adopt "administrative, technical, and physical safeguards for the protection of customer records and information...reasonably designed to" ensure the security of and protect against threats to or unauthorised access to or use of such information.

The FTC has applied its statutory authority to enjoin "unfair and deceptive" business practices under the FTC Act to enforce data security practices in the marketplace. Specifically, the FTC has brought enforcement actions against companies for engaging in practices that the FTC believes present an unreasonable risk to the security of the personal information of employees, customers and consumers. This "reasonableness" standard has been the central component of more than 50 FTC settlements with companies over their data security practices in which the

FTC has alleged that defendants' security practices were unfair under Section 5, even if they were not contrary to public statements and even if there was no financial harm to consumers. Through these settlements, the FTC has emphasised that companies handling consumer information should implement a data security programme that contains administrative, technical and physical safeguards appropriate to the organisation's size and complexity, the nature and scope of its activities, the sensitivity of the personal information and the cost of available tools to improve security and reduce vulnerabilities.

For organisations maintaining health information, the Department of Health and Human Services (HHS) Office for Civil Rights may enforce the Security Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Similar to other data security regulations, entities covered by HIPAA must "use any security measures" that allow them to implement "reasonably and appropriately" various security standards. In making such a determination, organisations must take into account various factors, including their size, complexity and capabilities; the costs of the security measures; their technical infrastructure, hardware and software capabilities; and the probability and crit-

icality of potential risks to health information.

Various US states also have requirements that companies maintain reasonable data security practices. And the EU General Data Protection Regulation (GDPR) takes a risk-based approach to security, requiring that data controllers and processors, "taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons...implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk".

How do companies comply with these standards in a holistic fashion? By engaging in a thorough and thoughtful cyber security risk assessment. A cyber security risk assessment should be conducted pursuant to a recognised framework. One of the most well-known and used risk management framework is the Cybersecurity Frameworks established by the National Institute of Standards and Technology (NIST). Several regulators have cited that framework in connection with urging companies to conduct risk assessments, and a crosswalk between the HIPAA Security Rule and the NIST Framework has been created by HHS

to assist companies in that sector.

A risk assessment under the Framework will lead organisations to identify, discuss and understand organisational objectives, priorities and risk tolerance. Organisations must also undergo a process through which they identify the types and locations of data, as well as the systems containing or accessing that data. During this step, companies must also understand and document what legal requirements govern that data and those systems, what contractual requirements may be implicated, and what threats and vulnerabilities may be applicable to those systems. For example, certain types of personal information may be subject to breach notification laws, and thus have regulatory risk in the event of unauthorised access or acquisition, whereas company intellectual property has little regulatory risk, but large reputational and business risk.

Next, companies undergo an assessment of all of the security controls that have been implemented in the various systems and over the various data sets. This is achieved through an in-depth review of the organisation's policies, procedures, and governance and training documentation, as well as questionnaires and interviews of key individuals from major business divisions,

locations and functional areas (including human resources, information technology, information security, legal, finance, marketing, communications, compliance, and the like). Armed with the information previously gathered, companies will assess (and this is the hard part) the likelihood of a cyber security event and the impact that the event could have on the organisation. To do this, companies must consider all of the information gathered, including the sensitivity and type of information, the locations of that information, the security controls in place to protect that information, the legal, regulatory and contractual requirements governing that information or system, and the threats and vulnerabilities to that information or system, all in the context of the business's identified priorities and resources. This inevitably involves decision making that should be considered by the organisation's decision makers and should be overseen by counsel to protect any legal advice given on the risks and the prioritisation of those risks with the appropriate attorney-client privilege.

Once a company has determined the likelihood and impact of any given event on data or systems, it can prioritise any remediation according to that assessment. This risk treatment

process allows companies to assign owners and resources to the various prioritised risks and to track progress of the implementation of controls to address those risks and, longer-term, the organisation's cyber security maturity over time.

Though the pronouncement to have "reasonable" or "appropriate" data security controls (or technical and organisational measures) may seem vague, both HIPAA and the GDPR delineate the factors considered when completing a risk assessment in the text of the regulation. Several other regulators, through enforcement actions or guidance, similarly indicate a risk assessment requirement. For example, FTC enforcement actions, guidance and settlement orders indicate that companies should conduct a risk assessment to identify reasonably foreseeable risks to the security of personal information. The FTC has brought enforcement actions against companies for their alleged failure to perform an adequate risk assessment under these guidelines. The SEC and OCR have too.

And both Massachusetts and Oregon require companies to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality or integrity of its systems and information, assess whether the existing safeguards

adequately control for and limit those risks, and improve the controls, where necessary. New York requires financial institutions and insurance companies subject to the jurisdiction of the Department of Financial Services to comply with its Cybersecurity Regulation, which requires annual risk assessments. Thus, risk assessments are not only helpful, but also legally required.

A well-defined risk assessment will, likely more than any one security control or tool itself, instruct organisations on the most important places to focus cyber security resources (human, monetary or otherwise). The risk assessment can provide a baseline for annual improvement, and in many cases is required by the governing law. Given the flexibility of a risk assessment and its ability to take into consideration an organisation's unique needs, assets, resources, risk tolerances and legal environment, a risk assessment should be conducted to adequately address cyber security risk, whether legally required or not.

■ *Jami Mills Vibbert is counsel and John F. Banghart is the senior director for technology risk management at Venable LLP.*

Data breach notification: last US states pass laws to require notification

BY DAVID R. LALLOUZ, MICHAEL J. RIELA AND ANDRE R. JAGLOM

WITH THE ENACTMENT OF LEGISLATION on 26 March 2018 in South Dakota, followed almost immediately by the signing of a bill into law in Alabama on 28 March, all 50 US states have now enacted laws imposing data breach notification requirements. In addition, the District of Columbia, Puerto Rico, the US Virgin Islands and Guam each have their own data breach notification laws.

Spurred into action by years of high-profile data breaches and the mounting cost to consumers, businesses, insurers and governments, reaching into the billions of dollars, state legis-

lators across the country have formulated a variety of requirements that apply when breaches of personal information occur. These requirements are intended to ensure that the victims of data breaches receive sufficiently prompt notice of the occurrence of the event, so that they can take steps to protect themselves against identity theft. Further, in some circumstances, these laws require specified remedial action for the benefit of those victims.

The data breach notification laws differ from each other in their details and specific requirements. Nevertheless, there are many important commonalities in the major requirements of most such statutes. Below is a summary of the common themes and a number of significant differences among state breach notification laws.

APPLICABILITY OF BREACH NOTIFICATION LAWS AND TRIGGERING EVENTS

The breach notification laws typically apply to persons or businesses that possess personal information (also known as personally identifiable information, or PII) of any residents of the jurisdiction in question. Some – but not all – jurisdictions pro-

vide that the applicability of their breach notification laws is limited to businesses or persons that conduct business in the jurisdiction. Even a business whose activities in a particular state are minimal, or even non-existent, may not be exempt from the breach notification laws of that state. For example, a company may have employees or customers who are resident in a particular state, even if the company itself does not have an office there. Crucially, therefore, in the event of a data breach, the business must carefully examine the rules of each jurisdiction inhabited by any person whose personal information it possesses.

The requirements of the breach notification laws will apply upon the occurrence of an event often described in terms such as an "unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of personal information" (or, in some states, where it is reasonably likely that such unauthorised acquisition of information occurred).

COMPROMISED PERSONAL INFORMATION

The core of the trigger for the breach notification laws is the nature of the information that was improperly acquired. The

statutes are generally consistent in defining the type of personal information that, if accessed without authorisation, will result in the application of the notification requirements.

Personal information is often defined to mean an individual's first name or first initial and last name, in combination with one or more of the following (the list varies from jurisdiction to jurisdiction, but these are common examples): (i) Social Security number; (ii) date of birth; (iii) driver's licence or government-issued identification number such as a passport; (iv) financial account, credit card or debit card number (often, combined with a security code or password that would permit access to a person's financial account); (v) biometric information; (vi) medical information or health insurance information or identification numbers; and (vii) a username or email address combined with a password or security question and answer that would permit access to an email account.

NOTIFICATION REQUIREMENTS – RECIPIENTS, TIMING AND CONTENT

Once a data breach that triggers a jurisdiction's breach notification statute has occurred, the company must focus on comply-

ing with the notification requirements of each applicable state, in a timely manner.

All jurisdictions, naturally, require the notification of the affected individuals.

Many jurisdictions, though not all, also require notification to various state agencies, such as the state Attorney General's office (e.g., California, Florida, New York and many others), police departments (e.g., New York and New Jersey), and various other agencies, such as consumer protection bureaus. There is, however, a great degree of variance in the magnitude of the data breach that gives rise to the requirement to notify governmental authorities. A number of states require such notification only if the number of affected individuals exceeds a certain threshold (usually from 250 to 1000 individuals), such as California (500 affected individuals); Florida (500 affected individuals); and South Carolina (1000 affected individuals). Others, however, have no threshold, such as New York, New Jersey and Massachusetts.

Additionally, some states require notification to the national credit monitoring bureaus if the breach affected a sufficiently large number of individuals' personal information.

The timing of the notification is typically not specified precisely in the statutes, requiring more generally that notifications be given in the most 'expeditious' time possible, or without 'unreasonable delay' or some similar standard. A minority of states have more specific timing requirements following the discovery that a breach occurred (e.g., Arizona – 45 days; Connecticut – 90 days; Delaware – 60 days; Florida – 30 days).

Notification in writing (i.e., hard copy) is uniformly acceptable, although some states permit email notification (or another format, such as a broader notice to multiple individuals through the media, including cases where individual contact information is not available, or the cost to send individual written notices would be excessive).

Some but not all states require specific details be included in the notice, such as the date of the incident, a description of the incident, contact information of relevant state agencies, etc.

A few states, such as Connecticut and Delaware, require companies to offer free credit monitoring to affected individuals.

ENFORCEMENT

Many states' breach notification statutes contemplate civil actions providing fines and other penalties that may be sought by various state regulatory bodies, such as the Attorney General. Some states, such as California and New Jersey, also permit affected individuals to commence private lawsuits against a covered entity, for example if notification was not provided as quickly as required by the statute.

A business operating in the US or possessing the personal information of US residents must be prepared to act as swiftly as possible following discovery of a data breach to comply with the many applicable breach notification requirements. Given the multitude of state laws, comprising a vast number of requirements, many of which vary from jurisdiction to jurisdiction, it is important that businesses have a plan for compliance in place before a breach is discovered. That means knowing the states of residence for all individuals whose personal data the business holds, including employees, customers and others, knowing the notification requirements of each of those states, and having a plan in place with defined responsibilities for compliance when a breach is discovered.

The time sensitivity and complexity of these requirements make it all the more important for businesses to have qualified cyber security counsel at the ready, not only in the event of a breach, but before it occurs. Businesses should also investigate the costs and benefits of cyber security insurance to protect against potential liability as well as the costs of compliance.

■ *David R. Lallouz, Michael J. Riela and Andre R. Jaglom are partners at Tannenbaum Helpern Syracuse & Hirschtritt LLP.*

GDPR: increased risks surrounding cross-border data transfers

BY GREAT GU

SINCE THE GENERAL DATA PROTECTION Regulation (GDPR) enables the free transfer of personal data within the EU, below we discuss the transfer of data subjects' personal data records outside the EU to a third country. Additionally, this includes the onward transfer of data from a third country to another country outside of the EU.

Fundamentally, there are three requisite considerations when transferring data outside of EU boundaries: adequacy of data protection, application of appropriate safeguards and the application of any derogations or exceptions.

First, the adequacy of protection must be considered. Decisions specific to adequacy are based upon assessment and analysis of third country laws and enforcement. If a given country has been identified as having laws that meet the European standard of protection, then by default it will meet the "adequate protection" standard as defined in the GDPR.

At any time, the European Parliament and Council may request the European Commission (EC) to maintain, amend or withdraw the adequacy decision on the grounds that it exceeds the implementing powers provided for in the regulation. The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. In others words, transfers to the country in question will be assimilated to intra-EU transmissions of data.

The EC has so far recognised Andorra, Argentina, Canada (commercial organisations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing adequate protection. Adequacy talks are ongoing with Japan and South Korea. These adequacy decisions do not cover data

exchanges in the law enforcement sector which are governed by the Police Directive (Article 36 of Directive (EU) 2016/680).

For special arrangements concerning exchanges of data in this field, see the Passenger Name Record (PNR) Terrorist Financing Tracking Programme (TFTP) agreements. These safeguards are primarily legal constructs and are listed below.

Binding corporate rules. These are developed to allow large multinational corporations to adopt a system of policies for handling personal data that bind the company from an accountability standpoint. If a supervisory authority signs off on these rules, this helps simplify how multinationals manage and address global compliance issues.

Standard contractual clauses. Sometimes referred to as model clauses, essentially these are template clauses provided by the EC that can be used by data controllers and data processors. The templates must be used and implemented as-is and are therefore non-negotiable in nature.

Approved codes of conduct. These codes of conduct must be approved by the supervisory authority.

Ad hoc contractual clauses. These must also be approved by the supervisory authority. The purpose of these clauses is to ac-

count for the individual needs and nuances of a given company.

Reliance on international agreements. This assumes that countries may engage in a distinct agreement that allows for the protection of data. Many times, these agreements exist for reasons specific to national security and defence.

Finally, if a third country is not captured in the list of countries that are deemed adequate by the EC, and the safeguards listed above are not available, the only recourse for legally transferring EU citizen data is by way of derogation or exemption.

Derogations were initially defined in the EU Data Protection Directive, but the constraints are more narrowly defined in the GDPR mandate. Perhaps one of the most significant implications of the GDPR is that, unlike under the Directive, failure to comply with the GDPR's international data transfer provisions may result in hefty fines.

Violations of the data transfer provisions in Articles 44-49 are subject to the steeper of the two administrative fine provisions in the GDPR. Such violations may result in "administrative fines up to €20m, or in the case of an undertaking, up to 4 percent of the total worldwide annual turnover of the preceding

financial year, whichever is higher". The factors considered for imposing a fine include "the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor".

■ *Great Gu is APAC cybersecurity manager at AstraZeneca China.*

Author list

PAGE 132

Mike Gillespie, Director
Advent IM
bestpractice@advent-im.co.uk

Ellie Hurst, Marketing Manager
Advent IM
ellie.hurst@advent-im.co.uk

PAGE 176

Great Gu, APAC Cybersecurity Manager
AstraZeneca China
great.gu@astrazeneca.com

PAGE 75

Roberto Minicucci, Senior Director
Baker Hughes, a GE company
roberto.minicucci@bhge.com

Matteo Camprini, Principal Engineer
Baker Hughes, a GE company
matteo.camprini@bhge.com

Massimiliano Copponi, Senior Engineer
General Electric
massimiliano.copponi@ge.com

PAGE 100

Paul Wainwright, Partner
Browne Jacobson LLP
paul.wainwright@brownejacobson.com

PAGE 151

Guillermo S. Christensen, Partner
Brown Rudnick LLP
gchristensen@brownrudnick.com

Olivia Gonzalez, Associate
Brown Rudnick LLP
ogonzalez@brownrudnick.com

Anupreet Amole, Counsel
Brown Rudnick LLP
aamole@brownrudnick.com

PAGE 27

Domenic Puzio, Machine Learning Engineer
Capital One
domenic.puzio@capitalone.com

PAGE 118

Paul Lanois, Vice President and Senior Legal Counsel
Credit Suisse
paul.lanois@credit-suisse.com

PAGE 106

Moira Carroll-Mayer, Senior Lecturer
De Montfort University
mcm@dmu.ac.uk

PAGE 83

Scott Aaronson, Vice President, Security and Preparedness
Edison Electric Institute
saaronson@eei.org

PAGE 57

Emilian Papadopoulos, President
Good Harbor Security Risk Management
emilian@goodharbor.net

PAGE 66

Steve Povolny, Head of Advanced Threat Research
McAfee
steve_povolny@mcafee.com

PAGE 40

Jing de Jong-Chen, General Manager
Microsoft Corporation
jingc@microsoft.com

Rob Spiger, Principal Security Strategist
Microsoft Corporation
rspiger@microsoft.com

PAGE 34

Gerald Reddig, Head of Product Marketing, Security
Nokia
gerald.reddig@nokia.com

PAGE 50

Steven Hadwin, Head of Operations - Risk Advisory and Cyber Security
Norton Rose Fulbright LLP
steven.hadwin@nortonrosefulbright.com

PAGE 91

Victoria Baines, Visiting Associate
Oxford Internet Institute
victoria.baines@oii.ox.ac.uk

PAGE 141

Robert Allen, Partner
Simmons & Simmons
robert.allen@simmons-simmons.com

Paul Baker, Partner
Simmons & Simmons
paul.baker@simmons-simmons.com

Camille Tewari, Consultant
Simmons & Simmons
camille.tewari@simmons-simmons.com

PAGE 127

William Ridgway, Partner
Skadden, Arps, Slate, Meager & Flom, LLP
william.ridgway@skadden.com

PAGE 168

David R. Lallouz, Partner
Tannenbaum Helpern Syracuse & Hirschtritt LLP
lallouz@thsh.com

Michael J. Riela, Partner
Tannenbaum Helpern Syracuse & Hirschtritt LLP
riela@thsh.com

Andre R. Jaglom, Partner
Tannenbaum Helpern Syracuse & Hirschtritt LLP
jaglom@thsh.com

PAGE 160

Jami Mills Vibbert, Counsel
Venable LLP
jvibbert@venable.com

John F. Banghart, Senior Director for Technology Risk Management
Venable LLP
jbanghart@venable.com

ABOUT FINANCIER WORLDWIDE

Since 2001, Financier Worldwide has provided valuable information on corporate finance and board-level business issues through its monthly magazine and exclusive website content.

As a leading publisher of news and analysis on this dynamic global market, the organisation is recognised as a valued source of intelligence to the corporate, investment and advisory community.

EBOOK

FINANCIER
WORLDWIDE corporatefinanceintelligence