2Q2017 Global Cyber Newsletter

TransRe™

cyber

We value risk.

CONTENTS

WannaCry Special Report

With its truly global impact, the WannaCry (aka Wanna Decryptor or WCRY) virus has been the most notable breaches of the year to date. The ransomware, which targeted vulnerabilities in unsupported Microsoft Windows operating systems encrypted data and demanded a ransom of $300 payable in Bitcoins.

A self-propagating worm module within the milicious software enabled it to infect over **200,000 systems in more than 150 countries**. Victims included one of the largest telecommunications companies, Telefonica in Spain; the National Health Service (NHS) in the UK; French car maker, Renault; FedEx and Deutsche Bahn in Germany. The geographical spread ranging from Taiwan, India, Russia, Ukraine, Europe and the US.

Hospitals in the UK were left unable to access medical records with 16 closing with many appointments and operations cancelled.

Key to the virulent spread of WannaCry through computer networks was an exploit known as EternalBlue.

EternalBlue targets file sharing protocols and is understood to have been developed by the US National Security Agency (NSA) as one of its own cyber weapons. A group known as the Shadow Brokers dumped a number of potent exploits online in April including EternalBlue.

Microsoft took the unusual step of issuing emergency patches for Windows XP, 8 and Server 2003 which are operating systems that Windows ceased supporting a number of years ago. The NHS in particular, is believed to have run Windows XP which has not been supported by Microsoft since April 2014. This does impose significant cyber risks for those organizations still running these systems. Microsoft issued a patch addressing the vulnerability for all currently-supported OS over a month before the attacks, although not all users took advantage of the update.

There has been considerable speculation as to the origins of the virus including a number of cyber-criminal groups and state sponsors.

At the time of writing, businesses across the globe have been subjected to a second global ransomeware attack in two months. This time through the modified **Petya virus**. The encryption of files and demand of $300 in Bitcoins is not dissimilar to the WannaCry attack. Likewise, EternalBlue vulnerabilities are believed to have been exposed in the attack although, the mechanism of spread through networks is said to have been more sophisticated. Less sophisticated was the means by which the perpetrators sought to collect their bounty with a single bitcoin payment address for every victim and single e-mail address with which to communicate with the victims (now closed down). This has given rise to speculation that destruction or disruption was the motivation behind the attack rather than illicit gain. The attack is widely thought to have originated in the Ukraine with a large number of Ukrainian entities having been affected including the Ukrainian central bank, the state postal service and its largest telephone company. Alarmingly, radioactive monitoring of the Chernobyl nuclear plant was also affected. Whilst the fallout from Petya is still to be fully asssessed, Petya also claimed a sizable number of global victims including Russian oil company, Rosneft; the US pharmaceuticals Merck; Danish shipping firm, Maersk; international law firm, DLA Piper; British marketing firm, WPP and French construction company Saint-Gobain.

Whilst global quantum of insured losses resulting from the spread of WannaCry (and now Petya) is also a matter for much speculation, those defining cyber aggregation mechanisms within (re)insurance policies will be wary of the rapid infection across a wide geographical area. Traditional aggregation criteria such as time, locatality and cause of loss could prove challenging. As always, aggregation is a highly subjective matter.

WannaCry Special Report

Did you know...?

that the spread of the WannaCry malware was **slowed by complete accident** when a young cyber security analyst registered the domain name of a website which the malware repeatedly tried to contact each time it tried to hijack a computer. The domain name had previously been unregistered. The code worked by attempting to connect to the domain and, if unsuccessful it would ransom the system, but if successful it would exit the system. It is believed that this was a mechanism built in by the perpetrators to prevent analysis by security experts in a sandbox environment. A sandbox is a restricted operating environment for analysts to evaluate potentially harmful programs. By registering the domain the virus believed it was in a sandbox environment and exited.

Al Jazeera Attack

Africa, Asia Pacific

Al Jazeera, the Qatar based broadcaster was the victim of a **cyber attack against its systems**, websites and social media platforms amid growing tensions in the middle east. Qatar has been isolated recently by fellow Arab states over alleged links to terrorism.

Holiday Inn

Europe, Latin America, United States

UK based global hotel chain InterContinental Hotels Group (IHG) **suffered a malware attack** that exposed the payment card details of customers. The breach is understood to have taken place between September and December 2016 and struck over a thousand hotels in the chain. Card numbers, expiry dates and verification codes are believed to have been obtained.

Brazilian Banks

According to the cyber security firm Kaspersky, an un-named Brazilian bank suffered a massive hack on October 22, 2016: for roughly 5 hours, **the bank's entire online operation was hijacked**, sending customers to a "dummy" site that stole their account information. It is believed that all ATMs and POS systems were also compromised, and that the dummy websites inserted malware onto users home computers when they accessed the site.

Industroyer Malware

Security researchers say that the **Industroyer malware has the potential to target critical infrastructure**. Internet security firm, EST has described the malware as the most sophisticated since Stuxnet using industrial communication protocols used worldwide in power supply and other critical infrastructure. It is highly customizable and capable of directly controlling electricity substation switches and circuit breakers. Industroyer may have been involved in attacks on the Ukrainian power grid at the end of last year.

Wonga

Short term loan lender, **Wonga suffered a data breach affecting up to 245,000 customers** in the UK plus a further 25,000 in Poland. The breach may have included names, addresses, phone numbers plus the last 4 digits of credit cards and sort codes. The company doesn't believe that Wonga accounts and passwords had been compromised.

On May 23rd, **Target entered a settlement with 47 states** resolving legal issues with the 2013 consumer data breach. Target agreed to pay $18.5M to be distributed amongst the states – California received the largest share, at $1.4M. The money goes to the various states attorney generals' budgets to fund future enforcement actions. The only states not participating in the settlement were Alabama, Wisconsin, and Wyoming.
Earlier in May, Target also agreed to fund a $10M compensation account for consumers affected by the breach although finalization of that settlement is being held up by a single consumer, whose legal team is not satisfied with the amount. Note that this settlement comes after the December 2016 ruling of the District Court of Minnesota that rejected Target's standing argument. By selling, Target also avoids the risk of settling further pro-consumer precedents by proceeding with the litigation. Target has spent over $100M in settlements and other costs related to this data breach to date.

In June, it was revealed that 1.1 terabytes of data on nearly **200 million U.S. citizens had been left publicly accessible on an Amazon cloud server**. The information includes birthdates, home addresses, telephone numbers.

South Korean web hosting company Nayana paid in excess of **$1m following a ransomware attack affecting 153 Linux servers and 3,400 business sites in June**. The Erebus ransomware first emerged in malvertising attacks in September last year but has evolved its mode of attack allowing it to bypass Windows User Access Controls. The original demand of 550 bitcoins (over $1.6m) was negotiated down to less than 400 bitcoins.

In June, the **New York State Attorney General announced a $130k settlement with CoPilot Provider Support Services, Inc.** after CoPilot waited over a year to give notice of a data breach that exposed over 220k patient records. CoPilot provides support services to the medical industry, helping medical providers determine a patients insurance coverages for medications. The settlement is notable as an example of state regulatory action - as opposed to similar actions by the federal Department of Health and Human Services - and also because it highlights a common vulnerability: 3rd party service providers.

Africa, Asia Pacific

In Singapore the **Computer Misuse and Cybersecurity Act (CMCA)** has been amended by a new section 8A making it an offence to obtain, retain or supply personal information about another person (being an individual) obtained through cyber-crime where the offender knows or has reason to believe that the information been obtained illegally. Fines up to S$10,000 or imprisonment may be levied.

The enforcement of a part of **China's cybersecurity law that was set to go into effect in early June 2017 has been postponed for 18 months**. The move comes amid broad concern that the terms and requirements of the law were ill- or un-defined, leaving corporations without a roadmap to compliance.

Recent Regulatory Penalties

The Personal Data Protection Commission (PDPC) fined **Tech Mahindra** S$10,000. Tech Mahindra provided single sign on services to Singapore Telecommunications Limited. A coding error resulting in a customer's details being updated on 2.78m other customer profiles.

Europe

Recent Regulatory Penalties

The UK information regulator fined **Keurboom Communications** Limited a record £400,000 for nearly 100 million nuisance calls in an 18 month period.
Greater Manchester Police were fined £150,000 after 3 DVDs containing footage of interviews with victims of violent or sexual crimes got lost in the post.

11 charities breached privacy laws in a variety of activities including sharing data with other chartieis; obtaining data not provided by the donor and ranking donors based on wealth. Modest fines ranging from £6,000 to £18,000 were levied against a number of popular charities.

BaFin
Federal Financial Supervisory Authority

German regulator, BaFin has announced that it will **liberalize the guidelines relating to kidnap and ransom insurance for cyber attacks**. The insurability of such risks in Germany has, until now, been open to quesitons.

United States

Trump Administration Acts on Cyber Security

President Trump signed legislation on April 3, 2017, that rescinded the **FCC's data privacy regulations** – leaving a regulatory vacuum in that space. On May 11th, **Trump signed the long-delayed executive order** on cybersecurity. That order requires federal agencies to follow the NIST standards to assess cybersecurity risk and submit reports on that risk within 90 days. More controversial is the shift of significant responsibility for federal cybersecurity to the military. The Obama administration and many cybersecurity commentators oppose such a move, noting increased risk of military oversight of civilian functions in an area not traditionally within the military specialty. Also significantly, the order calls for increased development of the U.S. cybersecurity workforce.

Ransomewared Healthcare Entities Employing Loophole to Avoid Reporting

The **guidance** issued by the U.S. Department of Health and Human Services – Office of Civil Rights on health information privacy includes what is being referred to as a **"loophole"** in the reporting requirements That is, healthcare entities suffer a ransomware attack must report the incident unless there is a low probability that patient data has been compromised. While this practice may not be what was intended by the OCR, this practice is not uncommon; for example, the Hollywood Presbyterian ransomware attack was one of the most highly-publized of 2016, yet they never reported the incident, nor do they appear on the Wall of Shame.

Europe

Hackers Sentenced

Russian hacker Roman Seleznev, aka "Track2" was sentenced on April 21, 2017, in U.S. Federal Court to serve 27 years in prison, after being found guilty of defrauding 3,700 financial institutions in the U.S. or at least $169M USD. Additional charges are pending against Mr. Seleznev in Nevada and Georgia. Seleznev is the son of a Russian politician with close ties to Russian President Vladimir Putin – his father asserts his son is innocent and was "abducted" and is being held illegally. Another Russian national, Peter Levashov, was arrested in Spain at the request of the U.S. Department of Justice and is currently facing extradition to the U.S. to face hacking charges for allegedly running a botnet that stole banking credentials and generated spam emails. **A British national, Adam Mudd – a teenager – was sentenced to two years in jail for creating malware and selling it to cybercriminals for over £386k**. That program was used to created 1.7M attacks, costing at least $10M in mitigation costs. Finally, a Lithuanian national, Evaldas Rimasauskas, was indicted by the U.S. Department of Justice who skimmed $100M from Facebook and Google over the course of two years. The bulk of the money has been recovered. These actions by the DOJ, and the harsh sentence for Mr. Seleznev, are intended to deter other bad actors – the effectiveness of which is unknown.

Asia

Indian Biometric Data for 130 Million Potentially Exposed

The Bangalore, India, based **Centre for Internet and Society (CIS) issued a report** indicating that **four national or state-run databases were breached**, exposing biometric data of as many as 130 million people. India's Aadhaar biometric system uses fingerprints and iris scans to identify people, thereby linking them to a national banking, health, and data system. If the system was breached, the accounts and entitlements of the affected individuals would be compromised. **UIDAI, the government entity overseeing Aadhaar, denied that there was any data leak**.

Pacemakers Remain Vulnerable

Worries that **medical devices – particulary in the age of the IoT** – are vulnerable are nothing new. One recent study found that only 17% of medical device manufacturers had taken steps to secure their products. However, a **new whitepaper** suggests that pacemakers remain **uniquely vulnerable**. The researchers examined the devices / ecosystems from four different pacemaker / defibrillator manufacturers, and found 8,000 vulnerabilities in the code.

Insurers and reinsurers may need to re-evaluate the risk profile of businesses handling data to account for potential fines under GDPR

The General Data Protection Regulation (GDPR) will come into force on 25 May 2018 and introduce the possibility for substantially increased fines to be issued for data protection breaches compared to those which can be imposed currently. It will also introduce mandatory notification requirements to data protection authorities across all sectors. The GDPR will apply across Europe and therefore will have widespread international impact.

Within the EU service providers that process personal data on behalf of other organisations, data processors, will face new obligations and may be on the hook for substantial fines where failings are identified.

The toughened approach to data protection fines envisaged under the GDPR is something that many data controllers and data processors are already aware that they need to consider carefully when putting in place data processing contracts within the relevant jurisdictions. Insurers and reinsurers, including those with an international outlook, must also recognise the impact that the changes could have on the risk profile of businesses they provide cover to.

Fines under the GDPR

Under current data protection rules within the UK, for example, data processors cannot be fined by the Information Commissioner's Office (ICO) for a breach of data security. It is the data controller that is subject to any fine. Where data processors have contravened data protection legisla on then the data controller may seek to recover some or the entirety of that fine, together with any other associated costs, from the data processor under the relevant contract.

However, once the GDPR comes into force on 25 May 2018 data processors may also be fined directly by the relevant supervisory authority (the ICO in the UK). This is significant for two key reasons; (i) data processors, even smaller entities, must engage with the requirements of the GDPR; and (ii) the potential fines that businesses may face are increasing substantially.

A two-tiered sanctions regime will apply. Contraventions of certain provisions by businesses, which law makers have deemed to be most important for data protection, could lead to fines of up to €20 million or 4% of global annual turnover for the preceding financial year, whichever is the greater. For other breaches, the authorities could impose fines on companies of up to €10m or 2% of global annual turnover for the preceding financial year, whichever is greater.

The relevant provisions on data security are contained under Articles 5 and 32 of the General Data Protection Regulation.

The fines that could be imposed under the GDPR could be significantly higher than the maximum penalty that can currently be applied by data protection authorities. In the UK, for example, the ICO has the power to issue fines of up to £500,000 to businesses for serious breaches of the Data Protection Act.

The largest fine the ICO has imposed for a breach of the Data Protection Act to date is the £400,000 penalty it issued to TalkTalk, which followed a high-profile cyber attack and data breach. According to the company's latest annual report, TalkTalk's revenues for that year totalled approximately £1.8 billion. A potential fine of up to approximately £72 million could therefore have been imposed on TalkTalk in connection with the data breach it experienced had the GDPR applied at the time of the incident.

Impact of fines on the supply chain and insurers

The TalkTalk example is a sobering reminder of the step-change in the severity of penalties that could be imposed for breaches of EU data protection laws after the GDPR comes into force.

The changes represent a matter of considerable risk management for both data controllers and any data processors in their supply chains. Insurers should also be paying close attention to this, as the risk profile that smaller insured processors in a contractual chain could present may be fundamentally altered by the change. There's a real risk point here for insurers: SMEs or low level processors that previously may have been considered lower risk could now be viewed in a whole new light. The scale of the potential fines is such that reinsurers may also need to consider the potential risk posed.

Awareness of data protection has been growing in recent years, with more and more data breaches hitting the headlines and organizations battling to manage the impact such incidents have on their reputation and, ultimately, their bottom line. We expect that rate of awareness to increase as we approach the 25 May 2018 deadline when the GDPR comes into force. However, the 'big bang' will probably come in the short to medium term after GDPR takes effect and once the first substantial fines are levied.

Data processors and others that fail to pay attention to the reforms will be in for a rude awakening, including their insurers where appropriate due diligence has not been carried out in rela on to the insured's risk profile. In turn, this may impact reinsurers. It is remarkable how many SME businesses, including those that have insurance cover, even today have little to no appreciation of data protection considerations or security measures. Following the GDPR a failure by a data processor to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" could result in a fine of millions of euros. It is incumbent on insurers to reassess the risk they underwrite as a result, particularly where those fines may inadvertently be covered by existing policies.

To mitigate the risks of major fines within the supply chain, businesses should pay close attention to the liability arrangement within the relevant contractual frameworks; and ensure that appropriate technical security measures are put in place by each processor in the contractual chain. Insurers should be asking similar questions of their insureds.

As data has developed to be almost a currency in its own right, protection of that data has taken on an equally considerable value and the GDPR marks a huge increase in the potential risks that will come with processing that data not only to the relevant data controller or data processor, but also their insurers (and reinsurers).

Nick Bradley, Partner in the Insurance, Regulation and Products team at Pinsent Masons LLP

Ian Birdsey, Partner in the Risk Advisory Services (Specialist Cyber) team at Pinsent Masons LLP

LITIGATION NEWS

Africa, Asia Pacific, Europe

Facebook Litigation in Germany

Facebook has successfully **appealed** a German regional court ruling that the parents of a deceased child were entitled to access child's Facebook account to investigate bullying. The court said that the ruling was made in accordance with telecommunications secrecy law which precludes heirs from viewing communications of deceased relatives. Facebook cited concerns over the privacy of other users that she had communicated on the platform had such access been granted.

In a separate case the German courts rejected an **injunction** brought by a Syrian refugee seeking to prevent Facebook from publishing slanderous images. The refugee, Anas Modamani, had been pictured with German chancellor Angela Merkel at a refugee center in 2015. Subsequent posts on Facebook had falsely linked Modamani to terrorist attacks. The court ruled that Facebook was not obliged to proactively seek out and delete defamatory posts.

Facebook, Twitter and Google have previously reached agreement with German authorities to remove hate speech from platforms within 24 hours.

Law Firm Faces Lawsuit for Mere Threat of Data Breach

Chicago law firm Johnson & Bell was sued in April 2016 by a former client alleging that the firms' network security was out-of-date and left his confidential data vulnerable - but notably, it was not alleged that there had been any breach. Amongst the allegations, the suit is based on Johnson & Bell's alleged breach of contract in failing to live up to their privacy promises, and unjust enrichment. Although initially filed under seal, the suit has since been unsealed and the plaintitffs law firm bringing the action revealed they have brought additional suits against other law firms. Although the ultimate success of such suits remains to be seen, these cases are a reminder that law firms and other professional services and vendors - can just as easily be targeted, and could lead to the exposure of the protected data of all their clients.

P.F. Chang's Litigation Moves Forward

The P.F. Chang's litigation is already well known for having helped establish how standing questions will be addressed in data breach cases early on, however, the case itself continues its slow progress. Most recently, on April 26, 2017, the **District Court denied P.F. Chang's renewed motion to dismiss**, and moved the case forward into the discovery phase. If the case does proceed to trial, it could set another precedent, as many similar cases either didn't survive the preliminary motions to dismiss or settled.

Home Depot Settles Data Breach Lawsuit

In late April 2017, **Home Depot settled the shareholders derivative lawsuit** against the Board, CEO, and CIO. The settlement requires a litany of steps to be taken to improve cybersecurity at the company as well as transparency within the company, but the only money damages are up to $1.125M in legal fees. The settlement comes as the dismissal of the case was being appealed to the 11th Circuit. The Home Depot breach itself cost $152M with a total exposure estimated at $10B.

Anthem Settles Data Breach Litigation

The litigation related to the 2015 Anthem data breach has **resolved via settlement**. In addition to a massive $115M monetary component, the settlement is notable for requiring Anthem to assume responsibility for long-term, continuing efforts to protect and re-establish the affected parties identities, as well as compensate them for out of pocket costs and offer alternative compensation to those members of the class who do not enroll in those programs. Specifically, Anthem agreed to provide ID Theft Insurance ($1M limit), Internet Surveillance (monitoring the dark web for personal information of the class members), Identity Restoration Services / fraud resolution assistance, and additional protections for class members who are minors. **Attorney fees to the plaintiff's** account for nearly $38M of the $115M total.

High value targets in a low security environment has turned the heads of cyber criminals in the Asia Pacific region according to a recent **Marsh & McLennan report** with hackers 80% more likely to attack organizations in Asia. The reasons for the potential threat in the region are twofold; i.e. the growing speed and scope of digital transformation, and the expanding sources of vulnerability stemming from the increasing internet of things (IoT) connectivity.

AXIO Global

Insurance Industry Driving Force in Risk Management Initiatives

After big breaches in the retail space, it was the cyber insurance industry that was a driving force in moving the market to adopt end-to-end encryption by offering substantially different rates for those with such a system in place. According to **Axio Global**, it is now the insurance industry again that is forcing multiple industries to adopt new risk management strategies like anti-phising awareness training, strong network segmentation, and other such initiatives. In a world without global - or even national - protocols by requiring minimum technological and cyber security controls, the insurance indstry is helping establish industry standards and moving their insureds toward a more secure future.

The prevalence of ransomware has heightened awareness of cyber security among UK businesses according to a survey commissioned by the **UK Government**. The survey revealed virtually all UK businesses are exposed to cyber security risks and that 61% of the companies surveyed held personal data on customers. 60% store commercially confidential information on the cloud (69% in Finance and Insurance sectors); 46% of businesses identified at least one cyber security breach in the last 12 months. Fraudulent e-mails to staff was the most common type of breach (72%). 58% of those identifying a breach reported that there was no 'significant' outcome. 57% identified some impact e.g. need for implementation of new protections (38%) and time taken up by staff dealing with the breach (34%).

Meanwhile, only 52% had enacted the basic technical controls across five key areas laid out under the Government endorsed Cyber Essentials Scheme.

Industry Articles

RMS 2017 Cyber Risk Landscape

JLT Re—Unlocking The Potential of The Cyber Market

Symantec—2017 Internet Security Threat Report

Verizon's 2017 Data Breach Investigations Report

NetDiligence Cyber Risk News Alert

Contacts

Peter Cridland
Assistant Vice President
1.212.365.2032
pcridland@transre.com

Kara Owens
Global Head of Cyber Risk
1.212.365.2340
kowens@transre.com

Lauren Markowski
Cyber Risk Underwriter
1.212.365.2301
lmarkowski@transre.com

Rhett Hewitt
Cyber Risk Underwriter
44 (0)20 7204 8676
rhewitt@transre.com

Calum Kennedy
Vice President Claims
44 (0)20 7204 8645
ckennedy@transre.com

To receive future editions of the TransRe Cyber Newsletter, please CLICK HERE and include your name, title and organization in the body of the email.