TransReflections

Cyber Newsletter

July 2020

TransRe™
cyber
We value risk.

Table of Contents

Introduction

Welcome to our first newsletter of the COVID-19 era. Much has been publicized on the topic of whether the seismic shift to remote working and the increase in exposure to vulnerabilities will lead to an uptick in cyber claims. It shall be interesting to see how much of a spike in activity has been enhanced by the COVID environment, considering ransomware trends were already escalating over the past year.

Regardless of COVID-19, we would still have been commenting on ransomware trends since we continue to see ever more insureds impacted. One of the more shocking examples is Fresenius, one of Europe's largest private hospital groups and a world leader in dialysis products. In May 2020, the conglomerate was the victim of a Snake ransomware attack, although fortunately there appears to have little impact to care provision. It is challenging to monitor the daily notable cyber-attacks, assess their severity and figure out if they will translate into a large insured claim.

Understandably, the global pandemic has suppressed other newsworthy events. This month, Honda was also impacted by Snake ransomware. Snake is a variant that targets industrial control systems. A few years ago, the cyber insurance market would have been abuzz after a Marriott type incident and now we are growing accustomed to this type of attack. Assessing the impact on insurers is complicated because not all corporations (such as EasyJet) buy an insurance tower. The eagle-eyed amongst you might have spotted that Marriott and EasyJet are data breach incidents and not ransomware victims. However, we are now seeing ransomware variants such as Maze that threaten to exfiltrate data if the ransom is not paid. Maze extorts on fear of a data breach.

This year a substantial amount of ransomware claims originated from Australia, Europe and the US. Not only is the geography diversified but the sectors targeted are as well (managed service providers, logistics companies, FinTech's and traditional manufacturers). A good question to ask is if the ransom in these cases are being paid in full. For obvious reasons, cases are rarely publicly disclosed making it difficult to evaluate but $1M+ settlements are happening. Extortion payments are not permissible in all countries and often a victim's response will be influenced by this dynamic. Whether to mitigate the business interruption claim by paying the ransom is often a key consideration and might be the reason why we have seen some of the larger BI claims occur outside the US. Companies such as Pitney Bowes have also been unfortunate and have been impacted more than once. Are certain strains of ransomware such as Ryuk more impactful to insurers than others? These are some of the trends we are tracking.

The trends that we are seeing in the insurance market are playing out in increased attrition loss ratios rather than developing into a cyber cat. However, the global nature of the pandemic has highlighted two areas that the insurance industry might have previously been complacent. One is under the appreciation of systemic risks. The previously unthinkable such as sports around the world being shut down for three months (unless you count the Belarussian football league!) lends fresh perspective to contemplating the remoteness of the tail risk event for a cloud provider crashing. The global impact of the pandemic also resonates with cyber exposures. If a Ukrainian accountancy software provider suffers malware that causes the widespread havoc associated with NotPetya, what will be the extent of damage caused by an intrusion into a more well-known software provider? Lockdown and the disruption to global supply chains has provided insight of what an event might look like.

The second area is clarity of coverage. While we are seeing great strides this year to affirm or exclude cyber coverage we remain in a transient stage. The pandemic has forced further scrutiny of coverage across the insurance spectrum and we can expect to see many disputes over intent. During this difficult period, we should look forward to a more positive and engaged marketplace to tackle these challenges. There is some great work being undertaken by insurance associations on clarifying cyber exposure in all lines and we are fortunate to be part of an industry that has both the opportunity to adapt and to make progress to the challenges posed by COVID-19 and cyber risk.

Rhett Hewitt
July 2020

COVID-19 Special Section

Hackers Vow to Refrain During COVID-19

In mid-March, many hacking groups stated they would refrain from targeting healthcare providers during the pandemic. However, hospitals and other healthcare providers have still remained among the most frequently-targeted throughout the pandemic.

Zoom Under Scrutiny After Explosion of Use Due to Pandemic

Video conferencing software Zoom experienced a meteoric rise after much of the world moved to a remote working environment due to pandemic-related quarantines. Average daily uses rose from 10M a day to over 200M during the months of December through February. Zoom users quickly noted the company's encryption methods were sub-par and public-interest groups began pushing for the company to release information on their interactions with law enforcement since they were rivaling major tech players in usage. Issues with security lead to a number of intrusions and created a new phrase known as zoombombing.

U.S. Department of Health and Human Services Breached

In March 2020, the U.S. Department of Health and Human Services suffered an apparent DDoS attack. The attack itself did not target the section of HHS that enforces HIPAA violations and the incident was intended to confuse the federal governments' COVID-19 response.

Microsoft Issues Ransomware Warning to Hospitals

In April 2020, Microsoft issued a warning through its security blog to a number of hospitals that had vulnerable gateways and VPN settings. Microsoft stated they had seen evidence of sophisticated cyber-attacks targeting such vulnerabilities and that the hospitals were at risk for a ransomware attack.

Data Protection During Exceptional Times

The COVID-19 pandemic has presented challenges around data protection regulations and criminals have had the opportunity to exploit vulnerabilities.

The UK's ICO has acknowledged the exceptional times and severe frontline pressures on organizations with the recognition that, as a public authority, it should act in a manner that takes in to account the current circumstances.

In Europe, there have been calls by civil liberties groups for the European Data Protection Board (EDPB) to review a decree in May by the Hungarian government which purported to limit the exercise of certain rights and measures under GDPR during a state of emergency imposed by the government in response to the coronavirus pandemic.

The EDPB asserted that the mere existence of a pandemic or any other emergency situation is not a sufficient reason to provide any kind of restriction on the rights of data subjects. Any type of restriction must contribute to the safeguard of an important objective of general public interest of the EU or a member state.

Data protection regulators around the globe have issued guidance on how to handle data during the pandemic.

The ICO stated that organizations are not prohibited from introducing COVID-19 testing and asking employees if they have symptoms. In further guidance, the regulator has highlighted a number of data protection steps that include only collecting and using what is necessary and enabling staff to exercise their information rights.

The regulator has also issued guidance on the use of surveillance including CCTV and thermal cameras.

Tracing apps have been introduced around the globe to varying degrees. The Australia government has introduced an app (on a voluntary basis) where an encrypted identifier on a mobile app will recognize another user and tracks the date, time, distance and duration of contact. The data will be deleted on a rolling basis. The app will also contact other users if the person tests positive for COVID-19. Australian regulator, OAIC will have independent oversight of the government's use of the app under the Privacy Act.

Meanwhile, member states of the EU have introduced a 'toolbox' for the use of mobile contact tracing. The toolbox provides a practical guide for member states that is fully compliant with EU data protection laws and requiring that usage of the app must be on a voluntary basis.

Interpol has warned that cybercriminals are attacking businesses and individuals at a time when cyber defenses might be lowered to carry out spam campaigns, phishing or spread malware.

Notable Breaches

EasyJet Suffers Sophisticated Breach: 9M Customers Compromised

In May 2020, EasyJet disclosed a significant breach that occurred in January. The majority of 9M accounts compromised lost names and email addresses but there were a few thousand accounts that suffered lost credit card information. Last summer, British Airways was fined £183M for a much smaller breach. Even though the pandemic has decreased air travel and has affected many airlines, it remains to be seen how the appeal of the BA fine will turn out and how EasyJet will be treated by regulators.

Major Cyber Insurer Suffers Ransomware Attack

In March 2020, Chubb a key player in the cyber insurance industry was hit with a ransomware attack. Maze, one of the largest ransomware groups supposedly was responsible for the attack. Details of the attack are limited, and the hackers allegedly posted stolen information online.

Recent Xchanging Breach

London insurance bureau, Xchanging recently confirmed that it had also suffered a ransomware attack. The company believes the incident is isolated to the Xchanging environment and there is currently no indication that data has been compromised or lost.

Honda Ransomware Attack

Japanese car manufacturer Honda suffered disruption to operations in the UK, US, Japan, Turkey and Italy following a ransomware attack. Access to computer servers and e-mail were affected.

Official Website Cloned

In the German federal state of North Rhine-Westphalia, a fraudster cloned an official website that provided state emergency aid to self-employed individuals and small businesses during the coronavirus crisis. When users entered their personal details into the cloned site the fraudster was able to use the data and claim the funds for themselves. The scam forced temporary shutdown of the website.

UK regulator, the Financial Conduct Authority (FCA) has warned the public through its website and social media channels of an attempt to reproduce its Financial Service Register.

Australian Government Agency Hit by Cyber Attack

Service NSW, the Australian government agency that provides various government services, alerted police and authorities that customer information had been accessed during a cyber-attack. The attack reduced the visibility of products in its systems resulting in temporary shortages.

Beer Production Interrupted in Australia

Australian beverage giant, Lion confirmed that it suffered a partial IT shutdown as a result of a ransomware attack. The attack caused limited visibility of its products in its systems and as of a result there were temporary shortages of products.

Major South African Companies Targeted

In South Africa, Life Healthcare, the second largest private hospital operator confirmed they were a victim of a targeted criminal attack on its IT systems. Admissions systems, business processing systems and email servers were compromised by the attack.

Life Healthcare is the third major South African company to be targeted this year along with Nedbank, through a third party service provider's system. Data of 1.7M clients was compromised. In March 2020, Omnia Holdings experienced an attack on its IT infrastructure and was forced to restrict access across the business.

Regulatory and Legislative Update

Australian Regulatory Enforcer Sues Facebook

The Australian Information Commissioner sued Facebook for failure to protect their users' information. This Is Your Digital Life, an app that collects direct information allegedly collected detailed information from over 300K Australian Facebook users when the app was only installed by 53 users. Allowable fines under the Australian law total A$529B.

CCPA Enforcement and NY Shield Law Remain on Schedule

California's sweeping data privacy law, the CCPA, became effective January 1, 2020 and all enforcement actions were delayed until July 1, 2020. A wide range of businesses have lobbied the CA Attorney General to further delay the enforcement deadline due to COVID-19 complications and recent fine-tuning of the CCPA rules. The AG has committed to keeping the July 1 enforcement date. On the east coast, New York's Shield Law took effect as scheduled on March 21, 2020.

TikTok Investigated

Chinese-owned social media app TikTok is to be investigated by the Dutch Data Protection Authority (DPA) over the handling of children's data. The app has been popular with children during the coronavirus outbreak and the DPA will investigate whether parental consent is required to collect, store and use children' s data.

Regulatory Fines

The Italian data regulator issued a fine of €27.8M for the misuse of data. Millions of unsolicited marketing calls were performed without consent despite the fact that the recipients of the calls were listed on a public opt-out register.

In January 2020, electronics group, DSG Retail Limited was fined the maximum £500,000 by the ICO under the old Data Protection Act for an extensive compromise of its computer systems between July 2017 and April 2018. More than 5.5M payment cards were affected.

Regulatory Under-Funding?

As GDPR celebrates its second anniversary some have questioned whether data protection regulators are sufficiently funded to utilize the substantial power they have.

Litigation News

Supermarket not Vicariously Liable for Criminal Conduct of Employee

In April, the English Supreme Court finally ruled in favor of Morrisons supermarket in the landmark case brought by workers who had their data released online by a disgruntled employee.

Permission to Appeal in Google Case

The Supreme Court will hear an appeal in the case of Lloyd v Google where the claimant is seeking to launch a representative action against Google's use of browser generated information on Apple's Safari browser (the "Safari workaround"). The case is on behalf of more than 4M claims for the purported loss of control of their data.

European Court to Rule on Data Transfer to US

In July 2020, the European Court of Justice (CJEU) is expected rule on the latest challenge to the validity of standard contractual clauses, the process companies use to transfer data to the US.

Cyber Publications

Verizon 2020 Data Breach Investigations Report

Crowdstrike Global Threat Report 2020

Crypsis 2020 Incident Response and Data Breach Report

SPECIAL GUEST ARTICLE

Cybercrime and Data Privacy Regulation

By Justin Whelan, Partner HFW

It is likely that the post-Covid-19 new normal of ever-increasing remote working will see the global digital landscape continue to rapidly evolve. Prior to the pandemic, technology such as cloud adoption, IoT and AI were becoming more prevalent in everyday life. The reason for this is the exponential expansion of the reliance on data and how it is captured, processed, stored and transferred.

The reliance on digitalized data continues to shape and underpin all manner of worldwide business. From financial institutions' transactional facilities and the progression of the InsurTech ecosystem, to international power plant operational systems and marine navigational systems, and to localized building management systems and SME operations, the essence of data is and will be ever-increasingly pervasive.

There are daily reports of businesses suffering from security system breaches and the resulting theft, loss and falsification of data across all sectors. The Gulf Cooperation Council (GCC) states are no exception and as elsewhere around the world, the key legislative issues manifesting from the rising reliance on data are cybercrime and data privacy regulation.

Cybercrime

The GCC members have adequate cybercrime legislation in place with six nations having enacted specific anti-cyber/IT crime laws (Saudi Arabia in 2007, Oman in 2011, UAE in 2012, Bahrain and Qatar in 2014 and Kuwait in 2016). These laws are supplemented by each nation's own penal codes and by national e-transaction and commerce laws.

The GCC cybercrime legislative framework is further augmented by the 2010 Arab Treaty on Combatting IT crimes, which facilitates cooperation in transnational cybercrimes, and was ratified by Saudi Arabia, UAE and Qatar in 2012, Kuwait in 2013, Oman in 2015 and Bahrain in 2017.

These laws criminalize the theft, manipulation and misuse of data. By way of example, it is a punishable crime to enter or disable access to IT systems without permission in the UAE, as it is to circumvent IP addresses or to intentionally spam and run malicious software that causes an IT system to malfunction. The punishment for

this can result in a fine of up to AED 3M and/or five years of imprisonment.

However, cybercrime laws do not impose data protection requirements on the organizations that process data. That is the realm of data privacy regulations.

Data Privacy Regulation

Across the GCC there is not a region-wide data privacy regulation similar in scope to GDPR. Data privacy requirements are spread across a patchwork of different regional rules and regulations.

In Saudi Arabia, Kuwait and Oman there are no specific codified data privacy laws, with data protection generally controlled via the principles of Sharia's law. In Qatar, there are data privacy laws both offshore at the Qatar Financial Centre (2005) and onshore federally (2016). In Bahrain, 2019 saw the introduction of a Personal Data Protection Law superseding various previous data privacy rules across different legislation. This law applies to individuals and businesses in Bahrain as well as businesses outside the country that use third party data processing services within Bahrain. It imposes requirements to, for example, appoint a data manager and a data protection controller, and to also notify the Personal Data Protection Authority prior to the commencement of any automated data processing operations.

In the UAE, the offshore financial centres of the Abu Dhabi Global Market (AGDM) and the Dubai International Financial Centre (DIFC) have specific data privacy laws, updated in 2019 and 2020 respectively, which are largely based on European data protection principles. In Dubai, the Dubai Data Law (2015) imposes requirements on governmental entities. As with other GCC states, there are data privacy requirements within banking and telecommunications regulations. There is currently no onshore UAE federal cross-sector law and the regulatory environment is developing. The implementation of Federal Law No. 2 of 2019 on the Use of Information and Communications Technology (ICT) in the health sector heralded the first piece of federal onshore data protection legislation in the UAE. Regulating the health data processing of healthcare service providers, including insurers, brokers, claims management companies, key provisions around the collection, authorized access, transfer and storage of health data.

Also in 2019, the UAE's Telecommunications Regulatory Authority (TRA) announced a new policy to regulate devices and services connected to the IoT. The policy, aimed at imposing data protection requirements on technology providers, is part of the UAE's National Cybersecurity Strategy designed to introduce 50 initiatives over a period of three years and establish a secure cyber environment.

As the new normal evolves and GCC regulators look more to safeguarding data that is ever more transnational in nature, data privacy regulations in the region will continue to develop. In 2019, the TRA also announced that the UAE will introduce a federal cross-sector data protection law largely aligned to GDPR principles. Time will tell whether such regulations evolve into an overarching framework across the wider region of the GCC.

About Justin

Justin's practice area covers insurance and reinsurance claims, policy coverage advices and subrogated recoveries, largely within the property/energy/casualty and professional indemnity arenas. He has acted for a number of global insurers and facultative and treaty reinsurers, and advised a wide range of blue chip international insureds from a variety of industries. His work encompasses complex, multi-party disputes across an extensive span of subjects. Justin leads our dedicated Middle East cyber and data privacy team. He is experienced in cyber-related claims and data privacy advices and has spoken widely on cyber security, cyber insurance and data protection to numerous risk carriers, policyholders and industry experts across the Middle East, UK and Europe. Justin is well versed in commercial litigation in the Courts of the UAE and England & Wales. He has conducted numerous mediations and is experienced in other forms of Alternative Dispute Resolution.

IT Manager's View on COVID-19

By Neil Inskip, VP & IT Manager, TransRe London

During this pandemic there have been many heroes, the main ones being healthcare professionals and essential workers. It is safe to say that many IT departments have also come out of this situation quite well. Technology is a business enabler that has allowed, according to Gartner, 88% of companies to have their employees work remote. I'm not considered a hero, for me IT work has always been a "buttered cat paradox". The paradox arises when you consider the following, a cat always lands on four paws and buttered bread always lands buttered side down. What happens if you strap a piece of buttered toast to a cat and drop it? If I can keep the 'IT ball' in the air which includes keeping the bad guys away, strong user productivity and the improvement of technology, my mission is accomplished.

Social engineering attacks began at the start of the pandemic which was nothing new for IT staff. Any sort of global news creates a ripple of spam emails and SMS text messages. The thirst for news is what drives people to click on phishing links or attachments. In 2020, according to ProofPoint Inc., an alarmingly low 49% of US employees knew what the word phishing meant. Other international statics include the French coming in at the top when asked if they knew what smishing was (54% answered the question correctly). Spanish employees fared well and 80% knew what malware was and sadly 30% of US employees thought malware was a type of hardware to boost Wi-Fi signal.

At the start of the pandemic people saw firewall threats decline a bit and I think there are two reasons for this. The first reason is that users are not surfing the web in their workplace and creating "inside-out" issues, but also because it's easier for a bad actor to mail out millions of spam emails than it is to perform Advance Persistent Threats (APTs). On the dark web, there have been reports of "black-hats" discussing the ethics of hacking during a pandemic and some threat teams have been publicly calling out others. Security experts have also noted that this had marginal impact on the rate of hacking which generally is always on the incline. The teams who created the CLOP, DoppelPaymer, Maze, Nefilim and Netwalker Ransomware have all stated that they will avoid hospitals and medical facilities. As an example, DoppelPaymer was offering free decryption for facilities that were accidentally hit. The good guys have also stepped up to the plate with security companies offering free assistance to any essential services.

From another angle, the availability perspective or the "A" of the CIA triad (confidentially, integrity, availability – the venerable model for development of security polices). If working remote is part of your company's Business Continuity Plan then you are already in 'Disaster Recovery Mode', well done! The reinsurance industry is one that lends itself to electronification. We might have had to tussle with converting wet signatures to electronic ones, but apart from that life goes on. There are other industries that have not instigated their recovery plans and quickly returned to the new normal or should I say went back to Business as Usual (BAU). Other businesses it's really Business as Survival (BaS). In some instances, massive changes to a company's existing business model have occurred (diversification and cost cutting). Is there a trend to cut out/save money or forget about cyber defenses and data controls? Only time will tell, but whether you are doing BAU or BAS, a second crisis could simultaneously still occur. In any event, companies should be reviewing their activities, third party supply chains, risk registers and embedding a Business Continuity Plan into their organizations.

I hope I have provided some food for thought and I'll leave you conjuring images of floating cats (who doesn't like buttered cat? – Ed)…

TransRe™
cyber
We value risk.

New York

Underwriting

Alex Bustillo
T: 1 212 365 2376
E: abustillo@transre.com

Miguel Canals
T: 1 212 365 2266
E: mcanals@transre.com

Daniel Hojnowski
T: 1 212 365 2168
E: dhojnowski@transre.com

Actuarial

Joseph Marracello
T: 1 212 365 2159
E: jmarracello@transre.com

Claims

Peter Cridland
T: 1 212 365 2032
E: pcridland@transre.com

London

Underwriting

Rhett Hewitt
T: 44 (0)20 7204 8676
E: rhewitt@transre.com

Claims

Calum Kennedy
T: 44 (0)20 7204 8645
E: ckennedy@transre.com