TransRe
We value risk.

Global Cyber

Newsletter

2Q2018

TransRe
cyber
We value risk.

TransRe is a leading international reinsurance organization with a global reach and local decision making.

Our relationships are based on years of trust and experience. We have a flat organization structure that carries our A+ capital rated ability with our proven willingness to pay claims.

We proudly take a hands-on approach and write every product in every jurisdiction with a promise not to compete with our customers. The decision to partner with TransRe is an **EASIE** one.

TransRe
We value risk.

Welcome to our cyber newsletter.

We hope you enjoy the articles and updates that our editors have put together.

Silence is Not Always Golden…

While estimates of industry cyber premium vary, everyone agrees that the cyber market is growing at a fast pace – one of the few areas of growth in our industry. It's also generally agreed that cyber exposures are growing at a faster pace than cyber premiums. Like finding previously unknown fault-lines in California after an earthquake, we learn more about our cyber exposures with each new headline breach.

As an industry we need to address the economy's growing cyber insurance needs. Determining the best way to provide this coverage through the appropriate policies with few coverage gaps or overlaps at a sensible price is no small challenge. Additionally, if we are to ensure the long-term viability of our market, we also need to be prudent underwriters as cyber presents volatility from large, individual events as well as from events that occur systemically in our ever-connected world. Knowing where and how insurance companies may be exposed to cyber claims is step one of this process. Many insurance companies are currently working to affirmatively address cyber as a peril in all their P&C policies through specifically detailing coverage, or through excluding coverage. We believe this type of policy coverage transparency is critical. It provides insureds with a clear understanding of their coverage and therefore should ultimately assist in the claims adjudication process. It also provides (re)insurance companies with the ability to more accurately aggregate (and even model) their exposures with more confidence – instead of making conservative estimates on potential coverages across various lines of business. History has shown that there is a direct correlation between industry capital, capacity and coverage to its confidence in understanding and estimating its exposures.

The alternative is for the industry to remain silent within P&C policies on cyber coverage. To be sure, this is the current approach from some companies and we believe it serves no beneficial purpose to anyone within the insurance value chain. When silent, insured's lack coverage clarity and disputes with their insurance companies and brokers are sure to follow. Companies – insurance and reinsurance alike – could be running cyber aggregates significantly beyond their tolerance levels since there is really no policy transparency. Also, the "silent approach" also means going silent on price and underwriting; ie, there is no pricing for the exposure/coverage granted, and not a clear understanding of the risk involved.

Here at TransRe we constantly think about cyber's potential impact – both from a premium and loss perspective. We have created a framework to quantify this risk – not only from Cyber as a line of business, but also cyber as a peril. The events that have taken place, and those widely spoken about, have encouraged us to try to address cyber in our reinsurance contracts for all lines of business. By capturing the appropriate risk instead of making assumptions, we can focus our attention on providing a better cyber product for our insurance company clients. To aid in this process we now require CUO / Global Head of Cyber signoff on all reinsurance contracts that are silent. Underwriters across all lines of business and geographies are educated in cyber as a peril and try to gain clarity in contracts. This involves working with the cyber department, broker and client to understand how companies are handling this risk. As we continue to refine this process, we look forward to continuing to share our knowledge and experience with you.

Elizabeth Geary
Global Head of Cyber

Table of Contents

New European Data Protection Regulation Takes The Stage

Six years in the making and two since it was passed by the European Parliament, the General Data Protection Regulation (GDPR) finally became law in the European Union (EU) in May. Very little has not been written about the regulation however we stress the importance of its significance by mentioning it in this edition of the newsletter.

The new regulation seeks to update and harmonize data protection across the EU and it automatically becomes law in all 28 member states. It repeals its predecessor, the Data Protection Directive 95/46/EC, introduced over 20 years ago where much has changed in the world of data in that time.

The extraterritorial reach of GDPR will be felt much wider than the member states. The regulation applies not only to those processors and controllers of personal data established in the EU but also to non-EU organizations operating outside the Union who offer goods/services or monitor behavior within the EU. Organizations operating outside the EU and targeting customers within the union, for example via websites, will fall squarely within the territorial scope of the new legislation.

GDPR gives control of personal data back to the individual with enhanced rights and remedies. Among those enhanced rights are the rights of access, to rectification and the right to be forgotten. Also, notification to the supervisory authority is required not later than 72 hours of having become aware of a personal data breach. Organizations must give careful consideration as to how they will satisfy such obligations.

There are limited circumstances where personal data may be lawfully processed namely, where it has been obtained with consent; or where necessary for performance of a contract; or for compliance with a legal obligation; or the protection of a vital interest, or where there is a public or otherwise legitimate interest. If the lawful basis no longer exists the data should be deleted.

One of many areas where the regulation provides the data subject greater protection to reflect modern day practices is the area of consent. Consent must not only be freely given, specific and informed as required by the old directive but it must be unambiguous and delivered in a clear affirmative act. As such, silence, inactivity or pre-ticked boxes will not be adequate under the new legislation. Consent will not be considered freely given if there is no genuine or free choice or ability to refuse or withdraw consent without detriment. This calls into question some traditional practices by which consent has been obtained.

Existing consent will only be sufficient if it complies with GDPR otherwise fresh consent will be required. The responsibility will be on data controllers and processors to demonstrate that appropriate consent has been obtained. Readers will have noticed a surge in requests from businesses of all sizes seeking consent to retain their data in a bid to ensure compliance with the new law. Some businesses have sought fresh consent while others have simply alerted customers to updated privacy rules.

The prospect of substantial fines (of up to 4% of total worldwide turnover or €20m) for failure to comply with the regulation has often grabbed the headlines but the time and cost in preparation for the regulation's onerous ongoing obligations will have been felt by many organizations already. The UK government Department for Work and Pensions is believed to have spent nearly £15m in preparations for GDPR incorporating system remediation; review of existing record storage arrangements and staff training. Other government departments have spent substantially less.

Of course, it is hoped that the new law will also provide opportunities. For insurers, it is anticipated that it will drive demand for cyber insurance particularly across the EU where it currently lags behind the US.

European law makers believe the objectives and principals of the prior legislation remain sound but the new regulation is designed to be a strong and more coherent data protection framework for modern day data challenges. Time will tell whether it achieves the desired harmonization of data protection across the EU. The regulation still provides some discretion to member states in certain areas and its application and enforcement will be monitored with interest over the coming months and years as will the preparedness of organizations to meet the challenges GDPR will bring.

Notable Cyber Breaches & Threats

Australian Health Clinic records exposed

An attack on a family planning clinic in New South Wales, Australia exposed the records of approximately 8,000 clients who had contacted the clinic via its website in the last two and half years. Names, contact details and dates of birth and reasons for contacting the clinic were exposed. More sensitive medical records remained secure.

German energy firm attacked

Reports in Germany suggest that Federal prosecutors have opened a preliminary investigation into a cyberattack on a subsidiary of a German energy company, EnBW last year. It is understood that hackers breached the networks of the firm but did not gain access to the systems it uses to control energy supplies. The unknown attacker breached the network by hacking the portal used by an external service provider gaining access for a few minutes. No damage was caused.

Mexican banks lose $15m to attack

The central bank of Mexico confirmed that over $15m were siphoned off in fraudulent transfers from 5 unnamed companies. The attack was detected in April.

Facebook data misuse scandal… 'sorry not enough'

The fallout from the Facebook / Cambridge Analytica saga has been enormous and it serves as a stark reminder of the potential impact of cases involving mass data misuse.

Personal data from around 270,000 Facebook users plus public data from their friends was harvested by Facebook during a 2014 quiz. It is alleged that the data was sold to Cambridge Analytica where it was used to psychologically profile people and deliver pro-Trump material during the presidential campaign. The practice of obtaining data in this way was not unusual at the time but Facebook's rules did not authorize the sharing of that information. Cambridge Analytica claims that it did not use the data, and deleted it when Facebook told it to.

Facebook faces a number of investigations across the globe. In the U.S., in the wake of Facebook-founder Mark Zuckerberg's somewhat controversial appearance before Congress, members of the House of Representatives released copies of 3,500 advertisements related to the 2016 U.S. Presidential election that had appeared on Facebook that have been linked to a Russian

hacker group with ties to the Russian government. Now, several public-interest groups have moved to force Facebook to take several significant actions to ease monopoly concerns and protect private data. The company has also taken out full page adverts in British newspapers to apologize for what it describes as a 'breach of trust'. Cambridge Analytica and its parent company SCL Elections is to cease trading and applied to commence insolvency proceedings as a direct result of the publicity surrounding the matter.

The EU advisory body, the Article 29 Working Party now the European Data Protection Board has welcomed investigations by national privacy authorities and established a Social Media Working Group in light of the investigations.

The Indian government has issued notices to Facebook and Cambridge Analytica with a May deadline to respond to questions relating to the data of its citizens.

Under Armour / MyFitnessPal Suffers Massive Breach

Personal information, including usernames, emails and passwords of roughly 150 million users were potentially stolen in a breach that occurred in late February and was discovered in late March. While the size of the breach places it among the larger data losses, the type of data lost is typical of other breaches – and there has been no indication that actual fitness / health data was breached. However, in an unusual twist, Under Armour has actually been praised for its response: a BBC report quotes a security researcher as offering credit to the company for making the announcement within four days of discovering the breach. Elsewhere, the company was praised for security decisions made pre-breach that helped contain the damage, and for relatively quick detection of the breach.

Saks Fifth Ave and Lord & Taylor Breached: Payment Information Stolen

Also released in early April, Saks and Lord & Taylor, both subsidiaries of Hudson's Bay Co., suffered a hack that appears to have encompassed payment card information for millions of customers. The hackers have claimed to have five million credit and debit card numbers and have released them for sale on the dark web. In this case, the breach appears to have begun in May 2017.

Orangeworm Targets Healthcare Sector

Symantec identified a targeted attack campaign in April that appears to focus on healthcare and related industries, including healthcare providers, pharma companies, and IT providers for healthcare entities and healthcare equipment manufacturers. 40% of the confirmed victim organizations are related to the healthcare industry (the largest group by a significant margin) within the U.S. (again, the largest region by a significant margin), commonly targeting machines with software that is used by and controls imaging devices like x-ray and MRI machines. The purpose of the attack remains unclear.

TeenSafe Service for Parents Hacked

TeenSafe allows parents to monitor their children's online / phone activity, including tracking of location – but the account information for roughly ten thousand users has leaked online after the company failed to secure their servers.

Dixons Carphone

Dixons Carphone has confirmed details of a breach compromising 5.9 million payment cards. Approximately 100,000 of these were non-EU issued payment cards which did not have chip and pin protection. In addition, 1.2 million records containing 'non-financial' data including names, postal addresses and e-mail addresses were found to have been accessed. The company said that there was no evidence that the information had left its systems or that the breach had resulted in any fraud. The ICO, the Financial Conduct Authority and the police had been informed.

Ticketmaster breach

Ticketmaster, the ticket sales and distribution company, confirmed the identification of a malicious software which exported customer data to an unknown third party through a customer support product hosted by Inbenta Technologies. UK customers who purchased or attempted to purchase tickets between February and June 23,2018 and international customers between September 2017 and June 23,2018 may have been affected. This is said to be less than 5% of its global customer base. The company believes that only certain UK customers were compromised but that international customers were being notified as a precaution. Customers in North America were not affected. Names, postal addresses, e-mail addresses telephone numbers, payment details and login details are said to have been compromised. The Inbenta product has been disabled across all of the company's websites.

Regulatory & Legislative Update

ICO “prefers the carrot to the stick”

Elizabeth Denham, the UK Information Commissioner confirmed in a speech to the Data Protection Practitioners’ Conference in April that she has no intention of changing the ICO’s proportionate and pragmatic approach after the implementation of GDPR and that hefty fines will be reserved for organizations that persistently, deliberately or negligently flout the law. Under GDPR there will be a two tiered sanctions regime with fines up to €20m or 4% of global annual turnover, whichever is the greater. The commissioner cited a new set of tools under GDPR to motivate organizations into compliance such as codes of practice, privacy seals and data protection impact assessments.

The commissioner has promised a wider investigation into data analytics. The ICO has also issued notice of intent to fine Facebook the maximum levy of £500,000 under the prior legislation, the Data Protection Act 1988 for its role in the harvesting of personal data referred to earlier in this newsletter

Notable fines of £325,000 and £250,000 were issued to the Crown Prosecution Service (CPS) and Yahoo UK Services respectively. The CPS lost 15 unencrypted DVDs containing evidence from victims of child sexual abuse in a transfer between offices. The DVDs were sent by tracked DX delivery in a box and left in an unsecured area accessible by anyone early in the morning before working hours. It was a number of days before the loss was discovered. The ICO considered the content of the DVDs to be the ‘very uppermost in sensitivity terms’. It took into account the number of affected individuals and nature of the data lost in determining the level of penalty. Yahoo’s penalty resulted from a data breach at the end of 2014 where the personal data of 500 million user accounts was compromised. Over 8 million users were affected in the UK. Data included names, e-mail addresses, telephone numbers, dates of birth, hashed passwords and some security questions and answers. Attackers were able to access Yahoo’s systems by exploiting compromised credentials.

Philippines regulator orders closure of online sales

The National Privacy Commission of the Philippines (NPC) has ordered fast food giant, Jollibee to suspend online delivery operations following the discovery of vulnerabilities with the very high risk that approximately 18 million people on the website may be exposed to harm.

Hong Kong's Data Privacy Commissioner Publishes GDPR Guidance

There is no shortage of guidance on the implications of the upcoming GDPR rules on various regions, however the Hong Kong Data Privacy Commissioner offers a step-by-step comparison for companies already operating under Hong Kong's Personal Data Privacy Ordinance. Like many regions, the GDPR's extra-territorial scope will bring its more-stringent rules to territories around the globe.

Trump Executive Order on Cyber Security

President Trump's May 2017 executive order called for a report back to him within a year – and that document has now been released. Any action by the administration remains to be seen.

EU Network and Information Systems Directive

While GDPR has taken the lion's share of the headlines, the Network and Information Systems Directive (NIS) was required to be implemented into the national laws of EU member states by 9th May. The directive is intended to raise overall security and resilience of networks and information systems across the EU. Its focus is network security and interruption to service with notification of incidents without undue delay. The directive applies to Operators of Essential Services (OES) and Digital Service Providers (DSPs) targeting businesses of more than 50 people with annual turnover less than €10m. Organizations in the energy, transport, health, water, financial services (including banks) and digitals infrastructure sectors fall within the definition of OES, while search engines, cloud computing and online marketplaces would be classified as DSPs. Member states will set their own rules on financial penalties for failure to comply. In the UK organizations may be fined up to £17m.

California Following GDPR in Upcoming Ballot Initiative

California is the most populous state in the U.S., and frequently on the forefront of legal changes – this November, California voters will decide whether to adopt what would be one of the broadest and far-reaching privacy regulations in the nation. The California Consumer Privacy Act of 2018 would provide protections for any California internet user and impose financial penalties for any violation. Because of California's population and influence, any such regulation in that state is likely to impact corporate standards nationally.

In a deal to avoid the above ballot initiative from going forward, the California legislature passed a bill which was signed into law by the Governor to address

digital privacy. The law is not as sweeping as the GDPR, nor as detailed as the ballot initiative called for, but it is viewed as a compromise – the ballot initiative received widespread popular support and enormous financial backing from real estate developer Alastair Mactaggart, but was fiercely opposed by the CA-based tech industry, including Google and Facebook.

- The new law gives Californians the right to inquire what personal data businesses hold, gives them the right to sue of privacy breaches, and to have their personal information deleted or opt out of having their data sold.
- This law could be seen as a model for future state laws across the country.

Image Credits: Roy Scott

Vermont Passes Law to Regulate Data Brokers

Occasionally lost in the conversation amongst data-retention, data-scraping, data-breaches and the like are the presence behind the scenes of data brokers: companies that work behind the scenes to collect information from multiple sources and sell the resulting aggregated mass of data. The new Vermont law requires data brokers to register, and the idea is to make it easier for citizens to find out what data of theirs is being held and take further action as needed.

MD Anderson Appeals $4.3M fine from HHS OCR for Multiple HIPAA Violations

After suffering three data breaches dating back to 2012 and 2013, the $4.3M penalty was issued for “willful neglect” and continued failure to encrypt their systems. MD Anderson appealed, but an Administrative Law Judge (ALJ) has ruled in favor of the OCR. MD Anderson has stated they will appeal this decision in what is one of the first challenges to the discretion and power of the OCR to levy fines for HIPAA violations.

Global Cyber Security

Kenya's new cybercrimes law

The president of Kenya has signed into law new cyber legislation. The Cybercrimes bill criminalizes abuse of persons on social media. In doing so, he rejected criticism of the new law that it was unconstitutional and violates the right to media freedom and expression. Chief among the criticism was that offences under the legislation are too broadly defined with harsh sentences that could inhibit online freedom of expression.

Kaspersky shifts data center to Switzerland

In a bid to appease the data security concerns of Western governments, Russian based Kaspersky Labs is to open data storage and processing facilities in Zurich. The site will house data from customers in the US, Europe, Japan, Korea, Singapore and Australia. Readers will recall that the US and UK governments had warned over the use of the firm's antivirus software by government departments due to spying fears.

Hotel door lock vulnerability exposed

Millions of electronic door locks across the globe fitted to hotel rooms have been found to be vulnerable to attack due to a flaw in the software. The flaw enabled the creation of master keys to open doors without leaving an activity log.

It is not the first time that hotel doors have created cyber news. In 2017 an Austrian alpine hotel was the subject of a ransomware attack on the electronic key system when hundreds of guests were locked out of rooms following the hack.

Email no longer secure

To the extent email was ever secure, two common email encryptions – PFP and S/MIME – have critical vulnerabilities that allow emails sent encrypted to be displayed in plaintext. The Electronic Frontier Foundation first published about the vulnerability after German researches discovered it and predictably dubbed the vulnerability "EFAIL".

EUROCONTROL Air Traffic Center Suffers Outage

On April 3, 2018, a systems failure at the EUROCONTROL Centre in Brussels grounded thousands of flights, potentially affecting 500,000 passengers. The outage appears to have been the result of an internal software issue rather than any malicious act.

Cryptocurrency Corner:

- Amazon patents technology to be used in a subscription feed for governments and law enforcement that combines bits of data from various sources to identify bitcoin users, their transactions, and their locations. In short, the technology would reverse-engineer the identity of the bitcoin user by piecing together all the bits of the transaction, thus piercing the veil of the until-now untraceable currency.
- Before his resignation in May, New York Attorney General announced an inquiry into 13 cryptocurrency exchanges – the inquiry was to investigate whether these exchanges are improperly skirting the rules that apply to traditional exchanges. The status of the inquiry is up in the air after Schneiderman resigned following accusations of physical abuse.
- The alleged mastermind of the theft of 600 cryptocurrency mining computers worth an estimated $2M escaped prison and Iceland and appears to have successfully fled the island country for the European mainland.
- South Korean cryptocurrency exchange was hacked, leading to a sell off that reduced the cryptocurrency market value by $42B.

U.S. Mobile Phone Providers Share, Fail to Secure Real Time Tracking Data

In what has been described as the biggest breach no one is talking about, a company called LocationSmart has been working with AT&T, Verizon, Sprint, and T-Mobile, to collect real-time location data on all users of those networks. Not only is the data very personal, it is also not secure: one researcher was able to sign up for a “Free Trial” with Location Smart and instantly pinpoint any cell phone in the U.S. Even further, a company called Securus Technologies sells the ability to track individuals using that data – often to law enforcement – and they have been hacked.

FBI Issues Warning for Home and Office Router Vulnerability

In late May, the FBI announced that unnamed foreign cyber actors were targeting home and office routers (and other networked devices), and had already compromised “hundreds of thousands” of them. The malware used is called VPNFilter, which can not only render the devices inoperable by their owners, but potentially collect data, exploit the devices for other purposes (for example, a DDoS attack), and block network traffic. The fix is relatively simple: reboot the devices, upgrade their firmware, and use strong (not default!) passwords.

Strava Fitness App Used to Catch Suspect

A bicyclist in Virginia allegedly assaulted another bicyclist on a trail, and then took off. Police used the Strava fitness tracking app, which includes a public-facing location section for connecting with others in your area, to populate a pool of suspects who were in the area. From that, the suspect was identified and arrested.

DDoS For-Hire Site Shuttered by Interpol

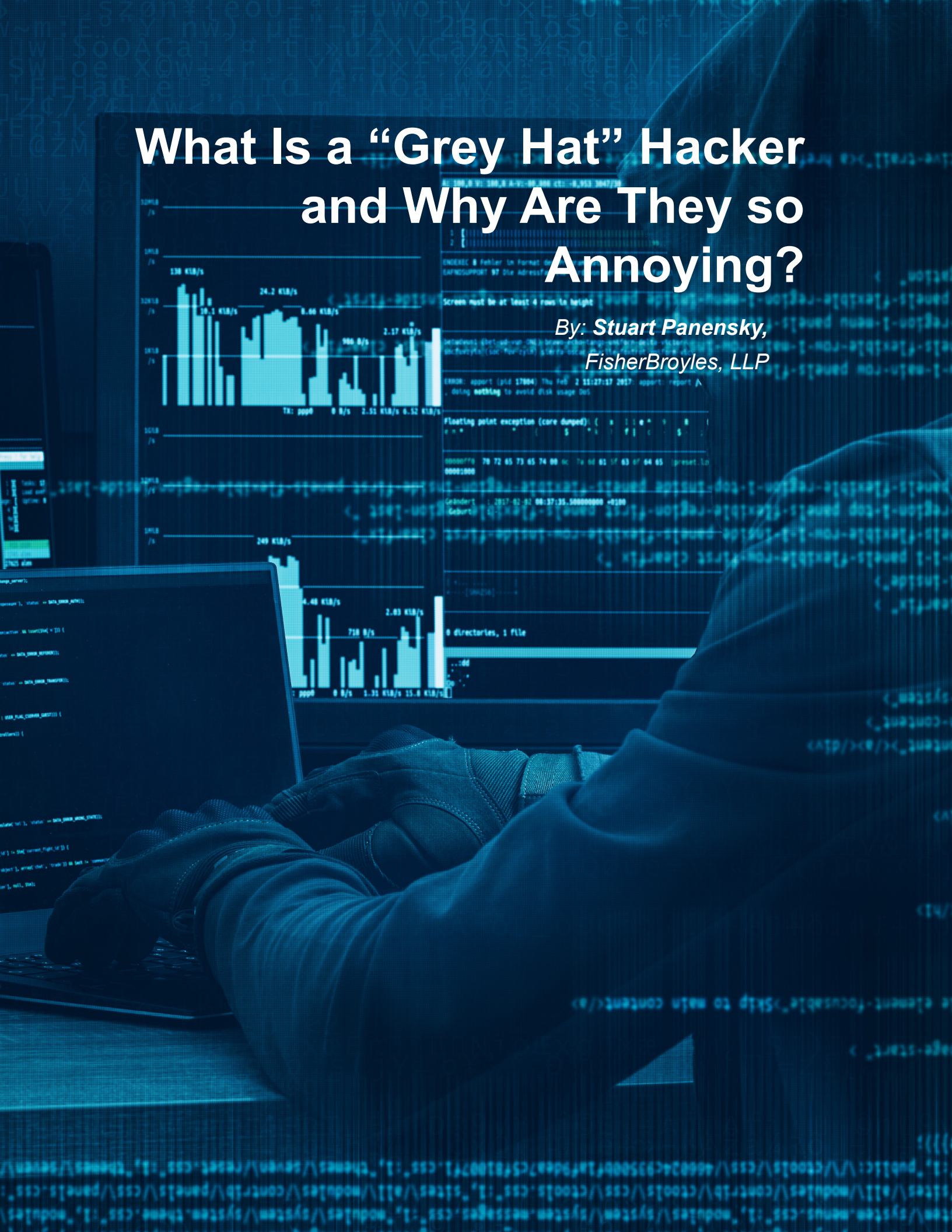
In late April, Interpol announced they had arrested the administrators of Webstresser.org and shut down the site. The site allowed anyone to pay to have a DDOS attack launched against the website of their choice. Law enforcement claims that the site had 136k registered users and was responsible for 4 million attacks. While the website charged as little as $15 euros per month, an average DDoS attack can cost the affected business $200 - $1,000 per day.

Equifax Financials Reveal Insurability of Cyber Losses

The ongoing Equifax breach has already been one of the farthest-reaching and expensive cyber breaches in history. New numbers indicate that it has cost the company $243M to date, but they carried $125M in cyber coverage – a number that could significantly limit the impact to the bottom line. Since September 2017, Equifax has received $60M in insurance recoveries and received an additional $50M in payments for their costs.

Significant Flaws Found in Industrial Control Software

Security researchers have found that many Industrial Control Systems (ICS) have significant vulnerabilities – test attackers were able to penetrate network perimeters of 73% of industrial organizations, and in 82% of tested networks it was possible to leverage a small vulnerability to access the broader network. Elsewhere, other white-hat security researchers have discovered flaws specifically in Schneider software that is used for real-time operations management in oil and gas production and other industrial settings. Schneider has reportedly issued a patch, but it is unclear how quickly it can be applied or whether it can be applied without downtime, which can be complicated in production / utility settings. Such a cyber-security issue, in settings like these with significant physical damage potential, must be considered in the context of possible silent cyber liability on property policies.



What Is a "Grey Hat" Hacker and Why Are They so Annoying?

*By: **Stuart Panensky,***
FisherBroyles, LLP

The last healthcare data breach I handled arose when my client was contacted by a "blogger" purporting to be a journalist, (who our investigation determined was actually a licensed healthcare professional), who informed my client that she had a "source" that provided to her proof that my client caused the unauthorized breach of certain patient information. The blogger assured my client that the "sources" or rather "hacker's" motivations were entirely altruistic.

The patient information in question was a database of patient billing information that did not contain any clinical or diagnostic or substantive health information other than patient names, addresses and name of primary health insurer. The breach itself was an esoteric vulnerability that existed in my client's IT department's "sandbox" computer or a non-essential computer that IT used that was not part of the client's front-office practice. The client's front-office IT security happened to be comprehensive and robust. Nevertheless, here we all were, determining the most appropriate response to this breach and whether and how to confront the blogger/hacker. One thing was absolutely certain - this was going to cost the client a lot of money.

This was not my first assignment to counsel a company that was informed of a data breach from a non-law enforcement third party. I counseled a SaaS provider once who also was informed about some obscure security vulnerability by someone who the company did not know who proclaimed to be informing the client that he had hacked its systems for only the most virtuous of reasons, but then reported his purported findings against my client to the local news media and state attorney general. People have different definitions of virtue.

Who are these champions of privacy virtue? They are not exactly the most evil or nefarious of wrongdoers with hacking tendencies. So-called "black hat hackers" will knowingly break the law and impermissibly access someone else's network for ill-gotten profit or other monetary reasons. The blogger's source in my client's case does not exactly or directly profit from the use of the data he copied (other than raising awareness of how virtuous he is).

On the other hand, "white hat hackers" are usually certified and enter into contractual obligations with companies where they are expressly permitted to access a company's computer system for evaluation of security and then report its findings back to the company along with recommendations to cure any vulnerabilities discovered. Clearly, in my clients' examples above, the hacker did not have permission to access their computer networks.

Not black, not white … these "grey hat" hackers are difficult to define, categorize and handle. They believe they are doing society a greater good by knowingly breaking the law and impermissibly accessing someone else's computer network to discovery security vulnerabilities. They therefore are deliberate actors and act with intent when breaking the law. However, their sense of importance about what they are doing motivates their behavior far more than any sense of fear of punishment or simple respect of someone else's property.

Sometimes motivated by politics ("hacktivism"); sometimes motivated by a self-assigned sense of heroism, the grey hat hacker is not predictable and in my experience opportunistic in choosing their targets. Finally, as one of my client's lead cyber-security architect puts it, grey hats are "[s]ometimes just crazy people messing around".

In my recent case above, it was important to the client to understand the extent to which the grey hat hacker used, copied, transmitted or otherwise exploited the patient billing records. As counsel, I communicated with the blogger and arranged for the grey hat hacker to certify that he only downloaded the data a singular time, never transmitted it anywhere (other than to the blogger) and destroyed any and all existing copies. As you might predict, this affidavit from the grey hat hacker did not come without consideration from my client.

Risk professionals (IT, insurance, legal) are wise to be cognizant of the deliberate and intentional nature of the so-called grey hat hacker. These functions should perform their respective services fully aware that as their organizations and networks grow and evolve to be more integrated with cloud services and other internet-facing activity, there exists this class of people out there – these grey hats – that are searching, creeping, and exploring around, hoping to find vulnerabilities in your network that they can exploit… for the public good, of course.

Stuart A. Panensky *is a partner of "next-gen" law firm, FisherBroyles, LLP and leads the firm's Cyber-Risk; Data Security & Privacy practice group. Stu is an experienced business attorney and commercial litigator. Stu has a significant history of acting as "breach counsel" and counsels the professional services, technology, insurance, design, construction, environmental, retail, hospitality, financial institutions, healthcare, and other business sectors on privacy issues. Stu has experience counseling companies on Blockchain application and implementation issues and also has Insuretech experience.*

Founded in 2002, FisherBroyles, LLP is the world's largest distributed law firm partnership with over 230 attorneys in over 21 offices nationwide. The FisherBroyles' efficient and cost-effective Law Firm 2.0® model leverages talent and technology instead of unnecessary overhead that does not add value to our clients, all without sacrificing BigLaw quality. Visit our website at www.fisherbroyles.com to learn more about our firm's unique approach to the practice of law.

TransRe Speaks

Peter Cridland

will be speaking:

- **Friday, October 12th**

  CLM Cyber Summit - New York, New York

Litigation News

Right to be forgotten under scrutiny in Europe

The English High Court distinguished between the circumstances of two claimants that sought to have their respective rights to be forgotten upheld against Google. Anonymity of the claimants was preserved by the court. The first claimant (NT1) was involved in a property business involving members of the public and was convicted of criminal conspiracy. The second claimant (NT2) was involved in a controversial business that was the subject of public opposition over its environmental practices and pleaded guilty to two counts of conspiracy. Both claimants were imprisoned and sought to have links excluded from Google search results relating to their prior misdemeanors. The claimants requested removal under the Data Protection Act 1998 (DPA) on the basis that the links were inaccurate and/or likely to cause damage and distress in addition to the common law tort of misuse of private information.

In upholding NT2's request, the judge concluded that the crime and punishment information had become out of date, irrelevant and there was no sufficient legitimate interest to users of Google. He had acknowledged his guilt and expressed remorse with no evidence of a risk of repetition. Conversely, NT1 had continued a limited role in public life having been convicted of a business crime and had shown no remorse. The court considered that that it was justified and proportionate that the public should be able to view that information.

The principal was established by the European Court of Justice (CJEU) in 2014 (Google Spain v Costeja Gonzalez) that an internet search engine operator is responsible for the processing of personal data which appears on web pages published by third parties under the current EU Data Protection Directive (95/46/EC). In that case, a Spanish man was entitled to have search results about past bankruptcy proceedings deleted.

Earlier this year, the Conseil d'Etat in France declined to rule on the appeals of four individual who had they their cases rejected by the French data protection regulator (CNIL) relating to complaints seeking that Google remove links to third party sites containing sensitive data including criminal convictions. Instead, the French court has referred a series of questions to the CJEU seeking clarification of the specific responsibilities, powers and capabilities of search engine providers.

Facebook appeals to Irish Supreme Court in view of impending GDPR

Facebook is seeking an appeal to the Irish Supreme Court relating to its use of Standard Contractual Clauses (Model Clauses) to transfer data to the United States (US) for processing. The case followed a complaint to the Data Protection Commissioner (DPC) of Ireland by data protection activist Max Schrems who claimed that the data transferred to the US was not afforded the equivalent high level of protection offered under European Union (EU) law. Concerns were founded on the mass indiscriminate processing of US surveillance programs and an effective remedy for European citizens. Rather than apply its own discretionary powers to suspend or ban the transfer of data to a third country, the DPC sought a reference through the Irish High Court to the European Court of Justice (CJEU). The Irish High Court duly obliged finding that the concerns were well founded. In a move to avoid the wide ranging consequences of an adverse determination by the CJEU, Facebook has appealed to the Irish Supreme Court arguing, among other points, that impending GDPR will render the case moot or irrelevant.

Cyber Studies & Reports

- UK Government Cyber Security Breaches Report
- Verizon Data Breach Investigations Report
- Aon U.S. Cyber Update

Contacts

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.

Editors

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

Peter Cridland
Assistant Vice President
1.212.365.2032
pcridland@transre.com

Phylip Jones
Global Marketing Manager
1.212.365.2281
pjones@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

Miguel Canals
Cyber Risk Underwriter
1.212.365.2266
mcanals@transre.com

Elizabeth Geary
Global Head of Cyber Risk
1.212.365.2243
egeary@transre.com

Alex Bustillo
Cyber Risk Underwriter
1.212.365.2376
abustillo@transre.com