

Global Cyber

Newsletter

4Q2018





Experience

Accessibility

Strength

Innovation

Expertise

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.



Welcome to our cyber newsletter.

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

“The price of light is less than the cost of darkness”

Arthur C. Nielsen

As a reinsurer, we consistently request data from our clients as part of our underwriting process, and throughout the year. Policy listings (including company name, domicile, limit, attachment, pricing, etc.) show us the types of risks our customers support, as well as coverage, limit management and attachment strategies. Being a data-focused company not only better informs our underwriting decisions and pricing strategies, but also puts us at the forefront of being able to provide valuable feedback to our customers: our observations of their portfolio and our view of the market. TransRe has invested heavily in technology to automate much of the data processing required in this feedback loop. This has allowed our underwriters to more efficiently and completely analyze the data as part of a comprehensive underwriting evaluation.

We use one of our proprietary tools, Entity Data Analytics (mentioned in our analysis of the US Public Directors & Officers Market, Oct 2018) to aggregate data by name and evaluate exposures and realistic disaster scenarios across our portfolio, looking at limits exposed by insured, industry, coverage, geography, etc. Better data reduces the (conservative) assumptions we have to make, which in turn, leads to a more efficient use of capital, better pricing decisions and a greater amount of cyber capacity that we can deploy to support our clients.

Unfortunately cyber diversification is not as straightforward as a line of business like Property. With Property, we use detailed modeling files to help us diversify based on geography – a Florida hurricane, California earthquake (and fire) and Asian Tsunami have no correlation, for example. With Cyber, no one risk characteristic (industry, size of business, geography) can be solely relied upon as a differentiator. Instead, we must analyze multiple risk characteristics, and then look closely at aggregates and realistic disaster scenarios to “pml” the risk.

From our experience, the most important part of the data equation is to capture it correctly from the start; the analysis and models can only be as good as their inputs, and underwriting can only be effective when based on accurate information.

If there has been some hesitation to provide the data we ask for, it is likely because insurers are not always able to compile this data quickly and accurately. Whether due to legacy operating systems (too few fields of data capture) or multiple systems (M&A / geography), cyber writers often scramble to collect and share the data we need. This data issue often extends beyond the policy system, to the claims system where loss codes are unable to adequately capture and report cyber claims data at a detailed level.

Data will be a key cyber differentiator in 2019. The availability, integrity and completeness of cyber data will continue to improve as insurers invest in their operating systems, and partner with brokers and modeling companies. When we have good data, we can underwrite and manage risk effectively; enabling us to provide a better product, pricing and service, including market insights (see D&O report mentioned earlier).

Reinsurance is more than just capital. How we add value differentiates us from our competitors. We are on this cyber journey with you. The price of light is one we must pay to remain relevant to the cyber buyer. Nobody should want to be on this path in the dark.

Wishing you all the best in 2019,

Elizabeth Geary
Global Head of Cyber

Table of Contents

Notable Breaches PAGE 5

- Air Industry Woes Continue
- Amazon 'Technical Issue'
- Quora Suffers Massive Data Breach
- Additional Facebook Breaches Revealed

Global Cyber Security PAGE 7

- New York Times Report: Your Apps Are Tracking You
- Paris Accord on Cyber Security
- Merck: Not-Petya Shockwaves Still Reverberating

Crypto Corner PAGE 9

Litigation News PAGE 10

- UK High Court Dismisses Representative Action Against Google for Safari Workaround
- Kaspersky Loses Battle with U.S. Government
- Cryptocurrency Theft Covered by Homeowners Policy? Ohio Says "Yes"
- Morrisons Loses Effort to Dodge Liability for Leak
- National Union Loses Effort to Dodge Class Action Attorneys' Fees

Regulatory & Legislative Update PAGE 13

- Regulators in Europe Issue First GDPR Fines
- SEC Cyber Unit Issues Report: Can Lack of Internal Controls Violate Securities Rules?
- 2018 ... A Year for the Big Fines by the ICO
- Historical ICO Fine Greater Than £200,000
- Italian Competition Regulator Fines Facebook
- EDPB Issues Draft Guidelines on the Territorial Reach of GDPR
- California Creates IoT Security Law
- Political Agreement for a New European Cyber Security Act
- Oath Agrees to \$4.95M Fine
- Australia Passes Anti-Encryption Law

TransRe Speaks PAGE 17

- JLT Re MPL Leadership Conference
- Sprecheranfrage Risk & Reinsurance Summit
- 8th Annual Cyber Liability Insurance ExecuSummit

Cyber Studies & Reports PAGE 18

- Beazley Breach Insights
- Chubb Cyber In Focus
- Primer on Cyber Security Law and Policy

Special Feature PAGE 19

- Marriott

Guest Article PAGE 21

- Do I Really Have To Restart, Again?
- Facing Biometric Information Claims

Notable Cyber Breaches & Threats

Air industry woes continue

Hot on the heels of major breaches at British Airways & Canadian Airlines, Hong Kong based airline [Cathay Pacific](#) has suffered a data breach exposing approximately 9.4 million people. Data accessed included passport/government ID numbers and credit card details. Suspicious activity was first noticed on the company's website in March 2018 and confirmed by the company in May. Cathay Pacific said that it was working with [27 regulators in 15 jurisdictions](#) in relation to the breach.

British Airways has also revised its estimate to 429,000 people affected by the breach it suffered in August/September this year. A reduction in the original estimate of 380,000 cards compromised was offset by having to notify a further 77,000 holders of payment cards with security codes and an additional 108,000 without security codes.

Away from the airlines, [Heathrow Airport](#) was fined £120,000 by the UK's Information Commissioner following the discovery by a member of the public of a USB memory stick in October 2017 containing sensitive personal data. The device contained unencrypted files without password protection.

A nearly identical issue has been revealed in the U.S.: Customs and Border Protection [agents searched the electronic devices of more than 29,000 travellers last year](#). Some of those searches were "advanced" searches in which agents download electronic data from a device onto a USB memory stick for further investigation. The Department of Homeland Security, Office of the Inspector General found that CBP agents were routinely failing to delete this data once the investigation is complete, as they are required to do by regulation.

Amazon 'technical issue'

[Amazon](#) have said that a 'technical issue' resulted in customer names and e-mail addresses being disclosed on its website days before black Friday. The company confirmed that it has fixed that issues and contacted affected customers.

Quora suffers massive data breach

100 million users of the Q&A website, [Quora](#) have had their data compromised when its systems were exposed by a malicious third party. The website is popular for sharing questions and answers online. Compromised data included names, e-mail addresses and encrypted passwords entered online. Imported data from linked networks (authorised by users) with both public and non-public content was exposed.

Additional Facebook Breaches Revealed

Facebook [admitted in December](#) that their system exposed private photos of up to 6.8 million users to applications that weren't authorized to see them. It appears that the breach occurred from 9/12/2018 – 9/25/2018 and was discovered on September 25th. It is unclear why the breach was not revealed for nearly two months. The [Irish Data Protection Commission](#) has announced an inquiry into possible violations of the GDPR related to this breach. GDPR penalties of up to 4% of annual worldwide revenue are allowed, which in Facebook's case would [mean up to \\$1.6B](#).

September 25th was also the date that a Facebook admitted that between [29 million and 50 million accounts were breached](#) by hackers between 9/14/2018 and the 25th.

Facebook stock [dropped 7.25%](#) on 12/19/2018 as the scale of these breaches clarified, bringing total stock losses YTD to about 24%.



Global Cyber Security

New York Times report: Your Apps Are Tracking You

An [investigation](#) into the extent to which myriad apps track users revealed some frightening truths: countless apps – many of them free to download – track users movements to within mere yards, and do so thousands of times a day, then sell that data. While the data is “anonymized,” as detailed in the article, in many cases the identity of the users can be rebuilt fairly easily. This is big business: the sale of this type of data reached \$21 billion in 2018. These findings are another reminder that the true business purpose of most apps is to gather data – the content they provide is merely a means to that end.

Paris accord on cyber security

An [international agreement](#) on cyber security unveiled by French President Emmanuel Macron has hundreds of signatories including many nations and major US tech firms. The ‘Paris Call for Trust and Security in Cyberspace’ is a declaration on developing common principals for securing cyber space including the prevention and resilience to malicious activity online; protecting accessibility and integrity of the internet and co-operation on the protection of electoral processes. [50 nations, 90 non-profit organizations and universities](#) are said have signed up to the accord. The likes of Microsoft, Facebook, Google and IBM are also signatories although, the United States Government is not.

Merck: Not-Petya shockwaves still reverberating

As has been previously discussed, Merck suffered a huge loss resulting from the Not-Petya attack in June 2017, possibly topping \$2B in insured losses. While the cyber tower (reported at \$275M) has paid out without issue, Merck warned investors of potential coverage disputes for the remaining coverage in their [latest 10-Q](#) report (page 35). The company has already reportedly [replaced their insurance broker](#) in the fallout from Not-Petya.

Crypto Currency Corner

- ▼ At the end of last quarter, Bitcoin was trading in the mid-\$6,000 USD range, but the most famous cryptocurrency has plunged since mid-November, now trading around \$3,500. [Ethereum](#), [Ripple](#), and [Litecoin](#) are all significantly down over the last year, and in the last month.
- ▼ Despite the volatility of Bitcoin, it has found favour in countries whose own currency is similarly unstable: the rate of [Bitcoin ownership in Turkey](#) (18%) doubles the rate ownership rate in Europe (9%) and the U.S. (8%), largely due to the instability of the Turkish Lira over the last year.
- ▼ Economics experts [continue to debate](#) the long-term viability and value of cryptocurrencies.

Litigation News

UK High Court dismisses representative action against Google for Safari Workaround

The [case](#) arose out of Google's use of cookies to exploit exceptions to default settings in Apple's Safari browser ('Safari Workaround'). Actions on this issue are not new to Google. A regulatory action was commenced in the US in 2012 where the company agreed to pay a civil penalty of \$22.5m. In 2013 Google agreed to pay \$17m to a US state consumer action group representing 37 US states and the District of Columbia.

In the present case it was alleged that Google tracked and collated information regarding the internet usage of many millions of Safari users without the user's knowledge and consent contrary to the Data Protection Act 1998 (DPA). The sole claimant Richard Lloyd brought a representative action for all individuals who, between 9 August 2011 & 15 February 2012, were present in the England and Wales and satisfied certain criteria relating to the usage of Apple devices and software during that period. The potential Class being represented was estimated to be as high as 4.4m individuals with per capita figures for damages between £1bn & £3bn. No financial loss or distress was alleged but compensation claimed was for an equal, standard, "tariff" award for each member of the Class recognising the use to which the data was wrongfully put by Google.

The court concluded that the representative claimant and those he purported to represent had not suffered 'damage' as a result of a breach within the meaning of the DPA. In addition, the court was not satisfied that the breach of duty or its impact was uniform across the entire Class. For a representative action to continue the Civil Procedure Rules (CPR) require 'one or more persons have the same interest'.

The judge described the case as officious litigation embarked upon on behalf of individuals who have not authorised it, and that had shown no interest in seeking any remedy for the alleged breaches. The judge also observed that the main beneficiary of an award would be the litigation funders and the lawyers.

Kaspersky loses battle with US Government

Antivirus software firm, [Kaspersky](#) has failed in its attempt to overturn a ban imposed by the Department of Homeland Security on all government departments and agencies using the company's software. The Washington DC Court of Appeals court upheld an earlier decision of a district court which cited Congress's right to block the purchase of software provided by a specific vendor providing there is a genuine security risk associated with it. Kaspersky argued that such action was unconstitutional.

Similar espionage fears have surfaced recently over Chinese telecom equipment manufacturer, Huawei. The US, [Australia](#), [New Zealand and the UK](#) have taken steps to block or review the company's involvement in the development of critical infrastructure such as 5G networks.

Cryptocurrency theft covered by homeowners policy?

Ohio says "yes"

Insured James Kimmelman had \$16,000 USD stolen from his bitcoin wallet, and submitted a claim to his homeowners carrier. [His claim was approved](#), but limited to \$200 after the carrier determined that Bitcoin was "money" and therefore subject to the relevant sublimit. Kimmelman brought suit under breach of contract and bad faith in Ohio state court. Although the suit has not yet been concluded, it survived the insurer's motion for judgment on the pleadings – the court relied on the Internal Revenue Service Notice 2014-21 stating that "for federal tax purposes, virtual currency is treated as

property.” Therefore the court found that the suit could not be dismissed – at least not at this early stage – as it remains possible for Mr. Kimmelman to prove his case.

Morrisons Loses Effort to Dodge Liability for Leak

Stemming from a 2014 incident wherein a Morrisons employee stole data on nearly 100,000 staff, Morrisons has continually challenged that it is liable for the criminal misuse of its data. The High Court found against Morrisons in December 2017, and the [Court of Appeal confirmed that decision in October 2018](#). Morrisons has asserted its intention to appeal to the Supreme Court. Of particular note, the Court of Appeal stated that the solution to the “potentially ruinous” financial burden on corporations bearing liability for these breaches is insurance. [See, Court of Appeal decision](#) at paragraph 78.

National Union Loses Effort to Dodge Class

Action Attorneys’ Fees

In continuing litigation relating back to Yahoo’s practice of scanning user emails for advertising purposes, the U.S. District Court found that insurer National Union breached the duty to defend in initially denying the claim; however, the breach did not alter the terms of the policy, thus the court still enforced a deductible coverage endorsement deeming Yahoo responsible for their own defense costs. The Court ruled against National Union finding that the \$4M in attorney fees for the plaintiff’s class action suit Yahoo paid as part of the settlement were “loss” under the policy. The court also pointed out that the issue is largely moot in the instant case due to the fronting policy involved (\$1M limit subject to a \$1M deductible), and that the ruling was likely sought as an indicator for future litigation.

Regulatory & Legislative Update

Regulators in Europe issue first GDPR fines

Despite GDPR not yet being implemented in to Portuguese law, the [Portuguese data protection agency \(CNPD\)](#) applied GDPR principals in fining a hospital €400,000 earlier this year for failures relating to procedures in place to protect patient medical records. Doctors had unrestricted access to patient files regardless of their particular medical discipline. The system lacked appropriate technical and organisational measure to protect data as required under GDPR.

The data protection authority in [Baden-Württemberg \(LfDI\)](#) issued the first German fine under GDPR. A company was fined €20,000 following an attack that exposed the passwords and e-mail addresses of 330,000 users which were held in plain text and unencrypted. The modest penalty reflected the company's co-operation, prompt notification and comprehensive measure to improve its IT security architecture.

[Austrian regulator, DSB](#) fined an individual €4,800 for installing CCTV in front of his premises which recorded a large section of a public sidewalk. The equipment was not sufficiently marked as conducting surveillance.

SEC Cyber Unit issues report: can lack of internal controls violate securities rules?

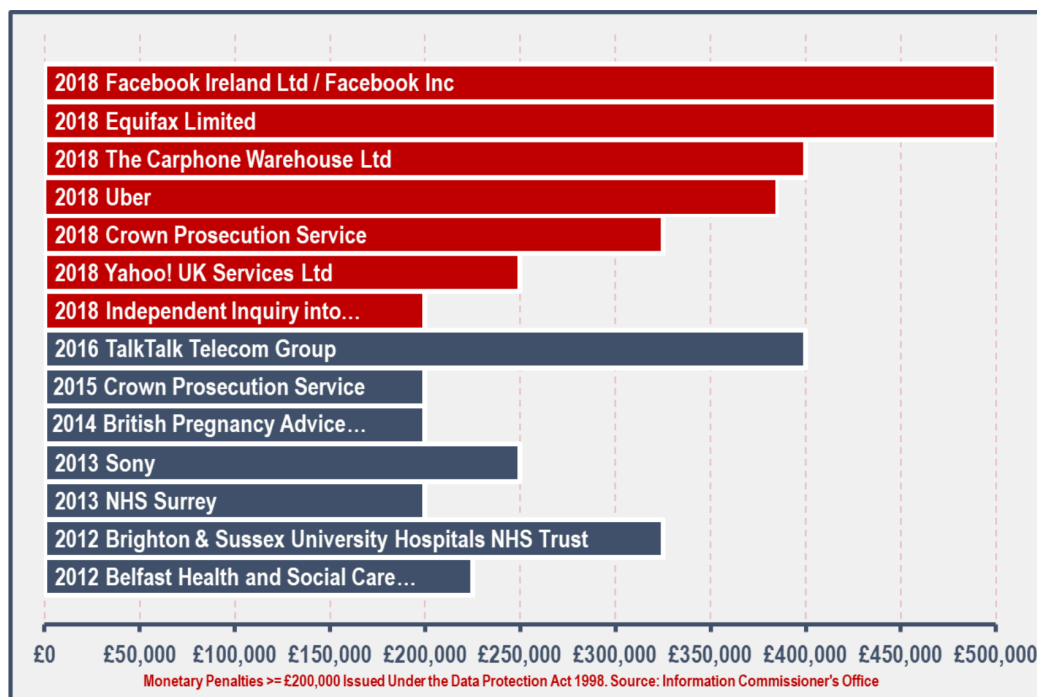
In October, the [SEC issued a report](#) on their investigation of 9 public companies who suffered "business email compromise" attacks – commonly referred to as spearphishing, or lumped under the umbrella of social engineering attacks. The report questions whether lack of appropriate internal controls, leading to a BEC, could be a violation of federal securities law. Also of note in the report: FBI statistics show \$5 billion in losses due to BEC since 2013, with \$675M in 2017.

2018 ... a year for the big fines by the ICO

In November [Uber](#), the global transport network company, was fined £385,000 by the UK's Information Commissioner's Office (ICO) for a cyberattack which took place in 2016. Records of 32 million non-US users, of which 2.7 million were based in the UK and 3.7 million non-US drivers, of which 82,000 were based in the UK, were accessed by the attackers. Uber in the US served as a processor for the UK affiliates and used the cloud based storage service of Amazon Web Service's Simple Storage Service ("S3"). The attackers claimed to have obtained the password credentials of 12 Uber employees based in the US in an earlier breach.

The Uber penalty is one of a number hefty fines issued this year in context of the ICO's powers under the now repealed Data Protection Act (DPA) including two maximum fines of £500,000 issued to [Equifax](#) and [Facebook](#). It is fair to say that many of the higher penalties issued in 2018 relate large scale breaches or particularly sensitive circumstances. Nevertheless, the frequency of higher value DPA fines represents a significant hike on the past few years. European regulators now have powers to impose significantly higher penalties under GDPR.

Historical ICO fines greater than £200,000



Italian competition regulator fines Facebook

In further bad news for Facebook the [Italian Competition Authority \(ICA\)](#) fined Facebook nearly Euro 10 million for violations of the country's Consumer Code in relation to its usage of subscriber data. Chief among the regulator's concerns was misleading consumers into subscribing to the platform without adequately and immediately informing them that the data would be used for commercial purposes. The ICA considered that Facebook exerted undue influence on consumers by imposing significant restrictions on users who limited their consent.

EDPB issues draft guidelines on the territorial reach of GDPR

The [European Data Protection Board \(EDPB\)](#) has issued guidelines on the territorial scope of GDPR (Article 3). The guidelines seek to ensure a consistent application of GDPR when assessing whether particular processing by a data controller or processor falls within the scope of GDPR for companies active in EU markets in the context of worldwide data flows. The draft guidelines are issued for a period of public consultation which ends 18 January 2019.

The [ICO](#) extended its extra-territorial arm to Canada in issuing an enforcement notice under GDPR to a Canadian firm, AggregateIQ Data Service Ltd (AIQ). The firm was being investigated by the regulator as part of a wider investigation into the use of data analytics in political campaigns for elections and the Brexit referendum. AIQ continued to hold personal data on UK individuals which the commissioner considered was held in a way that the data subjects were not aware of; for purposes which they would not have expected and without lawful basis for processing.

California creates IoT security law

The [new code](#) requires the manufacturers of “connected devices” to equip those devices with reasonable security features appropriate to the device, appropriate to the information it may collect, contain, or transmit, and that are designed to protect the device and information stored therein from unauthorized access. In short, it targets Internet of Things devices – from printers to home security cameras – that have traditionally been shipped from the manufacturer with the bare minimum of security (e.g., the password is “password”). These devices are then chained together and used by bad actors, for example in DDOS attacks. [The new law is the first of its kind in the U.S.](#), although it has its detractors for being vague, misguided, or for lacking enforcement provisions. The law takes effect 1/2020.

Political agreement for a new European Cyber Security Act

Similarly, a new EU [Cybersecurity Act](#) will establish a framework for a ‘comprehensive’ cyber security certification scheme for information & communications technology (ICT) devices. The framework will be a one stop shop for products, processes and services throughout the EU with a view to enhancing the security of connected products, internet of things devices as well as critical infrastructure. The legislation is intended to dovetail Network and Information Security Directive which became effective earlier this year. The political agreement now needs to be ratified by the European Parliament and the Council of the European Union.

Oath agrees to \$4.95M fine

Verizon-owned Oath, has [agreed to pay a \\$4.95M](#) fine to settle charges it violated children’s privacy by using visitors personal data to place targeted ads on users under the age of 13. The settlement comes under COPPA (“Children’s Online Privacy Protection Act”) after an investigation by the New York Office of the Attorney General.

Australia Passes Anti-Encryption Law

As discussed in last quarters newsletter, Australia has now passed the Assistance and Access Bill of 2018, which allows law enforcement to require private companies to disclose user information even where it is encrypted – in short, it [requires companies to build a “back door”](#) to any encryption they use. This has been [widely criticized](#) as it essentially builds a inherent weakness into the system, thereby reducing security for all. How this will affect the liability of private companies operating in Australia whose systems might be breached by this required “back door” – and the insurance implications of such a breach – remain open questions.

TransRe Speaks

Peter Cridland

will be speaking:

▼ Wednesday, March 6-8, 2019

JLT Re MPL Leadership Conference | “Silent Cyber and its Impact on MPL”

Elizabeth Geary

will be speaking:

▼ Tuesday, March 12, 2019

Sprecheranfrage Risk & Reinsurance Summit–Munich, Germany

Lauren Markowski

will be speaking:

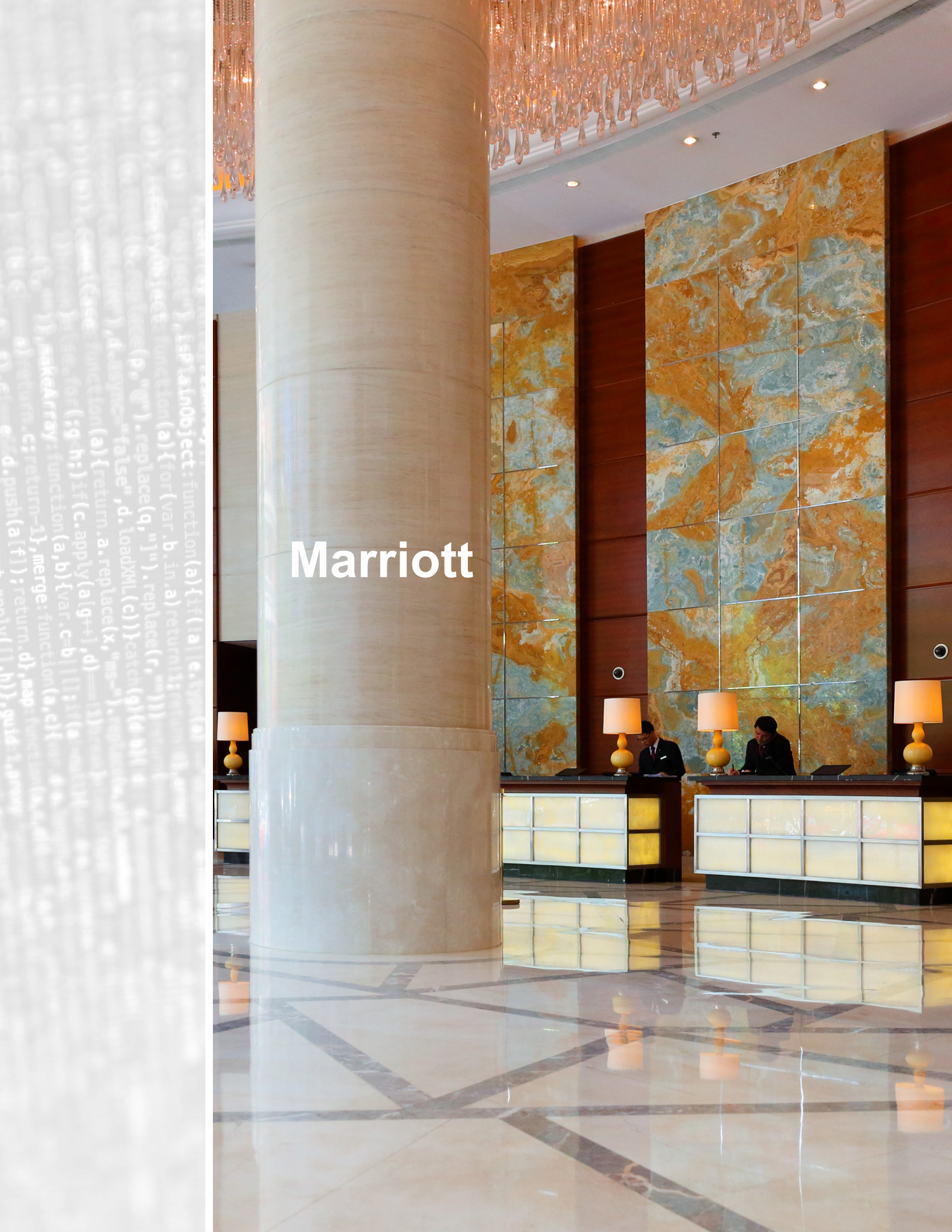
▼ Tuesday and Wednesday, March 19 & 20, 2019

8th Annual Cyber Liability Insurance ExecuSummit

Cyber Studies & Reports

- ▼ [Beazley Breach Insights](#) – October 2018
- ▼ [Chubb Cyber InFocus](#) – 4th Quarter 2018
- ▼ [Primer on Cybersecurity Law and Policy](#) – by Bobby Chesney

Marriott



Special Feature – Marriott

In late November Marriott announced it had been the victim of a [significant hack](#) affecting roughly 500 million customers. The affected system does not appear to be the system handling Marriott-branded hotels, rather it affects the legacy Starwood hotel system. Marriott purchased Starwood in 2016, but early information indicates that the bad actors involved in the incident have had access to the Starwood system since at least 2014. There has been no public discussion to date as to why this issue wasn't discovered in the due diligence process of the purchase transaction – similar to Yahoo's breach discovery during negotiations for Verizon's purchase, which ultimately led to a significant reduction in purchase price.

Kroll has been engaged to assist in the Marriott response and they have posted the official website with information on the incident [online](#). Meanwhile [independent investigators](#) have suggested that there is a link to Chinese state-sponsored hackers in the Marriott breach. On the regulatory side, mere hours after the breach announcement, the [New York Attorney General announced an investigation](#) into the breach and possibly delay in reporting the incident, with the [Texas Attorney General](#) following shortly thereafter with an announcement of their own investigation. At the same time, [U.S. Senator Ron Wyden](#) took the opportunity to release his draft of a new bill – the Consumer Data Protection Act – which aims to impose stricter penalties on companies who are hacked, included potential jail time for executives.

On the other side of the Atlantic, GDPR has been in full effect since May and [many commentators](#) are wondering if the Marriott breach – by far the largest since May – might be the first to merit the full weight of the new laws' penalties. GDPR famously allows for penalties of up to 4% of global revenue. According to [Marriott's 2017 Annual Report](#), global revenues were \$22.894 billion – 4% of which comes to a massive \$915,760,000 potential fine. Some predictions of a potential GDPR fine have been roughly half that maximum, or about \$450M, but even then, the [total cost of the breach could reach \\$1B](#). [One industry-expert](#) estimates the breach will be in the \$200M - \$600M range for 1st / 3rd party losses, not including fines / BI / stock price / non-cyber claims.

Error

Do I Really Have to Restart, Again?

By: Neil Inskip

I believe the modern workplace is plagued by two things, a broken photocopier and your PC constantly telling you to reboot for updates, the bad news is neither is curable. According to Murphy both diseases are likely to set in at the busiest time in the office as well, making both very annoying. While I like to think I'm slightly better versed at de-jamming a copier than most, I'm sure an article about it would not be appreciated in this publication. This time then, I take you through how IT staff and suppliers are working to keep your IT estate up to date and therefore safer from the bad guys.

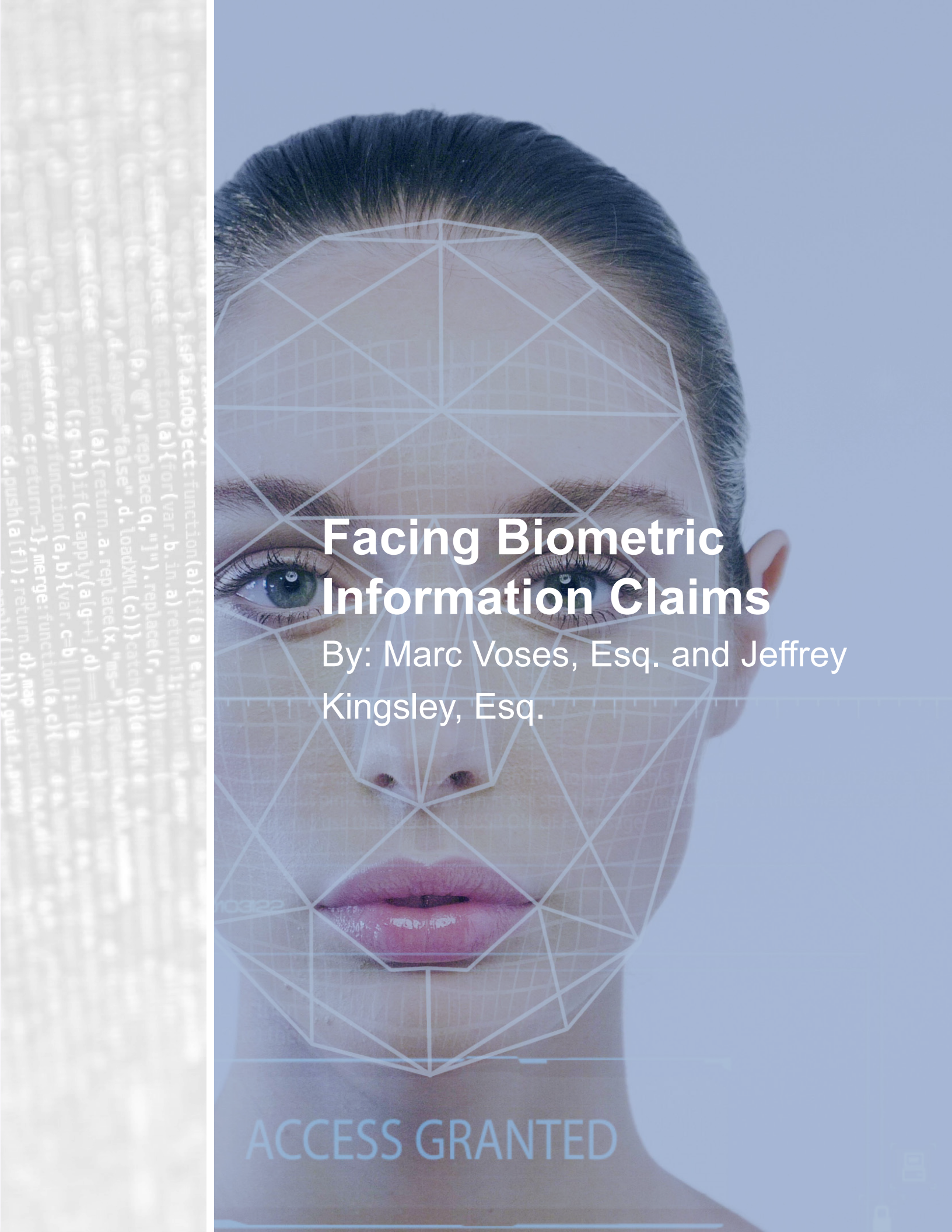
The US National Institute of Standards and Technology (NIST) will tell you that any cyber risk assessment matrix must demonstrate that risks are applied to identified assets (be that software, hardware or people), the same is true of patch management, how can you update what you don't know about. Luckily for IT departments there is a plethora of network asset discovery tools available to automate the identification, the key is to make sure it can detect whatever is in use at your organization. With a sound inventory available, you may then look to standardize, simplify or reduce the list, the less variables and nuances the easier the job. Possibly there is scope to "harden" some of those assets, for example you could have a server dedicated as print server, so services that allow it to run web sites can be disabled or removed. Many services and features are bundled in to a server operating system, if you're not going to use some of them it makes sense to disable them.

From there you can take a decision, keep them up to date or mitigate the risk with additional controls (firewalls, antivirus, etc), but it's at that point you will probably want to check what vulnerabilities your network has. I would say most large enterprises address this with automated network vulnerability scans on a frequent basis using a suitable software product and then overlay that with employing expert third party services on a bi-annual or less frequent basis. Both will provide a list of assets and their vulnerability score, highlighting priorities for immediate remediation. The third party will attempt to exploit all known weaknesses both from outside and inside your company, a practice known as "penetration testing".

With an automated asset list and a hit list of your most vulnerable assets the next step is hopefully to start automating patch management, possibly using the same product that did the asset discovery, I say hopefully, there may still be a manual level of intervention for some servers and PCs. Timing is everything by the way, if you

have a global enterprise using a datacentre in London it's likely that someone elsewhere in the world is going to be busy at the time you want to reboot a server to get a patch applied. The biggest problem with update patches is that sometimes you must reboot to get it applied, during the reboot the file(s) will be unlocked from use and can therefore be switched out for the newer version.

Server-side the IT department can usually figure out timing, sometimes patches need to be delayed by a phase of testing on non-production assets, just to sanity check they do not cause issues with other products or services. The dilemma is your PC workstation, the PC must be powered on to be updated and then it must be restarted in some cases to get the patch applied. Clearly long-term events like employee sabbatical or paternity leave may mean a PC is switched off for extended periods, leading to backlog of updates on returning to work and some updates can be large taking longer to install before releasing the computer to the user. Regarding the reboot the options are asking you the user when it's a good time, (like never right? Ignore that) or reboot automatically for you at a pre-defined time. The latter option must be scheduled by IT, it's the only way to be sure, but it would be great if you can do it for yourself. We know from virus and hacking incidents past, not doing it is not an option. If your PC is asking you to reboot, maybe do it now and then walk down the hall to see if the copiers are online while you wait, you may want to take that handwritten sign that reads "Not working, awaiting engineer visit" with you though.



Facing Biometric Information Claims

By: Marc Voses, Esq. and Jeffrey Kingsley, Esq.

ACCESS GRANTED

Biometric information consists of those unique biological traits that help identify you. Your fingerprints, facial features, retina and iris, shape of your hand or earlobe, your gait, voice patterns, DNA, and handwriting patterns are some examples of that information. For years, these distinctive identifiers have been collected and used for a variety of security purposes ranging from bank accounts to ordering food online. As technology in this area grew, it became clear that state and federal regulations that existed at the time did not address or even contemplate the responsibilities these companies should have in obtaining, using, and preserving those identifiers. State regulators took notice of these collection efforts and the potential misuse of this unique and irreplaceable information.

BIPA Lawsuits

A decade ago, Illinois passed the Biometric Information Privacy Act (“BIPA”), regulating the collection and storage of biometric information. BIPA put an end to private entities obtaining biometric information without first obtaining informed consent.

The first BIPA related litigation arose in 2015. Since that time, more than 60 class actions complaints have been filed alleging violations of BIPA. While most lawsuits have been filed in Cook County or the Northern District of Illinois, notable suits have also been filed in California.

BIPA lawsuits can be generally sorted into three groups of alleged violations: (1) lawsuits involving fingerprints obtained by employers in order to track when employees clock in and out of their shifts¹; (2) biometric information obtained by companies of consumers or other individuals²; and (3) facial recognition involving photographs³. Defendants have employed a number of different strategies to escape BIPA lawsuits with varying success. The outcome often dependent on the specific allegations and circumstances.

Two recent Illinois state court decisions highlight a dividing line in the analyses of BIPA lawsuits. In *Rosenbach v. Six Flags Entm’t Corp.*, 2017 IL App (2d) 170317, the plaintiff filed suit against a theme park where he was fingerprinted while purchasing a season ticket. The theme park did not obtain written consent or disclose its plan for collection, storage, use, or destruction of the biometric information.

The theme park moved to dismiss the complaint on the basis that plaintiff was not an “aggrieved person” as required by the statute. The trial court did not dismiss the claims under BIPA. On appeal, the question was whether the plaintiff was “aggrieved.” The appellate court determined a person had to suffer an actual injury,

adverse effect, or harm in order to be “aggrieved.” Moreover, the court stated that the legislature could have omitted the word “aggrieved” if it wanted to allow a private cause of action for every “technical” violation of BIPA. In the end, a technical violation of BIPA without alleging any injury or adverse effect was found not to be sufficient to state a claim.

The Illinois Supreme Court heard oral arguments in *Rosenbach* on November 20, 2018. If the Illinois Supreme Court reverses the decision of the appellate court, then mere technical violations will give plaintiffs standing under BIPA. This would fuel an increase in the number of lawsuits filed and statutory damages (up to \$5,000 per violation) paid under BIPA.

By contrast, in *Sekura v. Krishna Schaumburg Tan, Inc.*, 2018 IL App (1st) 180175, an Illinois appellate court distinguished *Rosenbach* to conclude that dismissal of a BIPA claim was not proper. The facts in *Sekura* involved a plaintiff enrolling with a tanning salon’s national membership database, which required a fingerprint scan. The fingerprint data was then disclosed to a third-party vendor. Plaintiff also alleged that she becomes emotionally upset and suffers from mental anguish when she thinks what may happen to her biometric data if the company went out of business or if her biometric data was shared with others.

The trial court initially dismissed the action based upon the reasoning in *Rosenbach*. On appeal, the appellate court rejected the argument that the term “aggrieved” is superfluous unless additional harm is required. The court concluded that the circumstances in *Sekura* were distinguishable from *Rosenbach* because the plaintiff’s biometric data in *Sekura* was disclosed to a third-party vendor.

Lawsuits venued in federal court have also seen defense strategies employed with varying success. For example, in *Monroy v. Shutterfly, Inc.*, the putative class action complaint asserted violations of BIPA in connection with Shutterfly’s facial recognition software scans wherein faces in an image are compared against others in the database. Shutterfly filed a motion to dismiss arguing that (1) BIPA does not apply to scans of facial geometry; (2) the application of BIPA would violate the Dormant Commerce Clause and the notion of extraterritoriality; and (3) plaintiff failed to allege actual damages.

With respect to facial scans, while BIPA provides that photographs are not considered biometric identifiers, the court determined that the facial scan conducted by Shutterfly fell within the ambit of biometric identifiers regulated by BIPA. Shutterfly argued that since BIPA

did not contain provisions concerning extraterritorial effect, it should not apply extraterritorially. The court was not persuaded by the extraterritoriality argument at the motion to dismiss stage because it was unclear whether the circumstances of the claim occurred primarily or substantially in Illinois.

Shutterfly also argued the Dormant Commerce Clause was violated because BIPA has the effect of controlling conduct beyond Illinois. The court rejected this argument on the grounds that BIPA regulated Shutterfly's operations in Illinois, not its operations in other states. Lastly, Shutterfly's argument that plaintiff failed to allege actual damages was rebuffed since plaintiff asserted his right to privacy was violated. Several of these defenses have previously been rejected in similar circumstances.⁴

As one may expect, the issue of Article III standing is often litigated in connection with BIPA claims. Both plaintiffs and defendants have been able to have suits dismissed or remanded to state court due to the lack of Article III standing.⁵

Settlements

Given the difficulty in maintaining and defending BIPA lawsuits, it comes as no surprise that these cases settle. What is surprising is the apparent lack of publicly available information concerning those settlements. Our research has revealed three matters with information sufficient to discuss.

The Sekura case mentioned above is one of those cases. Class action plaintiffs alleged that L.A. Tan's use of customers' fingerprint scans in lieu of key fobs for membership purposes violated BIPA since L.A. Tan failed to obtain written consent. L.A. Tan was alleged to have released customer fingerprint information to a third-party vendor. The certified class of approximately 37,000 settled for \$1.5 million, or \$125 for each class member. In *Norberg v. Shutterfly, Inc.*, photos of the plaintiff were uploaded onto Shutterfly, but plaintiff, who did not have a Shutterfly account, had his face analyzed and suggested to other members that other photos of plaintiff should be tagged with his name. *Norberg* did not reach the class certification stage, because an undisclosed settlement was reached with the named plaintiff.

Lastly, in *Carroll v. Crème de la Crème, Inc.* (Cir. Ct. Cook Cnty., IL, No. 17-CV-1624), plaintiffs alleged that Crème, a daycare/school provider, obtained and collected without consent fingerprint scans as a method for authenticating the parent or guardian's identity when picking up children

from its campuses. This information was collected and stored without consent. Plaintiffs settled for free credit monitoring services for one year to class members and other benefits, and a \$5,000 payment to the class representative.

Trends

BIPA lawsuits have been met with mixed reactions from carriers. Driving the issue of whether to cover a claim are the underlying facts and the availability of language in the policy that permits a carrier to push back on these types of claims. While few policies outright disclaim coverage for claims arising out of or related to BIPA violations, many others can exclude coverage under the wrongful collection of information exclusion. For claims involving employees seeking damages alleging BIPA violations, policy language may operate to preclude coverage for these claims because they arise in the employment context. In addition, employee claims that are subject to dispute resolution pursuant to a collective bargaining agreement may serve as the basis for disclaiming coverage for certain damages pursuant to a breach of contract exclusion.

For carriers that are affirmatively seeking to underwrite these risks, coverage is oftentimes provided pursuant to a manuscripted wrongful collection endorsement, which may be subject to a sublimit, but always carries with it an increase in premium. Irrespective of a carrier's current position, biometric information collection and storage is an emerging risk that will grow exponentially over the next five years and needs to be managed. Unlike financial account information, or driver's license and passport numbers that can be re-issued, biometrics are permanent and unique identifiers.

While Illinois is the first state to provide for a private right of action, California's BIPA will provide a similar right starting in 2020. As other states follow Illinois and California, the number of lawsuits alleging BIPA violations will increase and could see significant settlements that include statutory damages, fines and penalties. The cost to resolve collection and use claims will be dwarfed by those for data breaches involving biometric information because those cases will be more difficult to dismiss at an early stage of the litigation.

Marc Voses is a partner in Goldberg Segalla LLP's New York City office, and serves as the chair of the firm's Cybersecurity and Data Privacy Practice Group, and a partner in the Global Insurance Services Group. Jeffrey Kingsley is a partner in the firm's Buffalo office and serves as the chair of the firm's Global Insurance Services Practice Group overseeing a team of 65 attorneys, handling matters from cybersecurity to extra-contractual bad faith litigation.

¹ See, e.g., *Aguilar v. Rexnord LLC*, No. 17 CV 9019, 2018 WL 3239715 (N.D. Ill. July 3, 2018). ² See, e.g., *Rosenbach v. Entm't Corp.*, 2017 IL App (2d) 170317. ³ See, e.g., *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017). ⁴ See, e.g., *In re Facebook Biometric Information Privacy Litig.*, No. 3:15-cv-3747, 2018 WL 2197546 (N.D. Cal. May 14, 2018) (cross-motions for summary judgment denied); *Rivera v. Google, Inc.*, 238 F. Supp. 3d 1088 (N.D. Ill. 2017). ⁵ See, e.g., *Goings v. UGN, Inc.*, No. 17-cv-9340, 2018 WL 2966970 (N.D. Ill. June 13, 2018); *Howe v. Speedway LLC*, No. 17-cv-7303, 2018 WL 2445541 (N.D. Ill. May 31, 2018); *McCollough v. Smarte Carte, Inc.*, No. 16 C 3777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016); but see *Patel v. Facebook Inc.*, 290 F. Supp. 3d 948 (N.D. Cal. 2018).



Contacts



To receive future editions of the TransRe Cyber Newsletter, or to Opt-Out of future editions, please [click here](#).

Editors ▼

Calum Kennedy ▼

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

Lauren Markowski

Cyber Risk Underwriter
1.212.365.2301
lmarkowski@transre.com

Elizabeth Geary

Global Head of Cyber Risk
1.212.365.2243
egeary@transre.com

Peter Cridland ▼

Assistant Vice President
1.212.365.2032
pcridland@transre.com

Rhett Hewitt

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

Alex Bustillo

Cyber Risk Underwriter
1.212.365.2376
abustillo@transre.com

Phylip Jones ▼

Global Marketing Manager
1.212.365.2281
pjones@transre.com

Miguel Canals

Cyber Risk Underwriter
1.212.365.2266
mcanals@transre.com

Disclaimer

The material and any conclusions contained in this document are for information purposes only the authors offer no guarantee for the completeness of its contents. The statements in this document may provide current expectations of future events based on certain assumptions. These statements involve known and unknown risks, uncertainties and other factors which are not exhaustive. The authors of this document undertake no obligations to the publicity revise or update any statements, where as a result of new information, future events or otherwise and in no event shall TransRe or any of its affiliates or employees be liable for any damage and financial loss arising in connection with the use of the information relating to this document. Although TransRe makes reasonable efforts to obtain reliable content from third parties, TransRe does not guarantee the accuracy of or endorse the views or opinions given by any third party. This document may point to websites or other documents; however TransRe does not endorse or take responsibility for the content on such websites or other documents. [Click Here to Unsubscribe](#)
[Click here](#) for more information on our privacy policies.