Cyber Insights for Insurers

Q1 Review , May 2019

Welcome to Cyber Insights for Insurers*, from the* ***Cyber Practice Group*** *of* ***Aon's Reinsurance Solutions*** *business. As always, we aim to equip you with relevant trends and analysis to enhance your cyber insurance underwriting, portfolio management and claims handling, plus prepare you for changes in privacy law, the regulatory environment, and the threat environment.*

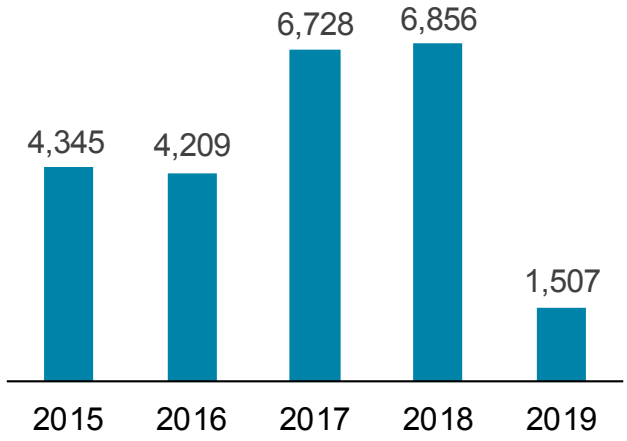
Key themes this quarter

- **Article III standing to sue** for data breach class action lawsuits remains uncertain.
- Severity trumps frequency in Q1 **ransomware** attacks.
- **"Supply chain" attacks** highlight aggregation risk potential.
- **Internet-connected devices** are being addressed by new European standards and a pending law in California.
- Proposed **US Senate bills** demand corporate accountability for data breaches, including jail time for corporate executives, and new comprehensive privacy legislation.

Cyber incident trends

2018 cyber incidents have now outpaced 2017 to reach a record high. In Q1 of 2019, the number of reported incidents fell short of a particularly active Q4 of 2018 but showed gains over all other 2018 quarters.

Exhibit 1: Cyber incidents by year



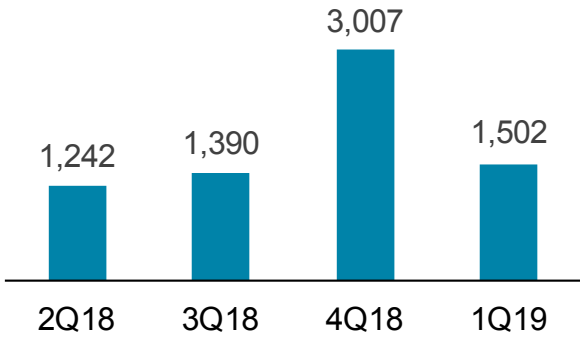
Source: Risk Based Security, analysis by Aon. Data as of April 2019.

As suspected, incidents reported in 2018 have now eclipsed 2017 when accounting for late entries. This now makes 2018 the year on record with the most reported cyber incidents.

Empower Results®

In 2019, notable trends for the first quarter included *UDPOS* malware and the *Magento* injection attacks targeting a variety of industries, including online retailers. See our **Industry Threat Analysis** and **Aggregation Monitor** sections for additional details.

Exhibit 2: Cyber incidents by quarter, 2018-2019



Source: Risk Based Security, analysis by Aon. Data as of April 2019

The frequency of ransomware events declined in 2018 and through the first quarter of 2019. It appears, at least for now, that criminals are more focused on targeted, highly invasive attacks than on high frequency/low severity forms of ransomware.

This trend notwithstanding, ransomware remains a preferred tactic for cybercriminals; it offers a much shorter path to monetization than data breaches, making it attractive to highly sophisticated criminal organizations and "script kiddies" alike. This quarter featured several notable ransomware events worth examining in greater detail.

Ransomware variant *LockerGoga* hit Norsk Hydro, a Norwegian aluminum producer, particularly hard – again highlighting the business interruption impacts of ransomware. According to reports, Norsk lost $40 million as a result of the attack, with some business units still affected at least a week after the initial infection. *LockerGoga* did not self-propagate like *WannaCry* and *NotPetya*, which limited its aggregation potential. In the case of Norsk, the actors behind the attack most likely distributed the malware after initially penetrating and analyzing the victim's environment. Based on preliminary analysis of *LockerGoga*, sources have reported the malware and attack was likely attributable to the criminal actor group known as Fin6.

In addition to *LockerGoga*, Fin6-affiliated actors were also linked to *Ryuk*, another ransomware variant that was active during the quarter. Jackson County, Georgia, USA reportedly paid $400,000 following a *Ryuk* infection. In addition, *Ryuk* also infected Tribune Publishing, among others.

Automated reconnaissance tools are still being developed and deployed to identify easy targets. A recently discovered automated scanning malware, *Xwo*, searches for vulnerable or misconfigured connected services, including default login credentials, to identify potential targets for secondary malware infection. The command and control infrastructure associated with *Xwo* is shared with *MongoLock*, a ransomware variant that targets MongoDB databases, and *XBash,* a "wiperware" variant that destroys data. *Xwo* is likely used as a reconnaissance-phase tool before the initial compromise, ransomware or wiper payload is delivered to the victim.

Aon Analysis: *Severe ransomware events have the potential for significant business interruption losses and associated claims costs, especially when manufacturing firms are the victims. Ransomware is here to stay – simply because attackers can quickly monetize their efforts if the victim pays. Data breaches, by contrast, generally require a "fence" or carding shop for criminals to monetize stolen data, which can complicate the remuneration process. Finally, the continued prevalence of automated reconnaissance and attack tools underscores the need for insureds to patch their exposed architecture and reduce their attack surface as much as possible. The misconfigurations or vulnerabilities identified by these tools can easily be a starting point for a ransomware infection or data breach. For their part, insurers must evaluate a company's patching cadence as an important risk attribute.*

Spotlight on fraud coverage

Social engineering has created new forms of fraud, and the insurance industry is grappling with where, and whether, to cover these losses.

Email phishing is the most common method that malicious actors use to begin attacking a victim. One category of phishing attacks involves social engineering – aka business email compromise (BEC) – to impersonate a trusted source and trick the email's recipient into wiring them money. This kind of loss is called "fund transfer fraud."

Due to the intricacies of insurance policy language, these social engineering tactics have been an area of coverage disputes, particularly for **crime policies**. Here, we review a few important examples.

Cases finding no coverage

In *Apache Corp. v. Great American Ins. Co.*, No. 15-20499 (5th Cir. 2016), the Fifth Circuit ruled in favor of the insurer, finding social engineering to be general fraud, rather than the "computer fraud" required under the policyholder's crime policy.

Apache Corporation had lost $7 million by wiring vendor invoice payments to a bogus bank account. The insurer denied Apache's claim for coverage, arguing successfully that the scheme's success hinged on Apache calling the imposter to confirm the bank account change over the phone. In other words, the email was merely part of a process, and Apache's loss was general fraud, not computer fraud specifically.

Cases finding coverage

In 2018, the Sixth and Second Circuits ruled in favor of policyholders, indicating that the tide may be turning, finding coverage for social engineering schemes under crime policies:

- In *Medidata Solutions, Inc. v. Federal Ins. Co.*, No. 17-2492 (2nd Cir. 2018), the Second Circuit affirmed a district court ruling that the computer fraud provisions of a crime policy **covered** losses incurred when a Medidata employee transferred $4.77 million in funds in response to two spoofed emails and a call from an imposter.
- In *American Tooling Center, Inc. v. Travelers Casualty & Surety Co.*, No. 17-2014, 2018 WL 3404708 (6th Cir. 2018), shortly after the *Medidata* ruling, the Sixth Circuit found coverage when an employee wired $834,107 to imposters posing as a third-party vendor in China. The court's rationale was that this case involved computer fraud directly causing the insured's direct loss, despite the carrier's contention that it was not a "direct loss" caused by the "use of a computer."
- In *Rainforest Chocolate, LLC v. Sentinel Insurance Company*, 2018 VT LEXIS 240 (Vt. Dec. 28, 2018), the Vermont Supreme Court held that the "false pretense" exclusion in a business-owner policy did not exclude the loss when an employee wired $19,875 based on a manager's email sent by an imposter. The court reversed the lower court, criticizing the policy drafting and finding the exclusion was ambiguous – for example, the use of "physical loss" and "physical damage" in the exclusion, versus the use of "loss" and "damage" throughout the policy. The case has been sent back to the trial court to address the forgery and money and securities coverage provisions.

In addition to coverage disputes on crime policies, we are now seeing so-called **"third party social engineering"** claims arise where financial institutions are presumed to be at fault for fraud committed against their customers.

In *O'Neill v. Bank of Am. Corp.,* 2018 WL 5921004, 2018 U.S. Dist. LEXIS 193302, at *2-4, (E.D. Pa. Nov. 13, 2018), a law firm in Pennsylvania learned a difficult lesson when it sued Bank of America to recover client funds stolen by hackers. In 2017, hackers had accessed the email account of a shareholder of the law firm and then tricked one of his partners via email, instructing him to urgently wire $580,000 from their Bank of America account to the hacker's bank account in Hong Kong. The law firm alleged that Bank of America bore ultimate responsibility when it could not stop the wire transfer after discovery of the ruse. The federal judge dismissed the law firm's case, effectively saying that Bank of America bore no responsibility for social engineering by a third party.

Although companies in Bank of America's situation are not at fault, they could still suffer brand and reputation damage from the social engineering campaign. We are now seeing some insurers offering "third party social engineering" coverage to address this exact issue for businesses. Yet other insurers may choose not to offer this coverage, because the impacts to insureds would not be direct losses.

Aon Analysis: Typically, standalone cyber insurance policies exclude fund transfers and the loss of money or securities. Crime insurers are offering separate limits or sublimits for BEC/Social Engineering loss, while doing specific underwriting of controls and charging additional premium for the coverage extension. Cyber-related perils are finding clear delineation between the cyber and crime policies, which is encouraging. That said, most insurance policies are silent on the issue of third party social engineering, and insurers would do well to clarify whether such coverage is provided.

Data breach litigation

Article III standing to sue for data breach class actions will remain split among U.S. courts, at least for a while longer.

The U.S. Supreme Court declined to hear *Zappos.com, Inc. v. Stevens, Theresa, et al* (Docket No. 18-225). This case would have addressed the issue of "Whether individuals whose personal information is held in a database breached by hackers have Article III standing simply by virtue of the breach even without concrete injury, as the U.S. Courts of Appeal for the 3rd, 6th, 7th, 9th and District of Columbia have held, or whether concrete injury as a result of the breach is required for Article III standing, as the U.S. Court of Appeals for the 1st, 2nd, 4th and 8th Circuits have held."

The U.S. Supreme Court's declination means an ongoing split in the Circuits, leaving business groups and breach victims with uncertainty on the issue.

Aon Analysis: Despite the ongoing split decisions in the Circuits, the recent appeals indicate the growing pressure on the U.S. Supreme Court to revisit the data breach standing issue. Insurers will want to review third-party coverages granted in cyber liability products once the Supreme Court decides to hear a standing to sue case.

Law & regulatory issues

Internet-connected devices (IoT) are under greater regulatory scrutiny, with new European standards and a pending law in California.

In February, the France-based European Telecommunications Standards Institute (ETSI) published ETSI TS 103 645, a high level outcome-focused standard for the security of Internet-connected consumer products or Internet of Things (IoT) devices. The purpose of these rules is to address security deficiencies in IoT devices, and to serve as a baseline for future IoT certification schemes. ETSI are aware of how poorly secured products threaten consumers' privacy, and furthermore, how some devices may be exploited for large-scale distributed denial of service (DDoS) attacks. Examples of the devices covered by the standard include children's toys, baby monitors, smoke detectors, door locks, smart cameras, TVs, speakers, wearable health trackers, home automation and alarm systems, and appliances.

Under this new standard, compliant products will be expected to meet thirteen recommendations to bridge the security gap, including unique passwords, a vulnerability disclosure policy, minimized attack surfaces, software integrity, and an end-of-life policy for software components that are updateable.

The ETSI standard as a whole is not mandatory, but some provisions are – e.g. no default passwords and a vulnerability disclosure. The question is whether the standard will be used. Without enforcement, the danger is that commercial pressures to get products to market quickly will suppress best practices and security-by-design by IoT device manufacturers. Some take the view that GDPR compliance could be an incentive for using ETSI, if European regulators formally decide to take the standard into consideration in any GDPR action against an IoT manufacturer.

The ETSI standard is the latest effort to regulate IoT devices, adding to California's introduction last year of Senate Bill 327, which we discussed in our December 2018 issue. Senate Bill 327 becomes effective January 1, 2020, and requires "reasonable" security of connected devices.

Aon Analysis: So far, IoT laws and standards have stopped short of fines or penalties, but insurers should watch continuing developments in this area.

Recently proposed US Senate bills demand corporate accountability for data breaches, including jail time for corporate executives, and new comprehensive privacy legislation.

U.S. Senator Elizabeth Warren (D-Mass.) has proposed a Senate Bill paving the way for criminal charges for wrongdoing by corporate executives.

The Corporate Executive Accountability Act would apply to executives of companies with annual revenue exceeding $1 billion. The bill would make it unlawful for such an executive "to negligently permit or fail to prevent" three types of violations:

1. Any federal or state crime for which the company is convicted or enters into a deferred prosecution agreement ("DPA") or a non-prosecution agreement ("NPA");
2. Any federal or state civil violation for which the company is found liable or settles and that "affects the health, safety, finances, or personal data of" at least 1 percent of the United States population or at least 1 percent of the population of any state; or
3. Any federal or state criminal or civil violation for which the company is convicted or found liable and which was committed while the company was operating under any judgment, DPA or NPA relating to a different criminal or civil violation.

Senator Warren's proposal includes penalties of a fine and/or imprisonment for up to 1 year for a first offense, and a fine and/or imprisonment for up to 3 years for a second offense.

The Washington Post reported that business groups and defense attorneys have criticized the drastic criminal penalties.

Separately, U.S. Senator Edward J. Markey (D-Mass.) has proposed a Senate Bill (OLL19313 S.L.C.) introducing comprehensive federal privacy legislation to protect American consumers' personal information.

The Privacy Bill of Rights Act establishes rules for online and offline companies and bans the use of individual's personal information for harmful or discriminatory purposes, such as housing and employment advertisements based on demographics including race and gender. The bill includes data minimization requirements, provides the Federal Trade Commission (FTC) with rulemaking authority, and enables the State Attorneys General to protect the interest of residents and bring action against companies that violate the privacy rights of individuals. In addition, individuals will have a private right of action empowering them to defend their own privacy rights.

Senator Markey has commented that "a true 21st century comprehensive privacy bill must do more than simply enshrine notice and consent standards."

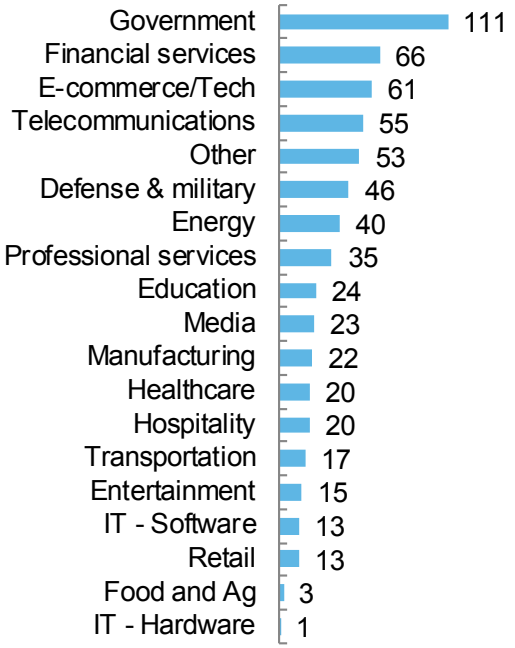
Congressional leaders in both parties have expressed an interest in new privacy legislation and are doing serious work to that end. Emerging bills, frameworks and comments reflect a move toward shifting the burden of managing data privacy onto companies to handle data fairly.

Aon Analysis: The proposed Senate privacy bills signal a heightened awareness by members of the 116th US Congress to address privacy concerns at the federal level while states continue to develop their own consumer privacy protections. Although a US federal privacy law could be a significant driver of change, the real drivers so far are GDPR in Europe and the CCPA in California.

Industry threat analysis

In Q1 of 2019, Government maintained a healthy lead as the most targeted industry group. Financial Services, E-Commerce, and Telecoms round out the four most targeted industries – a pattern we have seen quarter after quarter.

Exhibit 3: Threat alerts by industry, Q1 2019



Source: CrowdStrike, analysis by Aon. Alerts are compiled by observing deep and dark web information, new malware development, and other data points that indicate the intentions of threat actors. An alert indicates an imminent incident or event has been observed.

Beginning in February, retailers faced a spate of point of sale (POS)-targeted attacks. The *UDPOS* malware, which was first discovered in 2018, infected a number of retailers. Traditionally *UDPOS* infected POS systems by masquerading as an *LogMein* executable update. Once infected, the skimmed data is sent via User Datagram Protocol (UDP) DNS traffic to a command and control server.

Financial Services, E-commerce, and other business-to-consumer entities continue to face malicious JavaScript library injections aimed at skimming payment card data and personally identifiable information (PII) to a malicious third party. As reported previously by Aon, these attacks continue and may constitute a legitimate aggregation breach risk for insurers.

Aon Analysis: *Although chip and PIN technology has rendered some POS malware less threatening, the risk persists. Indeed, as threat actors have pivoted away from traditional POS malware, they have focused their attention on the next generation of "POS" malware – targeting online retailers and vulnerable scripts used for processing payments. Underwriters should be aware of the increased risk to these types of businesses.*

Aggregation risk monitor

The number of recorded cloud outages fell after a volatile Q4. Average downtime remained well below the industry standard waiting period deductibles.

Exhibit 4: Cloud provider downtime during Q1:
Top US providers vs. other regions

Provider	Outages (count)	Avg Downtime (minutes)	Total Downtime (minutes)
North America	159	26	4,176
AWS	3	1	2
Microsoft	6	32	190
Google	1	2	2
IBM	6	1	7
Rackspace	54	26	1,401
All Others	89	29	2,575
Europe	125	10	1,310
APAC	160	10	1,608

Source: Cloud Harmony, analysis by Aon

Market leaders AWS, Microsoft, Google, and IBM experienced low volatility during the quarter. Over the past two quarters, however, Rackspace has totaled 144 observed outages, after two successive quarters of only two total outages. Most of these outages were not attributable to a specific cause, although some were a result of scheduled maintenance.

Aon Analysis: *Cloud aggregation can take many forms. Although many focus on downtime as a potential aggregation event, hardware vulnerabilities could also lead to mass breach events of a specific cloud provider. Insurance ERM teams should develop scenarios both for contingent business interruption as well as mass breach events.*

Exhibit 5: Annual cloud provider downtime:
Top North American providers vs. others

Region	Outages (count)	Average Downtime (minutes)
North America		
AWS	5	9
Microsoft	31	72
Google	2	29
IBM	257	18
Rackspace	146	36
All Others	2643	4

Source: Cloud Harmony, analysis by Aon

Software supply chain vulnerabilities are a growing aggregation hazard

Multiple, severe software supply chain exploits led to considerable aggregation risk during the quarter. Kaspersky reported ASUS Live Update, a proprietary tool for ASUS notebooks, pushed malicious code to thousands of machines. Although thousands of computers were potentially compromised, only 600 were specifically targeted via their MAC addresses, according to reports. The attackers targeted and compromised an ASUS server used to push software and firmware updates to ASUS computers.

Aon Analysis: *Although this particular attack targeted a small subset of only 600 computers, one can easily envision a much more severe scenario. Supply chain attacks targeting a specific piece of widely used software, like the Ccleaner and M.E. Doc, have significant aggregation potential. Insurers should monitor specific aggregation paths and diversify their portfolio of risk when appropriate.*

Formjacking continues to be a source of potential aggregation risk.

Continuing a theme from last quarter, JavaScript injection – or formjacking – attacks have skyrocketed, infecting as many as 4,800 websites per month. Formjacking allows criminals to simply skim credit card data and other personal information to actor-controlled servers. As of writing this, over 300,000 websites were running vulnerable *Magento* code used for processing web-based payments.

Aon Analysis: *By attacking a widely used e-commerce package like Magento, criminal groups can easily infect thousands of websites, potentially skimming tens of thousands of customer credit cards – at once. These sorts of "mass breach" attacks significantly truncate the attack kill-chain, allowing the attacks to quickly exfiltrate data without having to navigate a victim's network or defenses. Insurers should monitor the patching cadence of their insureds as a proxy for good cyber hygiene.*

Finally, Microsoft's *Windows 7* is reaching its end of life "extended support" on January 14, 2020 – less than one year from now. Like *Windows XP* today, *Windows 7* will no longer receive updates and patches.

Aon Analysis: *Insurers should take note of this event and underwrite legacy Windows 7 environments accordingly. Windows 7 currently has 37% of the desktop OS market.*

.

Contact Information

Jon Laux, FCAS, MAAA
Head of Cyber Analytics
+1 312 381 5370
jonathan.laux@aon.com

Craig Guiliano, CISSP
Cybersecurity Specialist
+1 312 381 1566
craig.guiliano@aon.com

Dawn Kristy, JD
Cyber Claims Advocate
+1 312 381 5483
dawn.kristy@aon.com

Catherine Mulligan
Global Head of Cyber
+1 212 441 1018
catherine.mulligan@aon.com

Luke Foord-Kelcey
International Head of Cyber
+44 (0)20 7086 2067
luke.foord-kelcey@aon.com

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Disclaimer