Cyber Insights for Insurers

Q3 Review, November 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.*

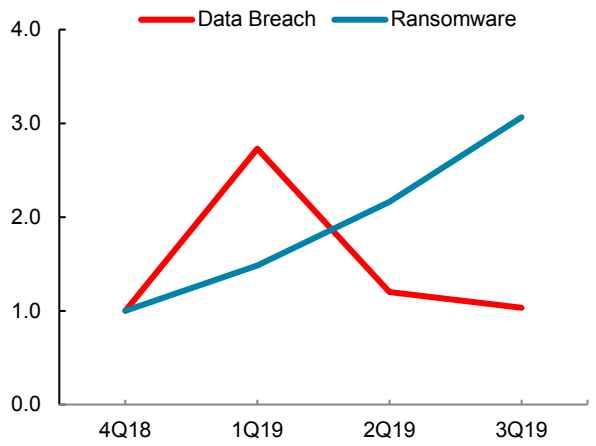
Key themes this quarter

- Ransomware has increased significantly in both frequency and severity this year.
- The first class-action lawsuit has been filed in the UK under GDPR.
- California's CCPA becomes effective 1/1/2020 – we compare its latest stipulations with GDPR.
- Other states are also moving forward with privacy laws.
- Unfounded concerns have been raised about the potential linkage between having cyber insurance and being a ransomware target.

Cyber incident trends

Ransomware incident rates are up threefold since Q4 2018, largely due to the growth of ransomware as a service (RaaS) and increased utilization by cybercriminals.

Exhibit 1: Cyber incident rates by quarter 2018-19
(Index: Q4 2018 = 1.0)



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

Reports indicate that sophisticated organized crime groups are increasingly turning to ransomware. In particular *Ryuk*, an extremely active ransomware variant, has been attributed to WIZARD SPIDER, the experienced criminal group that maintains *Trickbot*.

AON
Empower Results®

The costs of ransomware attacks continue to increase across all sectors, with payments *tripling* from an average of USD12,762 to USD36,295 during the second quarter alone. The total cost of ransomware to a company includes both recovery expenses (including ransom payments, forensic fees, and assistance rebuilding servers) and downtime costs. The average downtime increased from 7.3 days in Q1 to 9.6 days in Q3. Downtime costs are typically 5-10 times larger than the actual ransom amounts, due to lost productivity and revenue opportunities.

RaaS variants are playing a key role in raising downtimes as well as frequency. RaaS allows even novice hackers and black hat operatives to adopt traditional Software as a Service (SaaS) models to enable criminal enterprise. Cybercriminals may write ransomware code and sell or rent it under an affiliate program for a quick profit to others intending to launch an attack. In addition, RaaS providers may offer an entire platform to manage ransomware campaigns. Various RaaS packages can be found in the market, reducing the need to code malware. This malicious franchise-like deployment model allows virtually anyone to become an "affiliate" of an established RaaS package or service.

The most prolific RaaS tool during the quarter was *REvil*. According to threat intelligence, *REvil* appears to have been developed by the same actors as the previous RaaS variant *GandCrab.* Due to the nature of RaaS, actors use a variety of attack methodologies. The method of initial compromise varies from phishing to watering hole attacks that compromise the popular content management system (CMS) WordPress. Based on these methodologies, victims of ransomware appear to be targets of opportunity.

RaaS has contributed to upward trends in both frequency and severity of claims due to less reliable data recovery and ransom payment success rates. These factors depend largely on the ransomware variant and threat actor group. Less reliable data recovery is symptomatic of novice hackers utilizing RaaS models, which can prompt longer and more costly ransomware attacks. As many as 96% of organizations that pay a ransom receive working decryption tools, but full data recovery is becoming less certain. Incident duration has increased for *Phobos* ransomware cases, where data recovery rates are as low as 85% due to the complex and unreliable decryption tools provided by its current criminal affiliates, who are typically less organized amateurs. This has led to protracted negotiations and complications that arise during decryption. Ransomware variant *Sodinokibi* uses an automated TOR site for payments, which provides victims with a decryption tool. Victims that paid for a decryptor lost 8% of encrypted data during recovery. *Ryuk* ransomware caused even greater damage with 13% of data lost during the recovery process.

Ransomware Claims – Myths and Realities

On September 19, media reports discussed several situations where cyber insurance played a role in resolving ransomware attacks. It was noted in those reports that Rockville Centre Public Schools, Wakulla County School District, and the city of Stratford, Ontario were all attacked by ransomware, and all three had cyber insurance policies in place. It is noteworthy Rockville Centre paid a $10,000 deductible while their insurance carrier paid $88,000 in Bitcoin after putting the district in contact with a third party able to negotiate down the initial ransom of USD176,000. The district superintendent justified paying the ransom based on the infection targeting and encrypting backups. School districts are ideal targets for cybercriminals due to their uniquely vulnerable network security. Credible threat intelligence reports have found no linkage to suggest that cybercriminals are choosing their ransomware targets because of the purchase of cyber insurance. Moreover, FireEye and CrowdStrike continue to highlight the assistance that cyber insurance has brought to ransomware resolutions.

Aon Analysis: *Media reports have confused correlation with causation. Ransomware attacks are widespread, and all sectors and industries are vulnerable. As many as one quarter of small and medium enterprises are estimated to collapse if unable to trade for a month due to an attack. In some instances, paying the ransom may make*

sense to reduce business downtime. However, paying ransoms also entices sophisticated and unsophisticated groups alike to increase their attacks. Relying on a competent and experienced incident responder to navigate – and, if necessary, assist in ransom payments – has become more important than ever. Cyber insurance policies provide these services and offer valuable aid to companies in resolving ransomware attacks.

Aggregation risk monitor

Cloud outages during the quarter were minimal across the globe, averaging well below industry standards for waiting period deductibles. US market leaders experienced very little average downtime for the third quarter in a row.

Exhibit 2: Cloud provider downtime during Q3: Top US providers vs. other regions

Provider	Outages (count)	Avg Downtime (minutes)	Total Downtime (minutes)
North America	138	6	887
AWS	-	-	-
Microsoft	6	1	5
Google	-	-	-
IBM	3	72	217
Rackspace	-	-	-
All Others	129	5	666
Europe	95	9	808
APAC	121	5	580

Source: Cloud Harmony, analysis by Aon

Amazon Web Services (AWS) Route 53 DNS Service was impacted by a DDoS attack.

On October 22, AWS' Route 53 DNS service suffered a distributed denial of service (DDoS) attack. According to AWS, the attack targeted domains associated with Simple Storage Solution (S3) buckets, but also impacted other AWS services, including Elastic Compute Cloud (EC2). Although public reporting indicated an 8-hour attack, AWS health indicators and third-party monitoring services did not report a significant outage of Route 53 or S3 services (only several minutes at the time of this report). AWS stated the attack caused "resolvers for a small number of AWS names to fail," suggesting the impact of the attack was not a system-wide outage. Additionally, AWS claimed its Advanced Shield DDoS protection service assisted in mitigating the attack. Due to the interconnected nature of DNS, other service providers were ultimately impacted.

Aon Analysis: *There are some similarities to the Dyn attack in 2016; both involved DDoS attacks on DNS services. However, AWS appears to have largely mitigated this attack through its DDoS protection service and unlike with Dyn, AWS service was not completely disrupted. It is still unclear if this attack targeted Route 53, all S3 services, or specific S3 buckets. As of late October 2019, no known insurance claims have materialized from this attack.*

GitHub has again been used as a central distribution channel for malware.

Trickbot, the prolific banking Trojan-turned *Ryuk* downloader has been distributed via GitHub repositories. GitHub was built to serve as a DevOps platform and file repository. Millions of businesses and individuals download tools, plug-ins, and applications from GitHub, making it a central software supply chain target. In the past, GitHub has also been used by the Magecart web application payment card skimming group to distribute malicious plug-ins.

Aon Analysis: *A key source of potential aggregation remains software supply chain compromises. Many thousands or perhaps millions of individuals and businesses may unwittingly download malicious software from third-party websites like GitHub. Additionally, we have seen otherwise legitimate updates corrupted by sophisticated groups, including nation states, to target victims. Although patching remains a critical component in preventing malicious attacks, care must be taken by administrators to ensure updates and plug-ins downloaded from third-party sites are untainted.*

Spotlight: global privacy law

For over eighteen months, insurers and businesses have sought to fully understand and comply with the EU General Data Protection Regulation (GDPR) which took effect on May 25, 2018. The GDPR consists of 99 Articles that include mandates on the consent given by data subjects in the European Union (EU) before their data is processed by an entity, time limits on retaining data, the appointment of data protection officers, the designation of an EU representative, and a list of regulations on the collection, processing and storing of personal data.

The passage of GDPR was a watershed event and has inspired new regulation in other jurisdictions. Mostly notably, businesses in the US are now contemplating their compliance requirements under the California Consumer Privacy Act (CCPA) which is set to take effect on January 1, 2020. New laws have been passed in New York (SHIELD), Nevada, and Maine as well.

Given all this recent activity, we are devoting the remainder of this issue to provide a summary of the latest information available about the current data privacy laws and what they mean for insurers.

The first class-action lawsuit under GDPR has been filed in the UK.

As many as 500,000 customers of British Airways (BA) may participate in class-action lawsuit against BA over its 2018 data breach.

As reported in our last issue, in July 2019, the Information Commissioner's Office (ICO) in the UK proposed a GBP183 million fine on BA, the first levied under the GDPR for non-compliance. The ICO looked at the variety of information compromised and the insufficient protections when it levied a fine representing 1.5% of the company's global turnover.

Aon Analysis: *Class-action lawsuits for data protection breaches have not been common in the UK. Under GDPR, markets may now anticipate compensation awarded to data subjects in litigation as well as regulatory fines and penalties.*

CCPA vs. GDPR

The CCPA grants California consumers the right to know about and control the personal information that businesses collect about them.

Since compliance with the GDPR does not ensure compliance with the CCPA, businesses are relying upon the advice of counsel to navigate toward compliance. The stakes are high as businesses seek to avoid fines and penalties for non-compliance as well as costly litigation following data breaches.

A comparison of the main points of each law appears on the next page. Here, we highlight some of the key similarities and differences:

Scope
GDPR is broader in scope and territorial reach. GDPR applies to entities regardless of size, revenue or the amount of personal data processed. The CCPA carves out non-profits as well as small businesses with revenues up to $25 million.

Protections
GDPR puts protections on personal data about data subjects. CCPA protects personal information (PI) about consumers, with employees and B2B transactions coming under the law in 2021. These laws are substantially different in approach, but similarly broad in effect. It is worth noting that CCPA includes the PI of households, not just individuals.

Individual Rights
The laws provide individuals with similar rights to access and delete the data that entities hold about them, although GDPR also gives individuals the right to Correction, Rectification, and Opposition of data as well as Data Portability. It is worth noting that under GDPR one must *opt in* to sharing data with third parties, whereas under CCPA adults age 16 and older are given the right to *opt out*.

Litigation, Fines and Penalties
GDPR is more stringent than CCPA, but both significantly increase the financial penalties that entities must pay for missteps. The GDPR fines have been much discussed, their insurability still debated, and as noted earlier, class-action lawsuits for data breaches are now a reality.

Table 3: Key Points of GDPR and CCPA

GDPR European Union – effective 25 May 2018	CCPA State of California – effective 1 January 2020
Who & what is protected?	
▪ **Data subjects** = identified or identifiable persons to whom personal data relates ▪ Protects the data privacy rights of all persons in EU ▪ **Personal data** is any information relating to an identified or identifiable data subject	▪ **Consumers** = California residents regardless of physical location ▪ **Employees** & **B2B** transactions (deferred 1 year) ▪ **Personal information** (PI) that identifies, relates to, describes, is reasonably capable of being associated with, or linked to a consumer/household
Who is regulated?	
Data controllers and **data processors**: ▪ Established in the EU that process personal data ▪ Not established in the EU that process EU data subjects' personal data	Any for-profit entity doing business in California, that meets one of the following: ▪ Gross revenue > USD25 million ▪ Buys, sells, receives or shares PI of >50,000 consumers, households, or devices annually ▪ Derives ≥ 50% revenue from selling or sharing PI
Individual rights	
▪ Access, Deletion, Opt-In to sharing information with third parties, Correction, Rectification, Opposition, Data Portability ▪ Default age for consent is 16 (minimum 13 by member state law)	▪ Access, Deletion, Opt-Out from sharing or having PI sold (aka right to say no) ▪ Minors under 16 may opt-in to selling of their data (aka right to say no) ▪ Non-discrimination: Equal service or price if exercise rights under CCPA
Security	
• Requires data controllers and processors take appropriate technical and organizational measures to ensure security level appropriate to the risk	• No directly imposed data security requirements, but private right of action available for data breaches caused by failure to maintain reasonable security practices
Exemptions	
▪ Related to national security, criminal justice, personal or household activities	▪ HIPAA, GLBA, FCRA, DPPA, Publicly available, government records ▪ Clinical Trials ▪ Contracts with third parties or service providers
Enforcement actions for non-compliance (fines)	
▪ Severe: Up to EUR20 million or 4% of total global turnover of prior year, whichever greater; ▪ Less Severe: Up to EUR10 million or 2%, whichever greater	Civil penalties of: ▪ USD2,500 per violation, or ▪ Up to USD7,500 per violation if intentional ▪ 30 days to cure violation
Private right of action (penalties)	
▪ Data Breach ▪ Security Breach	▪ Data Breach ▪ Unauthorized access of PI (due to lack of reasonable security procedures) ▪ Actual damages, or Statutory damages from USD100 to USD750 per consumer per incident ▪ 30 days to cure violation
Insurance coverage	
▪ Network Security & Privacy Liability ▪ Regulatory Fines & Penalties	▪ Network Security & Privacy Liability ▪ Regulatory Fines & Penalties

The penalties for non-compliance with CCPA are much more benign: USD2,500 per violation or USD7,500 if the violation is intentional. But the CCPA provides California residents the right to sue companies for data breaches of their personal information if the company fails to use reasonable security measures to protect it. Residents can seek statutory damages of between USD100 and USD750 per consumer per incident under the law. This private right of action for a data breach has been touted as the first of its kind in the nation, allowing consumers to sue following a data breach without having to prove they suffered actual harm or damages. Based on the amendments passed on October 11, however, class-action lawsuits may only be brought for data breaches pursuant to California's data breach notification law when the personal information is "nonencrypted and nonredacted."

California's Data Breach Notification Law has also been amended.

The California Data Breach Notification Law has been expanded, also effective January 1, 2020, by requiring businesses to notify consumers of compromised passport numbers and biometric information. In security breach notifications, the new law requires instructions on how to notify other entities that used the same biometric data to no longer rely on data for authentication purposes.

Aon Analysis: *Under CCPA, statutory damages eliminate the difficult task of calculating actual damages caused by a breach, which could encourage an uptick in lawsuits by data breach plaintiffs. Cyber claim frequency is likely to increase due to the expanded definition of personal information. Moreover, the private right of action also paves the way for greater litigation, if the courts do in fact tamp down on the ongoing ambiguity in the Article III standing to sue rulings. Cyber claim severity is also likely to increase due to non-compliance fines and penalties as well as actual damages or statutory damages soon to be in play under the private right of action. But with restrictions on class-action lawsuits, the impact to severity is likely to be moderated. Businesses may find it easier to demonstrate that they did not violate their "duty to maintain reasonable security procedures and practices." Finally, while some reports have found that GDPR fines and penalties are not insurable, fines and penalties in California are more likely insurable.*

Other US State Privacy Laws

Nevada

As of October 1, 2019, Nevada's new Internet Privacy Law, SB 220 (SB220) officially went into effect, making it the first state to follow in California's footsteps. The new law amends the state's existing online privacy law for owners and operators of Internet websites or online commercial providers.

Under this new law, like the CCPA, a consumer can submit a notice to an operator to opt out of the sale of their information to third parties. Unlike the CCPA, there is no private right of action. The bill authorizes the AG to seek an injunction or a civil penalty of up to USD5,000 for each violation by an operator.

SB 220's definition of "sale" is not as broad at the CCPA's and includes several key exceptions. SB 220 also does not amend the law's existing definition of "covered information." By contrast, the CCPA's definition of "personal information" is generally broader.

Aon Analysis: *Businesses were only given five months to comply with this law, so Nevada will be a jurisdiction to watch in terms of enforcement actions for non-compliance.*

Maine

In June 2019, the US State of Maine has passed An Act to Protect the Privacy of Online Customer Information which takes effect on July 1, 2020.

The law provides strict measures for the approximately 80 broadband internet service providers (ISPs) in Maine, requiring them to obtain express consent from a customer before selling to or sharing data with a third party.

While the CCPA gives customers the right to opt out, the law in Maine prohibits ISPs from utilizing customer data unless the customer *opts in* – which is more stringent like the GDPR.

The new law will only apply to ISPs serving customers that are physically located and billed for services in the State of Maine.

Aon Analysis: *Once again, this law illustrates the differences and similarities – and the resulting compliance challenges – that businesses will face with the patchwork of US state laws.*

New York SHIELD Act

On July 25, 2019, New York's governor signed into law the Stop Hacks and Improve Electronic Data Security Act (the SHIELD Act), which amends the New York's data breach notification and cybersecurity law. The SHIELD applies to "any person or business that owns…computerized data which includes private information," regardless of corporate structure, revenues or location.

The SHIELD Act will apply to businesses and employers in New York – and may also apply to those with no physical presence in New York – imposing more expansive data breach notification requirements on companies by:

- *Broadening the scope* of "private information" to include personal information (such as a social security number or driver's license number), biometric information, and email addresses with their corresponding passwords or security questions and answers
- Expanding the definition of a security "breach" to *include unauthorized access* of computerized data that compromises the confidentiality, security, or integrity of private information
- *Expanding the territorial scope* of the breach notification requirement to any person or entity with private information of a New York resident, not just those conducting business in New York
- Updating the *notification requirements* and procedures that entities must follow when there has been a breach of private information
- Creating requirements for companies to implement *reasonable safeguards* to protect the confidentiality, security and integrity of private information.

Recent amendments provide some exceptions and clarify that businesses will be deemed compliant with SHIELD if they comply with another information security law such as HIPAA, the GLBA, or the requirements of the New York Department of Financial Services. Such covered entities are not required to notify affected New York residents after a breach; however, companies must still notify the New York Attorney General, the Department of State Division of Consumer Protection, and the Division of the State Police regarding the breach.

Unlike the CCPA, the SHIELD Act does *not* authorize a private right of action or class action litigation. But similar to CCPA, the AG is authorized to bring enforcement actions, and violations may result in civil penalties. The SHIELD Act provides that the AG may seek an injunction, an award of damages for actual costs or losses incurred or a civil penalty of the greater of USD5,000 or up to USD20 per instance of failed notification (not to exceed USD250,000).

The SHIELD Act's breach notification amendments were effective on October 23, 2019, while the new data security requirements will take effect beginning March 21, 2020.

Aon Analysis: *Companies covered by SHIELD will likely have to report a greater number of cyber incidents to regulators, due to the expanded definitions of "private information" and of a "breach". Defining a data "breach" as unauthorized access is a much lower threshold than its traditional meaning, i.e. data exfiltration. As a result, it seems likely that cyber insurers will see an increase in claims frequency from companies covered by SHIELD. But claim severities appear unlikely to change much, given the relatively modest penalties imposed. If cyber insurance policies are found to cover these civil penalties, small businesses are most likely to benefit from the added protection.*

Conclusion

As we approach the inception of these myriad US state privacy laws, this complex web of regulation – and the absence of a federal privacy law – are becoming increasingly taxing to businesses. US underwriters and actuaries will have to keep track of these changes and the potential impacts to claims frequency and severity. For businesses of any size and scale, it is likely that both CCPA and SHIELD will apply, and insurers will have to adjust their views of risk accordingly.

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

Julia Cederroth
Cybersecurity Specialist
+1 312 381 0451
julia.cederroth@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
Head of International
+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