Aon
Cyber

Cyber Insights for Insurers

Q3 Review, December 2018

Welcome to Cyber Insights for Insurers*, from the* ***Cyber Practice Group in 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

- **US regulators** continue to look for a better approach to cybersecurity and data privacy protection.
- **Banking trojans** and **Javascript injections** plagued consumers as well as e-commerce and online retailers.
- A closer look at the illicit dark web marketplace reveals a **bustling underground economy**.
- In several recent cases, courts in the US and UK are holding businesses **increasingly liable** for data breaches.
- A protracted US **cloud outage** occurred in the third quarter, but no evidence has yet surfaced of contingent business interruption claims.

Threat activity to watch

Ransomware attacks have declined since peaking in second quarter 2017, while phishing campaigns continue to pay for cybercriminals; banking trojans remain in the spotlight.

Malicious spam and phishing campaigns continued to dominate the threat landscape during the quarter. In September, malicious emails – delivering either malicious URLs or attachments – exceeded all malicious traffic reported during first quarter. Spam and phishing campaigns relied heavily on social engineering techniques that focused on business email compromise (BEC) or delivered advanced banking trojans, ransomware, or keyloggers to intended victims.

In the third quarter, ransomware activity declined slightly relative to previous quarters, but attacks remain elevated compared to pre-2017 levels. The devaluation of cryptocurrencies, such as Bitcoin, has not stopped ransomware actors. The actors behind the *SamSam* ransomware increased their ransom demands to compensate for Bitcoin's devaluation over the quarter. As reported in last quarter's *Cyber Insights for Insurers*, the *SamSam* actors target specific victims for maximum effect, with more severe impacts than indiscriminate ransomware – sometimes thousands of computers are infected. Unsurprisingly, victims of *SamSam* tend to pay the ransom more often than victims of other ransomware variants. Since January 2016, victims of *SamSam* have paid a total of $6.7 million in ransom.

AON
Empower Results®

Banking trojan activity rose again, driven by *Emotet*, a modular piece of malware that primarily functions as a downloader or dropper of other banking trojans. The frequency and potential severity of Emotet infections led to the issuances of several alerts by US-CERT and other governmental and private security entities throughout the quarter. Emotet can evade typical signature-based detection and identify the presence of anti-virus software. Emotet generally spreads via email, includes worm-like capabilities, and can conduct spam campaigns from an infected host. Emotet's willingness to drop other banking trojans based on the host environment illustrates how threat actors continue to cooperate in order to prosper.

Aon Analysis: *Spam and phishing remain the delivery method of choice for malicious actors. Companies can help prevent spam and phishing attacks by using essential technologies and protocols, including: Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC). While these protocols are effective, underwriters must also confirm that insureds supplement their technical controls with security training and awareness.*

Underground marketplaces are thriving, despite law enforcement efforts

During the quarter, British Airways, Ticketmaster, and other online retailers and e-commerce sites fell victim to malicious Javascript injections at the hands of MageCart, an increasingly sophisticated criminal group. The results included over 600,000 records and payment card details compromised. According to Crowdstrike, Magecart may now include three separate groups conducting their own campaigns against vulnerable websites, using the same tactics, techniques, and procedures to compromise sensitive information.

When the criminals behind banking trojans or ransomware need to monetize their gains, carding shops and dark web marketplaces not only facilitate the sale of stolen banking and credit card information, but also provide the necessary infrastructure, scripts, and intelligence to continue the heist. This ecosystem of criminal activity fuels the cycle of illicit activity.

During the quarter, global law enforcement arrested additional members of the prolific Carbanak Group, shuttered multiple dark web marketplaces, and seemed to make concerted efforts to target malicious domains and hosts. Nonetheless, copycat marketplaces have quickly filled the vacuum left by closed sites.

Although Empire Market launched in early 2018, in the third quarter the marketplace saw a notable increase in the number of users, stolen credit cards, compromised credentials, protected health records, hacking tools, and other illicit items. For those familiar with AlphaBay, formerly "the world's largest dark web market" which was shut down by law enforcement in 2017, Empire Market looks, functions, and offers the same products and services as its predecessor.

Similarly, malicious marketplace Joker's Stash received millions of US and European credit card dumps, which were offered for sale – some of which are associated with major, high profile breaches in North America and Europe. The discerning buyer can choose cards associated with a specific geography (e.g. US or UK) as well as the inclusion of personally identifiable information (PII) and CVVs. Many of the posters offer refunds within a given timeframe.

Aon Analysis: *Underwriters insuring e-commerce and online retailers should encourage their insureds to continuously scan their websites and mobile apps for unauthorized JavaScript code. By scanning their websites, companies can quickly identify malicious code.*

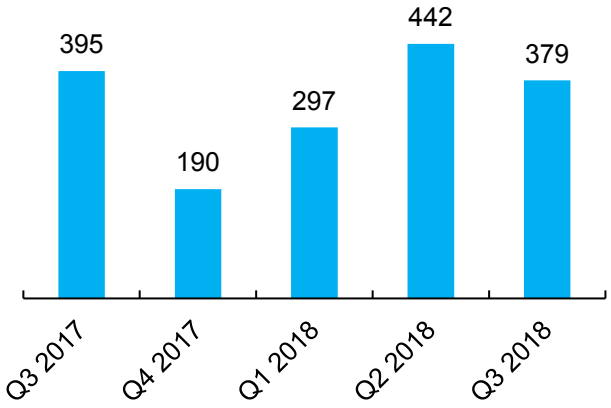
Unfortunately, the underground economy continues to flourish, providing the necessary tools and mechanisms for criminals to carry out attacks and sell their wares. As long as these marketplaces exist, criminals will continue to be enabled to act.

Industry threat analysis

Financial services reclaimed the position as the most targeted industry for the quarter, followed by government services.

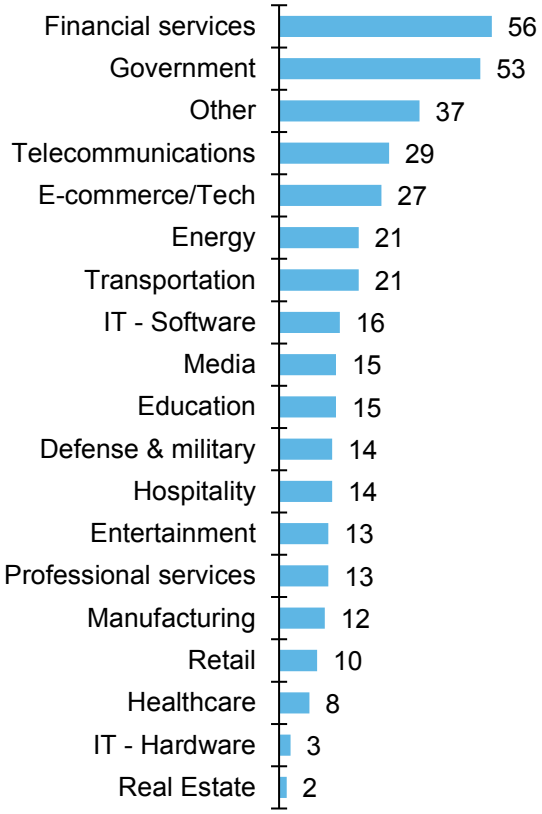
Third quarter appeared to continue a trend from the third quarter of 2017 – a slight decline after peak alerts during the previous quarter. Financial services surpassed e-commerce and government to receive the most industry alerts for the quarter. The holiday season may shift the tide once again with targeted attacks against e-commerce eclipsing those targeting financial services, due to the prevalence of online shopping and criminal actors hoping to take advantage.

Exhibit 2: Threat alerts by quarter



Aon Analysis: *With holiday shopping in the US alone expected to increase by at least 4%, criminal groups will likely look to capitalize on shoppers' poor cyber hygiene and web-related vulnerabilities exploited by sophisticated criminals like MageCart. Attack trends in the fourth quarter will most likely indicate elevated risk for e-commerce sites and online retailers, while nation-state actors may take much-needed holidays before getting back to work after the New Year.*

Exhibit 3: Threat alerts by industry



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.

Data breach litigation

WM Morrison Supermarkets was found vicariously liable in the first UK data breach class action.

A disgruntled Morrisons employee copied the payroll data of 99,998 employees to a personal USB drive and posted the data on a file-sharing website. He later sent the data to three UK newspapers and was subsequently convicted of a criminal offense.

In October, the UK Court of Appeal held the WM Morrison Supermarkets vicariously liable for the torts committed (i.e. malicious data breach) by the rogue employee against other employees.

The UK Court of Appeal stated that insurance is a viable option for companies to mitigate against dishonest or malicious employees.

Aon Analysis: *The decision on Morrisons means that employers can be held liable for the actions of employees, even if an employee's intent was harm to the employer rather than self-gain.*

Evidence suggests that data breaches perpetrated by insiders have greater severity than those conducted from outside a company's network. The Morrisons case has implications for cyber insurance buyers, who will be held to account for the actions of rogue employees. Additionally, employee sentiment is now more important for underwriters to consider.

Pennsylvania Supreme Court finds negligence in a failure to protect employees' PII.

In *Dittman v. University of Pittsburgh Medical Center*, current and former employees of the University of Pittsburgh Medical Center (UPMC) filed a class-action lawsuit following a data breach in which PII of 62,000 employees was accessed and stolen from UPMC's computer systems and used to file fraudulent tax returns. Plaintiffs alleged negligence and breach of implied contract, claiming that their employer had a duty of care to protect their PII. Further they alleged damages from the fraud and an increased and imminent risk of becoming victims of identity theft crimes, fraud, and abuse.

The trial court dismissed the case due to lack of allegations of physical injury or property damage under the Pennsylvania economic loss doctrine (requiring more than solely economic damages based on negligence). The Superior Court affirmed.

The Pennsylvania Supreme Court reversed this decision, noting that criminal acts of third parties in executing a data breach do not alleviate UPMC of its duty to protect employees' PII and financial information from that breach. Furthermore, the Court rejected both lower courts' interpretation of the economic loss doctrine, stating that Pennsylvania recognizes "that purely economic losses are recoverable in a variety of tort actions" permitting recovery for the underlying data breach.

Aon Analysis: *Dittman allows current and former employees to sue their employers who suffer a data breach (or other security incident) involving their PII. Employers and their insurance carriers will need to consider these costs and whether this will become a trend in US courts.*

Coverage analysis

The Second and Sixth Circuits ruled in favor of policyholders, finding coverage for social engineering schemes under crime policies.

In *Medidata Solutions, Inc. v. Federal Ins. Co.*, No. 17-2492 (2nd Cir. 2018), in a much-anticipated decision on payment instruction fraud, the US Court of Appeals for the Second Circuit affirmed a district court ruling that the computer fraud provisions of a crime policy provided coverage for losses incurred when a Medidata employee transferred $4.8 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), the Sixth Circuit reversed a federal district court, thus finding that the $834,107 wired to imposters posing as a third-party vendor in China amounted to computer fraud directly caused the insured's loss, and that the crime policy provided the coverage.

Aon Analysis: *When payments are fraudulently diverted to an alternative bank account, which insurance policy applies? Typically, standalone cyber insurance policies exclude funds transfer and the loss of money or securities, whereas crime policies may provide coverage via specific clauses that lay out the circumstances. Coverage litigation is costly and time consuming, with no guarantee of a successful outcome. Thus, commercial policy wordings analysis remains an important step in managing the risk of payment diversion schemes and fraudulently-induced wire transfers.*

Law & regulatory issues

US Congress passed the CISA bill to invest in cybersecurity and protect critical infrastructure.

In November, the US Congress passed the Cybersecurity and Infrastructure Security Agency (CISA) Act (H.R. 3359). CISA creates a new cybersecurity agency within the Department of Homeland Security (DHS). The bill aims at securing federal networks and protecting critical infrastructure from cyber and physical threats by elevating the cybersecurity mission within DHS, enabling it to engage with industry and government stakeholders and recruit top cybersecurity talent.

Aon Analysis: *Prioritizing cybersecurity and highlighting the need to protect federal networks and critical infrastructure is an important step in the right direction. Re/insurers are beneficiaries of such efforts to improve cyber resilience.*

California passes the first Internet of Things law.

In September, California Governor Jerry Brown signed legislation making California the first state to expressly regulate the security of connected devices, aka the Internet of Things (IoT), effective January 1, 2020. This law differs from the California privacy laws that protect PII, being focused on the security of IoT devices and any information contained in IoT devices.

The new law regulates manufacturers of connected devices, defined as devices that can directly or indirectly connect to the Internet and are assigned an Internet Protocol (IP) or Bluetooth address. Manufacturers are required to equip the device with a reasonable security feature appropriate to the nature and function of the device, the information it collects, contains, or transmits, and to design the device with protection against unauthorized access, destruction, use, modification, or disclosure of PII. Devices regulated under US federal law will be exempt from this state law (e.g. FDA-regulated medical devices).

Aon Analysis: *Although not perfect, this legislation in California is an important first step, since two bills that were proposed in Congress have not yet gained traction to establish federal standards. The regulation does raise questions about what "reasonable" security entails, and whether it will lead to greater acceptance of security by design. Insurers will want to watch this issue closely for potential products liability implications.*

Ohio Senate Bill creates legal incentives for companies to adopt greater cybersecurity.

Ohio's new Data Protection Act introduces a first-of-its-kind "reasonable security" standard into its new "legal safe harbor" legislation effective November 2.

The law provides companies conducting business in Ohio with a safe harbor affirmative defense in the event of a security incident or data breach.

The safe harbor affirmative defense is available when an entity adopts cybersecurity measures designed to:

1. Protect the security and confidentiality of personal information;
2. Protect against any anticipated threats or hazards to the security or integrity of the personal information; and
3. Protect against unauthorized access to and acquisition of information that is likely to result in a material risk of identity theft or other fraud.

The founding principle of the law is to provide organizations with a legal incentive to achieve a higher level of cybersecurity by maintaining a cybersecurity program that substantially complies with one of eight common industry frameworks. If businesses comply with any of the frameworks, then they are entitled to plead an affirmative defense to tort claims related to a data breach stemming from alleged failures to adopt reasonable cybersecurity measures.

The frameworks include CIS's Critical Security Controls, FISMA, the GLBA Safeguards Rule, HIPAA's Security Rule, ISO 27000, and NIST CSF.

Aon Analysis: *This new Ohio law treats compliance with industry frameworks as a demonstration that a company has taken reasonable security measures, and it provides an affirmative defense to any tort action related to a data breach. This law should incent companies to invest further in cybersecurity. Insurers can anticipate a potential reduction in privacy liability claims for Ohio businesses that comply with these industry standards.*

Use of biometric data is beginning to generate lawsuits and potential insurance claims.

The Illinois Biometric Information Privacy Act (BIPA) (effective in 2008) remains the only state biometric privacy statute with a private right of action.

BIPA prohibits an entity from collecting, capturing, purchasing, or otherwise obtaining a person's "biometric identifier" or "biometric information" unless notice, consent, and data retention requirements are met. In October, proposed class-action lawsuits were filed under BIPA against Con-Tech Lighting and Medline Industries relating to fingerprint time and attendance systems. In September, proposed class-action lawsuits were filed under BIPA against both fingerprint door-lock maker U-Tec and the Chicago Loews hotel for lack of disclosure on the storage and disposal of fingerprints as well as Wendy's burger chain for lack of disclosure on the storage and retention of fingerprints.

After becoming the epicenter of biometrics-based litigation, with dozens of cases pending alleging violations of BIPA (against employers, social media platforms, service providers, and other businesses), the Illinois Senate proposed amendment SB 3053 in 2018 seeking to provide exemptions to the application of the law to private entities that collect, store, or transmit biometric data if:

- Exclusively used for employment, human resources, fraud prevention, or security purposes, or
- Private entities do not sell, lease, trade, or similarly profit from the biometric identifier or biometric information collected, or
- Private entities that collect, store, transmit, and protect the biometric identifiers or biometric information in a manner that is the same as or more protective than how the private entity stores, transmits, and protects other confidential and sensitive information.

Specifically, the Illinois Senate is seeking to narrow BIPA's reach by expressly excluding digital photographs and data generated from digital photographs from the definition of biometric identifier, relevant to charges of inappropriate facial recognition by social media services. Furthermore, the amendment would narrow the scope of the law to Illinois, addressing concerns that BIPA is impermissibly being applied outside of the state.

Aon Analysis: *Since biometric data generally cannot change, databases containing that information are attractive targets for hackers. Beyond fingerprinting, facial recognition technology is growing and raising concerns over individual privacy. In November, a major US airline launched the use of facial recognition technology in Atlanta using biometric data from passport photos to speed up check-in and boarding on international flights. This process raises emerging risk questions about compliance with BIPA, the California Consumer Protection Act, and the GDPR.*

Aggregation risk monitor

Overall, the number of outages and total downtime exceeded in the second quarter for all regions. Cloud service during the quarter remained within the expected negligible amount of downtime, with the exception of Microsoft Azure, which experienced an outage in its Southeast region.

Exhibit 4: Cloud provider downtime during Q3:
Top US providers vs. other regions

Provider	Outages (count)	Avg Downtime (minutes)	Total Downtime (minutes)
North America	591	5	3,211
AWS	-	-	-
Microsoft	7	282	1,972
Google	-	-	-
IBM	35	3	107
Rackspace	-	-	-
CenturyLink	-	-	-
All Others	549	2	1,132
Europe	566	5	2,871
APAC	106	12	1,261

Source: Cloud Harmony, analysis by Aon

The third quarter data is consistent with trends observed in prior quarters – meaning very few incidents occurred which could potentially trigger claims meeting standard 8-12 hour waiting period deductibles.

However, Microsoft did experience a major service disruption of its cloud computing and storage services. According to Microsoft, a lightning storm affected its Texas data center's main and back-up power supplies, resulting in at least partial downtime for customers ranging from 25 hours to 71 hours in the extreme cases. Microsoft issued a lengthy response following the outage, which occurred on September 4.

Although one might expect this cloud outage to cause an aggregation of contingent business interruption claims for insurers, our research has yet to identify a claim that has been filed.

Aon Analysis: *Although insurers have focused on cloud outage as an aggregation scenario for cyber insurance – perhaps* the *aggregation scenario – the Microsoft outage illustrates that insurance claims from cloud outages are far from clear cut. In addition to clearing the waiting period hurdle, multiple layers of redundancies must fail before claims are possible. Even then, the potential for claims needs to be considered for each insured individually: What services are they specifically hosting in the cloud? Are these services revenue-generating? What fail-overs does the insured have in place, and did these fail-overs work as expected?*

This event suggests that the impacts of cloud outage events on insurers are nuanced. While an aggregation of cloud-related claims is possible, more research needs to be done to understand the true potential for impact on insurers.

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

This newsletter is made available for informational purposes and is not intended to be a substitute for professional or legal advice. No attorney client relationship is formed or implied between you and the authors(s) or Aon.

Contact Information

Jon Laux, FCAS
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
Head of Cyber Innovation
+44 (0)20 7086 2067
luke.foord-kelcey@aon.com