2019 CLM Annual Conference
March 14, 2018
Orlando, Florida

How to Handle Cyber - Best Practices for the Claim Professional and Other Cyber-related Practitioners

I. Cyber-Risk Defined

A. Understanding the Nature of a Cyber Attack

Cyber peril is different than other areas of insurable risk in that the nature of the risk involves human beings performing deliberate actions against the insured policyholder. Deliberate cyber attacks can be passive or active. An intruder typically begins with a reconnaissance mission to gather as much information publicly available about its target as possible. The information is publicly available either by accident or leakage. This attack is deemed *passive* because it is launched to greatest extent possible without giving any indication as to the existence of the attacker in the first instance.

Passive intruders may run scripts on Google, LinkedIn and other social networks to deploy web spiders trapping any and all data related to the target. With some basic programming, these pre-canned scripts are designed to gather server names, ip schemes, network diagrams, web portals, addresses, forward facing penetrations, wifi relationships, and other "ways in" to the target network that is available without interfacing with the network whatsoever. In other words, the intruder's ip address will not show up on any firewalls or other logs.

An attack evolves from its passive state to an active one when the attacker begins to interface with the target network. This typically involves scanning lists of ip addresses, probing and locating and testing vulnerabilities.

Active attacks also include "social engineering" attacks where the intruder interfaces with a human beings at the target in an effort to dupe them into letting the attacker inside the network. Attackers send emails that read "hey this is Bob from accounting, can you click here and follow directions?" Attackers may attempt a "phishing" expeditions, for example by placing a USB stick with a hand-written label that says "2014 salaries" in the cafeteria. All it takes is one person interested enough as to what is on that disk to insert in her computer. Of course, the intruder did not have the 2014 salaries, but rather a Trojan horse, a tunnel going outbound from the target network to the hacker's computer.

B. Exploring the Motivation of the Attackers

Cyber as a peril is really a risk in as much as it is the means of an attack on an intended target. The causes and origin of the attack itself is only one aspect of an incident investigation.

By far the most pervasive and common threat to data is the disgruntled employee. These threats are already on the inside of the network. They have access to data and a personal motivation. By the same regard, third party contractors, business associates and vendors pose a similar threat because of their respective access to the network they may target.

The more sinister threat worthy of exploration is the Advanced Persistent Threat ("APT"). The *hacktivist* collective, *Anonymous* is a perfect example of AVP in cyber-risk. When someone affiliated with Anonymous issues finds a new target or new issue, she or he will issue a battle-cry using Twitter, and other social networks among the hacker community.

Some attacks are relatively harmless and done to prove a point. For example, there may be a coordinated mass "pinging" of a target ip adresss. The massive traffic increase floods the domain causing it to fail. Innocent visitors may find the target network unavailable, thus being deemed a denial of service attack. Other attacks are far more malicious and involve identifying network vulnerabilities and publishing them on open forums.

APT's are advanced because they can involve scattered and loosely coordinated efforts between government-affiliated organizations, organized crime, or political groups. They are persistent because the same advances of technology that benefit our commerce so much also assist the attackers in maximizing the attacks and resisting any defense efforts made by the target network.

C. Differences in Threats by Industry

Different industries have interests in protecting different kinds of information. The health care industry is charged with the protection of Protected Health Information ("PHI"). All companies must keep personally identifiable information ("PII") secure. Financial institutions are charged with securing financial and banking information. Many companies protect different forms intellectual property which can be electronic in nature and thus subject to electronic compromise.

D. Contemporary Considerations for the Evolving Threats

New technologies lead to new risks and new kinds of information lead to new damages. The insurer must understand the nature of the technology used by its insureds.

II. Handling a Cyber Claim

1. Discovery
    a. Learning Your Systems Have Been Compromised
        i. IT

Many breaches in the security system are discovered by IT with the detection of unusual activity or a report from a user.

ii. Law Enforcement
At times, law enforcement advise companies that they are the victim of data breaches or other security events.

iii. PCI
Law enforcement also work with the payment card industry ("PCI") in the investigation of credit card fraud. Card brands and law enforcement investigate common points of purchase ("CPP") amongst stolen credit card credentials and will alert businesses to same.

iv. Media / Grey Hat
Some technically proficient people use their own ability to breach computer network to prove political points or raise revenue. So-called "black hat hackers" will knowingly break the law and impermissibly access someone else's network for ill-gotten profit or other monetary reasons. The blogger's source in my client's case does not exactly or directly profit from the use of the data he copied (other than raising awareness of how virtuous he is). On the other hand, "white hat hackers" are usually certified and enter into contractual obligations with companies where they are expressly permitted to access a company's computer system for evaluation of security and then report its findings back to the company along with recommendations to cure any vulnerabilities discovered. Clearly, in my clients' examples above, the hacker did not have permission to access their computer networks. Not black, not white … these "grey hat" hackers are difficult to define, categorize and handle. They believe they are doing society a greater good by knowingly breaking the law and impermissibly accessing someone else's computer network to discovery security vulnerabilities. They therefore are deliberate actors and act with intent when breaking the law. However, their sense of importance about what they are doing motivates their behavior far more than any sense of fear of punishment or simple respect of someone else's property.

2. Incident investigation
    a. Attorney as lead investigator (breach counsel)
    Organizations can attempt to cloak a risk assessment from disclosure by employing legal counsel to manage the review process. In this scenario, counsel would be retained by the organization to provide legal advice regarding data security exposures, and to develop a strategy for risk minimization. As part of this process, counsel, rather than the organization, would retain an independent cyber consultant to assist in the due diligence analysis and in the preparation of a cyber risk assessment report detailing the organization's vulnerabilities, threats and lack of controls, as well as

recommendations for addressing these issues. The report would be addressed to counsel, which would then be incorporated into a more comprehensive report for the organization.

b. Compromise Investigation / Computer Forensics
Breach counsel will retain a computer forensics specialist to determine the scope and extent of the occurrence, a process of remediation, cause and origin, and whether there was any data exfiltration.

c. Data analysis
If data exfiltration is confirmed, breach counsel will analyze the impacted data to determine whether any PII, PHI or other sensitive information was impacted.

d. Damages Assessment
The insured works with counsel to determine all aspects of damages and potential damages flowing from incident.

i. Ransomware
Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.

3. Notification

a. When to notify?
Importantly, not all occurrences result in consumer or regulatory notifications. Breach counsel will make recommendations to determine whether to notify the consumer based on the type of data that was compromised and other mitigating factors such as whether there is a risk to the rights of natural persons.

b. Changes in state federal and international data breach laws
The European Union GDPR has changed the landscape of data breach law. The following is a non-exhaustive list of **essentia**l actions with GDPR in mind.
Companies that collect any personal information from EU consumers ***must***:

- **Address Privacy at Highest Level**. Your Board / C-Suite / Senior Management must formally work on (and document such work in formal corporate records) development of a GDPR compliance strategy and direction/oversight of appropriate managers.
- **Data Mapping.** Determine where relevant data is collected and stored and how it gets from one point to the other,
- **Understand Expanded Coverage and Obligations**. The GDPR is not like its various predecessors. Under GDPR, even *minimal connections* of consumers not physically situated in the EU, may trigger application of the rules. Even US website operators need to be cognizant of and responsive to potential implications. To be clear, compliance – even substantial compliance - *requires changes* which are far more comprehensive that simply revising a website privacy policy.

- **Designate Responsible Managers**. Your company must (and others may benefit from doing so) formally *designate a qualified Data Protection Officer* who is responsible for the organization's privacy efforts. The DPO must be vested with appropriate authority to implement applicable requirements and possess pertinent knowledge and training
- **Think Affirmatively … to Consumer Consent**! Strongly *consider requiring affirmative consent* – i.e. checking a box, and not presenting a pre-checked box - from consumers to the collection and sharing of ALL personal information. Even under US law, such consents are often required. Even when not required, we believe it is the best practice to obtain them for all consumer data collection even if not required in a particular case.

- **Do Better Due Diligence ...** If your company utilizes a cloud or SaaS vendor for the storage or processing of sensitive (including personal) information, you must expressly discuss with, engage in meaningful technical review of and *confirm in writing* such provider's technical ability to itself comply with GDPR. Address whether vendors are Privacy Shield certified.
- **Have a Better Contracting Process**. Your agreements with third party providers must contain robust warranties, covenants and indemnities expressly pertaining to GDPR non-compliance. Discuss with us whether your company is a 'data controller' within the meaning of GDPR and the significance of such status. Data controllers should expect that their consumers will demand such robust privacy commitments.
- **Procure Appropriate Insurance Including Cyber Insurance**. Talk to your risk managers and insurance professionals as to your company's specific insurance needs. Some form of stand-alone cyber-liability is typically advisable. FisherBroyles attorneys can assist through the underwriting process that may now include detailed review of GDPR compliance efforts.
- **Consider M&A and Finance Protocol.** The two preceding points must be taken into account if you are considering the purchase of or lending money to a business with any EU connections in the same manner as more traditional legal, accounting, contract and physical asset due diligence.
- **Modify Website Policies**. GDPR significantly expands the rights of individuals to know about the sharing and use of their data as well as a totally new 'right to be forgotten, that is (in essence) to avoid their name coming up in web searches and have their records eradicated altogether. Public facing policies must be appropriately revised. Of course, there must also be actual compliance with the revised policies and so accompanying systems and practices will have to be modified accordingly.
- **Consider Location/relocation of Servers.** Companies collecting large amounts of data pertaining to EU citizens must consider where relevant servers should be physically situated to facilitate more efficient compliance with GDPR data transfer requirements.

4. Business Interruption & Other First Party

In response to cyber occurrences, policyholders may attempt to seek coverage under "business interruption" insurance which provided a policyholder with coverage for losses when the policyholder cannot continue its business operations due to a covered risk and when the policyholder suffers a loss of profits. Stated another way, it provides compensation for loss of profits or earnings that an insured loses because of a covered peril. The coverage is for net profits and other income that would have been earned but for the interruption. The loss must be caused by a fortuitous event inflicting physical injury to tangible property. That is, the event leading to the loss must be accidental. In addition, most business-interruption policies require that the suspension or interruption of business be caused by property damage. Again, that means physical injury to tangible property. Corrupted computer programs or data may or may not fall within this meaning. Finally, business-interruption policies typically compensate for profits or operating expense that are lost for the period of "repair or restoration" and require that there be a complete cessation of business or operations.

III. Third Party Issues

1. Litigation
    a. Article III Standing - Despite recent Supreme Court decisions commenting on the issue of constitutional standing, the Court has not directly addressed the issue in connection with cyber and privacy litigation. Circuit Courts have decided the issue in both directions.
        i. *Remijas v. Neiman Marcus* (7th Cir. 2015) and *Dieffenbach v. Barnes & Noble* (7th Cir. 2018): In *Remijas,* the Seventh Circuit ruled that the plaintiffs in that matter had demonstrated an "objectively reasonable likelihood" that harm would occur and consequently satisfied the constitutional standing requirement under Article III. In *Dieffenbach*, the Seventh Circuit rejected the district court's conclusion that the putative plaintiff's complaint failed to adequately plead damages. The Court held the plaintiffs' allegations of time spent addressing the breach, loss of availability of funds in their accounts, and payment for credit monitoring services were adequate under applicable state law to sustain the cause of action and proceed in litigation.
        ii. *Galaria v. Nationwide Mutual Insurance Co.* (6th Circuit, 2016): The The Sixth Circuit ruled that the increased risk of identity fraud was a sufficiently cognizable enough injury under Article III. The Sixth Circuit noted that, "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for [] fraudulent purposes…."
        iii. *In re SuperValu, Inc.* (8th Cir. 2017): The Eighth Circuit found no standing stating that plaintiffs could not "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *One

plaintiff was allowed to proceed with his claim because there was evidence of actual identity theft in that individual's circumstances.

iv. *Whalen v. Michaels Stores, Inc.* (2d. Cir. 2017): The Second Circuit found that the plaintiff had not suffered a "particularized and concrete injury" because there was no evidence of out of pocked damages. The court there also noted that the plaintiff did not face a risk of future harm where her credit card had been immediately replaced by the financial institution after it had been stolen.

v. *Attias v. Carefirst, Inc.* (D.C. Cir. 2017): The D.C. Circuit reversed the district court's dismissal for lack of standing, finding that "a substantial risk of harm exists already, ***simply by virtue of the hack and the nature of the data*** that the plaintiffs allege was taken." Emphasis added/

vi. *In re Zappos.com, Inc.,* (9th Cir. 2018): The Ninth Circuit held that even the plaintiffs that had only alleged that financial losses were "imminent" also had sufficient standing to sue. The Ninth Circuit noted that the "substantial risk that the harm will occur" is sufficient to satisfy Article III standing.

2. Federal Regulatory / Administrative Fines & Investigation

a. Federal Trade Commission

In FTC v. Wyndham Worldwide Corp. Federal Trade Commission ("FTC") action filed against Wyndham Worldwide Corp. ("Wyndham") under Section 5 of the FTC Act, which prohibits "unfair and deceptive acts or practices." Recent developments in the FTC action carry implications for cyber liability and how companies handle cyber security and data breaches.

On April 7, 2014, US District Judge Esther Salas denied Wyndham's motion to dismiss directly challenging the FTC's authority to regulate cyber security practices. Wyndham's motion asserted that Congress had not delegated such authority to the FTC under its Section 5 powers, and even if it did, the FTC failed to publish rules or regulations providing companies fair notice of the protections expected and "legal standards" to be enforced by the FTC. At the time, Judge Salas unequivocally ruled in favor of the FTC's authority. However, on June 23, 2014, the Court granted Wyndham's application and certified the matter for an immediate interlocutory appeal to the Third Circuit Court of Appeals.

The appeal involves two questions of law: (1) whether the FTC can bring an unfairness claim involving data security under Section 5 of the FTC Act and (2) whether the FTC must formally promulgate regulations before bringing its unfairness claim under Section 5 of the FTC Act.

Interlocutory appeals are rarely granted, are in the complete discretion of the trial court, and must meet certain requirements under 28 U.S.C. § 1292(b), including whether there is a substantial ground for difference of opinion on the matter. While Judge Salas's denial of Wyndham's motion to dismiss was certain as to the FTC's Section 5 authority and the issue of fair

notice, the Order certifying the matter for interlocutory appeal on the other hand, acknowledged Wyndham's "statutory authority and fair-notice challenges confront this Court with novel, complex statutory interpretation issues that give rise to a substantial ground for difference of opinion."
The Court further acknowledged that it was dealing with an issue of first impression with "nationwide significance… which indisputably affects consumers and businesses in a climate where we collectively struggle to maintain privacy while enjoying the benefits of the digital age."
As a result, the Third Circuit will be the first major appellate court to weigh in on the issue of whether the FTC has authority to regulate cyber security practices, and if so whether those regulations require specific legal standards and fair notice to those within the scope of FTC's enforcement.

b. Health and Human Services Office Civil Rights

The U.S. Department of Health and Human Services' Office for Civil Rights ("OCR") has notably increased enforcement of compliance with the Health Insurance Portability and Accountability Act ("HIPAA") and Health Information Technology for Economic and Clinical Health ("HITECH") privacy and data security rules regarding patients' protected health information ("PHI").

In addition to relying on self-reported breaches of patient data, the OCR is forming a "permanent audit program" that will monitor compliance with patient privacy rules by both medical service providers as well as by associated entities, such as billing companies. The OCR plans to audit hundreds of covered entities regarding PHI data security and computer network practices. Selected entities will receive notification and data requests this year.

The OCR audits are particularly designed to enhance compliance with data security standards for PHI kept on mobile devices. Typically, under HIPPA and HITECH, entities must self-report to the OCR breaches of patient data involving more than 500 individuals within 60 days of an event.

As the use of mobile devices like laptop computers, smart phones and tablets to store and access PHI continues to increase, several recent enforcement actions illustrate the risk posed to policyholders.

c. State Attorneys General
    i. Coordination between offices – Many state attorney generals are using technology to share breach information and threat information with one another.
    ii. Overlap between security and privacy.

IV. Relationship Between Claims and Underwriting

Facts about Your Applicant

A. Security Assessment:

1. Security ISO 27001/2 based conference call or supplemental app

2. Self-Assessment

B. Granular Analysis

1. Industry
2. Size
3. Type of data
4. Risk Management

a. People
b. Process
c. Technology

5. Incident response plan

V. Obstacles and issues

A. Silent Cyber

Traditional policies often do not specifically refer to cyber-related risks and are considered “silent”. Theoretically afford coverage for cyber losses in certain circumstances. Ambiguity in the eyes of the Policyholder. Unaccounted-for liability exposure for the Insurer

B. Property damage or bodily injury arising out of a cyber occurrence
C. Biometrics
D. Mobility
E. Internet of Things
F. Critical Infrastructure
G. Supply-chain interruption
H. Cyber-terrorism
I. “Hacktivism”
J. SaaS, PaaS, etc.
K. Social Engineering
L. Blockchain / Distributive Ledger Technology