
**2016 CLM Annual Conference**
**April 6-8, 2016**
**Orlando, FL**

# TALES FROM THE CYBER FRONT-LINES

## I. Cyber-Risk Defined

### Understanding the Nature of a Cyber Attack

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 as 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 a web spider 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.

### Exploring the Motivation of the Attackers

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.

## II. Responding to a Cyber Occurrence

### Compromise Investigation

The primary focus of the compromise investigation is to confirm the indicated avenue of the event and identify the post event network activity related to system infiltration and data exfiltration. Additionally, the compromise investigation identifies additional compromised endpoints and user accounts.

- Understand potential breadth and scale of the incident
- Identify locations of potentially compromised systems
- Identify and examine logs available for the incident
- Determine any priority systems or logs with a tier based system for further collection and examination
- Identify if an immediate, remote assessment or collection is required.

### Damage Assessment

The damage assessment focuses on ascertaining the data accessed or exposed, as well as providing an understanding of what the adversary sought, and what relevant issues will need to be addressed in future actions. The damage assessment can also provide further guidance on the impact of the data exfiltration on the victim's operations.

- Files accessed
- Indicators of file use and adversary intelligence gathering
- Files potentially or actually exfiltrated
- Adversary's next steps

**Remediation**

During remediation, systems are brought back to normal as quickly as possible while ridding the systems of the intruder. Additionally, incident indicators and system/application patch levels are utilized to identify short-, mid- and long-term remediation efforts that can further bolster the victim organization's security posture.

- Identify exploited known vulnerabilities
- Identify unknown vulnerabilities
- Recommend patching and upgrades
- System off-lining and rebuilding
- Long term remediation project

## III. Legal Considerations in Cyber-Risk

**Attorney as Quarter Back**

A significant concern of organizations is that the written reports generated at the culmination of security risk assessments, whether conducted internally or by an external party, may provide a roadmap for an adversary in some future proceeding. It is important for organizations seeking to protect such reports from unwanted discovery.

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.

**First Party Issues**

First-party damages are typically defined as damages suffered by policyholders to their own property. If a first party policy holder / property owner suffers damage to its own computer systems, network, and (in some cases) software applications, a claim will be filed under the first party insurance policy. These first party claims are typically for the replacement cost or remediation estimated cost associated with the damaged property.

**State Notice Laws**

On April 10, 2014, Kentucky became the 47th state to enact data breach notification laws. The new Kentucky law applies to "Information Holder[s]," defined as a persons or business entities that conduct business in Kentucky, including both those that own the personal information they maintain and those that maintain personal information for third parties.

The new law requires notification of the affected class of a data beach "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement". While the new law does not require notice to the Kentucky Attorney General or other any other state regulator, it does require notification to the consumer reporting agencies, again, "without unreasonable delay" if more than 1,000 Kentucky residents are impacted.

New Mexico is one of the three remaining states without data breach notification laws in place. However, H.B. 224, the newly proposed legislation would require businesses to notify customers of any breach allowing access to unencrypted personal information within 45 days. The law also requires notification to the state attorney general if more than fifty residents of the state are affected. Should New Mexico's bill be made law, Alabama and South Dakota would be the only states left without data protection laws in place.

Multiple states have also proposed legislation to strengthen laws already in place.

Florida recently enacted more stringent data privacy laws to bolster its existing statutes. Under the new Florida Information Protection Act of 2014 (FIPA), written notice to the Attorney General is required within thirty days for a data breach affecting more than 500 Floridians. Prior legislation allowed entities 45 days to provide such notice in instances where personal information was compromised.

FIPA also expands the definition of personal information to include user names and email addresses when passwords, security questions, or alternative information that allow access to an online account are also accessed. FIPA requires reporting to appropriate consumer protection agencies when a breach results in notification to an affected class of 1,000 or more people. FIPA took effect July 1, 2014.

That same day, Delaware's reinforced data laws went into effect. In particular, the new law affirmatively requires businesses to take "reasonable steps" when disposing consumers' personal identifying information to destroy or erase or otherwise make the protected data indecipherable. Notably, the Delaware's new law does not apply to financial institutions, credit reporting agencies or healthcare providers which are all subject their respective federal statutes.

Minnesota also recently proposed an amendment to its data breach notification statute which would require notification to individuals whose personal information had been

breached within 48 hours of such a discovery. Minnesota law currently only requires notification "without unreasonable delay". The bill would expand notification requirements beyond Minnesota residents to "any individual" affected by the breach. The amendment further requires businesses to make available one year of free credit monitoring services to affected individuals within thirty days of the breach.

### Business Interruption

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.

## Third Party Issues

### Litigation & Article III Standing

Recently, in its decision in In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litigation, 2014 U.S. Dist. LEXIS 64125, the United States District Court for the District of Columbia dismissed all but two claims in a consolidated data breach class action law suit on the basis that the plaintiffs lacked requisite constitutional standing to sustain the litigation.

The class action arose out of a 2011 data breach, specifically, the theft of unencrypted backup tapes that contained Protected Health Information ("PHI") for millions of military members and their families from the parked car of an SAIC employee.

Plaintiffs, who are potential victims of the data breach, filed the consolidated law suit alleging harm from an increased likelihood of identity theft and from an invasion of their privacy, among other things. Defendant filed a motion to dismiss arguing that the Plaintiffs lack standing to pursue relief since they cannot allege that they suffered an actual cognizable injury.

In granting the motion to dismiss, the Court agreed with a developing body of law "that the mere loss of data – without evidence that it has been either viewed or misused – does not constitute an injury sufficient to confer standing."

The Court cited the 2013 U.S. Supreme Court case, Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013) for the following principles as they relate to Article III standing, namely that "an injury must be present or certainly impending, that an attenuated chain of possibilities does not confer standing, and that plaintiffs cannot create standing by taking steps to avoid an otherwise speculative harm". Clapper, 133 S. Ct. at 1151.

For the SAIC Plaintiffs, however, the Court found that increased risk of identity theft and monitoring costs were entirely speculative and dependent on the unknown actions of the person or persons that stole the tapes. While the Court was sympathetic to the uncertainty encountered by plaintiffs as to whether their personal information would be misused, the threatened risk did not constitute an actual injury to confer standing. Likewise, monitoring costs to prevent future harm was not enough to confer standing where plaintiffs failed to show identify theft was impending or a "substantial risk" to the group. The Court also refused to confer standing based on plaintiffs' "invasion of privacy" claims holding that the majority of plaintiffs have not (or could not) allege that their personal information had been disclosed to a third party, and thus, any injury was, at best, speculative.

In re SAIC follows the 2013 decision in In re Barnes & Noble Pin Pad, 2013 U.S. Dist. LEXIS 125730, (N.D. Ill. Sept. 3, 2013), where the Court also cited Clapper in dismissing data breach claims for lack of Article III standing.

**Federal Regulatory / Administrative Fines & Investigation**

**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.

## 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 plans to include business associates in the scope of its audit program by 2015.

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.

Most recently, the OCR obtained an approximately $1.7 million settlement with Humana subsidiary Concentra Health Services related to the theft of two unencrypted laptops containing PHI data about approximately 1,770 patients. The OCR investigation also revealed several other breaches involving fewer than 500 individuals. $1.7 million for two laptops.

Similarly, the OCR recently agreed to a $250,000 monetary settlement with ACA Health Plan, Inc. of Arkansas related to an unencrypted laptop containing electronic PHI data of 148 individuals that was stolen from an ACA representative's car.

These and other similar settlements indicate that the OCR is taking a more proactive approach to investigating and deterring potential breaches of the HIPPA and HITECH privacy and security rules. Policyholders must take diligent steps to ensure that PHI—particularly on mobile devices—is properly encrypted and protected from disclosure.

Finally, we note that the scope of OCR's authority is expansive and its enforcement efforts are still young. How the OCR defines "business associates" for purposes of enforcement will, in part, determine the limit of its scope. It is presumed that the OCR will include medical billing services and laboratory testing facilities within the scope of its enforcement efforts. Will it also include medical malpractice law firms and information technology service providers? What about janitorial services and cloud-storage providers?

**Security Exchange Commission**

Cyber is still a relatively young risk and the various stakeholders in cyber-risk are at times, still trying to determine their particular role. This includes the officers and/or directors of companies for establishing enterprise policies, the information technology professionals charged with protecting data security and risk managers trying to minimize company exposure.

However, the regulators themselves are also trying to determine their particular place in data security. For example, this blog has previously discussed the role of the Federal Trade Commission and its prosecution of companies for poor data security policies and practices.

In this regard, public companies may soon be required to file a Securities and Exchange Commission ("SEC") Form 8-K after experiencing a cybersecurity event. The 8-K form, (which also still contains disclosure requirements for other less technology-driven events like coal mine shutdowns), can now be used to report material cyber events. While the 8-K form itself has not yet been amended to include a disclosure requirement for cyber-events, it is quickly becoming a "best practice" to make such disclosures using the 8-K

form. After the late 2013 Target data breach, the company formally disclosed same to the SEC via an 8-K form on February 26, 2014.

In accordance with the SEC "guidelines," it is recommended that material cyber breaches and even potential cyber-risks be disclosed via the 8-K form. The SEC, however, has not yet issued any formal rules regarding what cyber events require disclosure. As always, the disclosure obligation turns on whether the cyber event is material.

The SEC applies its traditional definition of materiality to cyber events: "[i]nformation is considered material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would significantly alter the total mix of information made available."

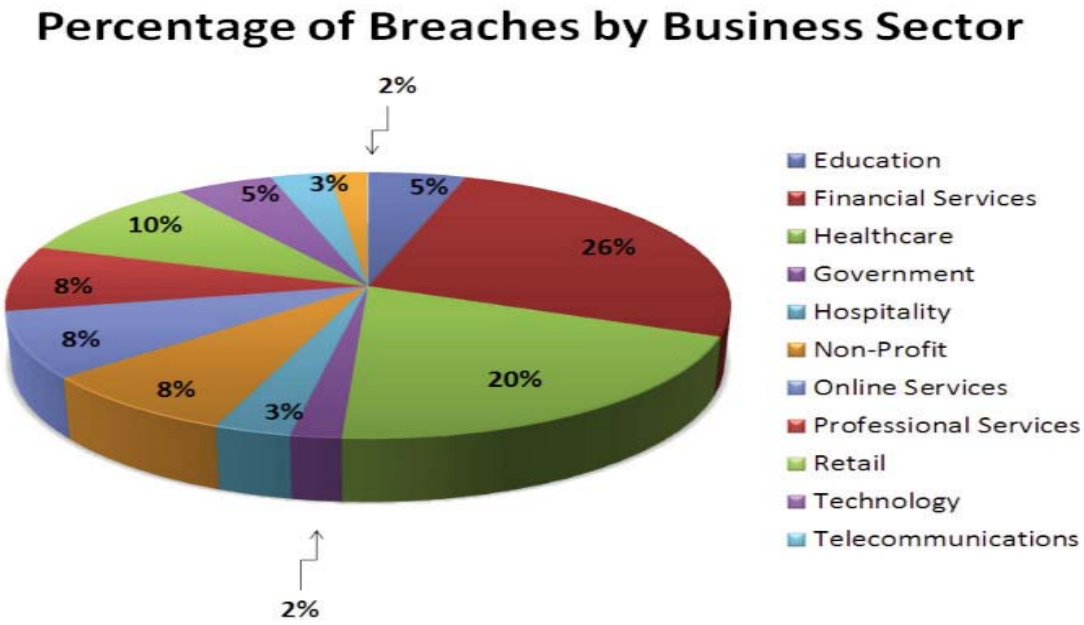
The 8-K form already requires disclosure of "material impairments" which includes disclosure of impairment to any of the company's assets including goodwill. Therefore, breaches of private consumer information, while not necessarily impacting a company's assets, may in any event require disclosure. After Target's data breach, its customer traffic hit its lowest point in the three years prior. Given the SEC guidance and the broad definition of materiality, more and more companies may consider filing 8-K disclosures in connection with data breaches.

In addition to actual breaches, SEC "guidance" indicates disclosure obligations for potential cyber risks. In April of this year, the SEC Office of Compliance Inspections and Examinations ("OCIE") issued a sample list of requests for information it may make to public companies including, but not limited to whether the company has a Chief Information Security Officer ("CISO") or equivalent position, any contingency/ response plans in place in the event of a cyber incident, an inventory of devices interfacing with customer data as well as an inventory of software and applications on the company's data system or network. The OCIE may even go so far as to request design drawings of network architecture.

OCIE will also look for whether companies have implemented cybersecurity risk management standards such as those recently recommended by the National Institute of Standards and Technology ("NIST"). Companies that store private consumer information will face further scrutiny including disclosure of authentication methods. Not only will OCIE request information regarding the company's cybersecurity standards, but also those of any third party vendor it may use that has access to the company's data.

Finally, OCIE will seek information regarding a company's practice of identifying data breaches that do occur, including information regarding penetration testing of IT systems and networks for weaknesses as well as how actual breaches are detected, tracked and responded to.

## IV. Underwriting Cyber Risk




NetDiligence's 2013 Cyber Liability & Data Breach Insurance Claims

**Who is 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. Takeaways

A. Advances in Technology
   a. Software as a Service
   b. Platform as a Service
   c. Internet of Things

B. Sophisticated Marketplace
   a. Broker sophistication
   b. Cyber in the Headlines
   c. Educated marketplace

C. Mobility

D. Big Data