DOCKET MEDIA LLC

PHONE: (424) 2-DOCKET
WWW.CYBERSECURITYDOCKET.COM
EDITOR@CYBERSECURITYDOCKET.COM

CYBERSECURITY DOCKET
GLOBAL CYBERSECURITY AND INCIDENT RESPONSE REPORT

# CYBER INSURANCE: A PRAGMATIC APPROACH TO A GROWING NECESSITY

BY JOHN REED STARK AND DAVID R. FONTAINE[1]

For today's public and private companies, cyber-attacks are not a matter of "if" but "when," and managing cybersecurity issues has become more a matter of corporate survival than an IT department line item. As so many cybersecurity experts have noted, "There's a saying in the cybersecurity industry that there are two types of businesses today: Those that have been breached and know it and those that have been breached and just don't know it."[2]

To manage this burgeoning yet still nascent threat, just like other routine day-to-day risk and hazards, companies have started to include cybersecurity concerns when considering enterprise risk management and insurance risk transfer mechanisms - such as cyber insurance. There is little doubt that cyber insurance will soon become yet another basic element of a company's overall insurance coverage program, just like general comprehensive liability, professional liability and officers and directors coverage. [3]

---

[1] John Reed Stark is President of John Reed Stark Consulting LLC, a data breach incident response and digital compliance firm. Mr. Stark has managed cybersecurity projects and incident response investigations for two decades, including 11 years as founder and chief of the SEC's Office of Internet Enforcement. He also served for 15 years as an Adjunct Professor at Georgetown University Law School teaching a law and technology course. David Fontaine is Executive Vice President, Chief Legal & Administrative Officer and Corporate Secretary of Altegrity, a privately held company that among other entities owns Kroll's data breach response services.

[2] "What's Next for Cyber Insurance?" By Andrea Wells, Insurance Journal (April 21, 2014) available at http://www.insurancejournal.com/magazines/features/2014/04/21/326382.htm

[3] See e.g. "Within six years, we're going to be well on our way to everyone having cyber insurance as just a basic set of insurance, just like property insurance," said Ari Schwartz, director for cybersecurity on the White House National Security Council, during a Sept. 8, 2014 panel discussion at the Nextgov Prime conference. "Cyber Coverage Will be a Basic Insurance Policy by 2020," By Aliya Sternstein, September 8, 2014 available at http://www.nextgov.com/cybersecurity/2014/09/wh-official-cyber-coverage-will-be-basic-insurance-policy-2020/93503/ ; http://www.pillsburylaw.com/publications/cyber-insurancemitigating-loss-from-cyber-attacks ("Cyber Insurance—Mitigating Loss from Cyber Attacks," by Rene L. Siemens, David L. Beck Pilsbury's Perspectives on Insurance Recovery Newsletter (Summer 2012) ("The market is rapidly growing for insurance that is specifically meant to cover losses arising out of cyber attacks and other privacy and data security breaches. These insurance policies are marketed under names like 'cyber-liability insurance,' 'privacy breach insurance' and

Today, a cyber-attack potentially implicates several different types of insurance coverage – depending on such factors as the type of attack, the extent, if any, of data loss, the relationship of the parties, the nature of the data involved (e.g. personal information, intellectual property, trade secrets, emails, etc.), the type of policy in issue and, if for third-party liability, the allegations asserted and the type of damages in issue.

Yet while the market for cyber insurance continues to grow dramatically,[4] no standard form of cyber insurance policy language has materialized. And, whether standard property casualty provisions even cover losses attributable to cyber incidents, remains subject to interpretation and potential dispute.[5]

In addition, the actuarial challenges of predicting/gauging the potential impacts of a cyber-attack can, in turn, make it difficult to match a cyber insurance policy with the unique risk profiles of global and technologically sophisticated companies; these are difficulties faced not only by insurance providers but also by even the most experienced executive team. Cyber-attack

---

'network security insurance.' Many companies and other institutions that handle legally protected information now view this kind of insurance as an essential part of their coverage programs.")

[4] "Demand for Cyber Insurance Skyrockets," by Corey Bennett (January 15, 2015) available at http://thehill.com/policy/cybersecurity/229568-skyrocketing-demand-seen-for-cybersecurity-insurance. See, also "Why Cyber-insurance Will be the Next Big Thing" by Mary Thompson (July 1, 2014) available at http://www.cnbc.com/id/101804150#; "Should Your Company Get Cybersecurity Insurance?" by Will Yakowicz, (December 17, 2014) available at http://www.inc.com/will-yakowicz/does-your-company-need-cybersecurity-incurance.html

[5] Relying on a general property insurance policy for cyber-attack coverage is risky. For example, in the data breach involving Sony, the breach reportedly exposed the personal information of tens of millions of users, and Zurich American stated in court papers that as a result, Sony was the defendant in over 50 class action lawsuits. Because the Sony policy required the policyholder (Sony) to perpetrate or commit the act of publication of the personal information, the judge stated., "Paragraph E (oral or written publication in any manner of the material that violates a person's right to privacy) requires an act by some kind of act or conduct by the policyholder in order for coverage to present." This decision highlights the hazards of relying on traditional CGL coverage policies for potential data breach coverage. *See*, *Zurich American Insurance Co. v. Sony Corp. of America, et al* (Supreme Court , State of New York 651982/2011). *But see Hartford Casualty Insurance Company v. Corcino & Associates et al* , where the District Court of the Central District of California ruled there is coverage under a GCL policy for a data breach involving hospital records of some 2,000 patients. *See also*, *Ward General Services, Inc. v. Employers Fire Ins. Co*., 114 Cal.App.4th 548, 556-57 (Cal.App. 4 Dist. 2003); *Southeast Mental Healthcare Center, Inc. v. Pacific Insurance Company, LTD*, 439 F.Supp.2d 831, 838-839 (W.D. Tenn. 2006); *America Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89, 93-98 (4th Cir.2003); *State Auto Property & Cas. Ins. Co. v. Midwest Computers & More*, 147 F.Supp.2d 1113 (W.D.Okla. 2001). Courts reaching a different conclusion have done so where the data is permanently lost to its owner, not merely improperly accessed. *See Computer Corner, Inc. v. Fireman's Fund Ins. Co.*, 46 P.3d 1264 (N.M. 2002) (holding loss of the pre-existing electronic data was tangible property damage covered by CGL policy where computer store repairing customer's computer permanently lost all the data); *American Guar. & Liab. Ins. Co. v. Ingram Micro, Inc*., 2000 WL 726789, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 18, 2000) (holding that computer data permanently lost during a power outage constituted "direct physical loss or damage from any cause" covered by first-party insurance policy); *NMS Services Inc. v. Hartford*, 62 Fed.Appx. 511 (4th Cir. 2003) (characterizing the erasure of vital computer files and databases as direct physical loss or damage to property for purposes of business income coverage).

damages are so multifaceted and unique – much more so than fire, flood, and other more traditional disaster scenarios – that there is no normal distribution of cyber-attack outcomes on which to assess the probabilities of future events and impacts. As a result, there are now a dizzying array of cyber insurance products in the marketplace, each with its own insurer-drafted terms and conditions, which can vary dramatically from insurer to insurer – some effective and comprehensive and others replete with loopholes, exclusions and other confusing features.[6]

Even the U.S. Department of Homeland Security has officially acknowledged that the cyber insurance market remains challenging for most companies to understand and can be overlooked for all of the wrong reasons:

> Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection. Many companies forego available policies, however, citing as rationales the perceived high cost of those policies, confusion about what they cover, and uncertainty that their organizations will suffer a cyber attack.[7]

To make matters worse, as opposed to disasters like fires, floods, tornadoes, etc., companies that experience a cyber-attack should not expect any assistance or even compassion from governmental bodies. In fact, for a variety of reasons, companies need to anticipate and plan for just the opposite: 1) U.S. government agencies are overwhelmed with protecting the nation's own infrastructure and do not have a SWAT team or a rescue team standing-by to assist individual U.S. companies in the defense or response to a cyber-attack;[8] 2) given the forty-seven or so separate state privacy statutory regimes and a growing range of federal agency jurisdiction (each wielding its own unique set of rules, regulations, laws and enforcement tools), instead of a helping hand, cyber-attack victims should expect subpoenas, enforcement actions and an onslaught of litigation; and 3) the public's view of cyber-attack victims is a skewed one, often

[6] "Many 'Loopholes' in Cyber Insurance Policies, L'Oreal CISO Says," By Clint Boulton, Wall Street Journal (October 3, 2014) available at http://blogs.wsj.com/cio/2014/10/03/many-loopholes-in-cyber-insurance-policies-loreal-ciso-says/; "Cyber Insurance: Worth it, but Beware of the Exclusions," by Taylor Armerding (October 20, 2014) available at http://www.csoonline.com/article/2835274/cyber-attacks-espionage/cyber-insurance-worth-it-but-beware-of-the-exclusions.html.

[7] http://www.dhs.gov/publication/cybersecurity-insurance.

[8] Testimony of Robert Anderson, Jr., Executive Assistant Director, Criminal, Cyber, Response, and Services Branch Federal Bureau of Investigation, Statement Before the Senate Committee on Homeland Security and Governmental Affairs, Washington, D.C., September 10, 2014 available at http://www.fbi.gov/news/testimony/cyber-security-terrorism-and-beyond-addressing-evolving-threats-to-the-homeland.

defined by anger, vilification and blame-casting, instead of understanding and recognition regarding the extent and nature of this very real threat to all types of companies.[9]

So what can companies do to protect against the damaging consequences of the emerging and in some ways immeasurable impacts of a cyber-attack? Traditionally, purchasing insurance coverage begins with a policy review, a risk breakdown and a range of other risk-related analytics. This article suggests a different approach towards the overall risk analysis.

We believe that a company should begin with a review of actual cyber-attacks experienced by others, analyzing and scrutinizing the typical cyber-incident response workflow and so-called "workstreams" that typically follow most cyber incidents. By analyzing and revisiting the practicalities and economics of these workstreams, a company can then collaborate with its insurance brokers and originators to allocate risk responsibly and determine, before any cyber-attack occurs, which workstream costs will be subject to coverage; which workstream costs will fall outside of the coverage; and which workstream costs might be uninsurable.

Akin to when someone with a genetic history of heart disease consults with a cardiologist to help identify the most suitable health insurance or when a new homeowner consults with a local firefighter to help identify the most appropriate property and casualty insurance, this methodology assesses risk from a practical and experiential point of view.

Along these lines, this article sets forth a *laundry list* of typical workstreams routinely experienced by a cyber-attack first responder who has handled cyber-attacks and data breaches for both government and private organizations for over 20 years, combined with the experience of a seasoned general counsel who has faced the challenges associated with a cyber-attack and dealt with issues relating to both obtaining and utilizing cyber insurance.[10]

## I. <u>Initial Response Workflow</u>

---

[9] "Fury and Frustration over Target Data Breach," by Anne D'Innocenzio and Bree Fowler, USA Today, available at http://www.usatoday.com/story/money/business/2013/12/20/fury-and-frustration-over-target-data-breach/4145503/.

[10] Two quick and important qualifications before beginning:

1) Given the unique technological signature of today's public and private companies, this list cannot present or even contemplate every workstream resulting from every cyber-attack. Rather, this list provides a solid basis for understanding and predicting the typical workstream-related costs related to the aftermath of a typical cyber-attack; and

2) These workstreams relate to tasks undertaken for managing of a cyber-attack, but not to the loss of business that will inevitably ensue after a cyber-attack. For instance, after a cyber-attack, business is typically lost not just because of the technological impact on the enterprise but also because of the extraordinary drag and distraction a cyber-attack imposes on a company, including its executive management (and not just its front line information technology personnel).

### 1. Preservation

Every response to a cyber-attack begins with the simple notion of preservation, i.e. collecting and preserving, in a forensically sound and evidentiary unassailable manner, any "electronically stored information" ("ESI"), devices, logs, etc. that could become relevant to investigation of the cyber-attack as well as to the defense of any subsequent claims or regulatory demands.[11]

Preservation is a critical workstream because incident responders will be scrutinizing every byte of data, including any fragments, artifacts or remnants left by the attacker in all sectors of any relevant device, including "deleted recoverable files,"[12] "unallocated and slack space"[13] or the boot sector.[14] These artifacts can include: Internet addresses; computer names; malicious file names; system registry data; user account names; and network protocols.

An equally important goal of preservation is to enable investigators to scour all ESI in search of

---

[11] With respect to logging, the type and preservation of logs can differ dramatically among companies – some companies may not have any log management system that aggregates logging information, which means that its logging information will be scattered and disorganized. Also, some companies may only preserve logs for a short period, such as thirty days, before "rolling over them" and thereby deleting the logs permanently.

[12] A ''deleted recoverable file'' is a file that is typically easily recovered with forensic software, such as a Microsoft Word document, PowerPoint presentation, PDF file, etc., where, perhaps unbeknownst to the user, a file record for that data still exists within the file system.

[13] The unallocated space and file slack of desktop or laptop personal computers typically provide important leads for digital forensic examiners. Here's why: Files saved to the hard drive of a computer are typically described as residing in ''allocated space,'' i.e., space on the hard drive allocated by the file system. When a user deletes these so-called ''active files,'' the files usually do not disappear from the hard drive. Rather, the operating system no longer allocates or saves that hard drive space for the file and simply designates that area of the hard drive as unallocated (i.e., unused) space. The data actually stay still—the file system just marks that portion of the drive as usable for other files. Within unallocated space, a digital forensic examiner can usually extract file artifacts, such as deleted files, temporary files (created when a user opens a file), file fragments, deleted internet history and other, albeit disorganized, but readable, bits of data. Indeed, evidence gleaned from unallocated space has become so important in the context of litigation that using a ''wiping program'' to render unrecoverable the artifacts from the unallocated space can even draw a discovery sanction from a judge. *See TR Investors LLC v. Genger*, No. 3994-VCS (Del. Ch. Dec. 9, 2009) (finding defendant Arie Genger in contempt of court for ''wiping'' the ''unallocated space'' of the hard drive of his work computer and file server in the face of an order that prohibited him from ''tampering with, destroying or in any way disposing of any Company-related documents, books or records''). This approach similarly applies to so-called ''slack space'' (that portion of a cluster unused by an active file), which can also contain similar information.

[14] A boot sector is a small piece of hard disk or external storage device space and the first file a Basic Input/Output System ("BIOS") loads when a computer is turned on. There are two main types of sectors: the Master Boot Record ("MBR") and Volume Boot Record ("VBR"). The boot sector can contain computer viruses, which are most commonly spread using physical media. An infected floppy disk or USB drive connected to a computer will transfer when the drive's VBR is read, then modify or replace the existing boot code. The next time a user tries to boot their desktop, the virus will be loaded and run immediately as part of the master boot record. It's also possible for email attachments to contain boot virus code. If opened, these attachments infect the host computer and may contain instructions to send out further batches of email to a user's contact list. Improvements in BIOS architecture have reduced the spread of boot viruses. Kaspersky Lab, "What is a Boot Sector Virus," available at http://usa.kaspersky.com/internet-security-center/definitions/boot-sector-virus.

so-called *personally identifiable information* or "PII." Companies experiencing a cyber-attack must determine whether the attacker exfiltrated (removed from the company's digital environment) any data containing personal information relating to any individuals, who may require notice of the cyber-attack; credit monitoring services; and/or other remedial action.[15] Finally, just about every cyber-attack response involves the forensic imaging and review of emails and other relevant communications from laptop computers, desktop computers, network servers, backup tapes, mobile devices, tablets, etc.

Preserving ESI can quickly become a challenging, costly and resource intensive workstream. Most companies have ESI in so many locations (both physical and virtual) that, after a cyber-attack, they struggle, amid the pressures of a forensic investigation, to locate and preserve relevant ESI and to piece together information about sometimes complex and disparate systems. Relatedly, it can sometimes take days after learning of a cyber-attack before a company remembers (usually because it notices the impacts) of its own electronic purging processes that delete data (such as relevant logging information) on a regular schedule. Without having proactively made the effort to map information sources and their key characteristics, these purging schedules can inadvertently cause sudden and unanticipated causes of spoliation.[16]

The cyber-attack investigation may have been triggered by a customer who complained that his or her data was used for a fraud; from a report that a computer system was found to be communicating with an unscrupulous Internet address; from the Federal Bureau of Investigation ("FBI"), U.S. Air Force Office of Special Investigations ("OSI"); US Secret Service or other law enforcement agency notifying a company of a possible cyber-attack into its systems; or a slew of other sources. Under any circumstance, investigators will first analyze whatever initial information is presented and use the preliminary evidence to help identify the likely locations of attack-related evidence. An investigator will consider all computer devices as likely locations to target for investigation. These devices will typically include: company laptops and workstations; network storage servers; firewalls; intrusion detection systems; webservers; customer databases; and e-mail servers.

The most effective cyber-attack investigative methodology is an iterative process of digital

[15] Protecting *personal identifying information* ("so-called PII") relating to individuals from identity theft has become a significant focus of U.S. state and federal agencies, and of new state and federal laws and regulations. In the U.S., though laws and regulations vary from state to state, and between state and federal law, as to exactly what information comprises PII, generally, the definition requires both a name and some additional item of information that could be used to steal a person's identity or access his or her financial accounts (or, in some cases, healthcare information) without authorization. For purposes of this article, we refer generally to protected information about an individual as PII, even though some state or federal statutes may use a different nomenclature or categorization.

[16] As an aside, where information relevant to identifying and describing potentially accessed/target/exfiltrated systems has never been data-mapped, establishing a strong and effective incident response plan for addressing cybersecurity risks can become difficult. Without any sort of responsible system overview or asset classification exercise, companies not only make mistakes in their cyber incident response plans, but companies can also make mistakes when applying available resources for security.

forensics, malware reverse engineering, monitoring and scanning. As analysis identifies any possible *indicator of compromise* ("IOC"), investigators examine network traffic and logs, in addition to scanning hosts for these IOCs. When this effort reveals additional systems that may have been impacted, those systems are forensically imaged and analyzed, and the process repeats itself.

Initially, the goal is to use the IOCs to determine the initial attack vector, trace the attacker's methods of traversing network segments and identify any malicious files introduced into a company's computer network. Ultimately, armed with the information gained through these efforts, the victim of a cyber-attack can target efforts towards remediating the attack fully, including: removing and quarantining certain machines; eradicating/disassembling malware; rebuilding relevant compromised systems (if possible); resetting account credentials; blocking attacker-related Internet Protocol ("IP") addresses; and strengthening its network and host monitoring tools to detect and block attempted cyber-attacker movement.

If possible, companies will take the extra care to acquire ''forensic bit-for-bit images'' of all relevant devices. Acquiring a forensic image or the production of an exact sector-by-sector copy of any computer, storage device, etc. verifies the completeness and accuracy of recovery while not altering the original media, thus preserving the status quo. Forensic imaging can preserve the ability to reconstruct deleted information, ascertain any evidence of wiping/defragmentation and evaluate the authenticity of data.[17]

Given the typically vast scope and breadth of requests, and the likelihood of hypercritical digital oversight later on, by law enforcement, regulators, class action lawyers or anyone else who may blame the victim for the cyber-attack, companies should strive for best practices during preservation. Best practices can include ironclad ESI collecting methodologies, meticulous protocols and painstaking documentation of evidentiary transitions to ensure an easily defensible and rock-solid evidentiary authentication and chain of custody. This methodology may also include the review the pre/post-acquisition ''hash values''[18] of the data to verify proper imaging of the devices, and verify the forensic collection of the ESI against an external time source (e.g., atomic clock) in order to determine the accuracy of the file system time stamps.
Often, investigative teams prefer a paradigm of ''over-preservation,'' even if the data is likely never to be analyzed.

With respect to warehousing all collected ESI, companies may opt to store the forensic images

[17] It is important to note that the concept of ''materiality'' does not apply in digital forensics. The slightest amount of data can have huge importance, hence the need for comprehensive forensic preservation.

[18] A hash value is a result of a repeatable calculation (hash algorithm) that can be performed on a string of text, electronic file or entire hard drive's contents. Hash values are used to identify and filter duplicate files (i.e., email, attachments, and loose files) from an ESI collection or verify that a forensic image or clone was captured successfully.

in a digital forensic lab facility that employs high-tech security including restricted access, video camera surveillance, evidence safes and other important security measures.

### 2. Digital Forensics Analysis

Given that the preservation phase can extend throughout the course of an entire digital forensic investigation (as the investigators continuously identify new systems that may contain relevant evidence), digital forensic analysis of the collected ESI and systems typically begins concurrently.

The most effective investigative methodology is one based on targeted incident response practices and does not solely rely on "signature detection" technologies, such as antivirus software. As noted above, careful investigators employ an iterative process of digital forensics, malware reverse engineering, monitoring and scanning. As analysis of known or suspected compromised systems identifies new IOCs, investigators will examine network traffic and logs, in addition to scanning hosts for these IOCs. When this effort discovers additional systems, those systems are forensically imaged and analyzed, and the process repeats. Armed with the information gathered during this phase of "lather, rinse, repeat," a victim company can begin efforts to detect additional attempts by the attacker to regain access and get closer towards containment of the attack.

### 3. Logging Analysis

In addition to user systems (like laptop and desktop computers), servers, etc., the logs of other systems such as firewalls and intrusion detection systems will also require preservation and collection. Exactly what logs are available relating to a cyber-attack depends on a company's overall cybersecurity policies and practices.[19] Logging information can include logs relating to events occurring within firewalls, operating systems, applications, anti-virus software, LANDesk,[20] web servers, web proxies, VPNs,[21] change auditors, DHCPs[22] and a broad range of

[19] "Deficiencies in security logging and analysis can allow attackers to hide their location, malware and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records, victims can remain blind to the details of the attack and to subsequent actions taken by the attackers. Sometimes logging records are the only evidence of a successful attack and without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. Many organizations keep useful logs for compliance purposes, but attackers rely on the fact that such organizations might not review their logs regularly, and never discover that that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files." See SANS critical Security Contrl #14 available at https://www.sans.org/critical-security-controls/control/14.

[20] "LANDesk is an asset management software system used to remotely inventory and manage desktop computers. It has the ability to report on installed software and hardware, allow remote assistance, and install operating system security patches." American University Office of Information Technology Frequently Asked Questions About LANDesk available at http://www.american.edu/oit/software/LANDesk-FAQ.cfm

other audit files.[23]

Most free and commercial operating systems, network services and firewall technologies offer logging capabilities containing a treasure trove of relevant evidence. However, understanding this treasure trove typically requires dedicated technical resources (such as a SIM/SEM) as well as specialized digital forensic examiners to conduct the investigative analysis.[24]

### 4. Malware Reverse Engineering

The term "malware" is often defined as software designed to interfere with a computer's normal functioning, such as *viruses* (which can wreak havoc on a system by deleting files or directory information); *spyware* (which can gather data from a user's system without the user knowing it); *worms* (which can replicate themselves in order to spread to other computers -- unlike a computer virus, a worm does not need to attach itself to an existing program)[25]; or *Trojan horses* (which are non-self-replicating programs containing malicious code that, when executed, can carry out an attacker's actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm).

However, the definition of malware is actually far broader and a bit of a misnomer. In the context of a cyber-attack, malware means any sort of program or file that is used by attackers to infiltrate a computer system. Like the screwdriver a burglar uses to gain unlawful entry into a company's headquarters, legitimate software can actually be cited as *malware*. For example, during an *"Advanced Persistent Threat"* or *"APT"* attack,[26] attackers will often use "RAR" files

---

[21] A virtual private network ("VPN") is a network that is constructed by using public wires — usually the Internet — to connect to a private network, such as a company's internal network.

[22] Dynamic Host Configuration Protocol ("DHCP") is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network.

[23] For the best results, such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (VPN, dial-up, etc.) should all be configured for verbose logging, storing all the information available for logging in the event a follow-up investigation is required. Operating systems, especially those of servers, should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, an organization should periodically scan through its logs and compare them with the asset inventory assembled in order to ensure that each managed item actively connected to the network is periodically generating logs.

[24] Analytical programs such as SIM/SEM ("Security Incident Management" or "Security Event Management") solutions for reviewing logs can provide value, but the capabilities employed to analyze audit logs are quite extensive, including just a cursory examination by a digital forensic examiner. Actual correlation tools can make audit logs far more useful for subsequent manual inspection and can be quite helpful in identifying subtle attacks. However, these tools are neither a panacea nor a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand what is gleaned from log files.

[25] "What is the difference between a computer virus and a computer worm?" UCSB ScienceLine, available at http://scienceline.ucsb.edu/getkey.php?key=52.

[26] So-called APT attacks are typically stealthy, sophisticated, targeted and relentless state-sponsored attacks which

as containers for transporting exfiltrated information, yet RAR files have a broad range of legitimate uses and are often used in the context of general corporate activities.[27]

Thus, reverse engineering malware is both an art and a science. Forensic investigators, incident responders, security engineers and IT administrators employ a broad range of practical skills to examine malicious programs that target, access and infect corporate computer systems. Understanding the capabilities of malware is not only critical for responding to information security incidents, but is also critical to an organization's ability to derive threat intelligence and to fortify defenses.

A malware reverse engineering specialist uses a variety of system and network monitoring utilities, a disassembler, a debugger and other tools useful for turning malware inside out. This sort of engineering is critical but costly, with hourly rates more akin to law firm partners than information technology specialists. Even finding a specialist with reverse malware engineering skills can quickly become a challenge -- educational institutions are only just beginning to turn out individuals with malware skills and most malware specialists are self-taught or are "home-grown" within digital forensic firms.

## II. Continual Long-Term Response Workflow

### 1. Surveillance

Once a company experiences a cyber-attack, one of the immediate needs is to "stop the bleeding," which begins with the installation of state-of-the-art surveillance tools. Surveillance tools can provide, for example, full "packet capture" [28] as well as alert devices on all network

---

employ carefully crafted and evolving reconnaissance, low-and-slow approaches that are typically difficult to detect, and are not flagged by antivirus technologies and other traditional cybersecurity tools. In fact, most malware used by APT attackers is undetectable by off-the-shelf antivirus products. The term APT has been coined to describe specific types of adversaries, exploits, and targets used for explicit strategic intelligence gathering goals. Victims of APT attacks include global financial institutions like Citigroup; large U.S. hospital groups like Community Health Systems; worldwide U.S. defense contractors like Northrup Grumman and SAIC; international defense contractors like Israeli defense firms Elisra Group, Israel Aerospace Industries and Rafael Advanced Defense Systems; well-known data security agencies like RSA and even large government agencies like OPM.

[27] Specifically, RAR is the native format of WinRAR archiver. Like other types of archives, RAR files are data containers that store one or several files in the compressed form. After you download a RAR file from Internet, you need to unpack its contents in order to use it. See "RarLab: Rar File Format," http://www.rarlab.com/rar_file.htm

[28] "Computer-network administrators have used packet sniffers for years to monitor their networks and perform diagnostic tests or troubleshoot problems. Essentially, a packet sniffer is a program that can see all of the information passing over the network to which it is connected. As data streams back and forth on the network, the program looks at, or "sniffs," each packet. A packet is a part of a message that has been broken up. Normally, a computer only looks at packets addressed to it and ignores the rest of the traffic on the network. But when a packet sniffer is set up on a computer, the sniffer's network interface is set to promiscuous mode. This means that it is looking at everything that comes through. The amount of traffic largely depends on the location of the computer in the network. A client system out on an isolated branch of the network sees only a small segment of the network traffic, while the main domain server sees almost all of it." http://computer.howstuffworks.com/workplace-

ingress and egress points to monitor for malicious activities on an ongoing basis and to broadcast alerts for unauthorized activity or other indications of compromise (IOCs). Getting these devices up and running not only requires expertise in their installation, but also requires continuing maintenance to swap out hard drives as logging data accumulates. As the data accumulates, additional workflow emerges to review and analyze the captured data, automated surveillance reports and especially, any suspicious notification alerts.

### 2. Remediation

Once forensic analysis is complete or at least well underway, investigators can use the digital forensics and malware evidence to remediate the malware, rebuild compromised systems, reset compromised account credentials, block IP addresses, and properly initiate network and host monitoring in an effort to detect additional attempts by the attacker to regain access. A company will also typically install or improve centralized log management; improve whatever vulnerability management system it had in place at the time of the cyber-attack; and review its password management, which may include for example, an upgrade if appropriate, to two-factor authentication.[29]

In the long-term, remediation can become especially costly because a company victim to a cyber-attack will usually need to install new hardware and software both for fortification and detection – sometimes even having to construct an entirely new network security suite. Victim companies may also want to install state-of-the-art software and hardware designed to identify attacker behavior and their tools, tactics and procedures such as Carbon Black,[30] Palo Alto firewalls[31] or FireEye MIR[32] within the entire attack vector including domain controllers,

---

surveillance2.htm.

[29] "Two-factor authentication adds a second level of authentication to an account log-in. When entering only a username and one password, that is considered single-factor authentication. Two-factor authentication requires the user to have two out of three types of credentials before being able to access an account. The three types are:

- Something known, such as a Personal Identification Number (PIN), password, or a pattern;
- Something in-hand, such as an ATM card, phone, or fob; and
- Something innate, such as a biometric like a fingerprint or voiceprint.

http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/

[30] "Carbon Black, within the Bit9 + Carbon Black Solution, delivers the first true continuous response solution. Carbon Black's primary goal is to reduce the cost and complexity of incident response by providing continuous endpoint visibility and signature-less detection capabilities to deliver full context, attack classification and situational awareness of the threats attacking your enterprise. Carbon Black can automate the tedious and time-consuming data acquisition process by continuously recording and understanding the relationships of the critical data necessary to unravel the full lifecycle and kill chain of an attack." See, https://www.bit9.com/solutions/security-incident-response/.

[31] "Palo Alto firewalls are part of the large suite of Palo Alto cybersecurity appliances designed to manage, implement and optimize new age firewall systems to safely allow applications, and tackle the threat of modern day malware." See, https://www.paloaltonetworks.com/network-infrastructure/cyber-security-appliances.

database servers and user work stations. In addition, companies victimized by a cyber-attack may choose to employ a custom designed scanning program to scan their systems for current and historical IOCs (which can be a worthwhile time and cost saver).

### 3. Exfiltration Analysis

Once the investigative team and the legal team determine that a cyber-attacker may have exfiltrated PII or any other relevant ESI, such as trade secrets,[33] intellectual property, sensitive email content, etc., an entirely new workstream of exfiltration analysis will typically follow. This exfiltration analysis phase of a cyber-attack response typically becomes an intricate and complex ediscovery exercise, which brings with it attendant costs and fees. Moreover, any mistakes made during the exfiltration analysis can have serious financial consequences; careful attention to detail is, therefore, required, otherwise distrust and skepticism can fester among interested parties (such as a regulator, class action plaintiff or other disgruntled party).

For example, if a company falls victim to a cyber-attack and forensic investigators find IOCs on 100 laptops of 100 different users, some companies may opt to conduct custodian interviews of all of the laptop users, to assist in determining whether, for instance, there exists PII on their laptops. However, a more scientific and consistent approach would be to technologically harvest all of the user-created data on those 100 laptops; process that data; warehouse that data on a hosting platform; and design and execute searches of that data geared towards identifying any PII. Aside from being less costly and requiring less resources, applying a technological methodology that utilizes universally accepted ediscovery principals and protocols is more easily defensible if ever challenged.

After the potentially exfiltrated ESI is forensically collected and secured, companies will likely need to warehouse the ESI in a data hosting facility with tools that allow for the smooth

---

[32] Among other things, MIR, owned by Fireeye, is designed to detect malware and other signs of compromise on endpoints across an enterprise and: 1) sweep thousands of endpoints for evidence of compromise, including malware and irregular activities; 2) enable remote investigate securely over any network, without requiring access authorization; and (3) collect targeted forensic data, with intelligent filtering to return only relevant data. See, https://www.fireeye.com/products/mir-endpoint-forensics.html.

[33] One legal practitioner/commentator has noted: “Cyber insurance does not cover any actual or alleged infringement, use, misappropriation or disclosure of a patent or a trade secret. Some cyber insurance policies, however, will offer coverage for infringement of intellectual property such as infringement of copyrights and trademarks, but not patent infringement or misappropriation of trade secrets. In addition, depending upon the cyber insurance policy, while there could be coverage for theft or an unintentional breach of third-party confidential corporate information - which may include third-party trade secrets or intellectual property - there is no first-party coverage for the insured organization. While a cyber insurance policy does not offer first-party coverage for the insured company’s patents or trade secrets, those seeking coverage have the option of purchasing a stand-alone intellectual property insurance policy.” See, “Cyber Security, Cyber Governance, and Cyber Insurance” by Paul Ferrillo, Harvard Law School Forum on Corporate Governance and Financial Regulation (November 13, 2014) available at http://blogs.law.harvard.edu/corpgov/2014/11/13/cyber-security-cyber-governance-and-cyber-insurance/#5b.

integration and search of the many different ESI types that can crop up. Data types can vary considerably -- from Word documents, Excel spreadsheets, PowerPoint presentations, PDFs and other common formats, to the more complex data formats residing within enterprise databases (such as SharePoint) or other customized business collaboration platforms. Relevant potentially exfiltrated ESI can reside almost anywhere, even within programing language or system directories, so searches must be exhaustive, consistent and scientific.

With respect to the more complex datasets, traditional search algorithms and methodologies may not suffice for exfiltration analysis and, for a variety of reasons, a victim company may need to hire a data analytics specialist to carve, parse and search efficiently the database. First, preserving, authenticating, analyzing and accurately producing data from enterprise databases can require unique methodologies. Moreover, the methodology employed will not only depend on the industry of the company involved (e.g., insurance, financial, design, telemarketing, consumer electronics, etc.); but might also require an entirely different enterprise architecture.

Second, a digital forensics team may ultimately have to authenticate database output for use in litigation, or may be called upon to identify problems with a database schema, front-end reports or other compromised workflows that are causing flawed database outputs. Finally, when proving to a state regulator that an attacker did not exfiltrate PII, a company will need a clean and proven methodology with respect to characterizations and descriptions of all data sets (especially if the data set is intricate, multifarious or otherwise convoluted).

### 4. <u>Physical Security Evaluation</u>

Contrary to many popular notions, cyber-attacks can sometimes begin with a physical breach, i.e. without initially using malware or other clandestine technological means. A physical breach could be perpetrated by an outsider to surreptitiously gather fodder for a social engineering scheme (such as a *spearfishing* campaign)[34] or by an insider (such as a so-called *bad leaver)*[35] to gain access to a company's network and wreak havoc.

Hence, in the aftermath of a cyber-attack, a company should take a holistic approach towards

[34] "Spear-phishing is an email spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority." See, http://searchsecurity.techtarget.com/definition/spear-phishing

[35] "The 21st Century Genesis of the Bad Leaver," by John Reed Stark, Bloomberg BNA Privacy & Security Law Report (November 2011) available at https://www.johnreedstark.com/wp-content/uploads/sites/180/2014/12/2011_BNA_21st-Century-Genesis-of-the-Bad-Leaver.pdf.

determining the source of the cyber-attack, and consider all possibilities. Along those lines, some cyber-attack investigations might entail the review of reception and entry checkpoints; ID scanner and other access records; video or still footage; physical logs; and even elevator and garage records.

# III. Government Relations Workflow

## 1. State Regulatory Compliance

As the regulatory protections afforded PII continue to expand, so do the risks in acquiring, storing and transmitting such information. Privacy laws vary by jurisdiction, are interpreted unpredictably, and are in a constant state of flux,[36] with some based broadly and others based on industry sector, such as, laws covering medical records,[37] financial transactions,[38] credit cards,[39] debt collectors,[40] insurers[41] or even library records.[42]

[36] For instance, California recently adopted new legislation implementing small but significant changes to its privacy laws. Specifically, on September 30, 2014, Governor Jerry Brown signed Assembly Bill 1710, which enhances consumer protections by strengthening the requirements businesses must follow in the event of a breach. Specifically, the new law:

- Requires the source of the breach to offer identity theft prevention mitigation services at no cost to the affected person for no less than 12 months if a Social Security Number or Driver's license number are breached;
- Prohibits the sale of social security numbers, except when part of a legitimate business transaction; and
- Provides that existing personal information data security obligations apply to businesses that maintain personal information, in addition to those who own or license the information.

See, https://cybersecuritylawwatch.files.wordpress.com/2014/10/assembly-bill-no-1710.pdf and https://cybersecuritylawwatch.files.wordpress.com/2014/10/cybersecuity-in-the-golden-state.pdf

[37] *See e.g*. Massachusetts Laws About Medical Privacy available at http://www.mass.gov/courts/case-legal-res/law-lib/laws-by-subj/about/privacy.html

[38] *See e.g.* State of California Department of Justice, Your Financial Rights available at http://oag.ca.gov/privacy/facts/financial-privacy/rights.

[39] Texas Attorney General's Office Credit Card FAQ, available at https://www.texasattorneygeneral.gov/faq/cpd-credit-card-faq.

[40] *See e.g.* Privacy Laws Affecting Debt Collection in Washington available at http://www.avvo.com/legal-guides/ugc/privacy-laws-affecting-debt-collection-in-washington.

[41] Several state departments of insurance have issued bulletins and regulations requiring insurers doing business in their states to send data breach notifications to the departments of insurance when an insurer has suffered a data breach. For example, Ohio Insurance Bulletin 2009-12 requires insurers to provide notice to the Ohio Department of Insurance of loss of control of policyholder information within 15 calendar days after discovery of the loss of control if it involves more than 250 Ohio residents. And, pursuant to Chapter 11 of Rhode Island Insurance Regulation 107, licensees of the Rhode Island Department of Business Regulation, which includes insurance companies, must notify the department of a data breach in the most expedient time possible and without unreasonable delay. Similarly, the Wisconsin Office of the Commissioner of Insurance, under a bulletin dated December 4, 2006, requires that insurers notify the office no later than 10 days after the insurer has become aware of unauthorized access to the personal information of the insured. The Connecticut Department of Insurance issued

Specifically, forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving PII. Security breach notification laws also typically have provisions regarding who must comply with the law (e.g., businesses, data/information brokers, government entities, etc.); definitions of PII (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).[43] These laws also often describe the responsibilities the so-called "record holder" has in terms of protecting information from unauthorized access or dissemination, modification and/or destruction and the obligation to report cyber-attacks affecting credit card numbers, social security numbers, birthdays, medical records and other identifying information. When such devices or the data on them are accessed, targeted, exfiltrated, etc. during a cyber-attack, a company's legal exposure to state regulators can be enormous.

Costs triggered by regulators can include individual notifications, heavy fines, injunctions, credit-monitoring services, government audits and even criminal liability. Inadequate privacy protections are particularly important to regulatory investigators; the investigators for example, will analyze carefully the victim's possible culpability for the cyber-attack, such as having inadequate network security or failing to adopt policies and procedures that are reasonably designed to ensure the security and confidentiality of PII.

In general, the data breach notification statutes of each relevant jurisdiction establish that:

1. Residents of the jurisdiction must be notified;
2. Notices to affected individuals must contain specific content (or are prohibited from containing certain information, as some states, such as Massachusetts, do not want publication of the methodology of the breach or the type of information at risk, while others require the disclosure of such information);
3. State attorneys general and other state agencies must be notified, and if so whether those notices must contain specific content and be provided before notification of affected

---

Bulletin IC- 25 on August 18, 2010 to require all entities doing business in Connecticut that are licensed by or registered with the Department to notify the Department of any information security incident. Notice must be provided as soon as the incident is identified, but no later than five calendar days after the incident is identified. The Connecticut Bulletin lists numerous facts that must be disclosed in the notification to the Department of Insurance, as they are known at the time, including details about the incident and remedial actions taken. Notice must also contain a draft of the notice the licensee or registrant intends to send to Connecticut residents. The Connecticut Bulletin also imposes a requirement on the licensee or registrant to report incidents involving a vendor or business associate. https://www.acc.com/chapters/ne/loader.cfm?csModule=security/getfile&PageID=1300198 at page 92.

[42] See, State Privacy Laws Regarding Library Records, American Library Association, available at http://www.ala.org/advocacy/privacyconfidentiality/privacy/stateprivacy

[43] See e.g. https://cybersecuritylawwatch.files.wordpress.com/2014/10/cybersecuity-in-the-golden-state.pdf.

individuals; and

4. Consumer reporting agencies, such as Experian, TransUnion and Equifax, must be notified.

## 2. Federal Regulatory Compliance

In addition to the labyrinth of state laws and regulations, entities may also be subject to federal rules and regulations mandating protection of PII and requiring that certain steps be taken in the event of a cyber-attack. Financial institutions in particular are subject to such federal regulations (and the term "financial institution" is defined very broadly).[44] In addition, health care-related companies face similar industry-specific regulations.[45] Public companies may also need to disclose cyber risks and incidents as part of their mandated disclosure of material information to potential investors.[46]

Historically, the U.S. Federal Trade Commission ("FTC") has been the most active with respect to privacy protections arising from a cyber-attack, and its jurisdiction continues to expand.[47] For instance, the FTC and other federal agencies that regulate financial institutions, including the Federal Reserve Board, National Credit Union Administration, Office of the Comptroller of Currency and the U.S. Securities and Exchange Commission, have issued regulations to implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003

---

[44] For example, the Gramm-Leach-Bliley Act ("GLBA") was enacted in 1999 to reform the financial services industry and address concerns relating to consumer financial privacy. Title V of the GLBA establishes a minimum federal standard of privacy and applies to financial institutions, including companies that were not traditionally considered to be financial institutions, such as insurance companies. *See* http://www.ftc.gov/privacy/privacyinitiatives/glbact.html on the applicability of Title V of GLBA to insurance.

[45] For instance, the U.S. Department of Health and Human Services ("HHS") has issued Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Privacy Rule governs the use and disclosure of an individual's personal health information ("PHI") by entities covered under HIPAA. The Privacy Rule also sets standards for an individual's right to understand and control how his or her PHI is used. It applies to health plans, healthcare clearinghouses, and to any healthcare provider who engages in electronic data interchange using one or more of the "standard transactions" as defined by HIPAA (collectively referred to as "covered entities"). The Privacy Rule includes a requirement that a covered entity mitigate, to the extent practicable, any harmful effect that is caused by an improper disclosure of PHI of which it becomes aware. Under the HITECH Act, discussed below, the Privacy Rule also applies directly to business associates of covered entities. 42 U.S.C. § 201 et seq. (HIPAA), 45 C.F.R. Part 160 and Subparts A and E of Part 164 (Privacy Rule). *See also* FTC Health Breach Notification Rule (16 C.F.R. Part 318),139 (August 18, 2009) (applying similar rules foreign and domestic vendors of PHR, PHR related entities and third-party service providers that maintain the information of U.S. citizens or residents. http://www.ftc.gov/healthbreach/

[46] Disclosing Cyber-attacks: How to Follow SEC Guidance, by John Reed Stark (November 1, 2011) available at https://www.johnreedstark.com/wp-content/uploads/sites/180/2014/12/2011_Disclosing-Cyberattacks-How-To-Follow-SEC-Guidance-JRS.pdf

[47] "FTC's Hammer Gets Bigger with LabMD Case--Federal Trade Commission," by Amy Worley, National Law Journal (January 26, 2015)) available at http://www.natlawreview.com/article/ftc-s-hammer-gets-bigger-labmd-case-federal-trade-commission.

(“FACTA”).[48]

FACTA is federal legislation directed at protecting consumers against identity theft as well as enhancing the accuracy of consumer report information. It prohibits businesses from printing out more than five digits of a credit card number, and allows consumers to obtain a free credit report every 12 months from each of the nationwide credit reporting agencies. The new regulations, which are commonly referred to as the Red Flags Rules,[49] are directed at preventing identity theft by requiring covered entities to develop and implement a written *Identity Theft Prevention Program* to detect the warning signs – i.e. the “red flags” – of identify theft in order to prevent and mitigate identity theft.

The Red Flag Rules apply to “financial institutions” and “creditors” that maintain “covered accounts,” as those terms are defined by the Red Flags Rule. Although the Red Flags Rule had been in effect since January 1, 2008 and traditional financial institutions regulated by the federal financial institutions regulatory agencies (such as banks) were required to comply by November 28, 2008, the FTC’s enforcement of the rule, which was extended a number of times, became effective December 31, 2010 with regard to entities *not* previously under its scope.

Other federal jurisdiction can trigger if a cyber-attack involves an educational institution, where the U.S. Department of Education (“DOE”) has an interest. For instance, any school or institution in the U.S. that provides educational services or instruction and receives funds under any program administered by the DOE is subject to the privacy requirements of the Family Educational Rights and Privacy Act (“FERPA”). Subject to certain limited exceptions, FERPA gives students (or in some cases their parents) the right to inspect and challenge the accuracy of a student’s own education records, while prohibiting schools from disclosing those records, or any personally identifiable information about a student contained in those records, without the student’s (or in some cases the parent’s) consent.[50]

Even the Federal Communications Commission (“FCC”) has begun flexing its regulatory muscle into the regulation of cyber-attacks. In October 2014, in a 3-2 vote, the FCC assessed a $10 million fine on two telecommunications companies for failing to adequately safeguard customers’ personal information.[51]

The victims of cyber-attacks can expect federal regulatory attention from some or even all of these federal agencies and will have to expend significant resources to manage regulatory inquiries and investigations, as well as litigation, should a federal agency suspect violations of

[48] Pub. Law 108-59, codified at 15 U.S.C. § 1681 et seq.

[49] 16 C.F.R. § 681.

[50] 20 U.S.C. § 1232g; 34 CFR Part 99.

[51] http://www.fcc.gov/document/10m-fine-proposed-against-terracom-and-yourtel-privacy-breaches

these broad and sometimes vague and arguably over-reaching regulations.

### 3. Law Enforcement Liaison

There exist a range of law enforcement agencies that may want to investigate a corporate cyber-attack and even apprehend the perpetrator. However, given the complexities of the crime and the nature of the foreign investigative jurisdictional challenges, the challenge is colossal and few prosecutions ever occur. But notwithstanding the unlikelihood of any successful prosecutions of cyber-attack perpetrators, law enforcement agencies will often have an interest in receiving briefings, reports, IOCs and other relevant information about a cyber-attack. Such agencies include the Federal Bureau of Investigation; the U.S. Air Force; the U.S. Secret Service; the Department of Homeland Security; the U.S. Postal Inspection Service; and a slew of others.

These law enforcement agencies may also request forensic images of impacted systems or may want to attach a recording appliance to a victim company's network in hope of capturing traces of attacker activity, should an attacker return to the company.[52] These requests raise a host of legal issues, including whether providing information to law enforcement could violate the privacy of customers or result in a waiver of the attorney client privilege.[53]

An emerging cybersecurity threat, especially with the evolution of certain types of malware, is receiving ransom demands as a condition of not carrying out a cyber-threat or otherwise relating to compromised data.[54] A cyber-attacker may threaten to inject a virus into a company's networks; to disseminate, divulge or utilize information exfiltrated from a company system; or to damage, destroy or alter a company's network or even physical facility.

---

[52] Cyber-attack victims will also hope that information sharing will be a "two way street," and that the investigating law enforcement authorities will collaborate with the company's investigative team and provide helpful information for the investigation, containment and the remediation of the cyber-attack.

[53] "What Law Firms Should Know About Cyber-attacks and the FBI," by Rachel Zahorsky, ABA Law Journal (May 23, 2013) ("The steady rise of cyber-attacks against U.S. companies -- with damages that include tens of millions of dollars, lost trade secrets and threats to critical infrastructures -- has prompted the FBI to even more greatly stress the importance of information-sharing on cyber intrusions. However, the decision to share sensitive data about a company or law firm's network comes with major legal considerations and should include discussions with legal department heads and outside counsel.") available at http://www.abajournal.com/news/article/what_law_firms_should_know_about_cyber_attacks_and_the_fbi/.

[54] For example, ransomware, as the name suggests, is a type of malware specifically designed to block or encrypt data, followed by a ransom demand. A warning massage usually pops up explaining that an attempt to uninstall or inhibit the ransomware's functionality in any way would lead to an immediate deal-breaker. Like most malware, ransomware spreads through social engineering techniques and traps sent from mostly unsolicited sources, such as spam, phishing emails with malicious attachments, links to bogus websites, and malvertising. Once a victim's system is accessed, an encryption type of ransomware installs itself and launches a complete hard disc scan, in order to locate documents of interest. The next step is encryption, which converts the targeted files into an unreadable form. Non-encrypting ransomware programs typically 'lock' the entire PC, terminating all processes that are non-essential to paying the ransom, and can eventually receive an 'unlock' code. "CyberExtortion," by Dimitar Kostadinov, InfoSec Institute, available at http://resources.infosecinstitute.com/cyber-extortion/.

Relatedly, cyber-terrorism poses a similar but potentially even more dangerous threat, stemming perhaps from a so-called "hacktivist" group[55] or at the direction of, foreign governments.[56] This can further complicate cyber insurance claims, which pursuant to a "terrorist exclusion" provision could be denied in the event such hacktivist groups are classified as terrorist organizations, and are identified as responsible for a cyber-attack.[57]

Be it a cyberterrorist or cyber-extortionist, handling this unique and relatively nascent type of threat requires special expertise (including local counsel from any involved foreign jurisdictions, as well as specially trained private investigators), which can add significant costs to any cyber insurance claim.

## IV. Constituency Notification Workflow

Once a cyber-attack occurs, in addition to government-mandated notifications, the need to make a broad range of other important notifications will also likely arise, each often requiring substantial effort, careful strategizing, c-suite attention and significant resources.[58] Specifically, as detailed below, a cyber-attack impacts multiple corporate constituencies (each having their own respective stakeholder) including:

1) Corporate Customers. Corporate customers will want to know all relevant facts relating to the cyber-attack, especially: if their data has potentially been compromised; if services will experience any disruption; the nature of remediation efforts; if there are any official or unofficial findings any investigation; or if there is any other information which can impact their operations, reputation, etc.

   Customers may also want images of malware and IOCs or to visit/inspect the company with its own investigation team. Customers may ask for weekly or even daily briefings and may demand attestations in writing with respect to any findings pertaining to their data. Some customers may also have contractual language establishing their rights when a cyber-attack

[55] "What is a Hactivist," by Peter Ludlow, New York Times (January 13, 2013) available at http://opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist/?_r=0

[56] "Obama Says Cyberterrorism Is Country's Biggest Threat, U.S. Government Assembles 'Cyber Warriors,'" by Christopher Harress International Business Times (February 18, 2014) available at http://www.ibtimes.com/obama-says-cyberterrorism-countrys-biggest-threat-us-government-assembles-cyber-warriors-1556337

[57] It is important to look for any definition of what constitutes a cyber-attack as it is in an insured's favor that the definition is not limited by a detailed and broadly worded description.

[58] Given that responding to a cyber-attack takes time and effort before drawing any sort of meaningful of conclusion, especially during the early phases of a cyber-attack investigation, the over-riding message to all interested constituencies, be they customers, partners, employees, regulators, FBI Agents or otherwise is: "We are moving quickly to preserve the evidence and gather the facts in this matter. We take this matter seriously and are conducting a thorough and independent investigation. We will let you know when we have more information to report."

occurs, which can include: i) notification within a certain amount of time (as low as thirty minutes); ii) on-site inspections; and iii) even the option of an independent risk and security assessment of the victim company (at the victim company's, and not the customer's, expense).

2) Partners. A cyber-attack victim's partners will have the same concerns and possibly the same contractual rights as customers, and will need equal care and attention. In particular, a company that falls victim to a cyber-attack will have to assess whether any intellectual property, trade secrets, corporate records, etc., relating to partners or other affiliates trigger notification or other contractual requirements.

3) Employees. Employees will undoubtedly become concerned and anxious after a cyber-attack, not only because their personal data may have been impacted but also because the future of the company (and their respective jobs) may be at risk.

4) Third Party Vendors. Outsourcing of services involving the transfer of, or allowing access to, PII from a company to its vendor, such as IT, payroll, accounting, pension and other financial services has become increasingly common. And not surprisingly, third party vendors have become one of the more prevalent attack vectors in the most recent cyber-attacks.[59]

   Given that cyber-attackers will often traverse across a company's network and gain entry into the networks of its vendors or vice versa, cyber-attacks can result in disputes as to the culpability for an attack, resulting in vendors and companies each pointing the finger at one another for their perceived respective cybersecurity failures.

   Thus, in the event of a cyber-attack, if any third party vendor has access to a company's networks, customer data or other sensitive information, the company will likely need to provide briefings, IOC lists, malware copies, investigative reports or other information relevant to the cyber-attack to the third party vendor. Providing briefings, IOCs and the like not only help protect the third party vendor from the attacker, but also help with any of the third party's own customer notification responsibilities.[60]

---

[59] "Third-Party Vendors a Weak Link in Security Chain," by Jeff Goldman, eSecurity Planet (March 6, 2015) ("Security shortcomings of third-party vendors are a cybercriminal's dream. So security pros should revisit how they manage vendor relationships.") available at http://www.esecurityplanet.com/network-security/third-party-vendors-a-weak-link-in-security-chain.html.

[60] Vendors who become entangled in the cyber-attack of a customer that includes PII of, for example, their customers' employees, can be subject to claims by those whose information is lost, as well as by their client. See, e.g., Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273 (S.D.N.Y. 2008). In that case, the court dismissed claims for negligence and breach of fiduciary duty brought by an employee against his employer's pension consultant whose laptop containing PII of employees was stolen; the employee sought on behalf of himself and others credit monitoring costs. The court dismissed the negligence claim in the absence of evidence that the information had been accessed or used. It also dismissed the claim for breach of fiduciary duties, again on the ground that the plaintiff had not shown he had suffered any damages. The court did allow the claim for breach of contract to proceed to allow discovery on the issue of whether the employee was a third-party beneficiary of the contract between his employer and the vendor under the terms of the contract. See also Ruiz v. Gap, Inc. 622 F.

In addition, if a company regularly incorporates requirements relating to cybersecurity risk into its contracts with vendors, these requirements may trigger notification responsibilities. Moreover, if third party vendors conduct remote maintenance of the victim company's networks and devices, it may also make sense to request copies of any relevant logs, or even access the third party system to scan for IOCs.[61]

Finally, given the dynamic between a third party vendor and a company, and the potential for pointing fingers and litigation after a cyber-attack, these notifications require special care and attention.

5) Board of Directors. Increasingly, cyber-attacks demand and receive board level attention and scrutiny. Accordingly, the board (or a committee thereof) of a victim company will require briefings, reports and may even hire its own independent investigator to review the findings of any digital forensic investigation.

6) Insurance Carriers.

Whatever the type of insurance held by the victim company, an insurance claim will undoubtedly follow, and insurance adjusters will scrutinize all invoices pertaining to the workflows enumerated in this article and will require briefings and documentation regarding all investigative efforts. For maximum objectivity, credibility and defensibility, rather than the company itself, the independent digital forensic firm investigating the breach, at the direction of counsel, should lead any briefings with insurance carriers.

Most importantly, a professional on the incident response team, preferably counsel, should also maintain carefully written documentation of all efforts of the response. This will help later on when gathering the "documentation package" to present to an inquisitive insurance adjuster when seeking an insurance reimbursement for the costs of the breach.

## V. Individual Notification/Monitoring Services

Once a company determines that certain individuals will require notice of the cyber-attack (if for instance, PII was potentially exfiltrated) a range of individual notification costs will quickly arise.

Customers are increasingly attentive to how a company notifies them when their sensitive data has been put at risk and these notifications have become an important part of the overall cyber-

---

Supp.2d 908 (N.D. Cal. 2009) (plaintiff sued a company's vendor for losing PII when a laptop was stolen containing information with job applications; the court dismissed the claims for lack of requisite appreciable harm in light of the fact that the plaintiff had not been a victim of identity theft but rather was claiming increased risk of future identity theft and seeking credit monitoring costs), aff'd, 380 F. App. 689 (9th Cir. 2010) (holding that under California law, a plaintiff must have either prior possession or a vested legal interest in money or property lost in order to claim restitution).

[61] This is why, prior to any cyber-attack, companies should review the information security procedures (including training) concerning third party vendors authorized to access a company's network.

attack remediation effort. Individuals will likely be lining up with questions about: the extent of the cyber-attack; the steps the company is taking to minimize the damage done; and the type and extent of credit and identity theft monitoring the company plans to provide. The costs associated with individuals whose PII may have been exfiltrated can include the sending of written notices, the provision of credit monitoring services, identity theft protection and other related services such as setting up a call center, an informational website and a toll free telephone number and email address.

## VI. Professional Services Workflow

### 1. Public Relations

Companies that experience cyber-attacks may suffer reputation-wrecking media and Capitol Hill attention all amid the untold damage of lost consumer trust and confidence. Along these lines, in most cyber-attacks, a victim company often engages a public relations firm experienced in handling not only crisis management but also highly technical and intricate communications with the public and with Congress. As mentioned earlier, unlike the victims of other heinous crimes, victims of cyber-attacks rarely receive sympathy or understanding but are more often instead disparaged, maligned and pilloried in the media[62] and questioned intensely by a skeptical and distrusting Congress.[63]

### 2. Law Firms

Every workstream discussed in this article requires careful navigation because, among other things, the legal ramifications of any workstream failure can be calamitous or even fatal for any public or private company. Clearly, outside counsel or inside counsel should lead each investigative workstream, quarterbacking the workstreams for the c-suite and sharing with senior management the ultimate responsibility for key decisions. Just like any other independent and thorough investigation, the work relating to a cyber-attack will involve a team of lawyers with different skillsets and expertise (e.g. regulatory; ediscovery; data breach response; privacy; white collar defense; litigation; law enforcement liaison; and the list goes on), and cyber insurance coverage should clearly cover these often multi-million dollar legal expenses.

[62] "Companies Slow To Alert About Data Breaches," by Craig Timberg, Andrea Peterson and Ellen Nakashima, Washington Post available at http://www.vnews.com/news/business/13332855-95/companies-slow-to-alert-about-data-breaches.

[63] "Lawmakers query banks about data security, by Craig D. Miller, Abovethelaw.com, (December 18, 2014) available at http://abovethelaw.com/2014/12/lawmakers-query-banks-about-data-security/ ; See, also "US Lawmaker Asks Sony for Details on Data Breach, " by Grant Gross, Computer World (December 23rd, 2014) available at http://www.computerworld.com/article/2863054/us-lawmaker-asks-sony-for-details-on-data-breach.html.

In addition to the governmental investigations and litigation mentioned earlier, the list of potential civil liabilities in the aftermath a cyber-attack is almost endless, including shareholder lawsuits for cyber security failures, declines in a company's stock price; as well as consumer/customer driven class action lawsuits alleging a failure to adhere to cyber security "best practices."[64]

Even more importantly, in the case of a cyber-attack investigation, attorney client privilege will arguably apply to the work product from the digital forensic investigators retained by outside counsel. This is not done to hide information; rather it helps protect against inaccurate information getting released in an uncontrolled fashion and allows for more careful deliberation and preparation for litigation or government investigation/prosecution, two scenarios more and more likely nowadays.[65]

### 3. Digital Forensics and Incident Response Firm

When a company experiences a cyber-attack, the company will likely need to hire an expert and experienced digital forensics/data breach response firm to investigate for several reasons. First, very few companies employ the kind of personnel who have the technological expertise to understand and remediate today's cyber-attacks. Second, like any company in a crisis, engaging an independent and objective investigator not only insures integrity in the response but also creates a defensible record if challenged later on (e.g. by regulators, class action lawyers, partners, customers, etc.). Finally, if the digital forensics/data breach response firm is engaged by outside counsel, a company can (arguably) maintain and secure the attorney-client privilege for the reports and other investigative documents pertaining to the attack. *See infra* "Counsel as Quarterback."

As an aside, when negotiating cyber insurance policies, some insurance policies will seek "panel" and "prior consent" provisions that purport to mandate that an insured hire a specific digital forensic/data breach response firm (even if the victim firm already has a prior existing relationship with a particular consulting firm). An insured should consider such a provision

---

[64] See e.g. "Sony Hit With Fourth and Fifth Class-Action Lawsuits Over Stolen Data," by Austin Siegemund-Broka, The Hollywood Reporter (December 19, 2014) available at http://www.hollywoodreporter.com/thr-esq/sony-hit-fourth-fifth-class-759563 (see complaint at http://www.scribd.com/doc/250633150/Shapiro-v-Sony); "Supervalu Hit With Lawsuit After Breach," available at http://www.bankinfosecurity.com/supervalu-hit-lawsuit-after-breach-a-7214; "Community Health Systems Faces Lawsuit," available at http://www.databreachtoday.com/community-health-systems-faces-lawsuit-a-7238.

[65] See also, "Law Firms Tout Cybersecurity Cred," by Christopher M. Matthews, Wall Street Journal available at (http://www.wsj.com/articles/SB10001424127887324883604578394593108673994; See, also "Law Firms Offer Cybersecurity Advice and Attorney Client Privilege to Firms," by Debra Cassens Weiss, ABA Journal available at http://www.abajournal.com/news/article/law_firms_offer_cybersecurity_advice_and_attorney-client_privilege_to_hacke

carefully; much like choosing one's own surgeon for a heart procedure, the victim of a cyber attack will likely want the freedom to select their own preferred digital forensics/data breach response and not be forced to engage any firm.

## Conclusion

Though Jimmy Durante could insure his nose ($50,000) and Bruce Springsteen can insure his vocal chords ($6,000,000),[66] insuring for the considerable and far-reaching breadth of cyber-attack fallout remains a challenge for public and private companies. Unfortunately, at present, there is no proven roadmap for analysis; no archive of empirical statistically significant data; and no quantification algorithm for calculating cyber-attack risk. In short, given the uncertainties and what some insurance professionals have referred to as the "actuarially immeasurable" results of cyber-attacks, the market for cyber insurance is, simply stated, a bit of a mess.[67]

Beyond the more predictable workstreams described herein, a victim company is also exposed to other intangible costs as well, including temporary or even permanent brand reputation and damage;[68] loss of productivity; extended management drag; and a negative impact on employee morale and overall business performance.

Sadly, the only certainty for public and private corporations is that cyber-attacks are inevitable; that cyber-attacks are almost always extraordinarily complicated; and that cyber-attacks will almost always require a host of costly responses, including the many unique and inter-woven workstreams discussed in this article.

Yet with respect to insuring for cyber-attacks, the traditional insurance paradigm of risk analysis does not yet apply. In the meantime, today's risk-averse companies can best gain insight into the question of cyber insurance by not only understanding the growing and complicated hazard of cyber-attacks, but also by considering carefully the workstreams that typically occur during their aftermath.

---

[66] "20 Celebrities Who Insured Their Body Parts for Millions," by Kristen Acuna, Business Insider (March 5, 2012) available at http://www.businessinsider.com/20-celebrities-who-insured-their-bodies-for-millions-2012-3?op=1

[67] "The $10 Million Deductible: Why the Cyber Insurance Business is a Mess," by Josephine Wolff, Slate (June 12, 2014) available at http://www.slate.com/articles/technology/future_tense/2014/06/target_breach_cyberinsurance_is_a_mess.html; "The Problem With Cyber Insurance," by Ira Scharff, Information Week (June 17, 2014) ("Insurers have yet to develop an evidence-based method to assess a company's cyber risk profile. This can result in high premiums, low coverage, and broad exclusions.")

[68] Economist Intelligence Unit Report, "Reputation Risk: Risk of Risks," available at http://databreachinsurancequote.com/wp-content/uploads/2014/10/Reputation-Risks.pdf.

DOCKET MEDIA LLC

PHONE: (424) 2-DOCKET
WWW.CYBERSECURITYDOCKET.COM
EDITOR@CYBERSECURITYDOCKET.COM