February 12, 2015

Weil

Alert
Cybersecurity, Data Privacy, and Information Management

Cybersecurity and Privacy Diligence in a Post-Breach World:

Incident Response Planning and Business Continuity Planning

By Paul Ferrillo and Randi Singer

"By the time you hear thunder, it's too late to build the ark."

— Unknown

In November 2014 – just two weeks after Admiral Michael Rogers, director of the National Security Agency, testified to the House Intelligence Committee that certain nation-state actors had the capability of "infiltrating the networks of industrial-control systems, the electronic brains behind infrastructure like the electrical grid, nuclear power plants, air traffic control and subway systems"[1] – Sony Pictures announced it had experienced a major cyber-attack, one many sources believe was likely perpetrated by or on behalf of a nation-state. This destructive cyber-attack was a game-changer for corporate America because it became clear that hackers are not simply focused on credit card numbers or personal information. Indeed, the attack on Sony was designed to steal the Company's intellectual property, disseminate personal emails of high-ranking executives, and destroy Sony servers and hard drives, rendering them useless.[2]

What the events of 2014 proved to corporate America is that there are no fool-proof methods for detecting and preventing a devastating cyber-attack. As FBI Director James Comey eloquently put it, "There are two kinds of big companies in the United States. There are those who've been hacked…and those who don't know they've been hacked."[3]

Thus, it is absolutely critical to understand what kind of data a company collects, how the company uses, stores, shares, processes, protects, and disposes of information, and how to develop and evaluate a plan to respond to attacks that target these data. Proper planning can mean the difference between a news story that begins, "Sony has just announced that Sony Pictures Entertainment co-chairman Amy Pascal is stepping down from her post,"[4] and one that announces a major cyber-attack, but concludes, "Anthem said it doesn't expect the incident to affect its 2015 financial outlook, 'primarily as a result of normal contingency planning and preparation.'"[5]

Proper planning includes incident response and information management business continuity planning, which are mission-critical. They are (or should be) part of a Board's enterprise risk management duties, and they are

particularly vital for certain federally-regulated entities with an obligation to protect consumer and client information and to keep it private. We have written in-depth elsewhere about incident response plans and their elements.[6] Here, we set forth a high-level summary designed to help evaluate a company's incident response and business continuity plans.

Incident Response Planning – You Can't Defend What You Can't See

Given that 97 percent of the IT systems of companies surveyed globally have been breached,[7] the question of how to protect a network from a breach is effectively a moot point. The better question is, how do you respond in the event of a breach when it occurs despite your best prevention efforts?

Incident response planning is exactly what it sounds like – a plan to detect and respond to indicators or actual evidence found on a network server or alert system that a malicious intrusion may be occurring.

In general, there are many indicators or precursors of a potential cyber-attack. Though there are far too many to list, potential triggers for a robust incident detection and response plan include:

- A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server.
- Antivirus software alerts when it detects that a host is infected with malware.
- A system administrator sees a filename with unusual characters.
- An application logs multiple failed login attempts from an unfamiliar remote system.
- An email administrator sees a large number of bounced emails with suspicious content.
- A network administrator notices an unusual deviation from typical network traffic flows.[8]

This non-inclusive list, based on the National Institute of Standards and Technology Computer Security Incident Handling Guide, illustrates one of the most basic challenges of working with advanced incident intrusion detection systems: they often generate thousands, if not tens of thousands of alerts of potential intrusions into a company's computer network every day. In fact, one recent report notes that potentially actionable (*i.e.*, "we better take a look at this") malware intrusions could number in the thousands per day.[9]

Even in the largest companies, resources are not unlimited, particularly given the shortage of skilled IT professionals in the marketplace today, so each company's incident response plan will necessarily reflect certain compromises. However, recent events offer some basic principles as to how companies can and should lay out their incident detection and response plans from a "process perspective":

- Incident responders need to understand the "normal" behavior of their network. Logs kept by intrusion detections systems provide detailed reports from firewalls, intrusion detection devices, and network traffic flow activity meters.
- Incident response handlers need to fully understand what is "normal" behavior on any given day and time, so that they then can determine what is "not normal" based upon any one particular alert. Visibility is one of the key issues to emphasize because no security system in the world will mean much if you can't tell the difference between alerts to which you should respond and alerts to which you must respond. Often, breaches happen because critical alerts are overlooked amid the noise of numerous other alerts of lesser importance.
- Firewall, intrusion detection, and network activity logs need to be maintained and accessible, so efforts can be made to correlate potentially malicious current activity with network activity in the past. It may be necessary to keep these logs handy for months, since many attacks take that long to be "noticed" by an unsuspecting company.
- Cyber events need to be correlated quickly. Many times, this function can either be outsourced to a third party vendor, or it can be performed mechanically with an appropriate hardware solution that can analyze all of the alerts in real time.[10]

- After reviewing evidence supplied by each of the above steps, incident response teams need objective criteria to determine which intrusions need to be escalated to a higher level and/or investigated further.[11]
- Finally, when a breach and/or exfiltration of customer or protected data is confirmed, a plan should be in place to quickly minimize the damage to your network infrastructure, your brand, and your customers and employees.

As there is no silver bullet in a constantly-evolving environment where hackers are often several steps ahead of cybersecurity professionals (or at least adapt quickly to new security measures), a lawyer conducting due diligence on a company's incident response plan should evaluate the approach and process of the plan. Malware leaves signs or indicators of "bad behavior" on logs. Network traffic monitors may show spikes at unusual times, or even better, at regular intervals. A robust plan will have a process in place to correlate all of the indicators as quickly as possible and then escalate those more "suspicious" events for further review. In many cases, automated processes that correlate aggregated log data using "big data" analytics may be of particular benefit given the time-sensitive nature of event-response: any particular piece of malware could have devastating consequences if it is not quickly captured and eradicated.[12]

Business Continuity Planning

Information management business continuity planning requires implementing procedures to recover data and information from a backup source as quickly as possible in order to get systems back online.[13] Business continuity planning was once the province of preparations for hurricanes, fires, and earthquakes, but in the wake of the devastating attack on Sony Pictures – as well as the companion announcement of the wiper malware attack on the Las Vegas Sands[14] – it is incumbent upon a company (and its board) to plan for the consequences of a severe cyber-attack, which might involve the loss of data, the loss of servers, the loss of computer hard drives, and even the loss of VoIP-based phone systems. As many have noted, "The biggest risk a company faces in today's uncertainty of cyber-attacks is not being prepared."[15]

Volumes can be (and have been) written about business continuity planning in general. Vendors abound in this area, many claiming to offer the "best" back-up and business continuity procedures. And of course, every company (whether it is U.S.-based or multi-national, or a financial institution, broker-dealer or "brick-and-mortar") is different when it comes to determining the most important elements of a business continuity plan, including which systems are critical to the organization, and how and when to bring them online. But in examining a company's continuity planning for a cyber-attack, at least the following issues should be addressed:[16]

1. Does the company have a written Business Continuity Plan?
2. Has the company done a Business Impact Analysis that identifies the company's most critical systems and the maximum downtime that can be tolerated if they go down?
3. What are the company's systems back-up procedures? How often is the full system backed up? Are back-ups maintained on the network? Has an "air gap" architecture been built into the company's back up-procedures so that a cyber-attacker cannot attack system back-ups because they are segregated and being held off of the network?[17]
4. Where are the back-ups held and how are they stored (network storage, external hard drives, or even in the cloud)?
5. How long will the back-up media be maintained? How quickly can the company get to the back-up data when it is needed?[18]
6. Once the back-ups are accessible, what are the company's exact procedures for (A) obtaining whatever hardware is needed for the system restoration, (B) the restoration of the company's critical operating systems and applications, (C) restoring other data to their then-known back-up state, and (D) testing the restored system to make sure everything is working properly?

7. Finally, as many telephone systems are internet-based, a telephone recovery strategy also needs to be in place.[19]

Like an incident response plan, a business continuity plan needs to be tested, the personnel responsible for implementing it need to be trained, and it should be periodically rehearsed so that all involved (including third-party or outsourced vendors) know their roles in getting the organization's information management system back on line.[20] Ideally, a plan should be put to the test through a full-scale functional exercise that includes a "full cut-over" and recovery to back-up data.

* * * *

In many cases, the company that you are diligencing may be your own. It is indisputable that enterprise risk management is part of a director's fiduciary duty to the organization and its shareholders. And cybersecurity today is undoubtedly part of enterprise risk management, and thus within a board of director's oversight role:

> The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct. Management and the board of directors have the authority and responsibility to set the top priorities of the company. If being secure, vigilant, and resilient is not defined as a priority and communicated within the organization, there is little hope that the organization will deploy sufficient resources to protect its information systems and to respond to cyber events appropriately.[21]

Though the drafting of incident response plans and business continuity plans can be complex, the last 13 months of cyber-attacks have taught us both types of plans should be in writing, in place, practiced, tested, and ready to implement at any time. Taking the time to plan may well determine the fate of a company following a cyber-attack.

1. *See* "NSA Director Warns of 'Dramatic' Cyberattack in Next Decade," available at http://www.wsj.com/articles/nsa-director-warns-of-dramatic-cyberattack-in-next-decade-1416506197.
2. *See* "Devastating malware that hit Sony Pictures similar to other data wiping programs," available at http://www.pcworld.com/article/2856032/destructive-malware-that-hit-sony-pictures-similar-to-other-data-wiping-programs.html.
3. *See* "Cyber Attacks on U.S. Companies in 2014," available at http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014.
4. *See* "Amy Pascal out as Sony Pictures co-chair," available at http://money.cnn.com/2015/02/05/media/amy-pascal-resigns-sony/index.html.
5. *See* "Health Insurer Anthem Hit by Hackers: Breach Gets Away With Names, Social Security Numbers of Customers, Employees," available at http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720?mod=WSJ_hp_LEFTTopStories.
6. *See* "The Importance of A Battle-Tested Incident Response Plan," available at http://blogs.law.harvard.edu/corpgov/2014/12/19/the-importance-of-a-battle-tested-cyber-incident-response-plan/.
7. *See* "FireEye suspects FIN4 hackers are Americans after insider info to game stock market," available at http://www.computerworld.com/article/2853697/fireeye-suspects-fin4-hackers-are-americans-after-insider-info-to-game-stock-market.html.
8. *See* NIST Computer Security Incident Handling Guide, Special Publication 800-61 (Rev.2) (2012), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.
9. *See* "Security Case Study: Responsys," available at http://info.prelert.com/responsys-case-study#IDS. The same study notes that one large network it studied was getting 100,000-150,000 cyber "events" per day.
10. *See e.g.* "An Adaptive Approach To Cyber Threats For The Digital Age," available at https://www2.fireeye.com/rs/fireye/images/fireeye-security-reimagined-part1.pdf (Discussing one such advanced solution).
11. Indeed, for regulated investment advisers and managers, the April 2014 SEC Office of Compliance and Examinations announcement listed most of these process steps as "required" answers that a regulated entity will have to give at its next annual examination. *See* "OCIE Cybersecurity Initiative," available at http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

12. *See e.g.* "Big Data Analytics for Security Intelligence," available at https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Analytics_for_Security_Intelligence.pdf (noting "Big Data tools have the potential to provide a significant advance in actionable security intelligence by reducing the time for correlating, consolidating, and contextualizing diverse security event information, and also for correlating long-term historical data for forensic purposes.").
13. Note that both incident response planning and business continuity planning are both questions that are required to be answered as part of the SEC Office of Compliance and FINRA Street sweep programs that are currently ongoing as respects cybersecurity.
14. *See* "Now at the Sands Casino: An Iranian Hacker in Every Server," available at http://www.businessweek.com/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas.
15. *See* "Why Companies Need a Business Continuity Plan," available at http://www.forbes.com/sites/christopherskroupa/2014/08/22/why-companies-need-a-business-continuity-plan/; "Hurricane, Fire… DDoS? Make Cyber Threats Part of Business Continuity Planning," available at http://insights.wired.com/profiles/blogs/pick-your-poison-hurricane-fire-ddos-cyber-threat-needs-to-be#ixzz3PsyG9vQc.
16. We again note the concept of business continuity planning is "fair game" when dealing with regulators. *See* SEC OCIE Cyber Security Risk Alert, at pg. 2 ("Please provide a copy of the Firm's written business continuity of operations plan that addresses mitigation of the effects of a cybersecurity incident and/or recovery from such an incident if one exists.").
17. *See e.g.* "Black Hat Keynoter: Beware of Air Gap Risks," available at http://www.bankinfosecurity.com/black-hat-europe-beware-air-gaps-a-7442/op-1 (noting the positives and potential negatives of an "air-gapped" based back up system).
18. The NIST "Contingency Planning Guide for Federal Information Systems," Publication 800-34 Rev. 1, available at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf, also suggests that certain organizations may also consider an off-site facility to not only keep their back up data, but keep hardware available so that they can resume business operations from the off-site facility. Such a site would obviously be more expensive, but for larger companies it would certainly be a feasible option to resume critical options as soon as possible.
19. *Id*.
20. *See* SEC OCIE Cyber Risk Alert, at pg. 3 ("[Does] the Firm periodically tests the functionality of its backup system. If so, please provide the month and year in which the backup system was most recently tested.").
21. *See* "COSO in the Cyber Age," available at http://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf.

Cybersecurity, Data Privacy, and Information Management is published by Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

If you have questions concerning the contents of this issue, or would like more information about Weil's Cybersecurity, Data Privacy, and Information Management practice, please speak to your regular contact at Weil, or to the editors or authors listed below:

Editors:

Michael Epstein	Bio Page	michael.epstein@weil.com	+1 212 310 8432
Randi Singer	Bio Page	randi.singer@weil.com	+1 212 310 8152

Contributing Authors:

Randi Singer	Bio Page	randi.singer@weil.com	+1 212 310 8152
Paul Ferrillo	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372