December 9, 2014

Weil

Alert
Cyber Security, Cyber Governance, and Cyber Insurance

The Importance of a Battle-Tested Incident Response Plan

By Paul A. Ferrillo

"The scope of [the Sony Pictures Entertainment (SPE)] attack differs from any we have responded to in the past, as its purpose was to both destroy property and release confidential information to the public.... The bottom line is that this was an unparalleled and well planned crime, carried out by an organized group, for which neither SPE nor other companies could have been fully prepared."

— Remarks by Kevin Mandia, "Sony Investigator Says Cyber Attack 'Unparalleled' Crime," *Reuters*, December 7, 2014.[1]

"The days of the IT guy sitting alone in a dark corner are long gone. Cybersecurity has become an obvious priority for C-Suites and boardrooms, as reputations, intellectual property and ultimately lots of money are on the line."

— Priya Ananda, "One Year After Target's Breach: What Have We Learned?" November 1, 2014.[2]

"Resiliency is the ability to sustain damage but ultimately succeed. Resiliency is all about accepting that I will sustain a certain amount of damage."

— NSA Director and Commander of U.S. Cyber Command Admiral Mike Rogers, September 16, 2014.[3]

We have definitively learned from the past few months' worth of catastrophic cyber security breaches that throwing tens of millions of dollars at "preventive" measures is simply not enough. The bad guys are too far ahead of the malware curve for that.[4] We have also learned that there are no such things as quick fixes in the cyber security world. Instead, the best approach is a holistic approach: basic blocking and tackling such as password protection, encryption, employee training, and strong, multi-faceted intrusion detection systems[5] really trump reliance on a "50 foot high firewall" alone. But there are also two more things that are critical to a holistic cyber security approach: a strong, well-practiced Incident Response Plan (IRP), and, as Admiral Rogers noted above, the concept of cyber-resiliency, i.e., the ability to take your lumps, but continue your business operations unabated.

In this article, we tackle two questions: (1) What are the essential elements of a Cyber IRP? and (2) Why are IRPs so important to your organization?

* * *

The Organizational IRP Paradigm: Basics and Important Initial Questions

For assistance with these questions, it is helpful to review The National Institute of Standards and Technology's (NIST) "Computer Security Incident Handling Guide,"[6] which notes:

> Computer security incident response has become an important component of information technology (IT) programs. Cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

In short, the NIST provides the raison d'être for an IRP: preventive measures are necessary, but not sufficient, to sustain operations in the face of the omnipresent cyber threat. A response capability, and a plan for executing it, is necessary and sufficient. It is important to note that each element of an effective IRP has multiple sub-elements, and multiple levels of complexity. Resultantly, effective IRPs must not and cannot be "one size fits all." They will differ depending on an organization's size, complexity, and industry sector, as well as on the types of personally identifiable information (PII) stored by the organization, and where that data is stored.

However, prior to examining the intricacies of an effective IRP, we need to focus on the questions that directors, officers, CIOs, partners, and other senior executives must ask about their company's IRP *prior* to learning that the inevitable has become reality: that "we've been hacked." Those questions become apparent in light of the ultimate goal of responding to a cyber threat: "get back in the game (safely)" as soon as possible in order to keep your customers, investors, and reputation intact. An attendant goal is to demonstrate to regulators, such as the SEC, OCIE, FINRA, or FTC, that you have paid attention and planned ahead. The questions, then, include, among other things:

- Does the organization have a standing, written, and enterprise-wide IRP?
- Has the IRP been tested, in terms of both its ability to discern between cyber "events" and cyber "incidents," and the organization's ability to execute the IRP following an incident?
- Does the IRP get the organization back in the game?

For the uninitiated, a cyber "event," according to the NIST, is "an observable occurrence in an information system or network." A cyber "incident" is a disruptive occurrence, a "violation of computer security policies, acceptable use procedures, or standard security practices".[7] In a recent book co-authored by Kevin Mandia – the founder (quoted above) of security consulting firm, Mandiant (now FireEye/Mandiant) – entitled *Incident Response and Computer Forensics*, Mandia simplifies this definition for today's cyber environment:

> An incident is "any unlawful, unauthorized, or unacceptable action that involves a computer system, cell phone, tablet, and any other electronic device with an operating system or that operates on a computer network."

In sum, a cyber "event" *may* ultimately be ok if it is determined, either by intrusion detection/surveillance systems or trained cyber technicians, that the event is something akin to "normal." It follows, then, that if following detection, an event rises to the level of a cyber "incident," it needs to be investigated further according to an IRP. Because if it is not "normal," it could result in catastrophic consequences if not properly and fully identified (network-wide), promptly addressed, and quickly remediated. Examples of incidents include denial of service attacks launched against a network, spear phishing attempts aimed at distributing malware within a network, nation-state hacks, or cyber extortion attempts.

Once the above questions have been asked and answered, an organization and its leadership are ready to respond to the inevitable discovery that "we've been hacked." Instead of "Now what?," the answer is "Now let's immediately invoke our IRP."

So, what does an IRP look like?

Essential Elements of an IRP

Though there are hundreds of cyber security consultants in the marketplace today that could provide a very complex version of an IRP, here are the basics (as least as we and NIST see them):

1. Preparation, Ownership, and Testing of the Incident Response Plan

Just as many high-rise buildings have their own emergency evacuation plans to respond to an event of a fire or another catastrophe, and practice them with their tenants several times a year, all companies should have a table-top tested, written IRP ready to respond to an incident of a cyber attack. Directors and officers should consider the following elements essential to an IRP:

A. Documentation, Management Buy-In, and the IRT: The IRP needs to be in writing, fully documented and regularly updated in order to prevent any surprises when it is invoked after an incident has been detected. For the same reason, it should have full sign-off and approval by senior management. The IRP should explicitly define the professionals (including in-house personnel as well as third-party vendors) who make up the Incident Response Team (IRT).

- The IRT must clearly delegate authority (who does what), and establish sustainable, open lines of communication and workflow (who reports to whom). It should include a legal component (either in-house or outside counsel, but most likely both) that is skilled in forensic investigations, disclosure obligations, and the preservation of evidence, since law enforcement may ultimately be involved depending upon the severity of the breach. Companies should also consider including both a Human Resources representative and a Finance Department designee on the IRT to anticipate and address issues that may arise after the incident.

B. Ownership: The IRT and IRP should be "owned" by *one person* in the organization who is designated as the head of the IRT. Reporting to the head of the IRT should be a deputy with strong incident response experience, and who can serve as an alternate owner of the IRP. Underneath the head and the deputy should be skilled incident response handlers with strong technical intrusion detection and forensic skills. The size and shape of the internal IRT may vary from company to company, and are obviously budget-dependent since 24/7 IRT coverage comes with a price.

Of course, if the organization is solely based in the U.S., it is possible to have only one owner of the IRP and one head of the IRT. In a global organization, however, the "one owner" policy may not be possible or even practical. Global organizations need to "globalize" their IRPs so that a local "owner" is in place who can be nearer to the action and to the designated third-party vendors. A local owner will also likely be more familiar with local laws relating to cyber and privacy-related disclosures that may be implicated during an investigation of a cybersecurity breach.

C. Identification and Selection of Third-Party Vendors: Many companies rely in part on third-party vendors to help guide them through a data breach.[8] An IRP should pre-identify and designate these vendors, who should be on a 24/7 retainer in the event of a breach. Outside counsel should be involved in retaining the vendors to preserve any applicable privileges, since evidence of a breach developed by the IRT and its vendors may become necessary if actual data loss is involved.

D. Crisis Communications Capabilities: The IRT should include both internal and external crisis communications strategists because, depending upon the severity of the breach and the potential for severe reputational damage, there will likely be disclosure obligations (both formal and informal)

following the breach. Formal disclosure of the breach to law enforcement authorities like the FBI or U.S. Secret Service may be warranted if the company suspects cyber criminality may have played a role in the breach. Notification of any "material" breach to investors may be necessary under U.S. Securities and Exchange Commission guidance, or in any event, may be necessary in order to reassure investors that the company is addressing the cyber breach and doing everything possible to protect investors and consumers. Finally, some sort of formal notification may be required in various local jurisdictions depending upon privacy issues. Because of potential formal notification requirements, it is important to have internal and/or external lawyers involved with, and overseeing, breach notifications.[9] In short, a good crisis management/investor relations firm with experience in major corporate catastrophic events should be on retainer. There is not much worse than a major hack and the associated costs involved other than losing the faith and trust of customers, clients and patients. That could cause a "death spiral" that may be insurmountable.

E. Practice, Practice, Practice.: Without it, IRPs and IRTs are no good. An organization needs to conduct drills on a regular basis (we recommend at least quarterly) so that all members of the IRT and associated third-party vendors know exactly what they are supposed to be doing in the event of a major cyber security incident. A good IRT works together like a crew team rowing a scull. Everyone needs to row in cadence. And in the same direction.

2. Detection and Analysis of Threat Vectors, or "Houston, We have a Problem"

No IRP will be effective without the ability to accurately detect and assess events and possible incidents. Typically, this requires a continuously changing array of both software and hardware necessary to detect incidents from a variety of threat vectors. Organizations need to be able, through "continuous monitoring,"[10] to identify "indicators" or "evidence" of an attack through network monitoring systems such as "event-based alert monitoring" and "header and full packet logging." Both are designed to collect transferred data to help the IRT generate digital signatures, network system activity logs, or identify data that might show evidence of compromise.

Because many cyber attacks today are found to flow from a one-time-only use of malware that has no recognized signature to identify it as a threat, many companies are now transitioning to a signature-less intrusion detection system. One long-term industry expert noted in a recent interview, "We don't know what to look for when nobody else has seen it. The [signature] model breaks down … How you protect yourself from a shotgun blast is very different than how you protect yourself from a sniper's bullet. Traditional protection mechanisms are geared toward those noisy mass attacks."[11] To combat this cyber attack technique, "Rather than relying on detecting known signatures, [many] companies marry big-data techniques, such as machine learning, with deep cyber security expertise to profile and understand user and machine behavior patterns, enabling them to detect this new breed of attacks. And to avoid flooding security professionals in a sea of useless alerts, these companies try to minimize the number of alerts and provide rich user interfaces that enable interactive exploration and investigation."[12]

Whatever the monitoring system in place (including antivirus software alerts), incident response information may contain evidence of either network traffic anomalies or of actual data theft which could lead one to conclude that there has been a data breach. Today, many monitoring systems are automated (and even outsourced) because large organizations can potentially have tens of thousands of incidents daily that need to be analyzed, correlated, and investigated. Logs should be kept and retained for some defined period (e.g., 30 days) as a matter of good course as they may be needed for a breach investigation.

3. Containment

Containment means "how do we stop the bleeding" so that no further damage can be done. As this is a complicated area, both in-house and outside legal experts and third-party vendors should be consulted. A containment program should involve:

- Removing the attacker's ability to access the network;
- A plan to isolate infected systems, forensically copy them and transfer them to another off-grid environment; and
- Triaging and analyzing the infection or malware so that an eradication plan can be formulated.

Assuming the company has come to the conclusion that a breach has occurred, and that PII has been compromised, it is important to have the IR/PR/legal team advise the IRT on potential disclosure obligations under federal law (like HIPPA), state law, or under the law of a foreign government (EU/UK directives), where applicable. Similarly, disclosure to the company's cyber insurance provider will be necessary. Depending on their terms and conditions (which should be continuously reviewed), many cyber insurance policies provide coverage that allows a company to take advantage of forensic and remediation services as well as the services of a "breach coach" and suggested third-party vendors if the company does not have such vendors on retainer.

4. Remediation and Eradication

Remediation and Eradication means "fixing the problem" as rapidly as possible after the threat vector is fully identified so that the attacker doesn't have time to change his method or mode of attack. Eradication efforts could involve:

- Blocking malicious IP addresses identified during the investigation;
- Changing all passwords;
- Patching holes in the network architecture that are identified during the investigation; and/or
- Fixing all vulnerabilities identified during the investigation.

5. Lessons Learned Post-Mortem

Cyber post-mortems are like many post-event discussions. Lessons can always be learned about what went right with the IRP (where the company excelled), what went wrong or what didn't work so well, and what areas can be improved upon by the entire IRT so that it can perform better during the next incident investigation.

Why is an Effective Incident Response Plan So Important to Any Organization?

We placed this section here at the end of the article because, frankly, we didn't want to give away the punchline too early. But we kind of did already with Admiral Roger's quote above. An effective IRP is absolutely vital to an organization because: (1) it has already been hacked (or doesn't know it yet), and (2) an organization needs to be able to take a "cyber punch," and get off the canvas to fight another day. An effective, table-top practiced IRP is important for a variety of other reasons:

- If the company is in a specific industry sector, especially the regulated financial services sector, regulators will specifically ask whether the organization has an IRP.
- A battle-tested IRP may be evidence of cyber security best practices if the company is later the subject of a lawsuit or regulatory proceeding resulting from disclosure of the breach.
- A battle-tested IRP will hopefully prevent an organization from having a cyber incident develop into a catastrophic event, either financially, reputationally, or both, which could cause the company's demise or death if there is a "run on the bank" following disclosure of the cyber incident.

---

1. See "Sony Investigator Says Cyber Attack 'Unparalleled' Crime" available at http://www.reuters.com/article/2014/12/07/us-sony-cybersecurity-probe-idUSKBN0JL00720141207.
2. See "One Year After Target's Breach: What Have We Learned?" available at http://www.marketwatch.com/story/one-year-after-targets-breach-what-have-we-learned-2014-10-31.

3. See “NSA Director Rogers Urges Cyber-Resiliency” available at http://threatpost.com/nsa-director-rogers-urges-cyber-resiliency/108292#sthash.V4bkayBQ.dpuf.
4. See “Sony Films Are Pirated, and Hackers Leak Studio Salaries” available at http://www.nytimes.com/2014/12/03/business/media/sony-is-again-target-of-hackers.html; “Hackers Using Lingo of Wall St. Breach Health Care Companies’ Email” available at http://www.nytimes.com/2014/12/02/technology/hackers-target-biotech-companies.html; “Hacking the Street,” a FireEye/Mandiant Special Report, available at https://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf.
5. See “Intrusion Detection FAQ: Can you explain traffic analysis and anomaly detection?” available at http://www.sans.org/security-resources/idfaq/anomaly_detection.php.
6. See NIST “Computer Security Incident Handling Guide,” Special Publication 800-61, (hereinafter, the NIST Incident Handling Guide) available at http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.
7. *Id.*
8. Three of the larger companies that we and our multi-national clients regularly deal with from an incident response perspective are FireEye/Mandiant, Verizon, and IBM. See https://www.fireeye.com/; http://www.verizonenterprise.com/products/security/; and http://www-935.ibm.com/services/us/en/it-services/security-services/emergency-response-services/?S_TACT=R02102GW&S_PKG=-&cmp=R0210&ct=R02102GW&cr=google&cm=k&csr=IT+Emergency+Response+Services_UN&ccy=us&ck=security%20services&cs=b&mkwid=sk3dL6Acl-dc_49046510203_4326fb30773.
   There are certainly other companies in the incident response space that have the ability to respond to domestic breaches, see e.g. http://www.krollcybersecurity.com/.
9. In some cases, and for some larger companies, it may even be important for companies to consider “off the grid” communications systems, like temporary cellphones and satellite phones so that key IRT members can communicate with each other in the event that the breach also effects a company’s corporate phone lines. See “Spike in Cyber Attacks Requires Specific Business Continuity Efforts” available at http://www.emergency-response-planning.com/blog/topic/cyber-security.
10. “Continuous Monitoring” is the hallmark of an Implementation Tier 4 organization in the NIST cybersecurity framework. See NIST Cyber Security Framework available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
11. See “On prevention vs. detection, Gartner says to rebalance purchasing” available at http://searchsecurity.techtarget.com/news/2240223269/On-prevention-vs-detection-Gartner-says-to-rebalance-purchasing.
12. See “Why Breach Detection Is Your New Must-Have, Cyber Security Tool” available at http://techcrunch.com/2014/09/06/why-breach-detection-ss-your-new-must-have-cyber-security-tool/.

If you have questions concerning the contents of this issue, please speak to your regular contact at Weil, or to:

Paul A. Ferrillo (NY) Bio Page paul.ferrillo@weil.com +1 212 310 8372

© 2014 Weil, Gotshal & Manges LLP. All rights reserved. Quotation with attribution is permitted. This publication provides general information and should not be used or taken as legal advice for specific situations that depend on the evaluation of precise factual circumstances. The views expressed in these articles reflect those of the authors and not necessarily the views of Weil, Gotshal & Manges LLP. If you would like to add a colleague to our mailing list, please click here. If you need to change or remove your name from our mailing list, send an email to weil.alerts@weil.com.