January 6, 2015

Weil

Alert
Cyber Security, Cyber Governance, and Cyber Insurance

Changing the Cyber Security Playing Field in 2015

By Paul Ferrillo

"If this incident [Sony] isn't a giant wake-up call for U.S. corporations to get serious about cybersecurity, I don't know what is. I've done more than two dozen speaking engagements around the world this year, and one point I always try to drive home is that far too few organizations recognize how much they have riding on their technology and IT operations until it is too late. The message is that if the security breaks down, the technology stops working – and if that happens the business can quickly grind to a halt. But you would be hard-pressed to witness signs that most organizations have heard and internalized that message, based on their investments in cybersecurity relative to their overall reliance on it."

— Author Brian Krebs, Dec. 20, 2014.[1]

"For those worried that what happened to Sony could happen to you, I have two pieces of advice. The first is for organizations: take this stuff seriously. Security is a combination of protection, detection and response. You need prevention to defend against low-focus attacks and to make targeted attacks harder. You need detection to spot the attackers who inevitably get through. And you need response to minimize the damage, restore security and manage the fallout."

— Professor Bruce Schneier, Dec. 19, 2014.[2]

Without a doubt, the last month in the world of cyber security has been tumultuous. It has now been confirmed that two companies in the United States have potentially been the subject of cyber-terrorism. Servers have been taken down or wiped out. Businesses have been significantly disrupted. Personally identifiable employee information has been shoveled by the pound onto Internet credit card "market" sites. The cyber security world has changed. And two of the most respected men in cyber security have both iterated similar messages: it is time for U.S. corporations to take this stuff seriously.

This alert does not aim to recount the parade of horribles of 2014; rather, we write to suggest three modifications that are highly achievable in the corporate world that have the potential to make our cyber security world a little bit better in 2015.

More Cyber Governance – More NIST Discussions – More Information Sharing

On the first day of Christmas, my true love gave to me: the NIST cyber security framework.

In reality, on February 12, 2014, the Obama Administration, through the National Institute of Standards (NIST), announced the NIST Cyber Security Framework to "allow organizations – regardless of size, degree of cyber risk or cybersecurity sophistication – to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure."[3] In sum, the Framework focuses U.S. infrastructure companies on 5 basic principles:

1. Describing their current cybersecurity posture
2. Describing their target state for cybersecurity
3. Identifying and prioritizing opportunities for improvement within the context of a continuous and repeatable process
4. Assessing progress toward the target state
5. Communicating among internal and external stakeholders about cybersecurity risk[4]

In sum, NIST focuses companies on two simple questions: (1) where are they currently with cybersecurity, and (2) where do they want to be in the future?

Even more elegant is the simple way the Framework steers conversations regarding how a company should review its core processes of protecting its most precious IP, trade secrets or customer information:

- **Identification** – Developing the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. In other words, what are the most prized IP assets, and where are they located, e.g. off-line servers, network servers, or the cloud.
- **Protection** – Developing and implementing systems to protect the company's most valuable IP assets.
- **Detection** – Developing and implementing the appropriate activities to identify the occurrence of a cybersecurity event. An event may be nothing after it is appropriately investigated. An event that is missed or not apprehended as something more severe might turn into a catastrophic incident resulting in a mega-breach.
- **Respond** – Developing an Incident Response Plan.
- **Recover** – Developing and implementing the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.[5]

A thorough reading of the history behind the Framework will point to two conclusions: (1) it was not meant to become the national standard for cyber security best practices here in the United States (the Framework expressly says adoption of its principles is "voluntary," though many will argue that it is already de facto a national standard being used by the government and its third-party vendors), and (2) the Framework was designed so that executives and employees of any company could, using a common language, determine the "what, who, where, when and how" to protect its most valuable intellectual property assets.

Though some take issue with the lack of specificity regarding implementation of the standard, we would argue that is the point. No company is the same. No IP is the same. Therefore, there is no one perfect method for protecting a company's data. But there was a need to help companies organize their discussions around cyber security in a way that could be used by all directors, officers, and employees, whether they are technologically savvy not, to better their cyber security posture and defenses. And that is what the Framework is all about.

However, if the Framework has become at the very least a national standard for cyber security, then are companies actually using it to facilitate discussions aimed to better their cyber security posture? How often are they using it? Annually? Quarterly? Are they using it at all? And if companies are not using the de facto national standard for cyber security, then why is that the case?

If companies are using the Framework, how are they documenting discussions concerning improving their cyber security posture? Or are they just not documenting their cyber related discussions at all? Good cyber governance starts with information and discussion, traveling from bottom to top and then from top to bottom. There is no "run and hide" option here as that could land a board of directors with a major cyber breach on its hands and no documentation to rely upon to show they exercised their fiduciary duties of oversight over the enterprise's risk management. It could also land the company in further hot water with the plaintiffs' bar, which is becoming ever more successful, requiring the company to prove it did as best it could regarding cyber security despite the fact that a hacker still accessed its network.[6]

More (and Better) Employee Training and Education

Employee cyber training and education concepts could themselves be the subject of any number of articles or books. We mention them here in an attempt to raise two points to consider:

1. Employee phishing and spearphishing training is imperative.

   Some of the most notorious espionage cyber campaigns against companies and industries have started from the most innocent looking emails sent to an unsuspecting company employee or executive under the guise of an email from a bank or credit card company. When the employee unsuspectingly opens the email or its attachment, it drops malware on the company computer, which quickly spreads to the network. "Once on a system, the malware gathers information such as the operating system version, computer name, user name, and local IDs, as well as system drive and volume information. All the data that is collected is encrypted and sent to a cloud account… in an apparent attempt to avoid detection by anti-malware tools."[7] Then the hacker goes to work stealing the company's most valued business information, including business plans, M&A-related information, consumer information, and personally identifiable information.[8]

   The above threat vector is called "phishing," or its more advanced cousin, "spear phishing,"[9] when an email "phishes" for an unsuspecting and usually innocent employee to inadvertently wreak havoc on a company by opening it. "91 percent of cyber-attacks start with spear phishing…."[10] "Phishing remains a very real threat to organizations of any size. Symantec research showing a 91% increase in spear-phishing attacks from 2012 to 2013 tells us that much."[11] Says another expert, "The pool of spear phishing targets in 2015 will be larger and not just limited to a select few, like executives…."[12]

   Many companies train their employees monthly using random phishing emails aimed to look like they came from either the company itself or another trusted source. Training employees on anti-phishing techniques should lower the success rate of phishing emails. Indeed one study showed that in one company, "between 26% and 45% of employees at those companies were Phish-prone, or susceptible to phishing emails. Implementation of [training] immediately reduced that percentage by 75%; with subsequent phishing testing over four weeks resulting in a close to zero phishing response rate across all three companies."[13]

   Training is a good idea. Investing in more training this year would be an even better idea.

2. Employee intrusion detection training is also essential.

   Many companies now employ a host of various intrusion detection devices to attempt to detect a cyber-intrusion. These devices generally collect reams and reams of information called "logs," which could contain evidence of either network anomalies or common host-based artifacts of data theft. These could include:

   - Evidence of abnormal user activity;
   - Evidence of login activity outside expected hours;
   - Odd connection durations;
   - Unexpected connection sources;
   - Evidence of abnormally high CPU or disk utilization;

- Evidence of File Artifacts associated with the use of common compression tools; and
- Evidence of recently installed or modified services.[14]

These logs are obviously very long and complicated. Given that many data breaches have occurred on a company's servers long before they are discovered (an average of 229 days), and given that many of the high-end intrusion detection devices companies are employing are very good technically, many argue that there is a perceived mismatch between man and machine.

We are not sure there is a good answer to the man v. machine question. Some intrusion detection systems are so sophisticated that a lot of the high-level examination and analytical work can be done automatically, saving time and effort chasing false alerts and highlighting potentially malicious activity. Others are not. We express no opinion other than caveat emptor.

Nevertheless, company employees should be thoroughly trained repeatedly about their intrusion detection systems so that false positives can be ignored and potential dangerous incidents can be identified. Many intrusion detection vendors offer such training routinely, and it should be taken advantage of at all levels, as the more time malware is on company servers, the more time there is for it to wreak havoc on the network.

A Table-Topped, Battle-Tested, Infantry-to-Board of Directors, Incident Response Plan

In previous alerts,[15] we have spoken at length about the value of Incident Response Plans (IRPs).[16] Below are some additional relevant facts:

- The Ponemon *2014 Cost of Data Breach Study: United States* reported that the average cost for each lost or stolen record was $195. However, if a company has a formal incident response plan in place prior to the incident, the average cost of a data breach was reduced as much as $17 per record. Appointing a CISO to lead the data breach incident response team reduced the cost per lost or stolen record by $10.[17]

  There has been much talk in the industry of the importance of a chief information security officer, or CISO. Though every organization has to make its own determination as to whether such a position is needed within its company, at the very least *someone* needs to be 100% responsible for network security issues. That role is often filled by the CISO.

  According to the above statistics, a CISO can often be an incredible asset to any mid-to-large size company. As noted in one recent retailer breach, the company "didn't have an advocate at the C-level, as an executive, advocating for IT security investment…. If [the company's] senior management had known of such risks and what was at stake, they would have "made very different choices" as to how it structured its organization, and how it invested in capabilities to defend the company's data."[18]
- IRPs should be practiced *at least* once a quarter and the owner of the IRP (presumably the CISO) should update the plan as needed to account for new plans, new vendors, or new data protection strategies.
- IRPs should be practiced by everyone – from IT departmental heads, to CEOs, to board members – and should include vendors, forensic consultants, IR/PR consultants and lawyers to make the training as real as possible. It's important to practice for the worst. If something less than that occurs, then everyone should be on the same page when the next incident happens. If something in the IRP doesn't work, then it would be good to know that beforehand, rather than during an actual data breach.

2015

For many companies, it is probably time to get serious. The events of December 2014 have proved that we have most likely entered into a whole new phase of cyber-intrusions, cyber-attacks and cyber-terrorism.

Our network perimeters have plenty of penetration points to attack. And the Emperor's New Clothes are showing.

The events of late 2014 will require a new round of discussion with boards of directors and their C-Suite executives about company cyber security policies and what companies can do to mitigate the cyber risks involved. The critical IP assets of a company need to be fully and completed identified and protected as best as possible, using a variety of strategies including virtualization and private cloud strategies. History has shown strong perimeter defenses are no barrier to a determined hacker. Board discussions must occur, changes/improvements need to be documented, and incident response plans (including provisions for the absolute destruction of data, not just theft or tampering) need to be reviewed, modified as necessary and practiced. At a minimum, companies can insure for some of their cyber risk exposures through cyber insurance. Network security takes a village, involving every employee of the company. A culture of security needs to be instilled in every person touching a keyboard or a keypad.

Additionally, as cyber breaches have impacted varying industries in the U.S., each has come away with separate lessons to be learned from each event. Because not all malware is one-of-a-kind, information sharing would be incredibly helpful to all organizations. We cannot defeat this problem alone. We need to work together in a public/private partnership to share threat information. In this vein, Congress should pass the Cybersecurity Information Sharing Act as soon as possible in the coming term.[19]

By using some of the strategies we outline above, we can hopefully do a better job this year protecting our companies, businesses, and employees.

We *need* to do better in 2015.

We wish our clients, business colleagues and friends a Happy, Healthy and Safe Cyber New Year.

1. See "FBI: North Korea to Blame for Sony Hack," available at https://krebsonsecurity.com/2014/12/fbi-north-korea-to-blame-for-sony-hack/.
2. Mr. Schneier, a security technologist, is a fellow at the Berkman Center for Internet and Society at Harvard Law School. His recent Op-Ed Essay in the Wall Street Journal is available at http://www.wsj.com/articles/sony-made-it-easy-but-any-of-us-could-get-hacked-1419002701.
3. See "NIST Releases Cybersecurity Framework Version 1.0," available at http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.
4. See the Framework, available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
5. *Id*. See generally, "Understanding and Implementing the NIST Cyber Security Framework," available at http://blogs.law.harvard.edu/corpgov/2014/08/25/understanding-and-implementing-the-nist-cybersecurity-framework/.
6. See e.g. "Banks' Lawsuits Against Target for Losses Related to Hacking Can Continue," available at http://bits.blogs.nytimes.com/2014/12/04/banks-lawsuits-against-target-for-losses-related-to-hacking-can-continue/?_r=0; "Another Target data-breach lawsuit can proceed, judge says," available at http://www.startribune.com/business/286412161.html.
7. See "'Inception' Cyber Espionage Campaign Targets PCs, Smartphones," available at http://www.darkreading.com/perimeter/inception-cyber-espionage-campaign-targets-pcs-smartphones/d/d-id/1318046.
8. See "Hackers Stealing Business Secrets to Game the Stock Market," available at http://www.newsweek.com/hackers-stealing-business-secrets-game-stock-market-288231; "ICANN targeted by Spear Phishing attack, several systems impacted," available at http://www.csoonline.com/article/2860737/social-engineering/icann-targeted-by-spear-phishing-attack-several-systems-impacted.html.
9. Spear phishing is a psychologically more compelling form of phishing based upon socially engineering the email to the unsuspecting employee. See e.g. "3 low-tech threats that lead to high-profile breaches," available at http://www.csoonline.com/article/2859482/data-protection/3-low-tech-threats-that-lead-to-high-profile-breaches.html?page=2.
10. See "APT Mitigation: The Human Way," available at https://www.mandiant.com/blog/apt-mitigation-the-human-way/.
11. See "Phish Your Own Staff: Arming Employees to Beat Modern Attacks," available at http://www.infosecurity-magazine.com/magazine-features/phish-your-own-staff/.
12. See "Spear Phishing: A Bigger Concern in 2015," available at http://www.bankinfosecurity.com/spear-phishing-bigger-concern-in-2015-a-7742.

13. See “New KnowBe4 Statistics Reveal Security Awareness Training Reduces Phishing Susceptibility by 75%,” available at http://www.knowbe4.com/about-us/press-releases/security-awareness-training-reduces-phishing-susceptibility-by-75/.
14. See Luttgens, Pepe and Mandia, “Incident Response and Computer Forensics,” (3rd Ed. 2014) at pg. 263-264.
15. See “The Importance of a Battle-Tested Incident Response Plan,” available at https://interact.weil.com/reaction/mailings/Cybersecurity_Alert_Dec_9_2014.pdf.
16. See “The Importance of a Battle-Tested Cyber Incident Response Plan,” available at https://blogs.law.harvard.edu/corpgov/2014/12/19/the-importance-of-a-battle-tested-cyber-incident-response-plan/.
17. See “Is Your Company Ready for a Big Data Breach? The Ponemon Second Annual Study on Data Breach Preparedness,” available at http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf.
18. See “Target’s Lack of CISO Was ‘Root Cause’ of Systems Breach,” available at http://blogs.wsj.com/cio/2014/09/30/targets-lack-of-ciso-was-root-cause-of-systems-breach/.
19. See “Eyes turn to the next Congress as Sony hack exposes cybersecurity flaws,” available at http://www.washingtonpost.com/blogs/post-politics/wp/2014/12/18/eyes-turn-to-the-next-congress-as-sony-hack-exposes-cybersecurity-flaws/.

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

© 2015 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.