REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
03-05-2018	FINAL	Nov 2017 - Mar 2018

4. TITLE AND SUBTITLE
The Sony Pictures Hack: The Government's Role, National Security, and the Way Ahead

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
LCDR Kurt Shulkitas

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The unprecedented 2014 cyber attack against Sony Pictures highlighted how vulnerable corporate infrastructure is to both sophisticated and relatively unsophisticated cyber effects-based operations. Without comprehensive regulatory measures to force more serious security measures, the private network infrastructure most of the government and military communications traverse will remain vulnerable to both advanced persistent threats and less sophisticated threat actors. This paper considers the Sony Pictures cyber attack from the perspective of its national security impact and attempts to recommend a way ahead to begin addressing the issues.

15. SUBJECT TERMS
Cybersecurity, cyber policy, cyber attack

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Kurt M Shulkitas
U	U	U	UU		19b. TELEPHONE NUMBER *(Include area code)* (206) 512-5821

NAVAL WAR COLLEGE
Newport, RI

The Sony Pictures Hack: The Government's Role, National Security, and the Way Ahead

Kurt Shulkitas

College of Naval Command and Staff

The November 2014 cyberspace attack against Sony Pictures Entertainment was unprecedented. Regardless of the true perpetrators of the attack, its massive scale, the financial losses attributed to it, and the audacity of demands levied upon an American corporation by what appeared to be a hostile nation-state caused an uproar. No American corporation had ever been dealt such a direct and openly hostile blow by a nation-state. Once the carnage settled and stakeholders stole a moment to take stock of the losses and determine what lessons, if any, should be taken from this experience, it became clear the United States had a problem. The United States requires clear cybersecurity regulations and an effective cooperation program between the public and private sectors to ensure the country's most important institutions remain protected from all but the most sophisticated cyber attacks. To that end, this paper will briefly introduce the Sony Pictures Entertainment attack, outline the national security concerns inherent to the event, and recommend a method of government regulation to ensure the "cyber commons" remain protected, open and available to users.

Sony Pictures Entertainment

On November 24th, 2014, Sony Pictures Entertainment announced that they had been the victim of a cybersecurity incident. The initial announcement simply stated, "we are investigating an IT matter."[i] It soon became evident Sony was facing an unprecedented and very public cyberattack that had compromised private employee data, internal communications, information on employee/executive salaries, copies of unreleased films and scripts, and other corporate proprietary data. Computer systems

were locked with an announcement of “Hacked by #GOP” framed red skeletons.[ii] Speculation began immediately that the Democratic People’s Republic of Korea (DPRK) conducted the cyber attacks because of the upcoming release of *The Interview*, a comedy about the assassination of DPRK dictator Kim Jong Un.

The damage was significant. According to a 2015 Fortune expose, 3262 of Sony’s 6797 personal computers and 837 of their 1555 servers were erased - the now empty hard drives overwritten seven times to ensure data was unrecoverable and their start-up protocols deleted. This incredible destruction was the first time Sony had an inkling someone had compromised their information systems. In one fell swoop, a multi-billion-dollar global entertainment conglomerate was paying employees with paper checks and communicating on Blackberries recovered from a storage closet. Later, the company would come to realize incredible troves of information was being extracted from their systems for months before the overt cyberattack.[iii]

On 19 December 2016, the Federal Bureau of Investigation (FBI) announced sufficient evidence existed to name the DPRK as the perpetrators of the cyber attack. The FBI national press release cited sensitive sources and methods but further stated that technical analysis of the deletion malware, correlation of IP addresses used in this attack and IP addresses used in previously cyberattacks, and tool similarities to those used in attacks against South Korean banks the previous year all correlated to the DPRK.[iv]

This unprecedented cyberterrorist act, possibly perpetrated by a nation state, shook corporate America and highlighted for the first time what fate could befall an organization that offended a capable and sufficiently motivated cyber adversary. Sony Pictures Entertainment had their data destroyed, proprietary information spread across the

internet, private (and embarrassing) executive communications released, and a trove of personal data stolen.

Interestingly, not all cybersecurity experts agree with the FBI's assertion that the cyber actors were North Korean, nor that the primary motivation was stopping *The Interview* from shaming the North Korean "Dear Leader." An attack analysis by Risk Based Security cited emails sent to Sony CEO Michael Lynton and Board Chairwoman Amy Pascal by the threat actors demanding financial compensation to avoid "great damage" to Sony.[v] Other cybersecurity experts are skeptical the FBI could assign attribution in such a short time period. Robert Graham, a researcher with Errata Security, asserted it was incredible the FBI only took three weeks to investigate and name a perpetrator, and that such an investigation could take months to thoroughly complete.[vi] Lingering speculation recently fired Sony insiders had access, motivation, and capability to conduct the attacks remains. Those who believe the speculation assert it was only after rumors of DPRK involvement that the attackers focused their threats on *The Interview*.

Various reports credit the quick identification of the cyberattackers to similarities with malware used against South Korea and DPRK-affiliated web server IP addresses. Additionally, the timing of the attacks proved particularly noteworthy given the upcoming release of *The Interview*. Conversely, fueling speculation that insiders perpetrated the cyber attack, a large number of technical employees were fired only months before – employees who knew how vulnerable Sony was to a cyber attack. It would have been relatively easy for knowledgeable insiders to gain access to tools similar to those used in previous attacks and route traffic through DPRK IPs.[vii]

But the attackers are only part of the Sony story. Director of cyber operations at EdgeWave Security, Mr. Tom Chapman, described how Sony Pictures Entertainment only had 11 personnel in their IT department, which included a Vice President, three senior managers, and three other managers. The top-heavy IT department manning left only three people to do the bulk of the actual IT work.[viii] No company who takes cybersecurity seriously would fail this dramatically at investing in the safety and security of its information systems, likely reflected in the level of investment exhibited by Sony executives. Additionally, a Norse Corp. cybersecurity firm looking to gain Sony's business found no physical security, no authentication procedures to access the networking areas, no receptionist/security guards, and scores of unattended cubicles with workstations logged in.[ix] A sense of complacency and lack of basic security awareness seemed to pervade Sony Pictures Entertainment, despite the fact that Sony's online gaming segment had suffered a massive cyber attack a few years earlier resulting in the loss of over 77 million user accounts and associated personally identifiable information. It seemed Sony was more interested in cost savings and trying to squeeze revenue from profitable business segments like Sony Pictures Entertainment to offset losses by other segments and made cybersecurity risk decisions accordingly.[x] Sony Cybersecurity Chief Jason Spaltro asserted "I will not invest $10 million to avoid a possible $1 million loss."[xi] While possibly true in the purest business sense, he was unable to foresee the incredible loss about to befall the company he was charged to protect.[xii]

The final component to the Sony hack that requires further emphasis is the incredibly difficult task of determining the attack attribution. In general, savvy attackers will route communications through countless proxy servers, compromised

servers/computers, country borders, corporate network firewalls, all to hide identities. In the Sony breach, the U.S. government didn't have the luxury of waiting months for a strong technical analysis – they were facing the prospect that a U.S. corporation would bend to the threats of a tyrannical dictatorship. President Richard Nixon sealed the fates of two U.S. diplomats kidnapped in Sudan in 1973 when he answered a question regarding whether the U.S. would meet the terrorists' demands with "as far as the United States as a government giving in to blackmail demands, we cannot do so and we will not do so."[xiii]

The Government's Role

The question of who holds primary responsibility to secure our nation's critical infrastructure is hotly debated both inside the government and private industry. Corporations need reliable, secure communications, but consensus is lacking that legislation regulating cybersecurity in private industry with directive cybersecurity measures is the most effective way to ensure access, accessibility, and security.[xiv]

The 1996 *Report of the Defense Science Board Task Force on Information Warfare – Defense (IW-D)* warned that increasingly interdependent infrastructures and our dependence upon them made the U.S. particularly vulnerable to cyber attack and a need exists for 'extraordinary action' to defend against information warfare.[xv] Almost two decades later, much of that infrastructure – predominantly built, owned, and maintained by private industry – remains vulnerable to increasingly sophisticated cyber attacks. In fact, private industry "owns and operates 85 to 90 percent of the cyber

infrastructure," and the clear majority of government communications travels on these private systems.[xvi] The U.S. Senate, long recognizing the danger, introduced the ill-fated Cybersecurity and America Cyber Competitiveness Act of 2013. The bill explicitly stated, "…vulnerabilities in information and communications networks and gaps in cybersecurity pose one of the most serious and rapidly growing threats to both the national security and the economy of the United States."[xvii] The proposed bill died in committee, but the question of how best to secure our nation's critical infrastructure remained. This legislative failure set the stage for President Obama's 2013 Executive Order directing voluntary implementation of a framework to improve critical infrastructure cybersecurity.[xviii]

While consensus exists both in government and private industry regarding the importance of robust, effective cybersecurity, there is disagreement that legislating protection standards on a field as dynamic as network and critical infrastructure security is an effective way to achieve it. Industries hesitant to accept additional government regulation assert they are best positioned to evaluate their specific cybersecurity posture and implement controls to protect their networks without being hamstrung by strict, potentially expensive or difficult to implement guidelines dictated to them through legislation. The oft utilized but overly simplistic argument is any regulation will stifle innovation.[xix] Additionally, private industry often limit cybersecurity expenditures to the assessed risk of losses. For organizations who assess losses would not eclipse expenditures on security, implementing tough cybersecurity standards are a low priority. The question becomes what mechanisms or precedents exist for the U.S. government to

either force or entice private industries to improve their cybersecurity postures to eliminate attack vectors for cybercriminals, cyberterrorists, and other bad actors?

Additionally, disagreements exist on the extent of regulation, with industries having less exposure to cybersecurity risks compared to their technology-dependent counterparts being less motivated to incorporate the same defenses. An example is Google, a technology giant with an incredible amount to lose should their information security be called into question. As an information broker, Google's business model depends on access to information and the assessments derived from that information. A destructive cyber attack could shake shareholder confidence, resulting in stock price losses, customer exodus, or similar negative consequences. On the other hand, a mineral supplier who uses information systems to coordinate delivery of raw materials and natural resources might be less affected, since their source of revenue and wealth is tangible natural resources and less technology-dependent than Google. Google is highly motivated to protect their information, but the mineral company may be less inclined to expend significant company resources to protect mail servers and a payroll. But manufacturing and resource companies are not immune to danger. A Wired magazine article cited a German report issued by Germany's Federal Office for Information Security detailing a sophisticated cyber attack originating from the business network and eventually resulting in massive damage to a blast furnace after the compromise of the control systems.[xx]

National Security Impacts and the Way Forward

Assuming past failures can be overcome and a robust regulatory framework agreed upon, passed through Congress, and signed into law by the President, the national security impact could be significant. Current frameworks, like the 2013 Executive Order Improving Critical Infrastructure Cybersecurity and the Cybersecurity Act of 2015, rely on the voluntary implementation of shared, standard cybersecurity frameworks and information sharing. As a means to bridge the gap between no regulation/no standard and a codified regulatory framework, the previously mentioned Executive Order and legislation encourage the sharing of threat information, best practices, policy coordination, and other initiatives to increase private industry's responsiveness to cyber threats. Those who fail to implement these regulations or future requirements leave the nation exposed and vulnerable to cyber intrusions, but no punitive repercussions exist. I raised this scenario with a colleague who works with the National Security Agency, and he simply said: "any opening will be found, and that vulnerability will be exploited to get into and move laterally throughout the network." In other words, a single vulnerability puts the entire network at risk.

The only solution to protecting critical infrastructure, then, is to build the entire network from the beginning to a minimum security standard with modern security protocols. Minimum controls should include patching known vulnerabilities, using proper hardware and software configurations, validating database architecture and software employ secure coding principles, undertake measures to isolate important network functions or critical components, prudently use monitoring, and any other

mitigation measures required by regulation or recommended as industry best practices. These minimum measures reduce the vulnerable attack surface and decrease cyber attack response time. When coupled with information shared by government partners, this hopefully protects national security interests and prevents data exfiltration.

Of course, national security experts want advanced cybersecurity initiatives and prefer private industry to take a proactive versus reactive role in cybersecurity. By exceeding minimum standards, security professionals reduce the attack surface available to potential cybercriminals, cyberterrorists, and less motivated nation-state actors. This only enhances national security at a time when the Department of Defense is increasingly relying on public sector industries to provide advanced research and technology solutions to traditional military problems. The April 2015 DoD Cyber Strategy refers to stronger private sector support no less than seven times as a means to strengthen the nation's overall cyber defensive posture and stay ahead of technological development.[xxi]

In a dynamic information environment, legislation likely will not specify specific controls, but it might approach the problem similar to the way credit card regulation developed – a liability shift from consumers to the industry. The government did this to the credit card industry in the 1970s when they acted to limit consumer liability in cases of fraudulent charges, which ushered in significant security improvements as the potential liability risks eclipsed what was previously acceptable to the companies.[xxii] Privacy concerns notwithstanding, this appears to be a viable way to ensure the implementation of the most modern security protocols without creating stagnant requirements that become obsolete before they ever get out of Washington.

Conclusions

Alfred Thayer Mahan, the preeminent naval strategist, described the oceans as "a great highway; or better, perhaps, a wide common, over which men may pass in all directions…"[xxiii] This concept was critical to his analysis of sea power and was the canvass upon which the conditions influencing sea power would exert themselves. Scholars, strategists, and policymakers would later co-opt Mahan's concept of a maritime common to the air and space domains, as well. Now, in the past decade, the concept of a cyber common has gained popularity. If cyberspace is to become the next commons, a shared, mutually agreed upon system of cybersecurity standards must be implemented to protect both public and private personas. Congress must lead the development of comprehensive cybersecurity standards delineating minimum compliance requirements and then must pass that bill. Relationships with private industry must be fostered to allow for trusted, ubiquitous information sharing between the government and public and private organizations. Finally, if mutually agreed upon standards cannot be determined, legal and financial liability for breaches must be shifted to the information stewards as an incentive to proactively defend networks from attacks. Until these minimum steps are taken, the United States will remain disproportionately exposed to the risks of a catastrophic "Cyber 9/11."

[i] Michael Cieply and Brooks Barnes, "Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm," *New York Times* (New York, NY), last modified Dec. 30, 2014, http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html.
[ii] Lori Grisham, "Timeline: North Korea and the Sony Pictures Hack," *USA Today* (McLean, VA), last modified Dec. 18, 2014, http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/.
[iii] Peter Elkind, "Part 1: Who Was Manning the Ramparts at Sony Pictures?," *Fortune Magazine* (New York, NY), last modified Jun. 25, 2015, http://fortune.com/sony-hack-part-1/.
[iv] FBI National Press Office, "Update on Sony Investigation." (Washington D.C.), last modified Dec. 19, 2014, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.
[v] "A Breakdown and Analysis of the December, 2014 Sony Hack." *Risk Based Security,* last modified December 5, 2014, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/#realityandtheblamegame.
[vi] Jose Pagliery, "What Caused Sony Hack: What We Know Now," *CNN Tech* (New York, NY), last modified Dec. 29, 2014, http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/.
[vii] Elkind, "Part 1: Who was Manning the Ramparts."
[viii] Wayne Rash, "Best Defense Against a Cyber-Attack Is to Know Your Adversary," *eWeek*, last modified Dec. 7, 2014, http://www.eweek.com/security/best-defense-against-a-cyber-attack-is-to-know-your-adversary.
[ix] Elkind, "Part 1: Who was Manning the Ramparts."
[x] Ibid.
[xi] Ibid.
[xii] Ibid.
[xiii] Brian Jenkins, "Why the US Swaps Prisoners but Doesn't Pay Ransom," *The Hill* (Washington D.C.), last modified Aug. 29, 2014, http://thehill.com/blogs/pundits-blog/defense/216214-why-the-us-swaps-prisoners-but-doesnt-pay-ransom.
[xiv] Amitai Etzioni, "Cybersecurity in the Private Sector," *Issues in Science and Technology* 28, no. 1 (2011).
[xv] "Report of the Defense Science Board Task Force on Information Warfare – Defense (IW-D)," Office of the Under Secretary of Defense for Acquisition & Technology (Washington D.C., 1996)
[xvi] Paul Rosenzweig, "Cybersecurity and Public Goods," *Hoover Institute*, https://www.hoover.org/sites/default/files/research/docs/emergingthreats_rosenzweig.pdf.
[xvii] S. S. 21, *Cybersecurity and American Cyber Competitiveness Act of 2013*, 113 Cong, last modified Jan. 22, 2013, https://www.govtrack.us/congress/bills/113/s21.
[xviii] E.O. No. 13636, Improving Critical Infrastructure Cybersecurity, (Feb 12, 2013), https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.
[xix] James Lewis, "Innovation and Cybersecurity Regulation," *Center for Strategic & International Studies*, last modified Mar. 2009, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/090327_lewis_innovation_cybersecurity.pdf.
[xx] Kim Zetter, "A Cyberattack has Caused Confirmed Physical Damage for the Second Time Ever," *Wired Magazine*, last modified on 8 Jan. 2015, https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.
[xxi] "The Department of Defense Cyber Strategy," Office of the Secretary of Defense (Washington D.C., 2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
[xxii] Etzioni, "Cybersecurity in the Private Sector."
[xxiii] Alfred Thayer Mahan, *Mahan on Naval Strategy* (Annapolis, Maryland: Naval Institute Press, 1991), 27.