Why Government Organizations Don't Care: Perverse Incentives and an Analysis of the OPM Hack

James Twist, Matthew Hutchison, Blake Rhoades, Ryan Gagnon

Many security experts have addressed the financial and personal security risks involved with the recent data breach at the Office of Personnel Management (OPM). This work supplements previous analyses of the event, and explores how the recently disclosed OPM breach has impacted the national security of the United States. By examining the elements of the breach - within the context of the stolen data and linkages to other data breaches - this work points to a larger offensive cyber campaign as the primary concern for U.S. leaders and policy makers. After thoroughly examining the details of the attack itself and its implications on DoD and national cybersecurity, we argue that government organizations lack appropriate incentives to secure their networks and personal data. The solution to this problem lies with organizational leaders, who must give guidance that incentivizes information security at the "tactical level."

Introduction

After General Benedict Arnold's traitorous maneuver to deliver West Point into the hands of the British in 1780, General George Washington wrote a letter to the post's new commander for the purpose of instilling a sense of urgency in his subordinate. In the letter, Washington's instructions were clear and direct:

> The enemy will have acquired from General Arnold a perfect knowledge of the defenses, and will be able to take their measures with the utmost precision. This makes it essential our vigilance and care should be redoubled for its preservation. You will do everything in your power to gain information of the Enemy's designs and give me intelligence as early as possible of any movement against you.[1]

1 General George Washington's September 1780 correspondence to West Point Commander. Archives. United States Military Academy, West Point, NY.

At the time, Washington considered West Point to be the most strategically significant position in America. Placed at a western point of the Hudson River, this garrison was the only American point of defense between New York City and Canada. The enemy's "perfect knowledge" gained through Benedict Arnold had grave implications for the future success of the continental army. Luckily for Americans, General Washington had the foresight to encourage his subordinate commander to take all provisions necessary to secure this strategic terrain.

Our nation once again finds itself in an equally perilous position. In the wake of the recent Office of Personnel Management (OPM) intrusion and data breach, the forewarnings given in Washington's letter remain prescient. The revelation that digital records associated with over 20 million government employee were stolen from OPM by presumed foreign government affiliated hackers has undermined our nation's national security structure and compromised key digital terrain. Now infamously known as the world's largest known data breach, the OPM breach places national leaders at a critical decision point for how we conduct cyber defense in the future. As Washington implored in 1780, we must now re-double our efforts to mitigate the enemy's ability to exploit its newfound knowledge.

Overview

The stolen OPM data is useful for a variety of purposes to a diverse group of adversaries. For advanced persistent threats, this vast treasure of information and data provide the means to undermine, subvert, or neutralize American national security protections. The files could easily be shared amongst several nation states or, via proxies, with criminal enterprises. Its utility ranges from intelligence applications to identity theft and facilitation of focused computer network operations. Numerous subsets of individuals are vulnerable from the compromise of this data including senior leaders, intelligence personnel, military service-members, government civilians, and family members. The sheer volume of people affected implies the problem is of massive scope which impacts our government as a collective whole. The true value of the stolen data is the authenticity, specialized nature, and years required for its compilation. The only constraints for its application and usage in military and intelligence missions is the creativity of our adversaries who now possess it in its entirety.

In this paper, we examine the OPM breach, the evidence left behind by

the attackers, and examine historical case studies to draw conclusions about the event's impact on the government community and our national security at large. Unfortunately very few political scientists are addressing this issue and policy makers are only now beginning to understand that cyber warfare has become a weapon of choice against the US government.[2] The protracted campaign to degrade or neutralize US national power is becoming more and more evident with attacks like that against OPM.[3] Collectively, these events undermine the government's mandate to secure our nation in cyberspace and to preserve our strategic power abroad. In order to disrupt the ongoing campaign, we argue that policy makers and national leaders must focus on dismantling the lax cybersecurity that plagues the government's networks. This focus starts by holding organizational leaders and commanders responsible for the security of their own networks.

Attack Description

This section of the paper describes the adversary's systematic approach to breaching OPM networks. The attack – which has now been notoriously deemed the world's largest known data breach - likely began as a series of network intrusions occurring as early as 2013 and enduring until the spring of 2015. Over that time period, apparent nation-state hackers took advantage of OPM's poor security posture (and it's poorly monitored relationships with third parties) to steal data that contained a massive amount of information about government employees, family members, affiliated contractors, and prospective government hires (see Annex A).

The public first became aware of the attacks began in July of 2014, when the New York Times publically disclosed that OPM had suffered a systems breach during the spring of that year.[4] According to OPM, the agency had not disclosed the attack to the public because it had completed a security review of its systems – one wherein the agency incorrectly assessed that they had stopped the attacks with appropriate countermeasures – and, more importantly, that no Personally Identifiable Information (PII) had been compromised. As was revealed by the

2 Frates, Chris. "Government Hacks and Security Breaches Skyrocket - CNNPolitics.com." *CNN*. Cable News Network, 19 Dec. 2014. Web. 28 Sept. 2015.

3 Other events include the WikiLeaks scandal, the Snowden Affair, multiple penetrations of our networks by Russian APTs, and directly relevant to this case, the vast pilfering of technology and defense contractor data compromising some our most sensitive military equipment. (See "Why the cyberwar is dangerous for democracies.") http://www.theatlantic.com/international/archive/2015/06/hackers-cyber-china-russia/396812/)

4 Schmidt, Michael, David Sanger, and Nicole Perlroth. "Chinese Hackers Pursue Key Data on U.S. Workers." The New York Times. July 9, 2014. Accessed July 2, 2015.

agency in June 2015, however, the attacks persisted well into the spring of 2015 and were only discovered while OPM was upgrading its security systems. During this discovery period in the spring and summer of 2015, investigators found that multiple attacks had occurred against OPM data servers and that the attackers had gained access to personnel files. While OPM initially suspected four million persons had been affected, they later updated that number to an astounding 22 million.[5]

The hackers likely gained access to OPM systems by exploiting its business relationships with third party contractors. According to security experts and well known cybersecurity firms, the hackers gained access to OPM's networks through carefully crafted phishing attacks against OPM and its partners.[6] Of note, OPM partners USIS and Keypoint were both breached by hackers preceding and during the OPM attacks, thus experts believe the hackers used third-party issued credentials to gain initial access to the systems. In addition to the phishing attacks, security researchers at ThreatConnect identified that the malicious site opm-learning.org was potentially used by the hackers as a secondary means of installing malware and maintaining access to the OPM network.[7] [8]

Multiple sources agree that the attackers then gained persistence on the OPM network by installing an exploit toolkit known as Sakula.[9] Using this sophisticated malware, the attackers were able to ex-filtrate government employee information from the OPM servers through their attack infrastructure, specifically the malicious domain opmsecurity.org. Using the "diamond-model of intrusion analysis,"[10] CrowdStrike and Mandiant have assessed with a high degree of confidence that the attack was perpetrated by Chinese APTs.[11] While the two firms disagree on the attribution of the attack to any specific APT group, they use their proprietary

5 Bisson, David. "The OPM Breach: Timeline of a Hack." The State of Security. June 29, 2015. Accessed July 2, 2015. http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/.

6 Phishing is an extremely common hacking method where an adversary attempts to gain access to systems through carefully crafted emails that are meant to fool individuals into relaying their usernames and passwords to those systems or by having them install malware, among other strategies.

7 Sakula malware utilizes Dynamic Link Library (DLL) associated with *PlugX* activity to conceal itself from its targets.

8 "OPM Breach Analysis: Update - ThreatConnect | Enterprise Threat Intelligence Platform." ThreatConnect Enterprise Threat Intelligence Platform RSS2. ThreatConnect, 9 June 2015. Web. 21 Aug. 2015. http://www.threatconnect.com/opm-breach-analysis-update/.

9 Ibid

10 Sergio Caltagirone, Christopher Betz, and Andrew Pendergast. "The Diamond Model of Intrusion Analysis." *Dtic.mil*. US Government, 2013. Web. 28 Aug. 2015

11 "Chinese Hackers Violated Systems at the Office of Personnel Management." *Security Affairs*. 11 July 2014. Web. 21 Aug. 2015

network monitoring and data analytics platform to identify several technical characteristics that support their analysis.

The OPM data breach was more than a singular event or a series of unrelated singular events; it was a protracted and thoughtful campaign by an adversary with a deliberate target. Using Lockheed Martin's "cyber Kill-Chain" methodology (see Annex B), we find that OPM's networks were under persistent reconnaissance and penetration for a period of time that spanned years. The individual events that led to the data breach were a part of a collective campaign against OPM and its partner organizations that went unnoticed by OPM Information Technology specialists. While OPM was quick to dismiss early attacks after the onset of the first breach that was revealed to the public in July of 2014, it becomes clear the initial events were a smaller part of a much larger campaign. The OPM IT team – with its small analytical capacity and limited capabilities – did not take a strategic view of what the adversary might be attempting to do during its initial breach.[12] In the face of an advanced persistent threat that is routinely probing our government systems, we cannot afford to take such a lax approach. In today's highly networked world, leaders must place emphasis –in the form of leadership direction and focus, policy, budgets and hiring – on cybersecurity as a priority for their organizations.

Protective Measures and Actions Taken by OPM

As we learn more about OPM's poorly defended networks, it becomes evident that the hackers need not have relied upon *advanced* tactics to infiltrate OPM's network; the security of the networks was lacking to a point the adversary could have relied upon basic methods and elementary tactics to be successful in their campaign. The November 2014 OPM Inspector General Report shows the agency's poor security program left OPM vulnerable to cyber-attacks in many areas and seemed to invite the catastrophe that would be revealed in the summer of 2015. As the data and case studies presented in this paper show, a culture of tolerance for negligent network security was the primary culprit that led to breach.

The intrusions and subsequent data theft were made possible by a

12 As will be demonstrated in subsequent sections of this paper, OPM's small information technology team did not have the resources and personnel that would have been necessary to detect what we now know what a persistent campaign against its networks. Due to its limited budget and small size, the OPM IT team tended to view intrusion events in and around its networks as stove-piped instances that had no connection to one another. Ultimately, this mentality would be proven tragically false and would lead to the world's largest known data breach.

fundamentally flawed approach to cybersecurity at OPM. As early as 2007, the OPM Inspector General (IG) identified agency security practices as a "material weakness" to national security, yet the agency did not hire its first professional IT staff until 2013.[13] By 2014, the agency had hired only seven IT staff members, with only four more in its training pipeline[14]. As of November 2014, the IG noted that OPM had failed to routinely audit its systems and that the agency had no understanding of what machines were or should be connected to its network; they had no list of servers, databases, or network devices.[15]

The apathy of OPM leadership is most obviously displayed in the organization's lack of focus on cybersecurity resources, processes, and a complete lack of a unified effort to defend its networks. OPM failed to adequately monitor its network for even the most benign of security threats and, as the annual IG reports show, the agency's IT staff had no sophisticated methodologies for identifying APT activity. As the agency dismissed earlier instructions from its IG to harden its networks, its adversaries reinvigorated their efforts to penetrate OPM networks and simply found other ways in. Because OPM lacked basic cybersecurity tools and capacity for analysis – such as the "Diamond Model" or the well-known "Kill-Chain" methodology – it had no hope for identifying the presence of an ongoing campaign against its systems.

The 2014 OPM Inspector General Report shows that basic protocols and standards for protecting the information were not followed by government employees. Seven systems out of twenty-five had inadequate documentation of security testing, four of which were directly maintained by OPM's IT department. In 2013, it was confirmed that hackers had stolen the Cold Fusion source code from Adobe, making it susceptible to reverse engineering attacks. Contrary to reasonable security practices, the OPM system administrator continued to use Cold Fusion in conjunction with outdated Operating Systems such as Windows XP. The report also found that many core systems that hadn't been updated since Y2K.[16] Additionally,

13 "OPM 2013 IG Report." *Opm.gov*. US Government. Web. 21 Aug. 2015.

14 Gallagher, Sean. "Why the "biggest Government Hack Ever" Got past the Feds." *Security and Hacktivism*. Arstechnica, 8 June 2015. Web. 21 Aug. 2015. http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/.

15 Gallagher, Sean. ""EPIC" Fail—how OPM Hackers Tapped the Mother Lode of Espionage Data." Security and Hacktivism. Arstechnica, 21 June 2015. Web. 17 Aug. 2015. http://arstechnica.com/security/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/.

16 Urrico, Roy. "OPM's Weak Security Led to Breach: Report." *OPM's Weak Security Led to Breach: Report*. Credit Union Times, 23 July 2015. Web. 21 Aug. 2015. http://www.cutimes.

due to the lack of realistic threat simulation by red-team tests and penetration attacks, the OPM networks were virtually defenseless when facing a real-life threat.[11] The IG report also showed that OPM failed to maintain accountability of its systems, and lacked procedures to enforce corrective measures for deficient and insecure systems.

As was indicated in the IG report, OPM did not encrypt its databases that contained large amounts of government employee information. OPM attributes the lack of encryption standards to "old" hardware and low budgets, yet federal PII standards require the protection of social security numbers, fingerprints, and other information - all of which were present on OPM servers.[17] Although OPM was in the process of implementing two-factor authentication (Common Access Card (CAC) and Personal Identification Number (PIN)), none of their systems were using this security feature at the time of the attack.[18] In the House Committee on Oversight and Government Reform hearing after the attack, OPM chief information officer Donna Seymour lamented on the difficulties of securing OPM's networks: "A lot of our systems are aged. […] Implementing [security] tools take time, and some of them we cannot implement in our current environment."[19] Seymour's defense is unacceptable and a fundamentally flawed approach towards securing government systems. Her logic shows the agency did not prioritize cybersecurity as a part of the agency's mission, and did not take steps necessary to overcome resource obstacles in order to prevent data breaches compromising US national security.

OPM was successfully attacked despite having DHS "Einstein" network monitoring sensors in place. While some speculate the sensors eventually detected the 2015 attacks, evidence shows that they initially failed to detect intrusions into the network due to Einstein's reactive nature and inability to evolve to dynamic threats.[20] Even if Einstein was more dynamic, most security experts agree that even

com/2015/07/23/opms-weak-security-led-to-breach-report.

17 Perera, David. "Office of Personnel Management Didn't Encrypt Feds' Data Hacked by Chinese." Cybersecurity. Politico, 4 June 2015. Web. 17 Aug. 2015. http://www.politico.com/story/2015/06/personal-data-of-4-million-federal-employees-hacked-118655.html.

18 Norton, Steven, and Clint Boulton. "Years of Tech Mismanagement Led to OPM Breach, Resignation of Chief." The CIO Report RSS. The Wall Street Journal, 10 July 2015. Web. 17 Aug. 2015. http://blogs.wsj.com/cio/2015/07/10/years-of-tech-mismanagement-led-to-opm-breach-resignation-of-chief/.

19 Boyd, Aaron. "OPM Breach a Failure on Encryption, Detection." *Federal Times*. 22 June 2015. Web. 4 Sept. 2015. http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/19/opm-breach-encryption/28985237/.

20 Unfortunately, the current version of Einstein has proven to only be useful for post-attack remediation. This is due to the fact that only known threats are uploaded to Einstein, which

dynamic intrusion prevention systems fail from time to time and must be heavily managed by qualified security personnel. While security technology is helpful in identifying adversarial behavior on networks, it cannot be seen as definitive solution for security networks. Given the advanced and persistent nature of cyber threats, organizations cannot rely solely upon national cybersecurity constructs as a plausible line of defense against cyber intrusions.

While DHS plays a role in protecting and coordinating defensive actions across the many organization's that comprise the government bureaucracy, this paper argues that each organization must have the capability to conducts its own threat analysis. If the government wishes to prevent events such as this from happening again, high speed and high tech security measures coupled with adequately trained IT staff must be implemented at all levels and for all organizations. This will allow leaders to detect and prevent known threats as well as to defend against unknown threats and react with agility upon discovery of new methods or advanced malware signatures. Each organization must be prepared to support its own cybersecurity at the tactical and operational levels while expecting DHS to provide strategic resources and support. Given its apparent reliance upon Einstein as its primary network security mechanism, it appears that OPM was too reliant upon DHS for cybersecurity and did not take ownership of its networks.

Despite the vast technical issues, the main failings of OPM do not lie in its legacy systems or inadequate security tools, but rather in its failure to enforce government IT policy and implement a supportive budget or hire skilled professionals to administer its system. This reflects the priority given to information security and protecting valuable data by OPM leaders. Even the best security tools and technologies are inert without trained and competent personnel. What's more, those personnel must be empowered through policy and leadership to secure networks and implement technological solutions as required. The post-incident response to the event also indicates an absence of effective policy, planning, and leadership throughout the remediation process. As a result, the fallout from the breach may actually increase due to poor post-incident response by the agency. To date – over three months after publically disclosing the breach – the agency has failed to notify the majority of the 22 million individuals who were affected by the breach.[21] In the

then inspects network traffic for all instances of threats that look like any other threat it has "learned" about; the current capability is not self-learning or dynamic enough to adopt to current threats.

21 McAllister, Niel. "Victims of US Gov't Mega-breach Still Haven't Been Notified." • *The*

absence of notification, government employees may get a false sense of security and assume that their data has not been compromised. As a result, the government employees effected may fail to take appropriate mitigation measures which could have limited the overall impact to the collective organization. Once again, such missteps by OPM indicate systemic issues with its security program's management; the lack of a post-incident response plan further detracts from the confidence in the US government's ability to secure its networks.

During the 2015 Black Hat conference, a new cybersecurity mantra, "if you can't protect it, don't collect it," emerged to reinforce norms that sensitive data should not be collected and stored if leaders or organizations are not willing or capable of allocating resources for information security.[22] [23] What's makes OPM's case tragic, is that a simple risk assessment and prioritization of resources to mitigate threats could have overcome their deficiencies; this is the responsibility of a leader in a government organization. In the case of OPM, the agency should not have stored PII unless it had the willingness and resources to protect such data, which – as we now clearly see – compromised national security. As leaders of a government agency with such a critical mission, Seymour – and Director of OPM, Katherine Archuleta - failed as leaders because (1) they did not prioritize cyber defense of its systems, (2) rectify resources deficiencies to support cyber defense, or (3) segregate the data of importance from the network.

Linkages to Other Events

Because of OPM's failure to defend its networks and respond appropriately to the breach, some in the cybersecurity community have downplayed the importance of focusing on the actors behind the attacks and instead called for an emphasis on cybersecurity "lessons learned" that will prevent future failures by the government. This paper argues that consideration of both are equally important. While the failure of OPM to secure its network is a natural point of focus, it is essential that we in the security community examine the strategic implications behind this attack as well. The previous portion of the paper focused on lesson's learned, and this portion focuses on the strategic context of the OPM attack. Initial indications from

Register. 2 Sept. 2015. Web. 4 Sept. 2015. http://www.theregister.co.uk/2015/09/02/opm_data_breach_notices

22 Black Hat is a seminal security and hacking conference that occurs each year in Las Vegas.

23 Bejtlich, Richard. "New Cybersecurity Mantra." *The Brookings Institution*. 3 Sept. 2015. Web. 28 Sept. 2015.

two well-known security firms, Mandiant and CrowdStrike, indicate that the OPM hackers were using Tactics, Techniques, Procedures (TTPs) similar to those of known Advanced Persistent Threats (APT) and have been attributed to previous attacks. The OPM breach is far from unique: over the last 5 years, there have been breaches of organizations that either shared the same TTPs as the OPM hackers, or have had related targets (i.e., the USIS/Keypoint breaches). By analyzing and comparing the data from these previous breaches, patterns can be established that shed light not only on how the hackers accessed these systems but also why. Once again, the Diamond model is a useful model to shape analysis and identify linkages between multiple events (see Annex B and C for ACI TAC interpretation of the data). [24]

The first attack we examine is against a firm with a long standing relationship with the US government. An organization formerly known as the United States Investigative Service, USIS – a contracted associate of OPM, which had been responsible for conducting government security clearance investigations since the late 1990s. Their contract was terminated following the discovery of a recent data breach. The USIS compromise started in April 2013 and was discovered in June 2014. During this period, approximately 25,000 personnel records were stolen. Although this number is large, the most important data that was stolen was not the records but rather the blueprints and information behind the structure of OPM's networks. The breach was linked to China, yet experts cannot pinpoint an exact origin. This intrusion was largely blamed on USIS's lack of network security. The government ironically sued USIS for its network security failures (in addition to its negligence that enabled Edward Snowden and Aaron Alexis to receive security clearances). In September of 2014, OPM cut ties with USIS and switched to another security contractor, Keypoint[25].

The Keypoint breach started prior to its relationship with OPM. While OPM attempted to secure its networks by switching service providers and "cutting off" access to USIS, it was instead contracting with another compromised associate. In total, about 48,000 personnel files were stolen, which is thought to have occurred during the timeframe from December 2013 to September 2014. While few details

24 "Methodology - ThreatConnect | Enterprise Threat Intelligence Platform." *ThreatConnect Enterprise Threat Intelligence Platform*. Web. 18 Oct. 2015.

25 Bisson, David. "The OPM Breach: Timeline of a Hack." The State of Security. Tripwire, 29 June 2015. Web. 17 Aug. 2015. http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/.

were given to the public about this initial compromise, Keypoint did publically disclose that a second breach occurred; the announcement was made in the aftermath of the 2015 OPM breach disclosure. This second breach included as many as 390,000 stolen files. [26]

A third attack against Anthem – an insurance provider that services government employees – is another significant event that shares some similarity with the OPM attack. This attack started in December 2014 and was discovered January 29th, 2015. The attacks on Anthem targeted information that specifically dealt with government employees and their PII.[27] Overall, 80 million customers were affected. Consistent with the OPM data breach, there is little evidence that the data stolen from Anthem has been used for financial fraud.[28] Also, both the OPM and Anthem breaches used stolen certificates from a Korean software company known as DTOPTOOLZ Co. in order to gain access to the compromised systems.[29] In fact, the methodology in which the attacks were carried out were almost identical, probably, by design rather than coincidence. In both instances the Sakula malware family was used, and in both instances a Command and Control, or C2, node was created with a fake domain name that mimicked actual domain names. Because Anthem was called WellPoint at the time, the breach used the fake domain name "we11point.com" with "1's" - instead of "l's"- in order to disguise itself as regular network traffic, just as the OPM breach used opmsecurity.org and opm-learning.org.[30]

Theses similarities point to an advanced, persistent attack aiming at a clear target, indicating that both OPM and Anthem were victims of calculated focus rather than opportunity.[31] Deliberate efforts to infiltrate government networks and its third party affiliates are indications of an ongoing campaign against the US. Subsequent portions of the paper will focus on trends in those various campaigns and the impact such efforts will have upon the US government and its national security.

The difficulty of attack attribution does not diminish the responsibility of examining the larger picture; as our study will demonstrate, the OPM breach is likely

26 Ibid.
27 "How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services." Anthem, 8 May 2015. Web. 17 Aug. 2015.
28 Threatconnect Intelligence Research Team. "The Anthem Hack: All Roads Lead to China." ThreatConnect Enterprise Threat Intelligence Platform RSS2. Threatconnect, 27 Feb. 2015. Web. 17 Aug. 2015. http://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.
29 Ibid.
30 Ibid.
31 Ibid.

the next phase of a much larger effort that seeks to undermine the US government's cybersecurity and national power. We expect the data obtained through the OPM breach could be used to shape the environment for future operations. Given this significance, it is important to examine the linkages between the OPM breach and similar attacks.

Usage for Stolen Data

Given the magnitude and comprehensive nature of data ex-filtrated from the OPM servers, there exist two broad categories of malicious usage for the data that affect government employees:

1. ***Illicit Financial Gains and Identity Theft*** - As has been noted above, PII data holds enormous value due to its fixed nature. While credit cards can be deactivated and replaced, social security numbers and biometrics data cannot be changed. Because of such properties, PII is highly valued on various darknet marketplaces; PII data substantiates an underground multi-million dollar criminal industry.[32] Because of the lucrative financial incentives involved, the first obvious use of this information to any common criminal would be to either sell the personal information on the deep web or exploit the personal information for financial gain through credit card fraud. However, if the Chinese government has the information, there are many more possibilities for what could be done with the data. We will elaborate on these possibilities below.

2. ***Espionage and Exploitation by Chinese Government*** - The stolen data is also thought to be of tremendous value for foreign espionage purposes. The Chinese government, for instance, allegedly uses such information and knowledge to support its attempt to recruit and/or blackmail American government workers. By using each piece of PII - as well as "big data" analytics and statistical approaches– the Chinese government can identify potential "weaknesses" or employees that may be susceptible to manipulation due to financial problems, medical problems, or other vulnerabilities to exploitation or subversion. The information could also be used to blackmail employees about embarrassing relationships or other personal information that they would not want exposed. Moreover, the TTPs that link the OPM attacks to its contractors and to Anthem strengthen the argument that the OPM attack was part of a larger campaign against government personnel, not an isolated event. The hypothesis of data being used for intelligence value is supported by fact that the data associated with all of the collective events has the common link of being associated to government individuals

32 From http://searchnetworking.techtarget.com/definition/darknet : "A darknet is a routed allocation of IP address space that is not discoverable by any usual means. The term is used to refer to both a single private network and the collective portion of Internet address space that has been configured in that manner."

An article published in the Los Angeles Times confirms that the stolen OPM data is already being used for espionage purposes:

> Foreign spy services, especially in China and Russia, are aggressively aggregating and cross-indexing hacked U.S. computer databases – including security clearance applications, airline records and medical insurance forms – to identify U.S. intelligence officers and agents.[33]

We assess the most important application of the data will facilitate additional offensive cyberspace operations and support numerous and various intelligence operations. Given the ease with which the data can be reproduced, it is likely the data will be used to achieve multiple ends. It is possible the hackers serve both national and criminal interests, and are willing to resell the data for multiple uses (both espionage and criminal activity). Diverse usage of the data would lend support to the Chinese government's "plausible deniability", as it easily refutes its involvement if the data were to manifest within the dark net. For these reasons, employees should assume their data will be used to support both espionage and fraud. Evidence gathered by the authors indicate that on some level, issues with criminal fraud and ID theft are already being experienced by small numbers of US Government employees.[34]

Perverse Incentives: Why Public Organizations Don't Care About Security

In order to better understand the dynamics behind the government's failing to secure its data, this section explores incentives that motivate data loss protection (DLP) in the private sector and compares them to the incentives towards DLP in the public sector. In both the public and private sector, organizations are responsive to incentives that drive decision making. Because private and public organizations are motivated by different incentives, their behavior is often distinct when it comes to cybersecurity. In the private sector, these incentives consist of market forces that drive firms towards profit, while the public sector incentives occur in various other forms.

In an October 2014, David Chavern, the United States Chamber of Commerce President of the Center for Advanced Technology and Innovation warned of the

33 Bennet, Brian, and AJ Hennigan. "China and Russia Are Using Hacked Data to Target U.S. Spies, Officials Say." Los Angeles Times. Los Angeles Times, 31 Aug. 2015. Web. 2 Sept. 2015.

34 King, James. "Stolen Data On Federal Workers Is Worth $140 Million." *Vocativ*. Web. 18 Oct. 2015.

startling difference between commercial collection of data and government collection of data.[35] Chavern recounts that the government has been quick to scorn companies for aggregating data on individuals at the possible cost of breaching their privacy, but has made no statements about the government's own programs and systems used to maintain similar datasets. Most commercial data collection has some mechanism for "opting out", however, the government has provided no clear guidelines for how to opt-out of its collection programs. More exacerbating is the government may be less motivated to increase data security as threats become increasingly sophisticated.

The 2011 Ponemon study, "The True Cost of Compliance" surveyed a set of organizations to determine how the costs for achieving and maintaining information security compliance compared to the costs of handling a data breach in association with noncompliance. The study found that costs for noncompliance are at least 2.65 more expensive than simply spending the required money to achieve baseline cybersecurity standards.[36] Furthermore, the fact that applicable laws and regulations are the number one motivator for organizations to place importance on compliance efforts is concerning.[37] Sarbanes-Oxley and Payment Card Industry (PCI) standards are in large part responsible for expediting the securing and auditing of security compliance at many organizations in the study. It is unclear whether any of these regulations apply to government organizations, and what punitive measures are possible for failure to comply.

In a common data loss case study involving ChoicePoint Inc., a 2005 data breach of public record aggregation and marketing data on thousands of consumers drew backlash from the federal government.[38] The loss of thousands of aggregated personal information profiles caused much of the current privacy debate to begin and caused state legislatures to begin introducing privacy laws nationwide.[39] The language used by US Congressional Representatives in a Hearing on Protecting Consumer Data as part of the 109th Congress, in the Committee on Energy and

35 Chavern, David. "The Power of Big Data." The Power of Big Data. October 16, 2014. Accessed August 11, 2015. https://www.uschamber.com/above-the-fold/the-power-big-data.
36 Ponemon Institute. "The True Cost of Compliance." January 2011.
37 Ponemon Institute.
38 Brodkin, Jon. "ChoicePoint Details Data Breach Lessons." PCWorld. June 10, 2007. Accessed August 14, 2015. http://www.pcworld.com/article/132795/article.html.
39 Sullivan, Bob. "ChoicePoint CEO Grilled by Congress." Msnbc.com. March 15, 2005. Accessed August 14, 2015. http://www.nbcnews.com/id/7189143/ns/technology_and_science-security/t/choicepoint-ceo-grilled-congress/#.Vc32ThRjZQI.

Commerce, is very significant to today's issues.[40] In Congressional testimony given by ChoicePoint legal staff and executives, Congress pointedly remarks that ChoicePoint was responsible for their buying, selling, and failing to protect customer data. In hindsight, it is evident that in many of the legal regulations of which ChoicePoint was noncompliant, federal agencies may also still be non-compliant. In fact, the hearing brought to light many data protection and privacy provisions under the Sarbanes-Oxley (SOX) and Gramm-Leach-Bliley Acts (GBLA) that require security standards under Securities and Exchange Commission (SEC) or Federal Trade Commission (FTC) regulations.[41] These data protection laws and regulations are relevant because according to a 2011 Ponemon data breach study, these laws were the most important corporate reason for a company to spend money on data security.

While the government's response to ChoicePoint was quick to denigrate their lack of data protection and privacy standards, it is unclear what the fallout will be for the loss of so much personal data in the OPM data breach. Furthermore, customers doing business with ChoicePoint had the option to choose other data providers in order to allow market forces to work on the data security expectations of the data compilation industry. OPM, on the other hand, was in the business of acquiring, storing, and managing employee data on millions of Americans, but had no market incentive to innovate and become more secure. Furthermore, it is unclear what federal regulations that apply to publicly traded companies also apply to government agencies as well. The data lost in the OPM data breach was far more extensive and personal in nature than any other breach to date. While other data breaches (ChoicePoint, Target, Home Depot, etc.) may have had financial effects on consumers and the economy, it remains unclear what damages will occur from the loss of OPM data, which included polygraph data, Standard Form 86 (SF-86) documents, and known associates and references for federal employees that underwent a security investigation.

When a major network intrusion to the extent of OPM occurs, incident responders may be able to quickly remediate the vulnerability that allowed unauthorized access and the loss of data. What is not known is if the intruder, while in the network, was able to insert other vulnerabilities such as malicious software or false credentials

40 Protecting Consumers' Data: Policy Issues Raised by ChoicePoint. Hearing before the Committee on Energy and Commerce, United States House of Representatives, 109th Cong. (2005).

41 Ibid

that could allow them re-entry even after the detected security flaws are corrected. A major step in an incident response is containment. In the case of total network compromise, it may take a long time before the network can be considered secure enough to resume normal operation and to fully trust that the data will not be lost again shortly after services are restored.[42] Given the comprehensive nature of the required response, organizations must be prepared to invest significant resources into the remediation of a cybersecurity event.

According to one security blog, suffering a major data breach "is like having a financial bomb go off in your company."[43] The cost cannot only be in loss of customer loyalty, but in legal and regulatory penalties, as well as costs for cleaning up after the breach. While it is certain that OPM is paying a financial cost at the expense of the federal budget, their primary objective is not to make profits and therefore financial damages will not help to fundamentally change the cybersecurity culture of the agency. Rather, the effects of the data lost by OPM to nation-state adversaries should cause all federal agencies to rethink their data security and protection measures and to be prepared for decades of vulnerabilities to network intrusions, insider threats, and espionage. In the absence of the market incentives that are proprietary to the private sector, public leaders must provide guidance that security is a priority for their organizations.

Impact to the DOD

The OPM breach is already being referred to as the "Biggest CI Threat in our Lifetime." It has clearly become the biggest breach in human history, affecting millions and virtually all current and former living government employees. Some employees are exposed more than others because of the breach (i.e. Americans with familial or social ties to Chinese, Russian or Korean foreign nationals), yet all are more vulnerable targets for financial fraud or foreign espionage.

To the US defense community, this attack is particularly disturbing. DOD has a responsibility to defend the nation from attacks in any domain in order to ensure that American citizens are secure. Logically, this includes the protection of

42 SANS Institute. "Incident Handler's Handbook." SANS Institute – InfoSec Reading Room. The SANS Institute, 2012.

43 Charman, Morgaine. "Cost Fallout of a Data Breach Felt for Years." Cost Fallout of a Data Breach Felt for Years Comments. February 4, 2015. Accessed August 14, 2015. http://www.vitrium.com/document-security-protection-drm-blog/cost-fallout-of-a-data-breach-felt-for-years/.

assets in both the public and private spheres. It is difficult to instill confidence in the American public, however, when government agencies fail to protect their networks in accordance with federal law. As many cybersecurity case studies demonstrate, the bulk of security incidents are caused either by (1) apathetic or untrained users - i.e. the OPM breach caused by a simple phishing attack - or (2) poorly mismanaged security programs - i.e. OPM's non-compliance with FISMA standards. Both of these problems can be attributed to poor leadership and bad management. If the U.S. government is going to make headway in securing its networks, it must start with organizational leadership.

In the ChoicePoint case study, the firm lacked market incentives to drive the company to secure its customer's data. Through policy and legal interventions, however, ChoicePoint was forced to adjust its cost/benefit analysis in favor of securing the data in the face of financial penalties. As stated earlier, no such mechanisms exist in the public sector at this point in time. While government employees are susceptible to punishment for gross negligence, this practice is rarely done in the public sector. In order to incentivize change in the government, commanders and leaders must take charge of their organization's network security posture, which means that IG-identified deficiencies are quickly addressed and not allowed to subsist for over seven years, as is the case of OPM. National leaders must, in turn, hold those individuals accountable and these areas of emphasis must be demonstrated through the proper allocation of budgeting and hiring of trained personnel. Leaders can no longer see network security as an "IT problem", but as a problem that can - and has - undermined the entire organization's ability to accomplish its collective function.

Impact to the Nation

Beyond the organizational level, the ongoing campaign of cyber-attacks has the potential to undermine our national security in a damaging and lasting manner. The internet has leveled the playing field for our nation's adversaries, providing technology to collect and transmit intelligence on US programs with speed and ease. As a consequence, American adversaries are postured to continue their success at exploiting vulnerabilities in poorly defended networks to export technology, data, and intellectual property at an increasing rate. Since the fall of the Soviet Union in 1991, the US military has been dominant in traditional warfighting domains: land,

sea, air, space. With the growing reliance of network centric warfare and the advent of cyberspace as the latest warfighting domain, the US finds itself at a crossroads in its efforts to maintain its leadership in the global arena. While nations like China and Russia have been relatively benign over the last two decades, American leaders and policymakers must not discount the newfound power that these nations now possess in the age of cyber weapons and exploitation.

Because of this tremendous gap between the capabilities of the US and competitor nations, the world has been a relatively safe place to live in terms of interstate conflict. Unlike previous eras, however, cyber weapons are remarkably cheap to make, easy to reproduce, and are capable of traversing time and space in a matter of seconds. Perhaps most alarming, all of this can be done with complete anonymity, giving the U.S. little hope of punishing or deterring the perpetrator or the facilitating nation state.

The adversary's computer network operation against OPM did not meet the threshold of physical destruction that conventional weapons can cause, but the potential for such an attack has increased. The attack on OPM demonstrates that cyber activities are an effective capability against the world's largest superpower. It provides evidence that nations can challenge US military supremacy, which undermines the international community at large. As the world's largest superpower and a significant proprietor of many global institutions, some scholars predict that a contested US military is dangerous for the global community at large.[44]

Summation and Closing

The solution to the cybersecurity dilemma facing the nation lies in the responsiveness of our organizations' collective response to this event and adoption of a culture that values cyber defense as a critical mission necessary to every organization. The OPM data breach highlights several ongoing complex issues related to the developing discipline of cyber operations. There are no easy, quick wins to contain the damage from this event. If we are to maintain our preeminence in the cyber domain, however, we must come to grips with these issues and overcome these obstacles. As this paper argues, the OPM breach should not be viewed as a singular event, but as an ongoing cyber campaign against government and related systems. In concert with the "Cisco 2015 Midyear report" and the Mandiant "M-Trends

44 Kagan, R. (2012). *The world America made*. New York

2015" report, we have identified several trends that are particularly relevant and concerning in the wake of the OPM hack:

1. ***Increased regularity of data breaches*** – Data breach frequency, size, and scope have and will continue to rapidly increase within the coming years. Advanced Persistent Threat actors will continue to attack unclassified networks that contain government and related information. High visibility targets include those associated with transportation and financial critical infrastructures.

2. ***Security's struggle with quickening pace of innovation*** – Security professionals are struggling to keep up with the pace of innovation that the adversary has been able to maintain. Cyber actors acting offensively will continue to have the advantage in the cybersecurity world. Patch management programs are currently being outpaced by the enemy's ability to innovate and find new vulnerabilities in systems.

3. ***A lack of quality cybersecurity talent*** – Currently, there is a grave shortage of competent IT security professionals in the workforce. In the case of OPM, this shortage was apparent throughout the 2014 IG report, which stated that the agency had only been able to hire four trained security experts to maintain security for its vast network of systems.

4. ***Stopgap solutions are preferred over defense in depth*** – As seen in the OPM case, companies are too often relying upon singular technologies as a primary defense against APTs. The OPM case shows that this logic is deeply flawed, and that organizations must employ "defense-in-depth" strategies in order to make their networks more secure.

5. ***Phishing and Whaling activities are on the rise*** – These activities are on the rise, and are increasingly becoming more sophisticated. Adversaries are using sophisticated methods involving data science to craft computer generated "landing pages" that are more effectively exploiting users.[45]

6. ***Stolen data being used for a variety of purposes*** – Our adversaries use aggregated data and singular data sets to extrapolate information for both intelligence and financial gains. Specific to espionage concerns, there is a growing fear that nation states will use the data to cross-reference separate data sets for the purpose of further exploiting the information to expose identities of intelligence personnel

45 Merriam-Webster defines phishing as "a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly". Whaling is a more targeted version of phishing: It aims to collect personal information from high-profile individuals such as CEOs or highly-visible individuals.

that are working abroad.[46] Worse yet, nation states like Russia and China are reportedly collaborating and sharing intelligence on their mutual efforts to exploit US systems.[47]

At the heart of the OPM event is a central question: What is our data worth? If we were to judge the value of the lost information based on the actions taken to mitigate the damages, failure to confront the adversary, and safeguard the victims, we might conclude that the data was worth nothing. If we assume a broader, more expansive view of the question we assess that this data should be valued in terms of trust, integrity, and confidence. These concepts are so inherent in our day to day actions and our assigned responsibilities that they often go unspoken in our review of performance and outlook for future operations and commitment of resources. In this case, the trust, confidence, and integrity of the US government's ability to protect itself from outside intrusion, safeguard the people executing the duties required in the everyday functions of our system, and maintain information assurance of its assets is now questioned. In our estimation, we should begin the process of assigning value to the data in our possession for the purposes of prioritizing its collective defense. In our view, if we are not able to commit to securing their data, then they should not be using or collecting it in the first place.

Achieving dominance in cyberspace implies that collectively America can safeguard its own networks from intrusion, and that any intrusion achieved by the adversary is limited, contained, and severed in short order with response actions to correct the deficiencies, prevent their reoccurrence, and hold the perpetrator accountable. Nearly six months have passed since the breach was acknowledged publicly, the accountable organization has still not begun in earnest the notification process to the 22 million Americans affected. Because of this, our credibility wanes ever more. The credibility of the government's ability to protect itself and her people has been damaged repeatedly. This in part creates a widening gulf between the

46 Betrand, Natasha. "Russia and China Could Be 'making It Impossible for the US to Hide' Its Intelligence Activities." *Yahoo Finance*. Yahoo, 31 Aug. 2015. Web. 4 Sept. 2015. http://finance.yahoo.com/news/russia-china-could-making-impossible-205952714.html.

47 "CNN and the Los Angeles Times reported this week that Russia and China – whose leaders are meeting in Beijing for two days to discuss bilateral negotiations – have used a massive database analysis to combine and cross-reference information obtained from cyberattacks on targets that range from the Office of Personnel Management to Ashley Madison to identify and potentially compromise operatives." Quote taken from http://www.upi.com/Top_News/World-News/2015/09/02/Russia-China-using-hacked-data-to-target-US-spies/6481441041586/, 2 September 2015.

public and private sector, leaving another vulnerability for the adversary to exploit and an obstacle for American cyber professionals to overcome. Perhaps this is the greatest impact. Trust and integrity play a great role in relationships. The US governments' relationships with its citizens and its dealings with foreign partners suffer when that trust is damaged.

In response to the question "what is our data worth?" in the public sphere, we propose a simple answer: that our data is only worth as much as the commander and organizational leaders value it. To correct our security deficiencies, the government must hold leaders accountable and instill a sense of urgency at the organizational level, just as General Washington did in the era of a post-Benedict Arnold army. Commanders at the "tactical level" must take ownership of their networks and instill a sense of urgency in their employees. This emphasis needs to be more than just rhetorical; it is something that needs to be appropriately reflected by standing orders, hiring processes, and security budgets.