Handing Over the Keys to the Castle

OPM Demonstrated that Antiquated Security Practices Harm National Security

Institute for Critical Infrastructure Technology

July 2015

In this digital age, information is secured, coveted, and exfiltrated by nation states, hacktivists, and ambitious actors because, now more than ever, knowledge is power. Modern needs dictate that only authorized users know information, that authorized users can access information instantaneously, and that the integrity of information is certain. In opposition to these aspirations, an incessant tide of cybersecurity threats, spread across an unfathomably complex cyber-threat landscape, batter the defenses around any valuable store of information. Adversaries seek to discern and exploit any minute vulnerability that could compromise the defenses and expose the wealth of knowledge inside. Information security professionals often view convenience and security as a tug-o-war over controls and resources. A fickle balance between convenience and security actually exists for the organizations with the knowledge to pursue it and vigilance to adapt their defenses to emerging changes in the threat landscape. The increasing annual number of successful breaches indicates that organizations and governments alike are not correctly balancing security with convenience due to antiquated systems and decades of poor security practices. If information is seen as a treasure hoard, then the cybersecurity infrastructure around it is the great fortress that is built by its people, founded on their technology, and maintained by their security practices. The employment of reliable technology, superlative security practices, and knowledgeable people culminates in a multilayered, integrated defense that is resilient to threats. The majority of inbound threats are thereby thwarted against its ramparts and the impact of the few successful breaches is minimized to acceptable losses. No adversary or persistent attack compromises either the cybersecurity infrastructure or the integrity of the information secured within.

Within the last month, the world has witnessed the failings of the ill-equipped personnel, antiquated cybersecurity infrastructure, and abysmal security practices at the United States Office of Personnel Management, which resulted in the exfiltration of granular personal information of at least 22.1 million, former, current, and perspective United States employees along with their families, friends, and known associates. The culmination of a series of breaches at OPM and two contractors, USIS and Keypoint, has provided a successful adversary access to granular information pertaining to arguably the highest value, 15% of the

United States population, everyone who has applied for or possessed a security clearance since the year 2000.

Background:

In November 2013, actors breached OPM systems and exfiltrated manuals relating to network assets and information about the internal infrastructure. In August 2014, USIS, an OPM offshoot/ contractor that conducted background checks, disclosed a breach of its systems, which upon investigation had lasted for over a year and may have compromised the information of approximately 27,000 DHS employees. All contracts with USIS ended and OPM delegated all background checks to Keypoint. In December 2014, Keypoint disclosed a breach of its network, which had lasted at least 10 months and may have compromised the information of 48,439 federal workers. In June 2015, OPM disclosed a breach, dating to October 2014, of systems maintained at a Department of the Interior shared-services data center and leading to exposure of an estimated 4.2 million personal records. About a week later, investigators from U.S. Cert and DHS discovered and disclosed a larger breach of the OPM systems dating to March 2014. Applicants for clearances complete a 127 page Standard Form-86 (SF-86) which contains all of their personal information, work history, family, associates, deviances, and proclivities. In the latter breach, 21.5 million SF-86 were successfully exfiltrated by an unknown actor. Discounting those affected by contractor breaches, those affected by both OPM breaches, and the family members affected by the breaches and information on the SF-86, then adversaries may have the personal information of 22.5 million Americans, many of which possess highly classified clearances.

The successive nature and duration of the breaches at OPM and its contractors indicate infiltration by an Advanced Persistent Threat (APT). Advanced persistent threat groups are motivated and highly dedicated adversaries who often receive resources and direction from larger organizations, such as nation states. APT activity can be identified through discernable operational patterns, remaining indicators of compromise of target systems, target profiles, coordination of attacks, resource investment, and the sophistication of the attack. APT's operate as an invasion force. They tenaciously pursue their goals by utilizing a wide range of

tools and tactics that best allow them to steal data, destroy infrastructure, or poison trusted stores of information undetected. They often acquire specialized information about the target, its infrastructure, and its personnel prior to a dedicated attack. The information is used to initially compromise the target, establish a foothold in their systems, and strengthen the adversary posture by establishing backdoor s and laterally moving to compromise other systems. The adversary uses prolonged internal reconnaissance to identify valuable data, the adversary exfiltrates the data over an extended period, and then the adversary laterally moves to another system to repeat the process until all valuable information is harvested or the breach is detected. Sometimes the malware or tools in the attack are specialized and can be used to attribute the attack to an actor group. Other times, information about the target and data stolen can be used to guess the motivation of the attack and narrow attribution to a pool of possible actor groups. However, adversarial motivation is difficult to portend because organizations do not always recognize the value of their data or consider that their adversaries may have targeted an organization in order to gain access to a different organization.

Details confirming how adversaries breached OPM and the indicators of compromise necessary for accurate attribution of the attack, remain classified. Numerous officials, including U.S. Intelligence Chief James Clapper, have attributed the attack to China. FireEye, iSight Partners, and other firms attribute the attack to a Chinese state sponsored APT group referred to as “Deep Panda.” Deep Panda steals PII from U.S. commercial and government networks for Chinese intelligence and counter-intelligence purposes. The group uses social engineering, phishing schemes, or 0-day exploits to gain access to a network, establish a persistent presence, and deploy remote access trojans (RATs) that allow recording and seizure of user sessions. Tools such as Scanline and PwDump are used to acquire legitimate credentials that the actors can utilize to escalate their privileges, create unmonitored accounts, or move laterally to other systems. The recent Anthem, VAE, Premera, Empire Blue Cross Blue Shield, and Carefirst breaches are attributed to Deep Panda.

The PII, work history, and organization information compromised in the Deep Panda breaches mentioned are categorically identical to the information targeted in the OPM breach.

The group has employed RAT's from the Sakula malware family in past incidents. Post OPM release of FBI-000061, warning agencies of the Sakula malware has fueled online speculation of its use, and Deep Panda's involvement, in the OPM breach. Further, in Threat Connect's analysis of the VAE and Anthem breaches, malicious domains targeting OPM (www[.]opm-learning[.]org and www[.]opmsecurity[.]org) were discovered to be linked to known command and control (C2) servers, which act as an adversary's "dropbox" or hop point for exfiltrated data. APT's often use phishing sites such as these to trick users into revealing legitimate credentials or to make spear phishing emails seem legitimate. These two domains were registered with 10 character random alphanumeric [.]gmx.com email addresses and Avenger (Steve Roger, Tony Stark, etc.) registrant names to a GoDaddy name server. Moreover, the opmsecurity domain was registered on April 25, 2014, 4 days before the registration of the theWe11point[.]com domain used in the Anthem breach and a few weeks prior to the first OPM breach in March 2014. The domain, opmsecurity, remained dormant until December 18, 2014, which may coincide with the December 2014 second OPM breach. OPM publically announced awareness of the second breach on June 4, 2015 and as a matter of coincidence or intent, the last observed activity on the opmsecurity domain was June 3, 2015. Further, unconfirmed online reports assert that the certificate assigned to the malware used in the OPM breach was signed by DTOPTOOLZ, a stolen certificate used in the Anthem breach. Threat Connect asserts with high confidence that this evidence indicates that the actor behind the VAE and Anthem breach is also the actor behind the OPM breach.

Astute readers may notice that this assertion is inconclusive. Even if these malicious domains are linked to Deep Panda, the evidence presented only indicates an attempt to attack OPM rather than confirmation of success. The registration and usage dates could be coincidental or cherry picked from Threat Connect's data set. Despite insider claims made by officials and reputable security firms, until DHS releases further details of the breach, the public and the media should be wary of attributing the breach to Deep Panda or another Chinese state sponsored group. Malicious actor groups often utilize the same or similar exploit kits. As a result, numerous groups employ the Sakula malware and numerous groups could have breached OPM. Given the lack of sophistication of the attack, the shabby defenses of OPM's

critical systems, and the immense value of the exfiltrated assets, almost any known actor group would have seized the opportunity to breach OPM if they had the knowledge of their internal systems and the resources to conduct the breach. Some quick open source intelligence on Google reveals mappings of OPM's internal infrastructure. As a result, without knowing what, if any, indicators of compromise left on OPM's systems, attribution may be neither definitive nor constructive.

Adversaries likely accessed OPM systems through valid user credentials, and then escalated their privilege by creating a new set of higher-level credentials once inside the network to facilitate lateral movement across systems. Privileged credentials also enabled the actor to cover their tracks and potentially make changes to systems. The valid credentials could have been obtained through spear phishing campaigns, malicious decoy websites, social engineering, or careless practices. These methods are rudimentary and have been the simplest avenue of attack for about 2 decades. The credentials may have been obtained from social engineering, spear phishing emails, the 2013 FEC breach, the 2013 OPM breach, the 2014 USIS breach, or the 2014 Keypoint breach. Additionally, some of OPM's contractors employed and granted root access to foreign nationals, who were in some cases, still located in their home countries. Finally, Recorded Future recently uncovered credentials for OPM and 46 other U.S. Government agencies on deep net paste sites such as Pastebin.

In any case, without indicators of compromise and comprehensive log information, attribution of a breach is difficult and in many cases impossible. The investigation is further complicated at the global political level because the United States has been known to engage in similar espionage activities. For their part, China calls the allegations "irresponsible and unscientific." Attribution comforts us and distracts the public with someone to blame; however, it does little else. The information remains compromised and a response remains necessary. While the incident is fresh, meaningful measures to ensure that breaches like this do not happen in the future will do far more to regain public trust in the short term and establish national information security in the long term than a dedicated focus on attribution will achieve. Action in the weeks after a devastating breach has the greatest potential of achieving

lasting, meaningful cybersecurity reform, and Congress and Federal agencies must choose whether to seize this moment to enact change or to let it pass and hope that they are not the next compromised target.

In terms of advanced persistent threats, the OPM breach was not a sophisticated attack. The failure of DHS or OPM systems to detect the breach does not indicate a level of sophistication on behalf of the adversary; rather, it only shows that the breach was sophisticated for 1970's legacy systems that operate on COBOL mainframe applications that have not been updated since the Y2K bug. Based on this decade old attack vector and the length of the breach, Covenant Security Systems President and Founder Danyetta Fleming Magana remarks that "it appears as though this was the equivalent of a car thief politely asking for the car keys and once handed them drove the car for over a year before being noticed." The failings of OPM that we all must learn from can be categorized according to the technology implemented, the governing policies enacted, and the people implementing the technology and policy.

Evolving Technology to Respond to Threats:

The media and hearings significantly focused on detailing the inadequacies of the OPM and to attributing the breach to a specific actor. Considerable focus has been given to predicting the future utilization of the information and offering mitigation strategies to victims and the government. Very little focus has been dedicated to learning from this calamitous event and proactively utilizing that information to prevent such occurrences in the future. The information exfiltrated from the Office of Personnel Management is already in the hands of an adversary and there is little that anyone can do to change that outcome. According to House Oversight Chairman Jason Chaffetz, for the past eight years, according to OPM's own Inspector General reports, "OPM's data security posture was akin to leaving all your doors and windows unlocked and hoping nobody would walk in and take the information." OPM effectively handed away the keys to the castle by maintaining an undefended cybersecurity posture. The United States must learn from the OPM breach and focus on proactively improving its cybersecurity posture at the OPM, and every other agency, to decrease the likelihood of future successful

breaches made possible from the compromised information or from persistent attacks against our antiquated cybersecurity infrastructure. The single most significant recommendation that that agencies like OPM could heed is to actually listen to the advice of the Inspector General and do everything within their power to meet or exceed regulatory measures.

The National Institute of Standards and Technology (NIST) is the federal technology agency that works with industry to develop and apply technology, measurements, and standards. NIST standards establish minimum criteria for a stable cybersecurity position. OPM failed to adhere to many of the regulatory security practices set forth by NIST and the Federal Information Security Management Act (FISMA). According to Dan Waddell of $(ISC)^2$:

> "*If there has been one concern with the NIST Framework, it has been that the Framework was intentionally designed to be very broad, so that agencies could cater security practices and technology to their individual needs. While adding new technology to the Framework might add efficiency for some organizations, it could potentially prohibit other organizations from implementing its guidance. That being said, it is critical to understand that technology is not the silver bullet for added efficiency. We don't want to just tack on technology as a knee-jerk reaction to an incident, since there are many other things to consider before tools can be applied. Any effective security program starts with a trained information security staff. With a knowledgeable and experienced workforce as the foundation, OPM or any organization attempting to meet the Framework's standards should then conduct a risk assessment and based on the results, effectively establish what is required from a controls perspective to reduce the risk of future incidents.*"

According to the Office of Personnel Management's Office of Inspector General (OPM OIG) January 2015 audit report, OPM was subject to FIPS 199, NIST SP 800-60, NIST SP 800-18 Rev 1, NIST SP 800-34 Rev 1, and NIST SP 800-53 Rev 4. The OIG found that "a majority of tested security controls appear to be in compliance with NIST SP 800-53 Revision 4, however there are potential areas of improvement." Despite this assessment, given the scope and nature of the attack, a number of the sections of NIST 800-53 Revision 4, pertaining to account management(AC-2), identification and authentication(IA-2), auditable events(AU-2), audit generation(AU-12), session audit(AU-14), incident handling(IR-4), and incident monitoring systems (IR-5), were not properly addressed. The disparity between the audit report and reality

may be due to the 6-month lapse between the assessment and the publication of the report, or it may be due to time-boxing or conducting the risk assessment of the systems in under a defined-time limited scope. In this case, the report states that, "In conducting the audit, we relied to varying degrees on computer-generated data. Due to time constraints, **we did not verify the reliability of the data generated by the various information systems involved**. However, nothing came to our attention during our audit testing utilizing the computer-generated data to cause us to doubt its reliability [emphasis attributed to Igor Volovich]". The security landscape at a Federal agency such as OPM is not static and its vulnerabilities are impossible to discover or address when relying on data simulation alone. According to Igor Volovich, an ICIT Fellow, "in a situation involving a critical information system, such as OPM's DMRS platform used for management of sensitive adjudication data, rated as "HIGH" impact under OIG's own SP 800-60 determination, a more thorough approach should have been applied, including non-technical methods such as interviews and manual reviews of audit artifacts. Relying strictly on computer-generated data, as OIG's 2014 audit did, may have denied the audit team the opportunity to identify controls deficiencies which eventually enabled the OPM compromise." This significant delay and this (likely erroneous) approximation of the security posture of the OPM systems does not contribute to an accurate risk assessment of OPM's critical systems.

According to the OPM OIG, numerous systems failed security inspection and were not authorized to operated (ATO) under the Federal Information Security Management Act (FISMA). These were not minor systems or any of the numerous "unknown" systems on OPM's network. As of 2014, only 75% of the OPM critical systems had valid authorizations to operate under FISMA regulations. Additionally, unconfirmed "whistleblower" accounts online indicate that many of the systems barely qualified or were "shored up" just for inspection. For clarity of the abysmal condition of the OPM IT network, consider that of the 47 major systems on the OPM network:

- 11/47 major systems belonging to OPM IT, not contractors, were not certified as secure
- 65% of all OPM data was stored on uncertified systems.

- 22/ 47 OPM systems belonged to contractors. OPM had limited or no visibility or control over these systems.
- 3/22 contractor systems were not tested for security in the last year. The rest are tested only once a year.
- 5/25 OPM systems were not monitored by any SEIM tools.
    - OPM has no requirement of SEIM on contractor systems.
- 7/25 OPM systems had inadequate documentation for security testing.
    - 4/7 systems were directly managed by OPM IT.
- 0/47 systems required Personal Identification Verification (PIV) cards. This violates the Office of Management and Budget mandate for federal systems.

OPM systems, including the central use authentication services used by most of their applications and the entirety of EPIC, were also operating without authorization. These systems should have been secured immediately or taken offline until security was insured. At this time, it is unclear how many systems were breached or how many of the breached systems were operating without authorization.

It is also possible that OPM was breached through an unpatched vulnerability in its legacy systems or one of its other unsecure systems. Speculation indicates that that actor may have gained some knowledge of the OPM internal systems through stolen documentation during the 2013 OPM breach, although some officials have dismissed these accounts. The 2014 OIG report found that weekly server patches were incomplete. When systems are not regularly patched, attackers can easily climb through the holes. Legacy systems, like those at OPM, often fail to be patched or updated because in many cases, the systems Frankensteined together over the past thirty years do not support modern software such as vulnerability management programs. In other cases, the patch may break other components of the adhoc system. The limited software based logging on OPM‘s legacy system was not fully deployed and knowledge of how the actor gained access, what the actor accessed, and where information was accessed from, is limited. OPM did not employ a configuration management system on its legacy network; as a result, information of changes the attacker made to the system is likewise

difficult to ascertain. Management of Legacy systems eludes seasoned technical professionals so, it is not surprising that the ignorant officials at OPM failed to implement rudimentary systems. In some cases, the hardware or software in use at Federal agencies, such as OPM, has outlived the company that created it and no support or updates exist. The only defense these archaic systems have to stop adversaries is that the adversary might be unfamiliar with the retired programming language used in the system code.

In response to the OPM and other high profile breaches, the Obama administration has ordered a 30-day Cybersecurity sprint in which agencies must perform vulnerability testing & patching, reduce the number of privileged accounts, and greatly expand the adoption of multifactor authentication. The OPM audit report states that OPM systems may not have been subject to an adequate security controls test since 2006; however, it is not alone in the failure to adhere to regulation and the overwhelming need for cybersecurity reform. The Department of Veteran Affairs has 6000 outstanding security risks in its Plans of Action and Milestones to improve its overall information security posture. The Department of the Treasury reports that the IRS suffers from many of the same vulnerabilities as OPM. The Department of Transportation lacks system level controls sufficient to protect the systems' security and ensure that the systems can be recovered in the event of a serious breach. Practically every Federal agency has published similar deficiencies. Without a sudden, significant influx of funding, most agencies cannot accomplish much within this time constraint. Some contend that the Cyber-Sprint will be mostly ignored by agencies who have already struggled to come to terms with their cybersecurity-threat landscape. Agencies with the available budgets may consider accountable governance products like SOPHIA to ease management of system patching, plan of action and milestone (POA&Ms) and establish centralized control.

Recent media buzz has flittered around OPM's bold decision to leave highly sensitive information unencrypted. OPM Press Secretary Samuel Schumach announced that "though data encryption is a valuable protective method, today's adversaries are sophisticated enough that encryption alone does not guarantee protection. OPM does utilize encryption in some instances and is currently increasing the types of methods utilized to encrypt data. These

methods include not only data at rest, but data in transit, and data displayed through masking or redaction." OPM Chief Information Officer Ms. Donna Seymour testified that encryption was not possible on the COBOL legacy systems in OPM's care. In actuality, libraries exist, such as PKWare, that integrate modern encryption on antiquated systems. The process may not have been cheap, but encryption was possible. Additionally, DHS Assistant Secretary for Cybersecurity Dr. Andy Ozment testified that encryption would not have helped in this case because the actors had valid credentials. Even though this response is accurate to the current situation, it is not an admirable stance that other agencies should emulate. Encryption is only one layer of the defense-in-depth model. Implementation of encryption delays adversaries' assessment of valuable data and may limit the utility of exfiltrated data. At the very least, it requires the adversary to expend resources to access the data. Every adversary has a threshold at which point the expenditure of resources outweighs the utility of the data. It is the goal of the organization to aspire to push an attacker towards their threshold. If OPM had implemented proper IT governance practices and assigned user access according to least privilege principles, then the benefits of encryption would have been much greater because a compromised account would only have access to a limited amount of unencrypted data. Even if the attacker moved laterally across systems, the scope of the breach would have been limited. Field level encryption at the database level would have further confounded some attacks and extended the window between exfiltration and data utilization to allow victims more time to respond.

Virtualization of the OPM work environment could have capitalized on field level encryption and prevented lateral movement by reducing the impact of a breached account. Access to information would be limited to only what the real user needed for their work function and the rest of the information would be encrypted or not available in the environment at all. Essentially key assets can be segmented or they can be sequestered away from other systems assets. VM session information could be used to baseline user activity to indicate anomalous behavior to the SEIM or UBA. Virtualization also offers change management, system redundancy, system integrity, and scalability for very little cost.

Agencies with available resources should consider deploying more comprehensive multilayered security. According to Richard Bejtlich of FireEye, "It's basically impossible for a target of any real size to be perfect across that whole exposed area. When the intruder gets that first foothold, somebody has to notice and then react to contain the intruder before he can accomplish his mission." DHS's Einstein 3A failed to detect the malware plaguing OPM until a signature, discovered during a CyTech Services product demonstration, was fed into the system. In its current form, Einstein only utilizes unclassified signatures in detection. This behavior is typical of IDS/IPS systems; however, it pits the user in a constant defensive stance. Richard Bejtlich continues, "if at any point during that timeline you notice they got in … and you contain them, then you win. That's the difference between a breach where something catastrophic happens and unauthorized access, which is just getting that initial foothold." Agency level IPS/IDS, Firewalls, vulnerability scanning tools, SEIMs, and data loss prevention (DLP) software would help to lessen the likelihood of future breaches. Large scale, effective deployment of DHS's Continuous Diagnostics and Mitigation (CDM) program would give agencies the tools necessary to track all the assets on their networks and detect anomalies. Identity and access management tools, scheduled to be included in DHS CDM, would allow detection of unusual IP network traffic and user behavior analytic systems (UBA) such as odd login hours, suspicious database requests, and any "out of the normal" behavior by insider threats or malicious actors. Security Operation Centers and Hunt Teams can detect threats before calamitous damage occurs. Incident Response programs can then take over, initiate recovery, and update the organization infrastructure and processes with learned lessons to ensure that the organization knows as much as possible about the threat environment and responds to each threat according to its potential impact and degree of sophistication.

Cybersecurity defense requires a novel approach that improves efficiency. Legacy and pre-Y2K defenses such as firewalls, anti-virus, and IPS/IDS cannot compete with advanced threats and must be phased out in favor of agile, integrated systems that can adapt and respond to deviations in the threat environment. HP Security Strategist and ICIT Fellow, Cynthia Cullen asserts, "from the strategic perspective, the industry at large has been talking for a long

time that security needs to be built in from the design phase forward." Similarly, in their paper Cyber Security's "Magnot Line: A Real-World Assessment of the Defense-in-Depth Model" and its corresponding update, FireEye estimates that 96% of organizations have been breached despite an annual global investment of $67 billion in cybersecurity defense. No matter the make or model of firewall, IPS, web gateway, sandbox, or end point system, attackers are still penetrating networks with ease. The security infrastructure of agencies must evolve to do more than rely on malware signatures alone, as DHS Einstein does, so that our national defense is not based on assumptions and the outdated information of past attacks. None of these antiquated components can stop 0-day exploits. After World War I, Georges Clemenceau critiqued that generals are always preparing for the last war rather than the next one. Cybersecurity reform needs to prepare agencies like OPM to face current and future threats rather than defending against retired attack models. Our adversaries are humans capable of adaptation and creative thought, not the static pieces of code or attack patterns that they generate. Successful defense depends upon matching the sophistication of the source of the attack, not just shielding yourself from their tools.

Modern cybersecurity defense systems must dynamically recognize threats and submit signals to trained personnel capable of recognizing the alerts that matter and responding in near real time. The advent of APT's has nearly institutionalized the practice of tailoring attacks to a specific victim. Meanwhile, defense-in-depth strategy has not evolved in proportion. It is as effective as trying to stop a laser pointer with a chain link fence. Novel malware can bypass detection, avoid runtime analysis and prevent post incident traces in a number of ways undetectable to current defense –in-depth norms. For example, malware often deployed on machines compromised through phishing emails, use an initial innocuous looking file download to place calls to C2 servers from the infected machine to download objects and processes independently, the malware is assembled, the malware is run on the infected systems, and then the malware is disassembled and removed except for the innocuous looking file. This process is akin to scenes in spy movies where an agent bypasses complex security by sneaking individual components of a weapon into a secure facility to attack a target.

Defense-in-depth strategies suffer because disparate programs are responsible for different parts of the defense strategy. Every time programs fail to effectively stop a threat or communicate vital information to another program, the integrity of the entire defense suffers. This leads to a piecewise fortress, built from Legos rather than concrete. According to FireEye, "organizations need a tightly integrated nimble architecture that enables big picture vigilance." Different layers of controls, deployed in collective defense that prevents single points of failure and ensures more than network perimeter security, should be the new standard. Cynthia Cullen adds that"[OPM's] general approach was dependence on a security perimeter. Once breached, they didn't have adequate layers of protection to protect the sensitive data they held." Agencies like OPM should aspire towards an integrated defense solution comprised of all of the familiar elements in addition to VM-based solutions, non-signature based detection, endpoint security (secure browsing, hardware/ transaction signing devices, etc.), rapid endpoint response, SEIMs, SOCs, UBAs, sophisticated sandbox environments, and dynamic routine threat intelligence services. Many firms offer these integrated solutions for purchase if budget requirements prevent in-house development. These systems may be more affordable as organizations reduce wasted spending on redundant, backward facing technology and redirect those funds towards continuous protection systems

OPM could have benefitted most from a User Behavioral Analytics (UBA) system. UBAs monitor user activity over a predetermined period and create a profile baseline. Provided that user thresholds are established prior to a breach and that identity access controls prevent the creation of unknown accounts, then the system detects and reports anomalous user behavior such as log in attempts at strange hours, access to databases outside of job function, and other suspicious activity. Recently, Recorded Future conducted open source intelligence and found login credentials of 47 U.S. Government agencies across 89 domains, as clear text or email-password hashed pairs that could be decoded with a rainbow table. Twelve of the agencies affected did not require multi-factor authentication for remote access and are therefore as vulnerable as OPM. Once inside the network the Users with valid credentials are considered "trusted," and OPM had no idea that a normal legitimate user was acting in an anomalous and illegitimate way. OPM lacked the tools, such as UBA, to detect a remote

attacker who controlled malware inside the network using legitimate credentials. Additionally, national cybersecurity would benefit if the AU section of the NIST standard were updated to address monitoring normal user behaviors for anomalous activity.

UBA systems greatly enable an insider threat-monitoring program. Further, UBA's can assist or serve as a data loss prevention program if configured to flag suspicious or large data transfers. Qualified information security personnel are required for effective deployment of behavioral analytic systems. While initially costly and resource intensive, the cost of UBA programs lessens after baseline establishment. UBA systems mitigate breach attempts from stolen credentials and insider threats. Behavioral analytic systems grant organizations the potential to process raw sensory data in near real time to act to mitigate active threats. Some systems can also fingerprint automated processes or machines to mitigate attacks from those vectors. OPM and many agencies with decrepit legacy systems cannot utilize UBA systems because UBA often relies on an active directory type structure. This should be considered yet another incentive to migrate to a modern infrastructure rather than stay on the antiquated COBOL systems that have been Frankensteined together over the past thirty years or more. Given the necessity for compliance to governance policy and the fear of rising insider threats as a result of the OPM breach, UBA systems should become more prevalent in standard defense infrastructure.

Evolving Policies to Govern Action:

By far, the greatest failure at OPM was their lack of comprehensive governing policy. Governance controls such as disabling any old or unused accounts, limiting account functions and access to least privileged, limiting the login time of accounts, constraining and defining acceptable access times, limiting the ability and function of remote access, and mandating regular patching and modernizing systems. The number of privileged accounts should be minimized, when possible, the access of each account should be restricted to a fraction of the total systems, and the implementation of change review by other privileged accounts, should be considered. According to the OIG, governance controls on VPN and remote connections

were non-existent, lacking even basic multi-factor authentication. In fact, none of OPM's 47 major applications utilized multifactor authentication despite the fact that over 80% of cyber-attacks emerge via applications. Multifactor authentication should have been OPM's first line of defense against any breach because it is easy to configure, cheap to implement, and it would have stopped attacks like this from ever realizing success. The actor, who likely compromised the system using stolen credentials, may have accessed the system from across the globe with no trouble whatsoever. Users at all agencies and industries need to practice greater caution when creating account credentials. Governance policies should clearly show the user how to create a strong password and the policy should require frequent, non-repeating credential update procedures. Credentials should never be reused on another site. As a result, the amount of time that compromised credentials pose a risk to the organization is minimized at no cost to the organization. OPM, and similar agencies, deploy governance systems that automate such processes and feature configuration management tools to detect, approve, and revert system changes. Rather than relying on random board approved or rash system changes, as OPM did, agencies would benefit by conducting a risk analysis and using the results to formulate scenario driven action plans that dictate incident response and disaster recovery and govern the change management system.

Had OPM practiced Six Sigma, ITIL, or CERT's Octave Allegro, then management would have recognized the need for greater security, greater governing policy, and greater planning. Risk assessment may have revealed the breach sooner and certainly would have dictated defending critical assets, like the SF-86 database, according to their value. Incident response plans would have prepared OPM for the breach by improving response time and ensuring incident data collection and preservation to assist in the investigation and attribution. Disaster recovery plans would allow for a more developed, timelier response that catalyzed public awareness and response, while reducing public distrust of Federal Agencies. IT professionals would have regularly tested OPM's security posture and IT infrastructure in real time drills or in tabletop, stepwise analyses of the processes of its incident response and disaster recovery plans. The first test of OPM's incident response would not have been one of its actual breaches. The continuous nature of the risk analysis cycle ensures that each iteration through the process

strengthens the security of critical assets, eliminates waste and ineffective practices, and improves the network through application of lessons learned and information from the OIG audits. These iterative processes ensure that the network is constantly monitored, that network activity is scrutinized, and that anomalous activity is addressed to ensure that the defense posture of the organization adapts to the shifts in the threat environment. Trained staff assume that the network is compromised (because it very well could be) and react with the upmost focus on protecting the confidentiality, availability, and integrity of all critical systems.

A central IT staff, who based their decisions on a comprehensive risk analysis / incident response process, did not govern IT projects at OPM. Rather projects were managed at the division level and there was no apparent central oversight. Many systems, operated by agency contractors, were out of the direct control of OPM's IT staff. Nearly half of the systems on OPM network belong to contractors and could not be immediately accessed by OPM. Further, OPM did not maintain a comprehensive inventory of servers, databases, and network devices. Auditing and security are impossible without a network map. Agencies should enact clear policies regarding network and account access. A centralized, dedicated IT staff should monitor the network and any changes to the network. According to Covenant President and Founder Danyetta Fleming Magana:

> "In many federal agencies there is a lack of clear oversight, authority and resources for a centralized and accountable management of cyber security. In most agencies, they function similar to OPM, a CISO with a loosely structured group of Information System Security Officers (ISSOs) and Information System Security Managers (ISSMs) with little to no authority to direct programs or implement required changes. Often times they are viewed and relegated to providing only minimal guidance necessary to "get through" a System Authorization or FISMA audit. As a result of such a constrained role in federal organizations, many CISOs also lack the authority to hold Programs accountable for implementation and compliance with the NIST regulatory guidance. In addition, CISOs and their teams are relegated too often to being underneath the CIO and part of their budget with limited authority to affect acquisitions; this model showed it's weakness in the OPM hack."

Only approved devices should be able to access the network. All devices on the network, including contractor systems, should be known and accountable to IT staff at all times. Any

agreements or contracts with contractors should clearly define conditions of transparency and access. Obviously, these agreements should be kept up to date. Systems corresponding to defunct agreements must be immediately severed from the network.

Current media reports indicate that the adversary may have used Keypoint or other contractor credentials to access OPM network and to gain access to the EPIC background investigative software tools. When considered alongside allegations that some contractors employ foreign national and granted them root level accounts invites discourse about contractor operation at Federal agencies. The contractor USIS was born out of OPM itself and operated on a hairline budget, after the Federal Government reduced the budget allocated for investigations. Keypoint operated on less of budget, supposedly using personal Gmail accounts, no IT infrastructure, and adhering to no meaningful security policies. Overall, for the sake of national cybersecurity, Congress needs to consider such avalanche effects when allocating annual budgets. Agencies must exercise greater caution and greater thought when dividing their budgets, when hiring contractors, and when governing their contractors. Recently, with the Target breach and many others, attacking a primary target through a secondary or tertiary service provider has become one of the easiest avenues of compromise employed by advance persistent threat groups. The culture of lowest bid contracting has definite consequences and any agency daring enough to engage in such practices for the sake of saved budgets should be sure to use governance policies to properly limit the access of the contracted party or accept the consequences of potential breaches. Federal agencies should set the example of stringent contractor vetting processes rather than exemplifying the cautionary tale.

Standardization of cybersecurity practices across agencies and industries via a regulatory “OSHA-like entity” should be considered as a possible way to unite disparate sectors and dissuade poor cybersecurity practices. Information about adversaries could be collected, shared, and used to monitor systems in a routine fashion that is impossible under the current cybersecurity culture. According to Gen Alexander, “We are dying by a thousand cyber paper cuts.” Each breach impacts more American citizens, who never accepted the transfer of risk, in more ways. Agencies and industries should be held accountable to each other and the public in

a meaningful, measurable manner. If we learn from our mistakes and ensure reform then a breach of this magnitude will never happen again; otherwise, the next breach affecting more than 22.1 million American citizens and their families may remain undetected.

Training People to Act:

The enormous advantage of the OPM breach is that it was detected and the agencies and individuals affected are becoming more aware of the compromise as information is released. Agencies need to take action to harden their systems against attacks that utilize information stolen from OPM. In the July 3, 2015 episode of ICIT Fellows Insights: Why OPM's Breach was a Game Changer, Risk to the Victims, & Recommendations, HP Security Strategist Cynthia Cullen points out that "what is not being discussed in the media is whether there is another shoe about to drop. When you have intruders in your network for such a long period of time, there is also potential that they may be modifying, deleting, or creating data within these systems. They could easily be creating security clearances for moles, that may be difficult to detect as what is the real data and what is the modified data." Actors may have stolen valid information that corresponds to legitimate accounts or they may have altered the data in the OPM system to inject false data or create false identities for malicious agents. Cullen later continues that because of the breach, the "veracity of clearances is questioned. Is the person sitting in the high security facility in fact an agent for another government whose clearance was inserted into the system?" Agencies need to know their employees in order to prevent a malicious agent from masquerading as a cleared individual.

All government personnel take basic precautions to limit the risk of impersonation and cascading compromises. Primarily, they should change all the passwords on all their personal and professional accounts along with the corresponding recovery questions. Agencies should disable remote account (forgotten username/ password) recovery for the foreseeable future. Manual requests to IT departments for forgotten credentials, while bothersome, are more secure than security questions based on information contained in the 127 page SF-86 form. When reestablishing account recovery questions, users should enable multifactor authentication, where possible, and answer questions with the answers from a memorable

book or movie instead of their real life. Agencies must be more diligent in scrutinizing new hires and more cautious of suspicious activity of current employees. If identity compromise seems prevalent in the next few years, then a new identity confirmation process will have to be constructed to verify the identity of cleared individuals. Social engineering attacks, spear fishing attacks, and identity theft are now far more probable than before the breach. Victims require training to remain vigilant and information about how to proceed forward with their lives. Individuals must know how to recognize spear phishing attacks, how to monitor their credit, and how to regain control of their lives.

Though the notion may clash with popular opinion, the outcome of the OPM breach may be better if the actor is state sponsored. A non-state sponsored actor is more difficult to identify. Further, the lone actor is more likely to distribute the vast stores of information to other adversaries for economic gain. A non-state sponsored adversary tends to hassle the individual victim. On the other hand, a state sponsored attacker will use the information against the state. So far, the exploitation of vast quantities of state sponsored stolen information PII for economic gain against the individual is not common. This may be due to the limited number of comparable breaches or it may be an unspoken agreement amongst states to prevent cascading impacts resulting from the precedent. Since the breach was discovered, proactive agencies and the federal government can more effectively mitigate and accept the risk than individual victims can. Compromises to other systems can be prevented through proactive measures and a push for cybersecurity reform. Agencies should repair known vulnerabilities and assess to the best of their abilities whether their systems have also been compromised. OPM and every other Federal agency should do everything possible to ensure that their networks are not infected, and then they should advance their defensive measures to prevent future infection.

A state sponsored actor may use the trove of information to construct a “linkedin-esque” database for their intelligence community. Given the pool of American included in the database such a tool will be devastating and invaluable unless the United States takes thoughtful proactive measures now to mitigate the risk and decrease the value of the asset. The shelf life of the database would be approximately 30 years considering the average age of

impacted individuals. Further, identity theft attacks from a non-state sponsored actor can impact generations of a family and have enormous lasting impacts on the United States economy. The potential of such a tool drastically increases if combined with modern big data practices and predictive models. Reform of the critical cybersecurity infrastructure as reformation of expertise of personnel, reformation of vulnerable, outdated technology, and reformation to end 25 years of poor cybersecurity practices can last far longer than 30 years and help to mitigate extenuating long-term consequences of the OPM's breach.

The popular concern propagated amidst the media is that individuals possessing clearances may be ransomed or blackmailed by a state-sponsored actor. While credible, this concern is greatly exaggerated because the pool of victims actually reduces the risk. The Adjudicative Guidelines for Determining Access to Classified Information dictate, "No coercive policing could replace the self-discipline and integrity of the person entrusted with the nation's secrets at the most effective means of protecting them." In theory, security clearances are given to the most ethical and trustworthy citizens in the United States of America. These individuals are less likely to assist an enemy nation state based on a threat of disclosure and they are more likely to disclose the attempt to the Federal government. The majority of espionage cases involving individuals that possess a clearance, such as Robert Hanson or Edward Snowden, derive from an economic or political motivation rather than a threat of duress. Despite all the technology protecting a network and policies governing a network, people remain our greatest resource; however, uninformed people also remain our greatest weakness. Without information training and awareness, future IT staff will continue to fail to secure critical systems and future employees will continue to fall victim to social engineering attacks.

Training remains the easiest and best strategy to mitigate adverse effects of the OPM breach such as insider threats, spear phishing emails, social engineering or future breaches. Every government employee, every victim, and every immediate family member of a victim need the training to recognize potential threats emerging from the compromised information. Victims and their immediate family members should also change all passwords and security

questions on all professional and private accounts. Security questions should be answered with information not contained in the SF-86 or social media, such as information about a character in a movie or book. Social media accounts and personal accounts should not be accessible from secure networks. Moreover, users should be suspicious of emails containing links or attachments, especially those from social media sources. Exabeam's VP of Marketing Mark Seward remarks that adversaries can inflict significant damage by "degrading staff moral and capability and keeping them busy addressing non-work related identity theft issues." Victims must remain vigilant against personal attacks and some may appreciate if agencies offered counselling to cope with the stress and emotional impact resulting from the breach. Victims and OPM would benefit in the long run if each applicant reviewed the SF-86 and other information in the OPM database to ensure information integrity. Since 15% of the U.S. population and their families will be trained in cybersecurity best practices, OPM's failure could result in immediate national cybersecurity awareness and training if properly managed.

The Federal Government must construct plans to reestablish public trust and capitalize on the cybersecurity awareness generated from the OPM breach. In their ICIT Fellows Insights session, Parham Eftekhari and Cynthia Cullen discuss how much public awareness the OPM breach has generated in the media and on social networks. Cullen remarks that the breach "has brought information security and cyber security, very much to the forefront." The Federal Government has the opportunity to utilize public awareness to galvanize cultural change. Post breach education of the information security best practices helps to demonstrate to the American public and the entire world that America will not remain a vulnerable target and that the breach has not caused a chasm of distrust between people and government. Representative Adam B. Schiff, of the House Intelligence Committee, explained

> "This latest intrusion . . . is among the most shocking because Americans may expect that federal computer networks are maintained with state-of-the-art defenses, the cyberthreat from hackers, criminals, terrorists and state actors is one of the greatest challenges we face on a daily basis, and it's clear that a substantial improvement in our cyber databases and defenses is perilously overdue."

Every success and system upgrade at every Federal Agency, including OPM, demonstrates progress away from our pitiful national cybersecurity position. According to New Light

Technologies Senior Technology Consultant & Program Manager Chris Schumacher, "the success of multiple intrusions into secure U.S. Government systems emboldens those who have already succeeded and encourages other would –be cyber attackers." No matter the immediate cost, demonstrations of cyber reform will deter greater expenditure from incidents and breaches in subsequent years. Technology alone is not the answer to cybersecurity reform. Securonix Chief Scientist Dr. Igor Baikalov offers that until agencies have implemented the controls necessary to secure sensitive data, "agencies might have to sacrifice efficiency for the sake of security." Governmental cybersecurity training will also mitigate future incidents, assuage the fears of victims through insight, and prevent the growth of insider threats. OPM would be benefit greatly from taking the most proactive measures. Within each agency, security practices should be coupled to the role of the individual for the greatest effect and the greatest user retention.

Recognizing the Consequences of Inaction and Striving Towards Progress

The necessity of reform of America's Cybersecurity infrastructure is demonstrated every month by every devastating breach in every sector. Two decades of poor practices has shifted the majority of the negative impacts resulting from incidents onto unwitting American citizens. The latest OPM breach directly affects 22.1 million citizens and indirectly affects the remainder of the nation. The OPM breach offers the opportunity to galvanize a movement for reform and to capitalize on its outcome to establish lasting change. As a nation, we want to keep our sensitive information hidden behind the layered defenses that our people construct from the most advanced technology and the best practices available. As in OPM's case, without the proper technology , the proper governance, the proper training, our national defenses falter the moment a strong adversary approaches or the second an adversary discovers a vulnerable gap in our obsolete defenses. Unknown adversaries abscond with the information entrusted to the Federal Government, our national defenses crumble, and the American people are left out in the cold.

ICIT | Institute for Critical Infrastructure Technology

*Expert research contributed by the following ICIT Fellows:

- James Scott (ICIT Senior Fellow – Institute for Critical Infrastructure Technology)
- Drew Spaniel (ICIT Visiting Scholar, Carnegie Mellon University)
- Dan Waddell (ICIT Fellow – Director, Government Affairs, (ISC)^2)
- Danyetta Magana (ICIT Fellow – President & Founder, Covenant Security Solutions)
- Mark Seward (ICIT Fellow – VP Marketing, Exabeam)
- Ralph Pisani, (ICIT Fellow – EVP of Field Operations, Exabeam)
- Rob Roy (ICIT Fellow – Federal Chief Technology Officer, U.S. Public Sector, HP)
- Cynthia Cullen (ICIT Fellow – Security Strategist, Northeast, HP)
- Stan Wisseman (ICIT Fellow - Security Strategist, Southeast, HP)
- Igor Volovich (ICIT Fellow – Institute for Critical Infrastructure Technology)
- Chris Schumacher (ICIT Fellow – Sr. Technology Consultant, New Light Technologies)
- John Menkart, (ICIT Fellow – VP Federal, Securonix)
- Dr. Igor Baikalov (ICIT Fellow – Chief Scientist, Securonix)

Contact Information

Legislative Branch Inquiries:

- James Scott, Senior Fellow, ICIT (james@icitech.org, 202-774-0848)

Federal Agencies and Executive Branch Inquiries:

- Parham Eftekhari, Senior Fellow, ICIT (parham@icitech.org, 773-517-8534)

Fellow Program Inquiries:

- Parham Eftekhari, Senior Fellow, ICIT (parham@icitech.org, 773-517-8534)

Links

Website: www.icitech.org

Social Media:

Ars Technica:

http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/

http://arstechnica.com/security/2015/06/report-hack-of-government-employee-records-discovered-by-product-demo/

http://arstechnica.com/security/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official/

http://arstechnica.com/security/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/

http://arstechnica.com/information-technology/2015/06/opm-director-on-security-issues-were-trying-very-hard/

http://arstechnica.com/tech-policy/2015/06/opm-shuts-down-background-investigation-portal-because-of-vulnerability/

The Christian Science Monitor:

http://www.csmonitor.com/World/Passcode/2015/0626/OPM-hack-may-finally-end-overuse-of-privileged-user-access

CNN:

http://www.cnn.com/2015/06/24/politics/opm-hacking-senate-briefing/

Computer World:

http://www.computerworld.com/article/2941754/data-security/opm-the-worst-hack-of-all-time.html

http://www.computerworld.com/article/2941758/cybercrime-hacking/6-reasons-why-there-will-be-another-opm-style-hack.html

http://www.computerworld.com/article/2943197/malware-vulnerabilities/fbi-alert-details-malware-tied-to-the-opm-and-anthem-attacks.html

The Daily Beast:

http://www.thedailybeast.com/articles/2015/06/24/hackers-stole-secrets-of-u-s-government-workers-sex-lives.html

http://www.thedailybeast.com/articles/2015/06/30/spies-warned-feds-about-opm-mega-hack-danger.html

Defense One:

http://www.defenseone.com/ideas/2015/06/keep-calm-and-spy-why-opm-hack-wont-bring-down-us-intelligence/116392/

http://www.defenseone.com/technology/2015/06/after-historic-hack-opm-chiefs-15-point-plan-may-be-too-little-too-late/116512/

Federal Times:

http://www.federaltimes.com/story/government/management/blog/2015/06/15/opm-hack-security-trust/71247842/

http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/19/opm-breach-encryption/28985237/

http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/24/opm-hack-cyber/29208581/

http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/23/keypoint-usis-opm-breach/28977277/

http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/18/prevent-opm-breach/28931583/

http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/07/02/opm-site-restrictions/29620705/

FireEye:

https://www.fireeye.com/blog/executive-perspective/2014/05/real-world-tests-real-world-results-are-you-building-another-maginot-line.html

Forbes:

http://www.forbes.com/sites/katevinton/2015/06/11/federal-union-says-opm-data-breach-hit-every-single-federal-employee/

http://www.forbes.com/sites/katevinton/2015/06/23/opm-director-blames-federal-breach-on-legacy-systems-in-senate-hearing/

Krebs on Security:

http://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/

National Journal:

http://www.nationaljournal.com/tech/a-timeline-of-government-data-breaches-20150706

Navy Times:

http://www.navytimes.com/story/military/2015/06/17/sf-86-security-clearance-breach-troops-affected-opm/28866125/

NPR:

http://www.npr.org/2015/06/15/414689778/u-s-officials-say-nearly-14-million-affected-in-opm-breach

PRWeb Online Press Release Distribution Services:

http://www.prweb.com/releases/2015/06/prweb12787823.htm

Recorded Future:

http://go.recordedfuture.com/government-credentials-report

Slashgear:

http://www.slashgear.com/opm-hack-tipped-in-link-to-anthem-breach-22390049/

Threat Connect:

http://www.threatconnect.com/news/opm-breach-analysis/

http://www.threatconnect.com/news/opm-breach-analysis-update/?utm_campaign=Media%20News%20Q2&utm_medium=blog&utm_source=opm-breach-original-click-new

Threatpost:

https://threatpost.com/stolen-government-agency-passwords-easy-to-find-online/113469

Tripwire:

http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/

The Washington Post:

https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html

https://www.washingtonpost.com/world/asia_pacific/china-calls-us-hacking-accusations-irresponsible-and-unscientific/2015/06/05/7989cad3-583f-417e-a0b7-34be46eb16ff_story.html

http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/02/opm-plans-to-release-more-information-about-data-breach/

Wired:

http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/

ZdNet:

http://www.zdnet.com/article/opm-breach-we-get-exactly-the-it-security-were-willing-to-pay-for/