Moving Forward

How Victims Can Regain Control & Mitigate Threats in the Wake of the OPM Breach

THE INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY

August 2015

ICIT | Institute for Critical Infrastructure Technology

Introduction:

In June 2015, the United States Office of Personnel Management revealed that a persistent adversary overcame their meager cyber-defenses and pilfered the personal identifiable information (PII) of the 1-in-15 United States citizens who either work for the Federal Government, have applied for or possessed a security clearance since the year 2000, or are an immediate relative or known associate of a cleared individual. Public outcry and outrage ensued in the following weeks. The White House issued statements defending the OPM administration and recently discussing measured retaliation against China, the alleged state sponsor behind the breach. Federal investigations and Congressional hearings investigated the details of the breaches, the faults of OPM, and the faults of its administration. The media sensationalized the event as the personal fault of individual members of OPM's administration and as an act of war from China or other nation states. For its part, OPM notified the 4.2 million victims of the first breach, OPM offered 3 years of credit monitoring to victims, and OPM issued some online guides about steps against identity theft. The 19.5 million victims who applied for a security clearance, possessed a security clearance, or are related to a cleared individual, are still awaiting their notification letters from OPM detailing steps to mitigate adversarial use of the granular personal information on the 127-page SF-86 form that was exfiltrated from the OPM database.

The information on the SF-86 forms provides an adversary with the opportunity to create a veritable database or "LinkedIn of espionage" that can be used to breach other Federal entities through physical or cyber means, coerce individual victims through blackmail or threat, or aggressively conduct counterintelligence by either targeting covert allies and assets revealed on the forms or by conducting big data analytics to forecast operational and behavioral patterns of United States citizens and agencies. An adversary threatens the security of every level of the United States Government and every United States citizen in a myriad of ways. The White House, Congress, and the media have focused heavily on attributing fault for the breaches. Considerably less effort has been dedicated to mitigating the impact of the breach at the individual level. Accurate attribution helps to direct intelligence and counter intelligence efforts, and it helps victims to regain some confidence in the Federal Government; however, even if a nation state, such as China, admitted to committing the breach, the information would still be lost, the damage would still be done, and the victims would still be in peril. Neither sale nor use of the information from the OPM breaches has been confirmed. Therefore, a great deal of the potential impact can be mitigated if attempts at proactive measures supersede attribution attempts.

A problem is an opportunity that has not yet been realized. At one level or another, the OPM breach affects every United States citizen. Citizens and national security will both thrive and survive if the United States seizes this opportunity to revitalize its antiquated cyber-security infrastructure and to invest the time and energy into redeveloping its foundation of cyber-security best practices and culture. By informing victims of the potential threats resulting from the OPM breaches and by informing the victims of the practices that they can adopt to prevent harm to their families, themselves, and the nation, victims are empowered to enact and evangelize change. As victims become vigilant and adopt better cyber-practices, they regain more control over their lives. In this manner, the threat presented by the OPM breaches is lessened proportionally because victims are less vulnerable and exfiltrated PII is less useful.

A victim of the OPM breach could be the target of fraud or espionage attempts a month from now, thirty years in the future, or any time in between. Alternately, a victim may never face consequences of the OPM breach. Compromise in the OPM breach does not guarantee sustained victimization. The compromise does present the opportunity to seize and the justification to practice greater control over your physical and cyber life. On the other hand, just because exploitation has not occurred does not mean that it will not occur. KGSS Inc., President and General Manager Adam Firestone reminds readers, “The sense of ‘it hasn’t happened yet’ leads to complacency and reduced vigilance which in turn renders any attack more likely to succeed.” The OPM breach is not a singular event. Many breaches happened before OPM and many will happen afterward. In fact, there is reasonable probability that every citizen in the United States has lost PII to a cyber-adversary in at least one breach. The OPM breach is unique in that it presents the opportunity to inspire reform of the United States cyber-security culture because the victims of the OPM breach have the power to enact and inspire the necessary changes. The Federal Government and victims of the OPM breach face short-term (6-12 months), medium-term (1-5 years), and long-term (5-10+ years) threats. As a result, everyone is well motivated to remain vigilant and to do everything within their power to mitigate the impact of the breach for their families, themselves, and their nation. Citizens and legislators should seize this opportunity for change rather than choosing to forget the consequences of apathy until an adversary weaponizes the OPM data or another adversary harms more citizens in yet another breach.

Background:

Within the last few months, 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 prospective 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 detailed 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.

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 the United States Computer Emergency Readiness Team (U.S. CERT) and DHS discovered and disclosed a larger breach of the OPM systems dating to March 2014. Applicants for clearances complete Standard Form-86 (SF-86) which contains all of their personal information, work history, and sensitive information on family, associates, deviances, and proclivities. In the latter breach, 21.5 million SF-86s 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 high-level security clearances that grant them access to very sensitive information.

The Adversary:

An Advanced Persistent Threat (APT) likely breached OPM and its contractors because the actor dedicated significant resources to the attacks and the actor remained in the target systems for a long time. APT 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. Cyber-forensic evidence and sources close to the investigation suggest that a Chinese state sponsored APT group referred to as “Deep Panda” may have breached OPM and its contractors. 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 enable remote administration of computers and networks. If true, then the 22.1 million victims of the OPM breaches need to prepare against intelligence and counterintelligence efforts against their person more than they need to guard against financial identity theft because Deep Panda’s previous attacks have not led to financial fraud from victims’ identities.

An actor motivated by economic gain will likely utilize or sell the data in the short or medium future. Nation-state sponsored groups are more patient and may wait for the dust to settle and complacency to set in. The PII stolen may have value for at least a decade because most of it relates directly to who an individual is rather than credit card accounts or other information that can be reissued. Alternately, an independent actor might wait until the 3 years of credit monitoring ends before using the data. To address this, legislators may consider supporting the Recovery Act, or other legislation that provides prolonged support to the victims of the OPM breach.

Threat to the Federal Government:

If a nation-state sponsored actor breached OPM, then there is a strong likelihood that the United States Federal Government itself was the target of the OPM breach, rather than the individuals supporting that government. Cylance Corporation, Global Chief Information Security Officer Malcom Harkins suggests, “The primary risk may be to the government itself. Having access to the personal information for millions who have clearances gives adversaries an advantage.” Threats to the United States resulting from the OPM breach will originate along physical and virtual attack vectors. According to ICIT Fellow Igor Volovich, “Relying on cyber methods alone to detect such activity would be myopic. A full spectrum of United States counter-intelligence capabilities must be engaged in order to detect attempts to exploit OPM data.” In the short-term (6 - 12 months), the Federal Government can insulate itself from the impact by notifying every individual affected by the breach, including those whose names are mentioned on the SF-86 forms. Agencies need to train employees to recognize and report suspicious behavior and attempts at exploitation inside and outside of the workplace. Agencies should ensure that reports are investigated and that employees are not penalized for reporting incidents. Federal employees with past tenure at multiple agencies are more likely to be targeted. Agencies should terminate access and aged accounts of employees who no longer work in each agency.

The adversary may not intend to utilize the stolen data. In fact, they may have only exfiltrated data out of convenience or the desire to obfuscate another crime. HP Security Strategist Stan Wisseman reminds readers “Adversaries could have modified data and impacted background investigation results.” The primary objective of the breach may have been to modify the OPM data at rest or to inject new data into the system to create new employees or alter the data of cleared individuals. Employees should request a transcript of their clearance file and contest any altered results. HP Security Strategist Cindy Cullen adds, “Security clearances are no longer trustworthy – OPM needs to be able to prove that the data has not been modified. If unable to do so, then all existing security clearances should be re-verified." Even if data from before the breach can be verified using an offline back-up version of the data, a hardcopy, or a version that has integrity checksums, OPM should reevaluate all clearances submitted or approved since the network was breached in March 2014. The necessity for reevaluation may present the opportunity to redesign and simplify the SF-86 form to contain only essential information, as suggested by Representative Thornberry.

In the medium term, the government needs to be cautious of seemingly sporadic tactical targeting aimed at positioning agents of the state sponsored actor. Igor Volovich suggests, "A possible scenario may see active interference in a career path of an employee whose lower clearance level and job role at the time of the OPM breach may have attributed to a reduced level of diligence in post-breach monitoring by the United States Government, enabling compromise through blackmail or similar methods by hostile foreign parties. Once compromised, the virtual landscape of the United States Government organizational structure represented by the OPM breach could enable a foreign entity to covertly engineer reassignment or promotion of such compromised individuals into positions of higher power and access." It is imperative that agencies openly discuss the potential impacts of the OPM breach with their employees and that they train those employees in rudimentary counter intelligence and cyber security. This will reduce the likelihood that an employee will become an insider threat due to disgruntlement or coercion. Overall, the Federal Government should do everything it can to serve its citizens and "keep good people good."

The Threat of Financial and Identity Theft:

Fiscal Theft:

Fiscal theft in the form of stolen credit cards or financial information generally occurs within the 1-18 months following a breach. Despite a few false claims, the financial information of OPM victims has not yet appeared for sale online. Victims of the OPM breach should enroll in the credit monitoring service offered by OPM by providing the minimal of necessary enrollment information. Monitoring service is helpful, but it is not a panacea for potential financial woes. Freezing credit at the three major credit-monitoring services (Equifax, Experian, and Transunion) will prevent the generation of new accounts. Credit monitoring is an alarm service that warns victims if an attacker applies for credit in their name. Credit freezing is the process of suspending all inquiries and approval activity against credit records unless a secondary authorization is received prior to the request for the transaction. This process can be tedious as prior planning and small fees are needed to freeze and unfreeze credit as necessary. When Congress reevaluates the protection offered to OPM victims in Fall 2015, victims would benefit from requesting a dedicated fund to cover credit freeze operations. The online process for credit freezes can be found at the site of each bureau. Further, Stan Wisseman suggests that victims review their state’s policy on establishing credit freezes and implementing permanent and temporary lifts. False tax returns are a very popular attack vector because the IRS has a difficult time distinguishing fake returns from real ones. Citizens should file their taxes as early as possible for the next few years to mitigate the likelihood that an actor will use their valid information to file a false return. Victims can regain considerable control in their lives by reviewing their personal financial statements on a weekly basis. Victims should immediately report any suspicious activity to their financial institutions and they should request new cards as a precaution against exploitation.

Identity Theft:

The granular personal information of 1-in-15 United States Citizens was exposed in the OPM breach. Malcom Harkins contends that ”the adversary could use this information to pose as one of these cleared individuals or in some cases this information could be used to detain these individuals if they are traveling abroad.“ Victims of the breach should monitor their active accounts and be wary of their surroundings when travelling abroad. Harkins continues, “Over the entire time horizon the individuals must be aware that their identity may be stolen and used for a variety of purposes to harm the individual or to harm the United States of America.” Similarly, a victim’s identity could be stolen and used to commit crimes as a targeted attack against the individual victim. Cindy Cullen describes that “Identity theft is generally considered to be for theft of financial data – i.e. obtain credit cards. Another area that identity theft can have major impacts on is in the creation of driver licenses or other identity documents. Then the thief gets into an accident or arrested in the person’s name. This can lead to extreme complication of having to prove it was not you driving or the person that was arrested. Even after proving it was not the OPM victim the arrest warrant may still exist in their name leading to ongoing challenges when pulled over for simple traffic violations. It can also impact the OPM victim’s ability to find employment when companies that perform background checks do not do the appropriate level of due diligence. This may not be able to be detected since this information is not disclosed when not obtaining the position." Cleared individuals can do their best to mitigate this risk by being vigilant of patterns, monitoring their financial profile, requesting new credit cards, and updating their online login credentials for each user account. Securonix Director of Insider Threat Stewart Draper reminds victims that "Employees and contractors who have titles or roles with privileged or elevated access in particular could see a significant increase in spear phishing or malicious code attempts over the coming months." Sadly, there is no way to recover the stolen information; however, victims should review the information that they declared on the SF-86 form and they should evaluate the ways that an adversary could utilize the information. Entertaining the scenarios and planning viable responses will enable the user to act if their identity is compromised.

Accounts and Personal Information:

Information can be categorized as the information about a person's identity, the information that a specific person knows, and the information that a specific person can access or possess. Currently, personal identity information is predominantly used as the control measures to safeguard other information. The OPM breach almost definitely began with a set of compromised user credentials. In fact, the majority of breaches begin with a set of compromised user credentials. If most breaches in the public and private sectors occur because one user fails to adequately secure their account or responds to a phishing email, and the mechanism for preventing inadequate security requires no cost and mere minutes of users' time, then the immediate step that victims of the OPM breach and other breaches should take is to secure their login credentials from malicious actors. This simple solution gives users control over their own cyber-foot print, but it also presents a responsibility that users of every nation have failed to uphold. Many of the victims of the OPM breach were awarded security clearances because they were deemed the most responsible citizens in the United States. These individuals can lead the United States in its most simple and effective reformation.

Enemy hackers often begin an attack against an organization by compromising a user's work credentials, through social engineering or email phishing scams. Sometimes they attack a user by compromising the user's email or social media account and then attacking every account that the user owns until the target organization's network can be accessed through reused login credentials or a password reset mechanism. The target user might work for the target organization, or they might work for a third party organization that merely has tangential access to the target organization. The OPM breach may have begun with a breach at one of its contractors, the Target breach began with a breach at HVAC Fazio Mechanical, and many other breaches began with compromised credentials at a partner organization. The process of using stolen credentials at one organization to either breach another organization or steal the credentials necessary to breach another organization is known as a cascading impact or cascading breach. Because victims of the OPM breaches work at every level of United States government and in the private sector, the OPM breach has an enormous potential for cascading breaches. Stewart Draper mentions that "With many non-government / DoD workers maintaining secret clearances there is also the risk that private sector companies could see an increase in targeted attacks against employees who hold these security clearances. Critical infrastructure industries such as financial, healthcare, energy and communications should be highly observant of external activities towards their networks" In fact, indicators of compromise suggest that American Airlines was recently breached by the same actor who breached OPM. Information from the breach gives the adversary travel information of specific victims who possess a security clearance and have flown using American Airlines. If the adversary is sponsored by an enemy nation state, such as China, then the combinations of victim travel patterns and victim information from the OPM breaches could endanger allies and assets abroad.

Most citizens construct passwords and recovery questions from personal information because the intrinsic nature of the information makes it memorable. Personal information is often the target of attackers and it does not change over time. This means that once personal information is compromised, it can be used to compromise a user's accounts or sold to another attacker, until the user no longer relies upon personal information to secure their cyber-identity. Since the personal information of every SF-86 applicant was compromised in the OPM breach, victims should immediately change the passwords and recovery questions on their personal and private accounts.

Even citizens who are unaffected by the OPM breach benefit from regularly updating their login credentials because personal information is widely available on social networks and email and social media accounts are easy to compromise. Victims of the OPM breach and other breaches will suffer more stress in the future from relying on personal information for login credentials than the stress incurred from remembering new, impersonal login credentials. To aid in the reform effort, the public and private sector need to stop asking for personal information. Social security numbers or account numbers should never be used as a login credentials. Security questions should not relate to public information such as “where were you born?” or “what is your mother’s maiden name?” This has the compound effect that sectors who require less personal security questions will store less valuable information and will be targeted less by attackers. Remember, security questions exist for account recovery purposes and there is no penalty if they are not registered with honest responses. Their single purpose is to help authenticate a user who has forgotten their password or had their account stolen. Victims of the OPM breach should input memorable false information as the answers to security questions for sites that insist on relying on personal information for security questions. This could include altering the date you graduated high school by a month, changing the hospital you were born in to your college town, or using your mother’s first name instead of her maiden name. Alternately, false information corresponding to a book or movie can be used. Security questions should instead focus on information that a specific person knows. For example, a Facebook security question might ask, “What song is your guilty pleasure?” Sites can increase security even further by allowing the user to input their own security question and response and then redisplaying the question to the user at login as a secondary check, in the same fashion that banking sites use for “security phrases”.

Every modern cyber-security textbook preaches greater-than-15-character passwords consisting of upper and lowercase letters, numbers, and special characters. These best practices also evangelize against password reuse and password sharing. Users should utilize a different username and password combination for each account on each website. Users should change their passwords every three months and they should enable multi-factor authentication where possible. Most users, including many in the cyber-security fields, ignore this best practice because in the real world, it is difficult to remember all of the different accounts that a user owns, let alone a different 15 character complex password for each account. The majority of users believe that their accounts are not worth compromising, so they fall complacent in shoddy cyber-security and they reuse a set or a few sets of credentials. Other users store their credentials on their devices or they employ password managers. Some users record their login credentials on paper or in their mobile device. Only an extremely small portion of users adhere to ideal cyber-security practices. As a result, public and private organizations are regularly breached through compromised credentials. Victims of the OPM breach and the legislative community have the power to curb this apathetic practice. Agencies should teach their employees how to both create and remember complex login credentials. Those employees should pass that knowledge onto their families. This cyber-security best practice could even be taught to schoolchildren if presented well. Regularly updating passwords (about every three months) is as easy as making a list of websites where a user has accounts, securing that list, and then marking a 15 minute - 1 hour reservation on a calendar every 3 months. Government agencies can automate credential update schedules through their governance systems.

Users can make easy to remember complex passwords using information that they know or information that they can access instead of information relating to their personal identity. Often, users find one “really good” password to which they grow attached and either never change or reuse on other accounts. Vigilant users, as the victims of the OPM breach need to become, must resist that temptation. Rather than grow attached to a particular password, focus your mind's sentiment towards developing and adopting a unique password generation schema that will assist you in rapidly and in repeatedly creating new memorable passwords. One such schema would be to open a book on your desk or mobile device and either remember or record the page number on a tablet. Take the first sentence and develop a pattern. For instance, the first sentence of Chapter 5 of *Frankenstein* reads, "It was on a dreary night of November that I beheld the accomplishment of my toils." Using the first five words and the length of the sentence, the password "I2w3o2a1d5n5#16" can be generated. The schema is as follows: Take the first letter of the six five words in a sentence, followed by the length of the word, capitalize each letter that is capitalized in the sentence and then end with the number of words in the sentence. This schema is very simple and it should only serve as an example for creating your own personal method of password generation. Entire words could be spelled out if they are above or below a certain length, capitalization altered, special characters employed, or any other alteration could be made to the schema. Song lyrics, children's' rhymes, or other seed data could likewise be used to create robust passwords. Users who wish to forgo schema creation should develop their own method for complex password creation and retention. Apathy is no excuse for lackluster security because a single compromised account can affect millions of other people. Users who wish to randomly generate passwords or use complex passwords that are difficult to remember can split the password and record the halves on two separate mediums, such as half on paper and half in a mobile device. News of recent breaches indicates that password managers or password vaults are often not as secure as advertised.

This is in part because these applications are single points of failure which draw the attention of attackers because compromising the single application directly leads to stolen credentials which aid in a number of other avenues of attack. Users should only resort to reliance on these applications when all other methods fail.

Potential of Sold Data:

The assumption that the adversary, possibly the group Deep Panda, is uninterested in fiscal exploitation of the victims is bolstered by the observation that the OPM breach occurred for over a year and the no information connected to the breaches was discovered on darknet, the unindexed portion of the internet frequented predominantly by hackers and criminals. That said, patterns can always change and victims should prioritize their safeguard measures and implement every change reformation within their power. The actor group may not be Deep Panda, they may alter their methodology by inclination or design, or they may sell the data that is not useful to their purpose. The actor may have held onto the data in order to conceal the breach, or they may be sifting through the information for juicy bits with the intent to sell the remainder. Even if the information was stolen for intelligence or counterintelligence purposes, the actor group could choose to sell or exploit the PII or financial information of specific individuals. In this manner, specific victims can be leveraged prior to a recruitment attempt, discredited through illicit activity connected to their accounts, or even coerced into altering their lifestyle. For example, if the fiscal damage is great enough to cause a victim's family to be unable to afford necessities, then a targeted victim could be forced to leave an organization to move to a different area or to leave the public sector for the private sector. The actor could then position a covert or coerced asset in the vacant position and infiltrate the organization. Without definite knowledge in the mind of the actor group, victims are advised to prepare against every reasonable scenario.

The Threat of Passive Espionage:

Monitoring:

Adversaries could monitor the victims of the OPM breach in the medium to long-term future in order to collect data for a sustained attack campaign. Victims of the breach need to exercise a healthy amount of paranoia and be vigilant for suspicious activity.

Blackmail:

In the weeks following the disclosure of the breach, the media popularized the notion that individuals possessing clearances may be ransomed or blackmailed by a state-sponsored actor based on information declared in the SF-86 forms. While credible, the risk is reduced by the fact that the victims are those already deemed trustworthy. Each victim must determine how damaging his or her stolen information could be to his or her life. They should hypothesize their available responses to an extortion attempt in each period. Embarrassing or uncomfortable discussions with loved ones may have to happen now or in the future and victims need to accept that possibility. Planning for possibilities reduces and in some cases eliminates the illusion that the adversary has the leverage to blackmail an individual. 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. As a result, victims who have declared economic hardship or significant political differences might be at increased risk of coercion attempts.

The Threat of Active Espionage

Recruitment:

In the medium-term (1-5 years) individuals need to be wary of adversarial attempts to solicit or coerce information that could be used against the United States Government. Newly cleared employees must be vigilant for the long-term. The easiest mitigation strategy is to avoid discussing work outside of work and to be suspicious of prying questions. Victims should report any suspicious activity or sudden changes in behavior of coworkers to a supervising authority. Reports should be invasive and thoroughly investigated without consequence to the monitored individual unless malicious activity is detected.

Physical Threat:

Federal employees should immediately report to law enforcement bodies, such as the police or FBI, any fear of physical violence, threats of physical violence, attempts at physical violence, or acts of physical violence against themselves or their families.

The Threat of Harm to Family and Friends:

Family and Acquaintances:

The primary victim of the OPM breaches may not be the primary target of future campaigns. We live in the digital age, where information is often more valuable to nation states than physical weapons. The SF-86 forms already provide an expansive profile of a given victim's personal life, activity, and history. According to ICIT researcher, Chris Schumacher, "Based on the sheer volume of direct personal data gathered on employees/contractors there is not much more to be gathered on them as a subject of directed or persistent hacking efforts. However, family members and current/former colleagues are now a much larger target for ongoing and future attacks. Bad actors now have just enough seed data to expand their attack footprint to attempt to gain access to the personal data of family members and colleagues of those affected in the first two OPM breaches." By targeting family and acquaintances with blackmail, phishing, and other attacks, the malicious actor collects new information and is less likely to trigger the warnings, such as credit monitoring, that victims of the breach rely upon. Stewart Draper points out that adversaries could also compromise friends and coworkers by masquerading as users on social networks such as LinkedIn or Facebook. It is the moral responsibility of victims to notify friends, whose names appeared on SF-86 forms, of the OPM breach in case the Federal Government fails to do so. A simple conversation can prevent compromise of that friend and even save them from physical harm in the event that they are an asset in a foreign country.

Many victims are more concerned with the impact that the breach will have on their children than they are concerned about the impact to themselves or the nation. The personal data of some victims' children was exfiltrated in the SF-86 forms that were stolen by adversaries in the second OPM breach. Given the power of social media, victims whose child's information was not exposed in a breach should still be wary and follow basic precautions. If a parent is a valid target to an attacker, then the child of that parent is either an avenue of attack or a higher value target to an attacker. Parental desire to protect our children presents an attack vector in even the most guarded and security conscious individual. A callous adversary could utilize this to compromise, exploit, or corrupt a victim of the OPM breach. Families with children who suffer from medical conditions or have children abroad are at additional risk. Exploitation of a victim's family requires a vast dedication of resources and will not likely happen on a large scale, but it is within the realm of possibility and parents need to be prepared. Chris Schumacher adds that, "[Children's'] age coupled with inexperience makes them a tantalizing target for intelligence operatives of every stripe." Children could become long-term targets for identity theft or fiscal fraud. Parents should conduct yearly credit checks and healthcare audits of their children's information, as well as their own. Because children will assume responsibility of this process when they are old enough, parents need to set an example and explain to their children why regular processes, like credit checks, are important.

Even if no exploitation of the OPM information occurs, families will greatly benefit from normalizing monitoring procedures because most other breaches result in credit card fraud, healthcare fraud, or fiscal identity theft. OPM victims have the opportunity to teach their children to notice and respond to suspicious activity, before irreconcilable financial harm is done, which could prevent a child from getting a job, going to college, or applying for credit.

Without training, children may not recognize an email or social media phishing scheme or social engineering attack. The ubiquity of social media makes finding a specific user trivial. Though it might seem inconceivable, attackers could befriend, recruit, blackmail, or coerce a child into providing information or becoming a long-term asset. Children have been the targets of some historical espionage campaigns, especially during the Cold War. Even in modern times, ISIL has experienced some success in luring susceptible individuals overseas using social media. Igor Volovich agrees that "Should a child be targeted for individual exploitation as a future asset, it is not outside the realm of possibility to imagine a long-term scenario where a foreign intel service identifies a promising prospect with high-level family connections identified during the OPM breach, oversees the child's development and education, covertly influences key events in their life, hoping to eventually see the prospect leverage family connections to enter government service in a position of privileged access or influence." Since the OPM data could be relevant for an estimated 30 years, and many parents who work for the Federal government inspire their children to follow in their footsteps, recruiting the child of a victim is actually a reasonable tactic for a malicious actor. Alternately, adversaries could make kidnapping, blackmail, or physical threats against children in an attempt to coerce parents into committing espionage objectives. These threats, while likely insubstantial, may seem more authentic if supported by details garnered from social media or unwarranted communication with children. To mitigate this attack vector, parents should stress the traditional adages “avoid strangers” and “if you see something, say something.”

Even if adversaries make neither contact nor offers, parents need to be on guard about their child’s cyber-presence. While parents should be aware of their children’s social media accounts, parents should not take drastic measures such as Orwellian monitoring or termination of social media. The key to moving forward and regaining control of victim’s lives is gradual integration of reasonable security practices into the familial comfort zone. Besides, many employers see lack of a sustained online presence as a red flag. Instead, the social media accounts of parents and their children should have their privacy settings maximized. Common sense practices such as “don’t talk to strangers” mitigate most social media attack vectors.

Rather than communicating with children, adversaries could just compromise their accounts through compromised credentials or phishing emails. Phishing emails often deploy malware that facilitates remote backdoor access to the PC or monitoring (keystroke, microphone, camera, etc.) of the user. Though most children use their own computers or phones to access email and social media and though no proprietary/ classified information should be on an employee’s personal computer, adversaries may still try to compromise a child’s account to access an OPM victim’s files. Some malware can spread across the network after it infects an initial host. The infection of a familial device could thereby compromise a victim’s device and lead to cascading impacts.

Basic Cyber-Security:

Users should deploy basic antivirus, anti-malware, and firewall applications on computers and devices on their home networks. Software on devices should be kept up-to-date to limit the avenues of attack. Most mobile devices feature hard drive encryption settings in the security settings tab that can assist in protecting the data on the devices. Victims who access confidential resources or the company network on their mobile device should probably employ sandbox or virtualization solutions to segment the data on their device. Employees and agencies should have an established VPN connection for remote work.

Agencies may wish to issue pre-encrypted/ secured devices. Agencies should also deploy multifactor authentication on all possible systems and tokenization on systems that require higher degrees of security.

Users should migrate to email providers that support encryption and security solutions in their product, such as Gmail. Whenever possible, personal email accounts should not be accessed from work devices and corporate email accounts should not be accessed from personal devices. Personal information may be used to create elaborate spear phishing emails to lure victims into revealing sensitive information that they know. Phishing emails tend to download malware onto the victim's system. As a result, victims and their families need to learn to recognize malicious emails before they are opened. Phishing scams often spoof a legitimate looking email address by slightly misspelling an email address or altering the top level domain (the .com, .org, or .gov that follows an address). Adam Firestone recommends that users "Employ the READ principle with respect to email (Is it Relevant? Is it Expected? Is it Attributable? Is it Digitally signed?)." Superfluous emails, such as those from social media should probably be ignored or automatically deleted. Users and their families should be wary of emails containing links or attachments. Instead of navigating to a link that is embedded in an email, try to type your destination into the address bar or a search engine and navigate from there. Email activity should be monitored (i.e. occasionally make sure that the emails in the sent folder are recognizable). Suspicious activity should be reported to the email provider and the account credentials should be immediately changed.

Keep Moving Forward:

An unknown adversary has exfiltrated the granular personal information of 22.1 million United States citizens during two long-term breaches of the network of the United States Office of Personnel Management. Victims need to accept that the data has been stolen and proactively mitigate the impact of potential threats. The victims of the breach have the power and the opportunity to fundamentally change American cyber-security culture by adopting some simple best practices in their homes and lives. Igor Volovich advises victims to "Trust your instincts, check which information you and your family our outputting, and who is communicating ostensibly privileged data back to you as a possible trust pretext. Know what's been lost through the OPM breach and be on the lookout for attempts to leverage this data for exploitation by third parties." Ultimately, victims can lessen the value of the stolen data and regain a considerable control of their lives by employing common sense, monitoring their accounts, and protecting their families.

*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)
- Malcolm Harkins (ICIT Fellow –Global Chief Information Security Officer, Cylance Corporation)
- Rob Roy (ICIT Fellow – Federal Chief Technology Officer, U.S. Public Sector, HP)
- Cynthia Cullen (ICIT Fellow – Security Strategist, HP)
- Stan Wisseman (ICIT Fellow – Security Strategist, HP)
- Igor Volovich (ICIT Fellow – Institute for Critical Infrastructure Technology)
- Chris Schumacher (ICIT Researcher – Institute for Critical Infrastructure Technology)
- Stewart Draper (ICIT Fellow – Director of Insider Threat, Securonix)
- John Menkart, (ICIT Fellow – VP Federal, Securonix)
- Dr. Igor Baikalov (ICIT Fellow – Chief Scientist, Securonix)
- Adam Firestone (Contributor– President and General Manager, KGSS Inc.)

Contact Information

Legislative Branch Inquiries:

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

Federal Agencies, Executive Branch, & Fellow 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: in f

Ars Technica:

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

The Baltimore Sun:

http://www.baltimoresun.com/news/maryland/bs-md-federal-workplace-opm-20150721-story.html

Bloomberg:

http://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines

The Christian Science Monitor:

http://www.csmonitor.com/World/Passcode/2015/0807/OPM-breach-a-shadow-over-Homeland-Security-s-appeals-to-security-pros

CSO Online:

http://www.csoonline.com/article/2852855/advanced-persistent-threats/10-deadliest-differences-of-state-sponsored-attacks.htmlDefense One:

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

Fed Scoop:

http://fedscoop.com/opm-losses-a-40-year-problem-for-intelligence-community

Federal News Radio:

http://federalnewsradio.com/opm-cyber-breach/2015/07/federal-news-radio-opm-hack-survey-07-22-2015/slide/1/

http://federalnewsradio.com/fed-access/2015/07/the-opm-cyber-breach-and-the-cleared-community/

Federal Times:

http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/07/10/lifetime-credit-monitoring-opm-breach/29958383/

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/2015/06/24/opm-hack-cyber/29208581/

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

Government Executive:

http://www.govexec.com/contracting/2015/08/some-opm-hack-victims/118867/

The Hill:

http://thehill.com/policy/cybersecurity/247339-senate-dem-pushes-bill-forcing-opm-to-offer-more-breach-protections

http://thehill.com/policy/cybersecurity/247714-house-bill-would-give-opm-hack-victims-lifetime-fraud-protection

Huffington Post:

http://www.huffingtonpost.com/adam-levin/open-letter-on-the-opm-br_b_7766708.html

ICIT:

http://icitech.org/icit-brief-opms-demonstration-that-antiquated-security-practices-harm-national-security/

http://icitech.org/preparing-the-battlefield-the-coming-espionage-culture-post-opm-breach/

Info-Security Magazine:

http://www.infosecurity-magazine.com/news/us-house-intros-lifetime-credit/

Krebs on Security:

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

http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

The National Interest:

http://nationalinterest.org/blog/the-buzz/revealed-what-china-saying-about-us-response-the-opm-hack-13524

Nextgov:

http://www.nextgov.com/cybersecurity/2015/08/contract-notify-and-protect-opm-hack-victims-now-out/118868/

Office of Personnel Management:

https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/

PC World:

http://www.pcworld.com/article/2954872/opm-anthem-hackers-reportedly-also-breached-united-airlines.html

Slashgear:

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

Tech Zone 360:

http://www.techzone360.com/topics/techzone/articles/2015/07/10/406516-what-need-know-the-opm-data-breach-incidents.htm

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

Tripwire:

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

U.S. Chamber of Commerce:

https://www.uschamber.com/above-the-fold/did-congress-already-forget-the-opm-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

Wired:

http://www.wired.com/2015/07/senator-sasse-washington-still-isnt-taking-opm-breach-seriously/

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

The XX Committee:

http://20committee.com/2015/06/08/hacking-as-offensive-counterintelligence/

http://20committee.com/2015/06/11/the-opm-hacking-scandal-just-got-worse/