**IT 530 Proposal: Increasing Security Measures for the United States Office of Personnel Management**

Sonya Duong, Madeleine Heick, Nnana Obioha, Dylan Patel, Corey Saksa

Marymount University

IT 530: Computer Security

Dr. Natalia Bell

September 30, 2022

Github: <https://github.com/sduong08/IT530_Project.git>

**Introduction:**

In 2015, The Office of Personnel Management (OPM) announced it was hacked by what is believed to be Chinese government sponsored hackers. OPM is the primary Human Resource department for the US Federal government and is responsible for overseeing Human capital management, Benefits for 8 million active Federal employees as well as retirees, and family benefits(n.d.). They are also responsible for vetting candidates for security clearances across both Federal employment as well as contractors. The impact of this hack was the disclosure of personal data of about 22 million people (Nakashima, 2021) including fingerprints for over 5 million people (Sanger, 2015) .

One of the biggest concerns was the information of people being vetted for security clearances, as the Chinese government now has the personal details of everyone with a security clearance from which they can attempt to recruit spies or attempt to steal the identities of cleared people to gain access to sensitive areas and information as well as their family members (Graff, 2020). There were several methods used to gain access to OPM’s data, including social engineering, phishing, and whaling which ultimately led to a malware attack that installed a backdoor tool called PlugX (Fruhlinger, 2020).

Since the Chinese government is an authoritative with little leadership turnover through the years, the Chinese intelligence can plan and run decades long operations. This means the US federal workforce and clearance holding contractors need to remain vigilant to ever changing cyber security threats even several years after the hack(Graff, 2020). It is often a common intelligence gathering practice to target low clearance holders or even family members of clearance holders to gain trust and influence them into applying for higher clearances.

We will in this proposal spell out continued training and implementation of an improved cybersecurity posture to include stronger passwords, MFA, firewalls and other protocols.

**Literature Review:**

Government agencies and organizations, especially those in the United States, are prime targets for hackers around the world, and sometimes even from their own citizens. One may wonder “Why? What is so special about this government agency or organization?” The answer to that question is that many government agencies contain “highly sensitive information, which are a goldmine for hackers and they work with a large variety of industries,” (Securelink, 2021). If the wrong person gets ahold of specific types of information, it can lead to loss of finances for the government. Finances play a big role in the motivation for hackers to target the government, especially hostile state actors since they can use it to their advantage in political cyber warfare, according to Khan in 2020.

There are many ways that hackers can hack into a government organization or agency. These hackers can even be someone currently working for the government and would be classified as an internal threat, while hackers from the outside are external threats. A hacker from within can be extra dangerous because they have access to different systems and softwares that the government agency uses and depending on the level of privileges they have, the hacker may be able to view specific classified information. If they decide to leak classified information, depending on the level of classification, it can be detrimental to the government and its citizens. For the United States government, there are a few classification levels that are used. UNCLASSIFIED material consists of information that, if released, will not cause harm to the country. CONFIDENTIAL material can cause damage to the national security of the country if it is disclosed prior to being authorized for release. SECRET and TOP SECRET material, if released without authorization can cause serious damage and grave damage, respectively, to the national security of the United States (*Code of Federal Regulations,* 2004). Another way that hackers can infiltrate the government's systems is by sending phishing emails to try and get login information or even personally identifiable information (PII) from current employees and users.

One way that government organizations can dissuade hackers from targeting them is by continuously updating security measures (i.e. provide patches, require authentication and authorization, changing passwords, etc.) Hackers look for organizations that do not seem well protected. Generally, government agencies usually have less money and resources to invest in the most-up-to-date security systems and technologies. Hackers can exploit old and outdated computer systems. Additionally, older computers and security systems are usually a lot harder and a lot more expensive to maintain. Thus government organizations should make it a priority to update their overall system whenever possible and provide training to their employees so everyone knows how to use the technology correctly (Yaraghi, 2022).

The United States government spends billions of dollars on IT projects. In 2015 alone they spent more than 75 billion dollars. However, many of these projects fail. One report indicates that of all federal projects that took place between 2003 and 2016 with more than $10 million in labor costs, only 6.4% were successful. One of the reasons this number is so low, is the fact that the projects are exceedingly large, thus unwieldy. Additionally, many of the government's IT systems that are currently in place are old and have not been updated. Often, the government comes to the conclusion that putting newer, more efficient, and less expensive IT solutions and technology into effect is an option because newer systems would not be compatible with the older ones currently in place (Yaragh, 2016).

To mitigate some of the IT issues the government faces, they could break large IT projects into much smaller ones. This would reduce the risk associated with any given project and increase the likelihood of the project being finished on time and within budget. Additionally, the government could become more transparent with their IT efforts. Lessons should be learned when projects fail. Failure should be documented and turned into policy in procedure that will reduce the chances of the mistake happening again. (It should be noted that this information does not have to be made available to the general public, especially if it is sensitive. The necessary people should know about it).The government can also aim to at least be competitive with the private sector when it comes to attracting talent. The US wants high quality developers, entrepreneurs, and executives to protect its data and improve its IT solutions. (Yaragh, 2016)

The Biden-Harris Administration has also made significant strides in improving cybersecurity when it comes to protecting the government. For example, an executive order signed on May 12, 2021, by President Biden has provisions that are moving the country towards a more modern cybersecurity defense network and improving the sharing of information between the private sector and the US government about issues relating to cybersecurity. This strengthens the country to respond to attacks as they occur (*Cybersecurity | Homeland Security*, n.d.).

The executive order also highlighted the importance of post-quantum encryption algorithms, which would help protect IT systems for attacks coming from large-scale quantum computers, which would be able to break most of the public-key crypto systems that are currently being used (*Cybersecurity | Homeland Security*, n.d.; *Post-Quantum Cryptography | CSRC*, n.d.). The aim of post-quantum cryptography is to create cryptographic protocols that will be secure against both classical and quantum computers while simultaneously interacting with protocols and networks currently in place (*Post-Quantum Cryptography | CSRC*, n.d.). The Biden-Harris administration has laid out plans to phase in the use of such algorithms. Furthermore, they seek to strengthen software supply chain security. This will be done by putting in place baseline standards for security for software sold to the government. These standards include requiring developers to make security data publicly available and providing more transparency into their software. Some security software used by the government has extensive vulnerabilities, which are easily exploited by hackers and cybercriminals. These standards would help decrease the chances of that happening (*Cybersecurity | Homeland Security*, n.d.).

**Proposal:**

Having a firewall can help monitor traffic that is coming in and out. Firewalls can help prevent attackers from getting into an organization. The firewall can help monitor and avoid virus attacks when installed. Another valuable benefit of a firewall is that it can help protect privacy. This can be from data getting exposed. When installing a firewall, finding the proper tool that matches the organization's needs and the current requirement is best. Employing white hackers can be very useful as they can detect gaps within network security. If the white hackers potentially find an opening, we can quickly patch it. For example, a white hat hacker can do a pen test where they will try to find vulnerable flaws in the system and within the firewall.

Patching security threats is a crucial part of an organization. Security patches prevent cyber attacks and protect an organization from breaches. A way to patch security threats is to have patch management. Having patch management can reduce downtime to the systems. This means applying patches during hours of operation. Another valuable benefit of patch management is that it can stay up to date on innovation and compliance. This can be done by regularly keeping the systems up to date without missing any patches. An example of management that can run patch management is ZenGRC. It is a governance, risk management, and compliance tool that can detect security threats (Just a Moment. . ., n.d.). Detecting security threats guides the organization on how to fix them. It is in many organizations as it is efficient and will monitor daily to find vulnerabilities.

Ensuring users are well equipped with best practices is a fundamental approach to preventing hacks. A method and organization can help ensure its users and network is well protected by using Multi-factor Authentication (MFA). MFA is a highly effective defense tool in protecting users and their systems because it requires the user to provide two or more verification factors to gain access to a resource, such as an application, online account, or VPN. Implementing MFA increases the confidence that an organization will stay safe from cybercriminals due to the added layer of complexity added to be able to hack an organization.

Another defensive strategy users in an organization can practice preventing hackers is ensuring users are aware of social engineering attempts. Organizations can use methods to ensure their users are developing. Best practices warn users not to provide personal information or information about your organization, including its structure or networks, unless you are sure of a person's authority to have the information. Security tip (ST04-014). CISA. (n.d.). If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use the contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups. Security tip (ST04-014). CISA. (n.d.).

An offensive tactic users in an organization can practice ensuring their organization is safe from hackers is by organizations and users within that organization continuously learning and understanding new preventive measures and technologies that emerge in the market. Organizations can execute this preventative measure by offering annual and quarterly training mandatory for all employees. Users can do their due diligence by being aware of phishing attempts and other manners in which people attempt to get personal information.

**Conclusion**

The implementation of a multi-pronged approach, which covers both human and technical issues, taking into consideration the current information about cybersecurity, is the best way to ensure that OPM does not experience another significant security breach. The information in this proposal shall update OPM’s cybersecurity posture in accordance with the industry.

**Reference**

*About us our mission, role & history*. U.S. Office of Personnel Management. (n.d.). Retrieved

September 30, 2022, from<https://www.opm.gov/about-us/our-mission-role-history/>

*Code of Federal Regulations.* (2004, April 1). Retrieved September 30, 2022, from

[*https://www.govinfo.gov/content/pkg/CFR-2004-title22-vol1/xml/CFR-2004-title22-vol1-sec9-5.xml*](https://www.govinfo.gov/content/pkg/CFR-2004-title22-vol1/xml/CFR-2004-title22-vol1-sec9-5.xml)

*Cybersecurity | Homeland Security*. (n.d.). Retrieved September 25, 2022, from   
 <https://www.dhs.gov/topics/cybersecurity>

Fruhlinger, J. (2020, February 12). The OPM Hack explained: Bad security practices meet   
 China's Captain America. CSO Online. Retrieved September 30, 2022, from   
 [https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-](https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html)

[practices-meet-chinas-captain-america.html](https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html)

Graff, G. M. (2020, February 11). *China's hacking spree will have a decades-long fallout*. Wired.   
 Retrieved September 30, 2022, from [https://www.wired.com/story/china-equifax-anthem-](https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/)

[marriott-opm-hacks-data/](https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/)

Khan, B. (2020, October 20). *Why are government agencies so vulnerable to hacking?* A10   
 Networks. Retrieved September 23, 2022, from [https://www.a10networks.com/blog/](https://www.a10networks.com/blog/why-are-government-agencies-so-vulnerable-to-hacking/)

[why-are-government-agencies-so-vulnerable-to-hacking/](https://www.a10networks.com/blog/why-are-government-agencies-so-vulnerable-to-hacking/)

*Just a moment. . .* (n.d.). Retrieved September 24, 2022, from [https://reciprocity.com/blog/tips-](https://reciprocity.com/blog/tips-for-patching-security-vulnerabilities/)

[for-patching-security-vulnerabilities/](https://reciprocity.com/blog/tips-for-patching-security-vulnerabilities/)

Nakashima, E. (2021, December 1). *Hacks of OPM databases compromised 22.1 million people,   
 Federal Authorities Say*. The Washington Post. Retrieved September 30, 2022, from   
 [https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-](https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/)

[clearance-system-affected-21-5-million-people-federal-authorities-say/](https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/)

Sanger, D. E. (2015, September 23). *Hackers took fingerprints of 5.6 million U.S. workers,   
 government says*. The New York Times. Retrieved September 30, 2022, from   
 [https://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-](https://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html)

[million-us-workers-government-says.html](https://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html)

Securelink. (2021, August 2). *Why government institutions are the perfect target for hackers*.   
 GovTech. Retrieved September 23, 2022, from [https://www.govtech.com/sponsored/why-](https://www.govtech.com/sponsored/why-government-institutions-are-the-perfect-target-for-hackers)

[government-institutions-are-the-perfect-target-for-hackers](https://www.govtech.com/sponsored/why-government-institutions-are-the-perfect-target-for-hackers)

*Security tip (ST04-014)*. CISA. (n.d.). Retrieved September 24, 2022, from   
 https://www.cisa.gov/uscert/ncas/tips/ST04-014

*Post-Quantum Cryptography | CSRC*. (n.d.). Retrieved September 25, 2022, from   
 <https://csrc.nist.gov/projects/post-quantum-cryptography>

Yaraghi, N. (2016, July 29). *Doomed: Challenges and solutions to government IT projects*.   
 Brookings. Retrieved September 25, 2022, from [https://www.brookings.edu/blog/](https://www.brookings.edu/blog/techtank/2015/08/25/doomed-challenges-and-solutions-to-government-it-projects/)

[techtank/2015/08/25/doomed-challenges-and-solutions-to-government-it-projects/](https://www.brookings.edu/blog/techtank/2015/08/25/doomed-challenges-and-solutions-to-government-it-projects/)

Yaraghi, N. (2022, March 9). *How can city governments protect themselves against ransomware   
 attacks?* Brookings. Retrieved September 25, 2022, from[https://www.brookings.edu/](https://www.brookings.edu/blog/techtank/2019/06/11/how-can-city-governments-)

[blog/techtank/2019/06/11/how-can-city-governments-](https://www.brookings.edu/blog/techtank/2019/06/11/how-can-city-governments-)[protect-themselves-against-ransom  
 ware-attacks/](https://www.brookings.edu/blog/techtank/2019/06/11/how-can-city-governments-protect-themselves-against-ransomware-attacks/)