OPM Breach

Honor Pledge: I acknowledge that the Capstone Project is an independent study project to be completed individually. On my honor, I have not received aid on my Capstone Project other than what was provided by my faculty mentor and any persons explicitly cited in my work. I further acknowledge that if I have given any aid to another student in this course, the instructor of this course was made aware of my contributions.

Contents

Project Objectives

In June 2015 the Office of Personnel Management (OPM) announced that there had been a security breach affecting 4.2 million federal employees (Nakashima, 2015). A month later, they stated that a second breach had affected a combined 22.1 million people. Among these individuals were current and past federal employees, contractors, friends, and family members. FBI Director James B. Comey stated in a meeting with reporters, "It's a treasure trove of information about everybody who has worked for, tried to work for, or works for the United States government (Nakashima, 2015)." This security breach is unlike others in the past because of the size and type of information that was retrieved. Hackers successfully stole files over a six-month period which included social security numbers, educational and residential history, previous employment history, immediate family member information and over 1.1 million fingerprints, detailed financial and health records, usernames and passwords. Officials believe that the breach was so extensive that every file stored in OPM databases since 2000 could have been hacked (Nakashima, 2015).

The aim of this paper is to examine the breach and to understand what has been done in order to prevent this from happening in the future. Apart from this there will also be an examination of the legislature that is currently available to agencies and their effort to protect personal information.

Testable Hypothesis

The testable hypothesis is: The government needs to restructure their security systems when storing sensitive information in order to decrease the amount of future breaches.

The point of view of this project will be from an outside source examining what information is known and relative to this influx of security breaches within the last year. Many have speculated that the OPM breach was part of a larger plan that has been in the works for over a year. Many previous breaches have been linked to possible information that was exploited to execute this breach. I want to convey to the reader a summary of the breach, what

the government is doing to prevent future incidents and examine alternative methods that could be implemented to ensure the security of personal information.

Faculty Mentor

I have asked Dr. Diane Murphy to be my advisor because I feel she is qualified to help me through this process.

Project Details

The OPM breach that occurred in June of this year has been among the largest breaches on a government agency. When first disclosed by OPM, officials stated that 22.1 million people had been affected. A separate 1.1 million individuals had their fingerprints stolen. Since then, the number has risen to 5.6 million individuals (Greenburg, 2015). The impact of this breach has resulted in a distrust of the safety of personal information. OPM is in charge of storing information on all of its employees across multiple agencies. Apart from this they also store all the application (SF-86) that federal employees fill out when applying for a security clearance. This information includes personal information on past jobs, places of residency, family and friends, criminal records and financial records. Officials have warned the public that the information that was stolen includes records on past and present employees as well as family members who may have been on any applications (Shinkhman, 2015).

Officials have been very cautious about what they have disclosed and this has made it hard to understand what was the motive for the attack. Previous attacks earlier in the year have suggested that China is building a database on federal employees which they can use to exploit employees who are in financial distress or blackmail (DigitalCommons, 2015). On September 30th the U.S. decided to pull spies from China as a result of the data breach. They feared that the Chinese government could use the stolen information and use a process of elimination to find intelligence spies operating within the U.S. embassy under false identities (Perez, 2015). The Chinese government has denied these acquisitions and Hong Lei, a spokeman for the Chinese Ministry of Foreign Affairs reiterated this by stating that, “The Chinese government firmly opposes any forms of hacking (Perez, 2015).” He also noted that

days before this the U.S. and China agreed to not conduct any cybertheft that would be integral to the commercial gain of the other country (Perez, 2015).

The OPM breach was executed by using compromised credentials that had been assigned to KeyPoint Government Solutions employees (DigitalCommons, 2015). KeyPoint is a federal background check contractor who was recently hired by OPM to facilitate with background checks on security clearances (DigitalCommons, 2015). KeyPoint was hired to take over the bulk of background investigations late last year after OPM decided to not resign a contract it USIS following a breach earlier last year. It was only a matter of months before KeyPoint was also hacked in December of 2014 (DigitalCommons, 2015). In this breach an estimated 50,000 employee records were stolen (DigitalCommons, 2015). Many sources have linked this breach with the OPM breach since the credentials used were assigned to KeyPoint employees. There have been many speculations over the decision of changing contractors in such a short time frame. Many have speculated that KeyPoint was never prepared to handle the workload that was transferred to them upon the termination of the contract with USIS (DigitalCommons, 2015). Employees from KeyPoint have stated that the company was never equipped to handle such a large volume of information given its resources (DigitalCommons, 2015).

The breach on KeyPoint systems is just a short list of breaches in the past years that have given way to other breaches. The level of sophistication of these breaches will only continue to increase as long as the government continues to use outdated legislation to protect from future attacks.

So far I have been read up on how the attack occurred and what effects it had on employees as well as the nation. It has been hard to find any detailed information on how the breach was detected since this is an ongoing investigation so there is not much information that has been made available to the general public. I have found that OPM databases were updated to run on the Department of Homeland Security's (DHS) Einstein program. Einstein is an intrusion detection program that uses sophisticated methods to detect intrusions (Privacy Impact Assessment, 2015). I have started to read up on this method but it is very technical and

hard to fully understand. I have also found legislation that is the backbone of federal information security systems. This legislation was proposed in 2002 and since has been amended to be current with information security systems present today. I have also started reading up on the Federal Information Security Management Act (FISMA) which was amended to give operational authority to DHS for implementation and authority to issues as well as set requirements for breach notifications for federal agencies (DigitalCommons, 2015). From here I have to analyze all this and see how this fits with my thesis and explain my findings.

Knowledge Being Applied

I have been using a lot of my knowledge learned from Cybersecurity Principles as well as Corporate Cybersecurity to analyze the information found. Apart from this I have used my networking knowledge to try and understand how Einstein works. Apart from this I am also using my experience working with NIST and ISO standards to understand and analyze the legislation that is currently available on how federal agencies protect personal identifiable information.

Risk Factors

The biggest risk factor that would affect me would be not being able to access knowledge on the data breach and what specific detection systems failed. This will make it harder for me to support my thesis since there is no concrete evidence of poor security countermeasures taken by OPM to protect personal identifiable information. Another risk factor is the fact that this investigation is still under way and there are a lot of unknowns that have yet to be reported. New information on the issue could later cause my thesis to no longer be supported by information that may be redacted or modified as more information becomes available.

References

Digitalcommons.ilr.cornell.edu,. (2015). *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*. Retrieved 20 October 2015, from http://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?article=2447&context=key_workplace

Greenberg, A. (2015). *OPM Now Admits 5.6m Fedsâ€™ Fingerprints Were Stolen By Hackers*. *WIRED*. Retrieved 18 October 2015, from http://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/

Nakashima, E. (2015). *Hacks of OPM databases compromised 22.1 million people, federal authorities say*. *Washington Post*. Retrieved 15 October 2015, from https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

Perez, E. (2015). *U.S. pulls spies from China after hack*. *CNNMoney*. Retrieved 25 October 2015, from http://money.cnn.com/2015/09/30/technology/china-opm-hack-us-spies/

Privacy Impact Assessment for Einstein 3 - Accelerated (E3A). (2013) (1st ed.). Retrieved from http://www.dhs.gov/sites/default/files/publications/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf

Shinkman, P., & Risen, T. (2015). *Harsh Truths From OPM Hack: More Monitoring is Coming*. *US News & World Report*. Retrieved 23 October 2015, from http://www.usnews.com/news/articles/2015/07/23/harsh-truths-from-opm-hack-more-monitoring-is-coming