Capstone Research Proposal

Mentor: Diane Murphy, PhD

Topic Description

In June 2015 the Office of Personnel Management (OPM) announced that there had been a security breach affecting 4.2 million federal employees. 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.” 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.

Officials have stated that these attacks were traced back to the Chinese government although the white house has declined to comment. The Chinese government has been behind multiple hacks in the recent years in an attempt to increase their intelligence collection. This breach has allowed them to gather personal information which can be used to target U.S. operatives in other countries as well as targeting specific individuals who could sell secrets to other nations. U.S. officials have said that foreign spy services can use information acquired in this breach to isolate U.S. intelligence operatives which are under diplomatic cover. OPM Director Katherine Archuleta has stated that they have not found any evidence that this security breach has been exploited for criminal purposes.

The security breach was discovered in April when a new cyber tool was installed on the OPM network. Officials stated that when the breach was discovered they had a hard time trying to estimate the amount of data stolen since it was over such a long period of time. Officials believe that this security breach was executed using stolen contractor login credentials.

This breach is important because this has been an ongoing issue in the recent years. The U.S. government has slowly been implementing new technology to allow agencies to conduct business in cyberspace. This has brought a new wave of issues and concern to the general public regarding how these systems will be regulated to prevent breaches from occurring. Many have blamed the implementation of internet capabilities to systems that were not designed to operate online. Another issue is how to regulate these breaches and the type of information that can be accessed online. Countries such as China, Russia, and Iran are spending millions on contracting hackers to infiltrate different agencies in the United States. Officials have proposed sanctions against Chinese hackers due to the amount of intellectual property that has been stolen in recent years. They have stated that the theft of 22 million security files cannot go unpunished. President Obama spoke to troops at Fort Mead where he explained that although tracking breaches have improved, “we can’t necessarily trace it directly to the state,” making it hard for the United States to enforce sanctions. He then issued this warning: “There comes a point at which we consider this a core national security threat. If China and other nations cannot figure out the boundaries of what is acceptable, we can choose to make this an area of competition, which I guarantee you we’ll win if we have to.”

Testable Hypothesis

Upon doing some research on the breach I found that this breach was hard to measure because there were multiple servers that were outdated and had no forms of security. Apart from this there is no regulation over the information stored on these servers. You could make the assumption that most government agencies are using similar techniques to secure their information. If OPM was hacked then agencies which handle less sensitive information can surely be hacked as well since those security protocols would be less. My position on this breach is:

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

Ways of regulating this would be creating a regulation board which is in charge of creating policies and regulations that must be implemented into every agency. Apart from creating policies they will also be in charge of monitoring and auditing agencies to ensure that these policies are being upheld. These agencies should also report to cyber firms which will monitor activity in order to understand the type of attacks. Learning more about what types of attacks are being executed in a specific agency will give a better understanding of the type of information is being targeted.

I believe part of the problem is that new technology is being applied to old systems that were not designed to operate online. Necessary steps should be taken to update the technology in which information is stored in order to use relevant tools to stop attacks. In the OPM hack officials stated that multiple computers were running outdated and unsupported operating systems. This is an invitation to hackers who have knowledge of the operating systems being used since they can exploit vulnerabilities to gain access.

In order to prove my hypothesis I will try to find as much information as I can in order to back up my thesis. I will try to find information on how the breach occurred as well as why it went undetected for such a long period of time. I think that part of the problem is that the government is such a large organization and it will take time to update every agency in order to minimize the risk of future attacks. I believe that in order to do that they will have to successfully restructure security systems.

Faculty Mentor

I have asked Dr. Murphy to be my mentor for this project. I have heard from many students that she is very knowledgeable in the field and could provide a professional insight on the issue. Apart from this I have been in her class and she provides good comments and positive feedback that will help me when writing the final paper. I spoke with Dr. Murphy about this last week and she agreed to be my mentor. She also thought this would be a good research paper since there is a lot of information regarding this breach.

Project Timeline

Since I am writing a research paper I think this project is reasonable and can be completed within a semester. In order to make sure that I am not rushing at the end to complete this project I will stick to the due dates of the assignments in this class. Apart from this I will also dedicate a few hours of research every week in order to have sufficient information to support my thesis. I will keep a detailed list of all my references so it will be easy to reference information when I start writing my paper. I will have to work on this project draft and add to it weekly so it will be completed by the due date next month. By spending time each week looking for information and adding to my draft I think I will be able to complete this project by the end of the semester.

TASK	DUE DATE	COMPLETED?
Topic Submission	9/18/2015	Y
Find 3 references	9/26/2015	
Find 3 references	10/03/2015	
Find 4 references	10/10/2015	
Write 3 pages	10/10/2015	
Write 2 pages	10/17/2015	
Complete 8 pages by	10/21/2015	
Review rough draft with peer edits	11/07/2015	
Write Sources page	11/11/2015	
Meet with Dr. Murphy and review draft	11/20/2015	
Start Presentation Slides	11/22/2015	
Revised Final Draft	11/25/2015	
Turn in Final Report	12/04/2015	
Complete Presentation Slides	12/05/2015	
Project Presentations	12/7/2015-12/11/2015	