Chapter 5 Case Project

**OVERVIEW**

Security breaches are a major concern in today’s information technology world. Network administrators and security specialists work to keep company and client’s information from falling into the hands of an unsecure source. However, sometimes, potential threats and weakness in security systems are found and privacy can be violated. This paper will discuss three entities who suffered a breach within the last year.

**DISCUSSION**

In early February of 2016, the US Department of Justice was the victim of an information security attack. The hacker claimed to have downloaded hundreds of gigabytes of data from a DOJ computer, giving him access to the personal information of over 20,000 FBI employees as well as 9,000 Department of Homeland Security employees which he planned to leak to the public. It was reported that the initial breach came from a compromised email account of a DOJ employee. From there, he was able to call the department and pose as a “new employee” who didn’t understand how to get past the portal. He was then able to access a virtual machine, logging in with the already acquired email information, and gained full access to the computer. This not only shows phishing at work but incorporates the human element of negligence.

Seagate Technology actually had warning about a phishing scam but succumbed to a security breach anyway. About a week before the March 1, 2016 attack, Seagate employees received word from KrebsOnSecurity about an email phishing scam that was directed at finance and HR personnel pretending to be from Seagate’s CEO requesting employee’s W-2 forms. Although the company offered it’s affected employees a two-year paid membership to a credit monitoring software, the damage of having personal information stolen that could be used for tax refund fraud could not be fixed.

Yet another sufferer was Verizon Enterprise in a security breach that affected more than a million of its customers. The hackers were able to collect basic contact information on about 1.5 million clients and the data was found for sale on an underground cyberforum. The cause of the breach was not confirmed but this was a huge wake up call to Verizon. The company was able to find and fix a vulnerable spot in its client portal that the hacker used to get in.

**SUMMARY**

Breaches can cause catastrophic damage for a company but it can also be an eye opener to just how important security is to information. Giving your employees the awareness to look for suspicious activity and implementing higher security measures can help prevent and deter future hacks.

**SOURCES**

<http://www.crn.com/slide-shows/security/300081491/the-10-biggest-data-breaches-of-2016-so-far.htm>

<https://motherboard.vice.com/en_us/article/9a3y4e/hacker-plans-to-dump-alleged-details-of-20000-fbi-9000-dhs-employees>

<http://krebsonsecurity.com/2016/03/seagate-phish-exposes-all-employee-w-2s/>

<http://www.crn.com/news/security/300080151/telecom-partners-say-cloud-security-is-top-of-mind-in-wake-of-verizon-breach.htm>