Cyber Security
Nambo Francis
University of Maryland University College Asia
April 19, 2017

Thesis Statement

Although computers have become part of organizations' greatest asset, cyber-attacks have threatened the daily operations of organizations through malicious attacks. The risk posed by these attacks has resulted in data breaches in financial institutions. Organizations have invested heavily in cyber security.

Definition of Terms

DDoS - Denial of Service
DBIR – Verizon Data Breach Investigation Report
HSBC- HongKong and Shanghai Banking Corporations

Introduction

Cyber security is that state of being protected against unauthorized or criminal use of electronic data. Most of computer specialist refers to cyber security as the body of processes, practices and technologies that is designed to protect programs, data, networks and computer from unauthorized access, attack or damage. Companies, governments and non-government organizations have invested heavily on cyber-security. For example, in 2010, the US government allocated 13 billion US dollars on cyber-security for a span of five years. This is because cyber-threats are advancing as technology grows. Vincent Adams, a CTO-public sector at Layer 7 has described cyber- attack as a threat which is escalating at high rate more than how we are keeping up with it (Fischer, 2012).

Effects of Data Breaches on Insurance Costs or Sales

From 2014, about 500 companies have experienced major data breaches example is Sony Company. This has made executives lose their job. Millions of consumers have had their personal data and credit card data comprised. In this part I will discuss how companies are losing due to data breaches.

Brian East 4/25/2017 9:41 PM
Deleted: has

Brian East 4/25/2017 9:42 PM
Comment [1]: Make sure you add that you reached these conclusions through analysis of literature on the topic.

Brian East 4/25/2017 9:42 PM
Comment [2]: You would still need to define what this means.

Brian East 4/25/2017 9:42 PM
Deleted: E

Sony Company in November 2014, hacking in its database led to the disclosure of unreleased movies, personal data that included social security numbers of about 47, 000 employees and celebrities and embarrassing internal emails. The data breach by hackers was very disruptive and traumatic to the Sony Company such that it delayed its 10-K filing. In addition the Company estimated a loss of about 15 million dollars. Dean in his blog gave some scale to the losses, which represented 0.9% to 2% of the projected sales by the Company. Also the company spent about 35 million in restoring IT and financial systems. Home Depot hacking in 2015 led to the hackers getting credit card numbers of their credit numbers of about 50 million customers and their email addresses although the security data breach had less impact it reveled personal identity of Home Depot's customers. In addition the Company received about 43 million pretax expenses that was data breach related. The company executives estimated this to about 0.01 percent of the Company's sales (Giacomello, 2015).

Brian East 4/25/2017 9:43 PM
Deleted: Company

Brian East 4/25/2017 9:44 PM
Comment [3]: Make sure to introduce sources by mentioning who write them and how they agree/disagree with the sources you mention either before or after them.

In late 2013 Target Company resulted in the theft of about 40 million payment cards and the loss of about 70 million records that included email addresses and phone numbers of customers. The breach was considered to very severe such that the CEO at that time was compelled to resign. It is estimated that the Company incurred the security breach expenses of about 4 million US dollars in the 4th quarter of 2014. The whole year it is estimated that the company incurred about 145 million US dollars. According the company's directors to total expenses was about 252 million US dollars. In addition in Target Company resulted to about 0.1% of Target's sales (In Lehto, 2015).

The Causes of Cyber-Attacks on Financial Institutions

Financial institutions are becoming the highly targeted institutions. Some of the emerging channels like online banking and mobile have opened doors for cyber criminals. Hackers are also using email phishing to banks customers. A report by DBIR breach shows that the common origin of cyber-attack in financial institutions is DDoS. According to the report about 32% of banking attacks were caused by DDoS. This was especially found at end month when payments are made. Online banking is usually flooded by DDoS in order to take the services offline. HSBC has experienced this as it has indicated in their blog that they have tried to fight DDoS but still the services are unavailable on every end month from around 29th to 4th the next month. The DBIR report has also noted that DDoS attacks are being employed by most of the cyber criminals to demonstrate their attack capabilities. Some of the cyber criminals are using DDoS services aimed at enabling financial institutions disrupt their online activities for their competitors (Santanam, 2011).

Bot attacks are also increasing from 2015. According to ThreatMetrix analyst, this scenario has paralyzed the daily activities for the financial institutions there by leading to loss of millions. Bots and other attacks like malware have bypassed traditional security breaches y mimicking as authentic customers (In Felici, 2015).

Historical Background

In the current world, it demands a degree of connectivity between financial institutions, businesses and governments. Digital technology has provided this opportunity to businesses and organizations have harvested lots of valuable benefits. However the modern world of connectivity has provided an environment of rich connectivity that has ranged from vandalism of computer assets to theft of critical information from organizations computers. The first method of cyber-attack was back from in 1960s which was hacking. In 1970s the hacking became evident as most of the hackers concentrated in phone systems. In the early 2000 hackers

employed malware and bot attacks to businesses and financial institutions. The current most common used type of attack being used by hackers is DDoS (Probst, 2010).

Conclusion

Organizations have invested heavily in cyber security to avoid after attack consequences. From my discussion it is evident that organizations a losing a lot due to cyber-attacks. The major cause of attack in financial institutions is the DDoS. The major effect of cyber-attack is financial loss. From the case studies Sony, Home Depot and Target companies has lost millions of dollars due to cyber.

References

Fischer, R., Halibozek, E., & Walters, D. (2012). *Introduction to Security*. Burlington: Elsevier Science.

Giacomello, G. (2015). *Security in cyberspace: Targeting nations, infrastructures, individuals*. In Felici, M. (2015). *Cyber security and privacy: 4th Cyber Security and Privacy Innovation Forum, CSP Innovation Forum 2015, Brussels, Belgium April 28-29, 2015, revised selected papers*.

In Lehto, M., & In Neittaanmäki, P. (2015). *Cyber security: Analytics, technology and automation*.

Probst, C. W. (2010). *Insider threats in cyber security*. New York: Springer

Santanam, R., Sethumadhavan, M., & Virendra, M. (2011). *Cyber security, cyber crime and cyber forensics: Applications and perspectives*. Hershey, PA: Information Science Reference.

Brian East 4/25/2017 9:45 PM

Comment [4]: Make sure to revise this list to reflect APA style for a References list.