Psychological aspects of cybersecurity

Human Factors, Threats, Culture and Liability: Psychological Aspects of Cybersecurity

Introduction

In today's society, cyber intrusion and attacks is becoming more prevalent. No one really knows the motivation behind such attacks. In some cases, it may be psychological and in others it could be a way to attain an adrenaline rush by invading a high-level security system. While cyber attacks has increased, our nation is putting execution actions in place to safeguard our critical infrastructure.

With all of that being said, Congress has a responsibility to the people/nation to protect and secure their freedom. Cyber attacks are malicious acts that target information systems, infrastructures, and computer networks. Normally, the sources of the attack are unknown and the reasons of the attack are unclear. In many cases, the attacks are labeled as cyber warfare or cyber terrorism. In the same fashion, the people who commit these crimes are described as communist, cyber terrorist, and black hat etc. However, when Congress is the focus of the attack normally the target of attack is our infrastructure.

Descriptive Labels Applied to Cybercrime

The descriptive label that would be applied to cybercrime is data security breach or cyber terrorism. Further explanation of " Data Security & Breach Notification Act 2012, mandates that companies have reasonable security measures to protect personal information and establish a uniform breach notification law (S. 3333 (112th): Data Security and Breach Notification Act

of 2012, 2012).” Cyber terrorism is when a computer is used as the weapon for attack. In some cases you will find that cyber terrorism is the way to seek revenge or used as a method to intimidate or coerce one. An example of a cyber-terrorism perhaps could be hacking into aircrafts system and changing the coordinates of the flight.

In 1996, President Bill Clinton created a Commission of Critical Infrastructure Protection. Congress new that the nation was at risk of cyber attacks. Therefore, to heighten awareness and maintain economic stability the board felt it was necessary to protect critical infrastructure. This was a mixture of electricity, computer networks, communication etc.; because all of these elements were vulnerable of cyber-warfare. With this in mind, the government was also thinking of protecting the public and private industries from such attacks. They were completely oblivious of the dangers how much or daily lives rely on computers. Notwithstanding the dangers and vulnerabilities they subjects themselves to when using the computer. Another issue is finding out who are the perpetrators and how the attack were initiated. The board felt it would be most helpful if they adequately protected critical system from intrusion. That meant ensuring the proper firewalls were enabled and the system was being monitored (http://csciwww. etsu. edu/gotterbarn/stdntppr/).

Threat Factors

In reality, if the United States Infrastructure comes under attack the enemy could cripple our defenses depending on how sophisticated the attacker is. The possible intent behind attacking our infrastructure, would be to target our water supply, transportation, telecommunication, energy, and last but

not least finance. Our way of living depends on critical infrastructure; if we were to lose these vital roles we would be vulnerable to the enemy. These operations are important and we have become dependent on these networks. The lost of electricity, telecommunications, transportation, energy, and water would render us helpless. Such an attack would disrupt our day-to-day life and cause mass panic and fear. Therefore, in order to prevent such an act from occurring, Congress has created a new executive branch to merge 22 government agencies that were already in existence. The goal was to secure the nation and preserve freedom. In addition, have the ability to fence off attacks and be prepared for unexpected disasters. To accomplish this task, the Department of Homeland Security had to unify the department in order to strengthen the components. Policy tells us that through partnership with other departments and operators of critical infrastructure would improve cyber security sharing information, which is ideal for the nation.

Water Supply

Attacking the water supply would be the most critical attack on the infrastructure. The water supply is controlled by computer systems, which is why it poses the most security risk. If the enemy was able to bypass the security features, they could release large amounts of water in any particular area. Destruction of large dams could unleash large amounts of water resulting in catastrophic flooding, loss of life and damage to property.

Another vulnerability would be the sewer system. The sewage system protects public health and the environment; while providing a series of

treatment that clean the water supply. Raw sewage has harmful bacteria and viruses that could be life threatening to human or animas if exposed to it.

“ Bioterrorism or chemical attacks could deliver widespread contamination with small amounts of microbiological agents or toxic chemicals could endanger public health (Terrorism and Security Issues Facing the Water Infrastructure Sector, 2006).” (http://fpc. state. gov/documents/organization/68790. pdf).”

Energy

The second most important infrastructure that could be attacked is energy. Energy is described in two separate classifications one being electricity and the other being natural gas. Electricity is used in everywhere i. e. houses, cities and regions. It is needed for day-to-day living such usage of machines and life saving mechanisms. For example, cyber terrorist has the ability to gain access to daily power report data. The report shows the flow of electricity in different regions.

As a result, a cyber terrorist would have the ability to know what the busiest sections of the grid were. It is important to realize with this information they could shut down the power gird at the busiest time of the day and cause hysteria, backflow, and confusion. Without power the United States, defenses are down. “ There have been incidents or credible intelligence to indicate that a potentially well organized, disruptive cyber attack is imminent against the electrical utility industry in general or BPA specifically, or Terrorist activity, either physical or cyber, has been perpetrated against civilian or

government sites within the boundaries of the United States... (Threat Conditions, n. d.).” http://info. bpa. gov/Emergency/ThreatConditions. aspx

Not only is electricity important to infrastructure but natural gas is too. Cyber terrorist can halt the use or redirect gas flows. Keeping the energy a float is important for maintaining the safety and economic success in the United States. The White House Initiative has an Executive order, which is led by the Department of Energy and the Department of Homeland Security. Their job is to ensure electric companies and grid operators have working knowledge of cyber security potentials and prioritize their actions and investments to improve cyber security. In addition their “ industry stakeholders in the energy sector, are also contributing to the development of the Cyber security Framework, which was announced as part of Executive Order 13636 on “ Improving Critical Infrastructure Cybersecurity. (http://energy. gov/articles/energy-department-announces-new-investments-over-30-million-better-protect-nation-s).”

Transportation

A disturbance in the transportation system would cause a chain of economic disruption. By interfering with transportation it hinder citizens and would progressively degrade the economy over time span. It would impede on scheduling as well as accessibility. In like manner, these methods would have a negative impact on cargo being transported from place to place. Moreover, cyber terrorist can target railroad operations by taking controls of the switches, additional they could take over flight software to divert aircraft. “ Sapphire” or “ Slammer” worm spread quickly through the Internet

attacking millions of computers and overwhelming them with data due to a flaw in a Microsoft program. (CONSUMER PRIVACY DEVELOPMENTS, n. d.).”

Transportation is important to critical infrastructure. In order to maintain a since of balance, proactive measures must be in place to strengthen and secure critical infrastructure. It is important to have the necessary assets including but not limited to networks and public confidence. Needless to say, the infrastructure must be secure in order to withstand and promptly recoup from an attack.

Finance

Telecommunication

Company Liabilities

Reducing vulnerabilities through effective internal cybersecurity policy controls

Conclusion

The threat of cyber crime has risen in the United States. Congress is having more debates on the nations ‘ s cyber security, terrorism, and breaches within our national systems. It was said by the “******* that we were in trouble because cyber attacks have resulted in the greatest transfer of wealth in history. (*****).” Although, Legislation have been proposed to govern the laws the bills have not been enacted. This is mainly due to the fact; the government and private industries have issues with the federal data security bills. Currently, the United States has a cyber security Executive Order in place.

The purpose for this order, is to protect their United States from cyber contusion and the attacks against the nations critical infrastructure. A threat to the infrastructure is major to national security. Our nation relies on the infrastructure to keep the mainframe secure and efficient against intrusion. As stated earlier, cyber attacks are becoming more vigilant therefore, the government had to make changes to the executive branch. In 2002, a new executive department was put into place called the Homeland Security Act. Homeland Security Act 2002, was created to " prevent terrorist attacks within the United States; reduce the vulnerability of the United States to terrorism; and minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States. (*Homeland Security Act of 2002)* "

References

Anonymous. (2011). *Data breach and electronic crime: the Sony's case* . Retrieved from gcsec. org: http://www. gcsec. org/blog/data-breach-and-electronic-crime-sonys-case

Anonymous. (2013). *Managing CyberSecurity Risk* . Retrieved from Protiviti: http://www. protiviti. com/en-US/Documents/Newsletters/Board-Perspectives/Board-Perspectives-Risk-Oversight-Issue44-Managing-Cybersecurity-Risk-Protiviti. pdf

Anonymous. (n. d). *About Sony Electronics – Life at Sony* . Retrieved fromhttp://discover. store. sony. com/: http://discover. store. sony. com/sonyjobs/pages/about/life. html

Anonymous. (n. d). *Corporate Mission* . Retrieved from neimanmarcus: http://www. neimanmarcuscareers. com/story/mission. shtml

Anonymous. (n. d). *Mission & Values* . Retrieved from About Target: https://corporate. target. com/about/mission-values

Anonymous. (n. d). *Throught the Years* . Retrieved from Target. com : https://corporate. target. com/about/history

Aspan, M. (2011). *Citi says 360, 000 accounts hacked in May cyber attack* . Retrieved November 23, 2011, fromhttp://www. reuters. com/article/2011/06/16/us-citigroup-hacking-idUSTRE75F17620110616

Bavisi, S. (2009). Penetration Testing. In Vacca, J. R. (Ed.), Computer and information security handbook. Boston, MA: Morgan Kaufmann Publishers.

Bodhani, A. (2013). Bad…In a Good Way. *Engineering & Technology* , 7(12), p64-68.

Campbell, Q., Kennedy, D. M. (2009). The psychology of computer criminals. In Bosworth, et al., (Eds.), Computer security handbook. New York, NY: John Wiley & Sons.

Chen, C.; Shaw, R.; Yang, S. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. Information Technology, Learning & Performance Journal, 24(1), p1-14.

Chen, T.; Walsh, P. (2009). Guarding Against Network Intrusions. In Vacca, J. R. (Ed.), Computer and information security handbook. Boston, MA: Morgan Kaufmann Publishers.

DATALOSSdb Open Security Foundation (2014). *Data Loss Statistics* . Retrieved fromhttp://datalossdb. org/statistics

Dittrich, D., Himma, K. E. (2006). Hackers, crackers and computer criminals. In H. Bidgoli (Ed.), Handbook of information security (Vol 2). New York, NY: John Wiley & Sons.

Elgin, B., Lawrence, D., & Riley , M. (2014, February 21). *Neiman Marcus Hackers Set Off 60, 000 Alerts While Bagging Credit Card Data* . Retrieved from businessweek. com: http://www. businessweek. com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data

Ethical Issues. (2013). Retrieved fromhttp://cps182cyber-crime. wordpress. com/ethical-issues/

Finklea, K. M., Theohary, C. A. (2012). Cyber-crime: Conceptual issues for congress and U. S. law enforcement. *Journal of Current Issues in Crime, Law and Law Enforcement.* 5 (1/2), 1-27. Retrieved fromhttp://web. a. ebscohost. com. ezproxy. umuc. edu/ehost/detail? vid= 3&sid= 79df209d-d6a2-4fd7-9761-f40b899a23e1%40sessionmgr4002&hid= 4209&bdata= JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#db= i3h&AN= 88850916

Frizell, S. (2014, January 29). *Holder: Feds Investigating Target Breach* . Retrieved from Time. com: http://business. time. com/2014/01/29/feds-investigation-target-security/

Germano, S. (2013, December 27). *Target's Data-Breach Timeline* . Retrieved from Wall Street Journal: http://blogs. wsj. com/corporate-intelligence/2013/12/27/targets-data-breach-timeline/

Goldman, G. (2011). Mass e-mail breach: Just how bad is it? Retrieved November 23, 2011, fromhttp://money. cnn. com/2011/04/06/technology/epsilon_breach/index. htm

Harris, E. A., Perlroth, N., & Popper, N. (2014, January 23). *Neiman Marcus Data Breach Worse Than First Said* . Retrieved from New YOrk Times: http://www. nytimes. com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards. html

Hassan, A. B., Lass, F. D., Makinde, J. (2012). Cyber-crime in Nigeria: Causes, effects and the way out. *ARPN Journal of Science and Technology* . 2(7), 626-631. Retrieved fromhttp://www. ejournalofscience. org/archive/vol2no7/vol2no7_11. pdf

Heavey, S., & Finkle, J. (2014, March 13). *Target says it declined to act on early alert of cyber breach* . Retrieved from Reuters. Com: http://www. reuters. com/article/2014/03/13/us-target-breach-idUSBREA2C14F20140313

ITU. (2012). Understanding cyber-crime: Phenomena, challenges and legal response. Retrieved fromwww. itu. int/ITU-D/…/cybersecurity/…/Cyber-crime%20legislation%20EV6. pdf

Kaiser, D. (2007). Insurance options vary as much as cyber attacks. *Business Insurance* , *41* (21), 24.

Katz, K. (2014, February 21). *Security info* . Retrieved fromwww. neimanmarcus. com: http://www. neimanmarcus. com/NM/Security-Info/cat49570732/c. cat? icid= topPromo_hmpg_ticker_SecurityInfo_0114

Krebs, B. (2014, 02 14). *Target Hackers Broke in Via HVAC Company* . Retrieved from krebsonsecurity. com: http://krebsonsecurity. com/2014/02/target-hackers-broke-in-via-hvac-company/

Lewis, J. (2013). Raising the Bar for Cybersecurity. *Center for Strategic & International Studies* . Retrieved fromhttp://csis. org/files/publication/130212_Lewis_RaisingBarCybersecurity. pdf

Mansoor, B. (2009). Intranet Security. In Vacca, J. R. (Ed.), Computer and information security handbook. Boston, MA: Morgan Kaufmann Publishers.

McAfee (2014). McAfee Labs Threats Report: Fourth Quarter 2013. McAfee Labs. Retrieved fromhttp://www. mcafee. com/us/resources/reports/rp-quarterly-threat-q4-2013. pdf

Metz, C. (2005). identity theft is out of control. (cover story). *PC Magazine* , *24* (14), 87

Sales, N. (2013). REGULATING CYBER-SECURITY. *Northwestern University Law Review* , *107* (4), 1503-1568.

Shackleford, D. (2013). New Pathways to Network Security . *Information* Security, 15(6), p10-15.

Sherr, I., & Wingfield, N. (2012, May 7). *Play by Play: Sony's Struggles on Breach* . Retrieved from Wall Street Journal : http://online. wsj. com/news/articles/SB10001424052748704810504576307322759299038

Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *International Journal of Cyber Criminology.* 5(1), 736-749. Retrieved fromhttp://www. cyber-crimejournal. com/warner2011ijcc. pdf

Waugh, D. (2001). Computer crime and ethics. Retrieved fromhttp://homepage. ntlworld. com/woofy/ethics/ethics. pdf

Williams, M. (2011, May 01). *PlayStation Network Hack Timeline* . Retrieved from pcworld. com: http://www. pcworld. com/article/226802/playstation_network_hack_timeline. html

Wolf, J., & Maclean, W. (2011). IMF cyber attack aimed to steal insider information: Expert. Retrieved November 23, 2011, fromhttp://www. reuters. com/article/2011/06/12/us-imf-cyberattack-idUSTRE75A20720110612

Youderian, A. (2013, August 08). *LulzSec Hacker Gets Year in Prison for Sony Attack* . Retrieved from courthousenews. com: http://www. courthousenews. com/2013/08/08/60130. htm