2014

Common Motivations and Personality Types of Cyber Terrorists

Amanda Floyd
Virginia Commonwealth University

Common Motivations and Personality Types of Cyber Terrorists

Amanda Floyd, *Virginia Commonwealth University*

Introduction

According to the Federal Bureau of Investigations, "The CSIS has defined it (cyber terror) as the use of computer network tools to shutdown critical national infrastructures or to coerce or intimidate a government or civilian population" (Tafoya, 2011). Cyber terrorism is on the rise and costs the government and large corporations millions and millions of dollars in both manpower and technology. Figure 1 illustrates just how much money is lost due to security breaches. The United States has seen both their military programs be hacked along with the most trusted systems of our defense contractors. The risk of another large scale cyber-attack is imminent and there's only a question of when, where and how much sensitive information will be compromised.

The ways of carrying out these terrorist attacks are just as diverse as the reasoning behind carrying them out. Who are these people behind this new age form of terrorism and what are their motivations for causing such technological destruction? This research will delve further into this question by exploring the personality types of known hackers and virus writers. Are their certain characteristics that are commonly displayed by these criminals? Is there a criminal profile that can be looked at in seeking out these criminals for prosecution? It is essential for our nation's economy and security that the United States' government keeps ahead of these criminals and their ever-evolving tactics. It is also increasingly more and more important to learn about these cyber terrorists and to learn from our past security breaches.

Overview

- A Norton Study in 2011 calculated the cost of Global cybercrime at $114 billion annually.
- In 2013, federal agents notified more than 3,000 U.S. companies that their systems had been hacked. The estimated costs to U.S companies and consumers is up to $100 billion annually.
- In 2012, more than $1 billion in venture financing poured into security start-ups. More than double the amount in 2010.
- According to the Defense News' website, in 2012 the Pentagon reported getting over 10 million cyber attacks a day.
- More than 2/3 of the cases against the theft of intellectual property are against China and Russia.

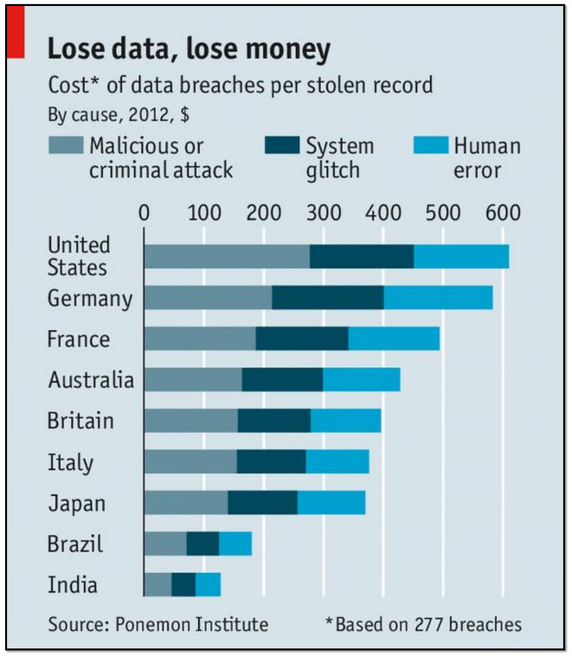

Figure 1. How much data breaches cost

The Who? And Why?

There are many different types and names given to hackers. However, they all fall under the same definition as someone who seeks to exploit weaknesses in a computer system or network regardless of their motivations, whether it be profit, protest or simply for challenge. Some computer hackers are members of an organized crime gang and carry out criminal activities for profit. Others are affiliated with nation states, and work with intelligence agencies as cyber warfare operatives. Others can be labeled as taunters, who get a thrill out of breaking into security systems just to show it can be done. There are also anarchist who work to dismantle and disrupt governments, most commonly affiliated with nation-states. Another extremely common type are "hacktivists" who exploit technology to make a public ideological, religious or political stance. The group Anonymous is considered to be a hacktivist organization. Below, Figure 2 illustrates a security breach.

Figure 2. Illustration of a hacking

Results

The research suggests that even though there are varying motives behind why cyber criminals attack they do share certain commonalities. Many hackers are highly intelligent and have a strong knowledge of and interest in computer software. Hacking can be seen as appealing to young students "who are going through developmental periods in which they are defining themselves, as well as challenging authority and rules" (Stone, 1999). They usually share a Robin Hood mentality and the anonymity that is offered through cyber space helps to usher in young adults who normally would not consider stealing or damaging someone else's property. These individuals are overwhelmingly male as there are few known females who engage in cyber terrorism. Hackers who use their talents for criminal activity come from all over the world and are connected to one another through a virtual reality. However, they can also physically connect through hacking conventions all over the world.

Conclusion

Although there are characteristics that these individuals share, there is no way to pinpoint a particular criminal profile for the prevention of future hackings. It would be a starting point to begin to educate tech savvy college students on the harmful effects of cyber terrorism and to show them how to divert their superior computer software knowledge to helping prevent future attacks.

Acknowledgments

I would like to thank my professor Dr. Jason Levy for being a great mentor and always expecting and encouraging his students to think outside of the box.

References

Fryer-Biggs, Z. (2012, March 24). *U.S. Military Goes on Cyber Offensive*. Retrieved April 6, 2014, from http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive

Nigam, H. (2011, July 19). *Mobsters, Taunters and More: The Four Kinds of Hackers*. Retrieved April 6, 2014, from http://abcnews.go.com/Technology/We_Find_Them/kinds-hackers-mobsters-taunters/story?id=13979327

Stone, D. M. (1999, March 7). *Computer Hacking*. Retrieved April 6, 2014, from http://education.illinois.edu/wp/crime/hacking.htm

Tafoya, W. L. (2011, November). *Cyber Terror*. Retrieved March 13, 2014, from http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror

The Economists. (2014, Febuary 22). *White hats to the rescue*. Retrieved April 6, 2014, from http://www.economist.com/news/business/21596984-law-abiding-hackers-are-helping-businesses-fight-bad-guys-white-hats-rescue

For further information contact
floyda@vcu.edu