CYBERCRIME TRENDS AND IMPACTS: ANALYSIS OF THE CHARGED CYBERCRIME CASES

AZENE ZENEBE, BOWIE STATE UNIVERSITY, USA
(azenebe@bowiestate.edu)
DAVID ANYIWO, BOWIE STATE UNIVERSITY, USA
(danyiwo@bowiestate.edu)

ABSTRACT

Cyber criminals target a variety of interests such as military intelligence, financial data, and intellectual property. These crimes not only affect the confidentiality, integrity, and availability of the data and systems accessed without proper authorization, but also, it impacted the economy of individuals, businesses and government entities in negative ways. Cybercrimes have gained worldwide attention as the number and complexity of crimes increase every year. Cybercrimes not only affect individuals, but they affect corporate-level businesses and government entities. This study presents the results of an exploratory study to determine the extent of cybercrimes, the targets of the crimes, source of the crimes, and types of interest harmed. In particular, the study analyzed the computer and cybercrime cases charged by the Computer Crime and Intellectual Property Section (CCIPS) of the US Department of Justice from July 2011 to June 2014.

Keywords: *Cybercrime, crime targets, interests harmed, charged cases.*

INTRODUCTION

Cybercrime is any crime that involved the use of computing device and the Internet. The computer or computing device may be the agent of the crime, the facilitator of the crime, or the target of the crime. According to the U.S. Department of Justice (DOJ), computer crime is defined as "any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution." Cybercrime includes: crimes in which the computer system (hardware, peripherals, software, etc.) is the target of a crime; and crimes in which computers and related systems are the means or "instrument" by which ordinary crimes are committed.

Cyber attacks target a variety of interests such as military intelligence, financial data, and intellectual property. By doing so they undermine the confidentiality, integrity, and availability of the data and systems causing a disruption in the natural flow of things that may occur. Cybercrimes have gained worldwide attention as the number and complexity of crimes increase every year. Cybercrimes not only affect individuals, but they affect corporate-level businesses, small businesses, as well as government entities.

Cyber criminals have different motives. They see amusement in the possible outcome if successful or have monetary profitability. Compromising a country's defensive systems – as occurred with the STUXNET worm - could be considered an act of war by some governments. It's therefore vital that research is available for the cybersecurity community to help develop both technical and policy-based methods to combat cybercrimes.

This paper presents the results of an exploratory study to determine the extent of cybercrimes, the targets of the crimes, source of the crimes, types of interest harmed, the economic impact, and possible punishments of the perpetrators by analyzing the computer and cybercrime cases charged by the Computer Crime and Intellectual Property Section (CCIPS) of the USA Department of Justice from July 2011 to June 2014. The paper has four sections, including the introduction. Section 2 presents the research methodology, followed by the results and discussion in section 3, and the conclusion in section 4.

RESEARCH METHODOLOGY

This exploratory research attempts to answer the following questions related to:

- Which security goals are breached? To what extent?
- What are the targets?
- Where do the crimes originate from?
- Who are the perpetrators?
- How many individuals where involved in the committing of the crime?

The data used in this study was extracted from cybercrime charged cases by the Computer Crime and Intellectual Property Section (CCIPS) of the United States Department of Justice from 2010 to 2014. CCIPS focus on combating computer and intellectual property crimes worldwide by working with other government agencies, the private sector, academic institutions, and foreign counterparts.

A total of 92 cases (see Table 1) were selected after reviewing each press release and determining if it is a charged cybercrime - computer and intellectual property crime. They are purposive samples, not random. To find additional data about the cases, additional articles from other sources such as *Computer Weekly, CNN*, etc. were used.

Table 1. Distribution of Cybercrime Charged Cases by Year

Year	Frequency	Percent
2010	11	12.0
2011	11	12.0
2012	28	30.4
2013	27	29.3
2014	15	16.3
Total	92	100.0

Some of the variables include type of interest harmed, target type, number of perpetrators charged, geographical origin of the perpetrators, date of breach, specific damages on the victims, and the fallout resulting from the security breach. A few of these variables are defined as below:

a. Type of interest harmed - The variable indicates whether the computer crime targets (1) Confidentiality- A breach of confidentiality occurs when a person knowingly accesses a computer without authorization or exceeding authorized access and views or copies proprietary or private information, such as a credit card number or trade secret; (2) Integrity- A breach of integrity occurs when a system or data has been accidentally or maliciously modified, altered or destroyed without authorization; (3) Availability- A breach of availability occurs when an authorized user is prevented from timely, reliable access to data or a system; and (4) Combination of two or three types of interests.
b. Target type – The variable indicates whether the computer crime targets (1) a private individual; (2) a private corporation; (3) a public governmental agency; and (4) both public and private agencies.
c. Perpetrators charged – The variable indicates whether defendant(s) is/are (1) individuals; (2) a part of an organized group; and (3) a part of state/nation agency/institution.
d. Type of perpetrators charged - The variable indicates whether defendant(s) is/are (1) Insider – an employee including a contractor of the attacked entity; or (2) Outsider – others including ex-employees.
e. Geographical origin of the perpetrators - The variable indicates the origin of the cybercrime or location of the perpetrators during the breach: (1) within the US; or (2) outside of the US.
f. The fallout: Specific Damages on victims by the Perpetrators (brief description)

RESULTS AND DISCUSSION

With respect to the security goals that are breached, the results in Figure 1 indicate that a breach of confidentiality (50%) is the largest type of interest harmed. According to the National Institute of Standards and Technology (NIST) *Special Publication 800-30*, the loss of confidentiality is defined as unauthorized disclosure of confidential information and can range from the jeopardizing of national security to the disclosure of private data. (*Feringa et al., 2002*). This jeopardized the livelihood of victims all over the world due to the impact resulting from identity theft,

and using the information gained as a profitable return. Normally when a breach of confidentiality occurs it is associated with another type of interest that is a part of the CIA triad that's why the combination of two or more interests (37%) is the second highest.

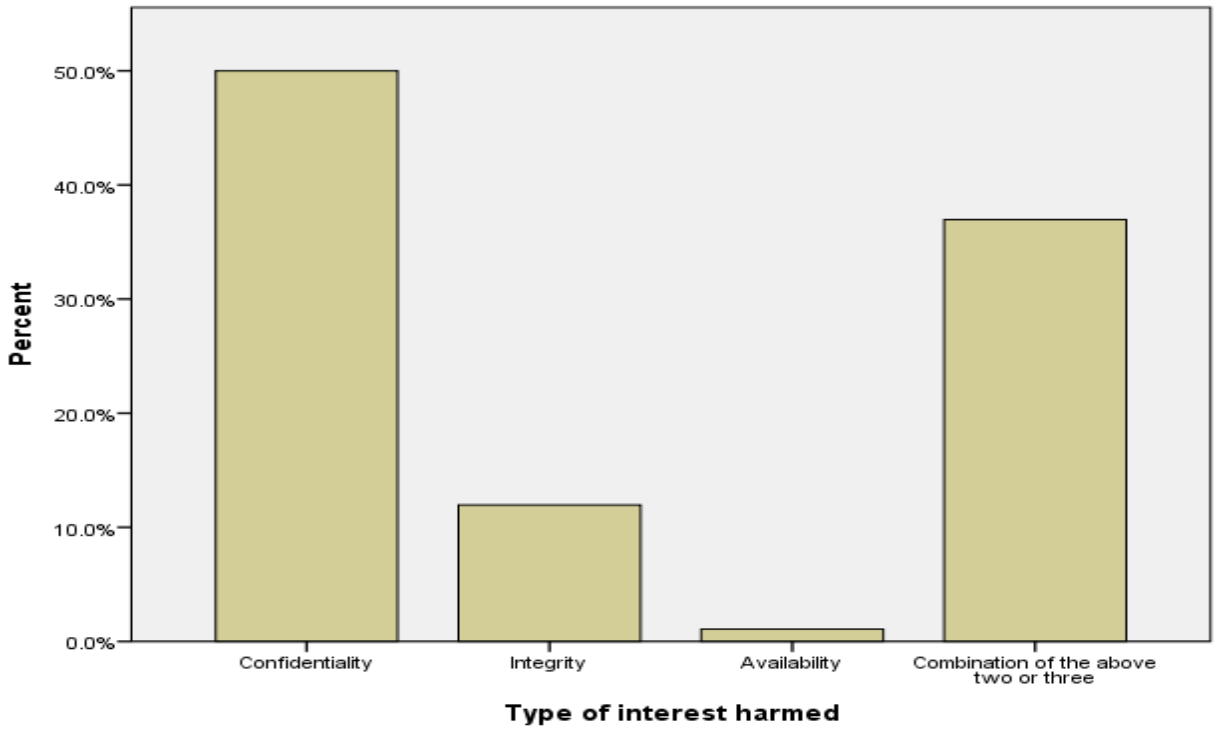

Figure 1: Type of Interest Harmed or Compromised by the Computer Crime

Majority of the targets for computer crimes included private individual (45.6%) through methods of social engineering, extortion, and leading victims to misleading sites that requires them to enter sensitive information in order to move forward. Cybercrimes also affected targets such as private organizations (33.3%), public agencies (4.4%) and both public agencies and organizations (16.7%) by gaining unauthorized access to their systems. Figure 2 presents the results.

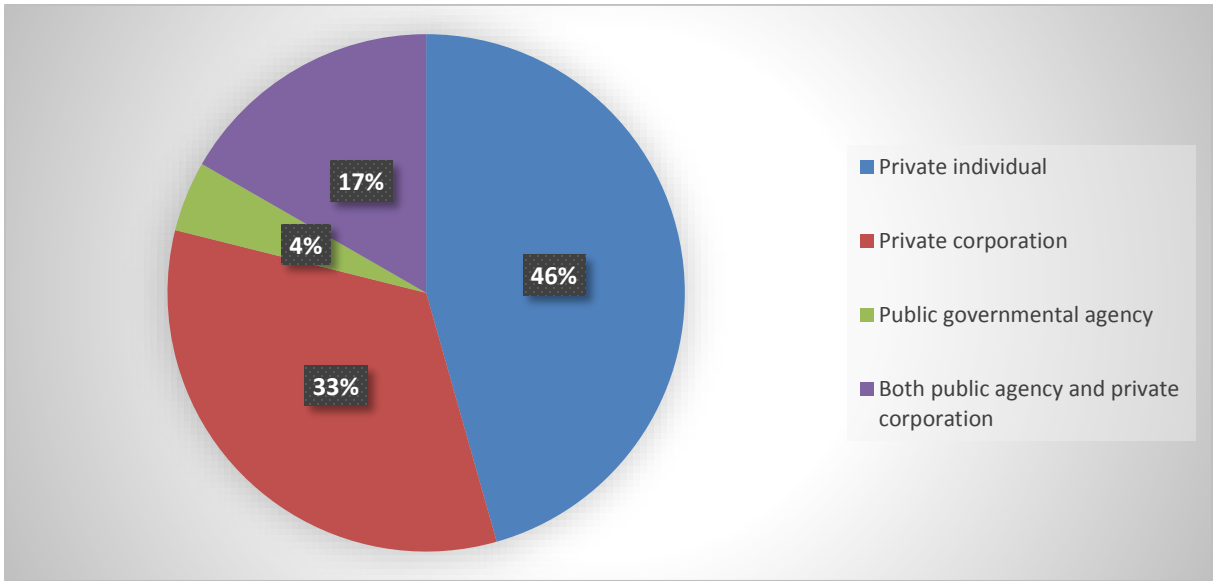

Figure 2: Target Types of Computer Crimes

Figure 3 presents the profile of the perpetrators with respect to whether they acted individually or in group. 65.5% of the charged cybercrimes were carried out by individuals perpetrators, 32.2% were by perpetrators in an organized group, and 2.3% were by perpetrators who were part of a state or nation agency. With abundant of cyber security attacking methods and tools, cyber hackers were acting individually and became successful. For example, a distributed denial of service (DDoS) attack can come from one individual controlling a large amount of machines in order to carry out his/her malicious attack. Attacks that would otherwise take a large amount of perpetrators working in a group are worms, viruses, and Trojans.

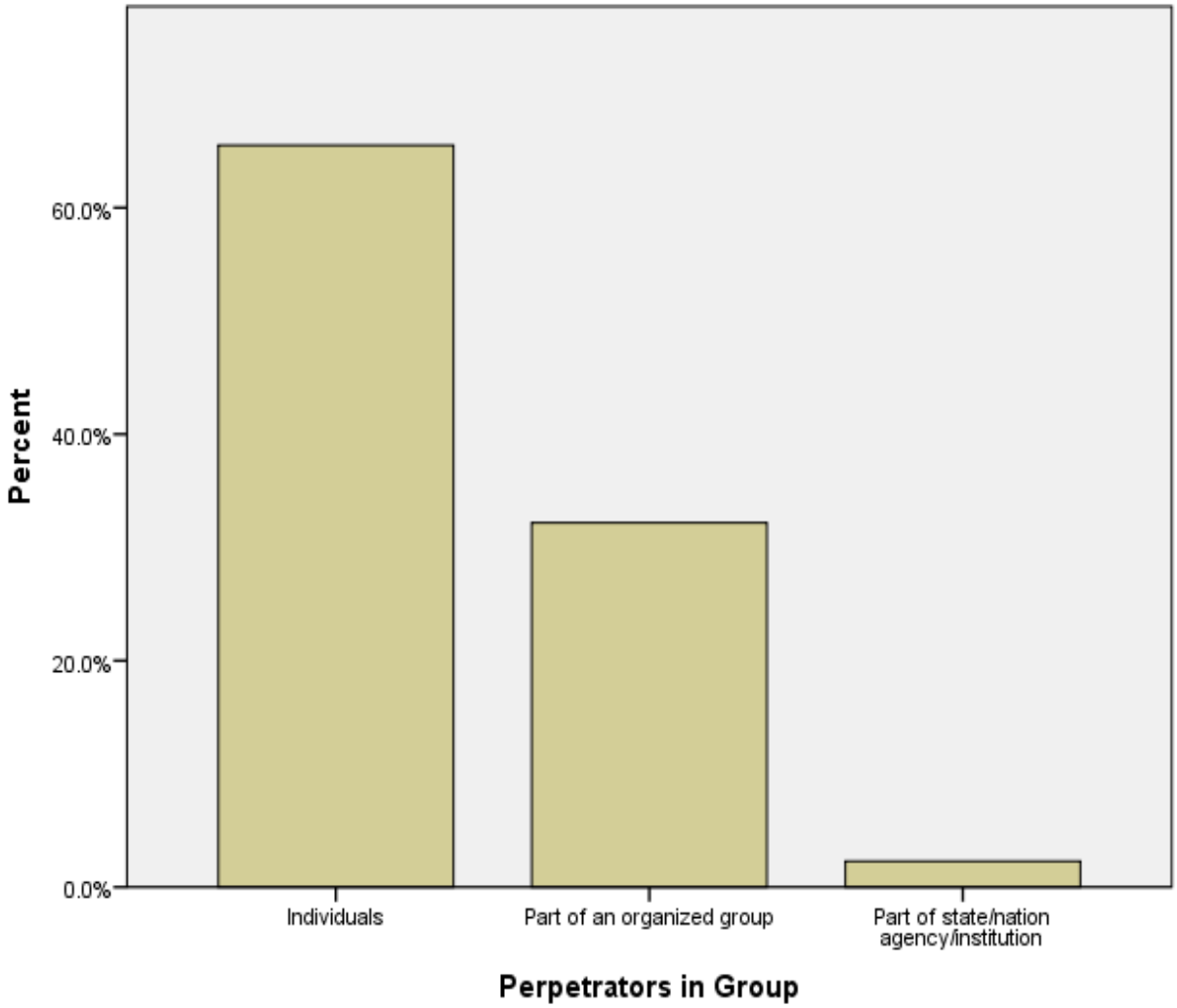

Figure 3. Perpetrators in Group or Not

Figure 4 presents the profile of the perpetrators with respect to whether they were insider or not. 23% of the charged cybercrimes were carried out by insiders including active employees and business associates at the time of the breaches, 77% were by outside perpetrators including ex-employees and ex-associates.

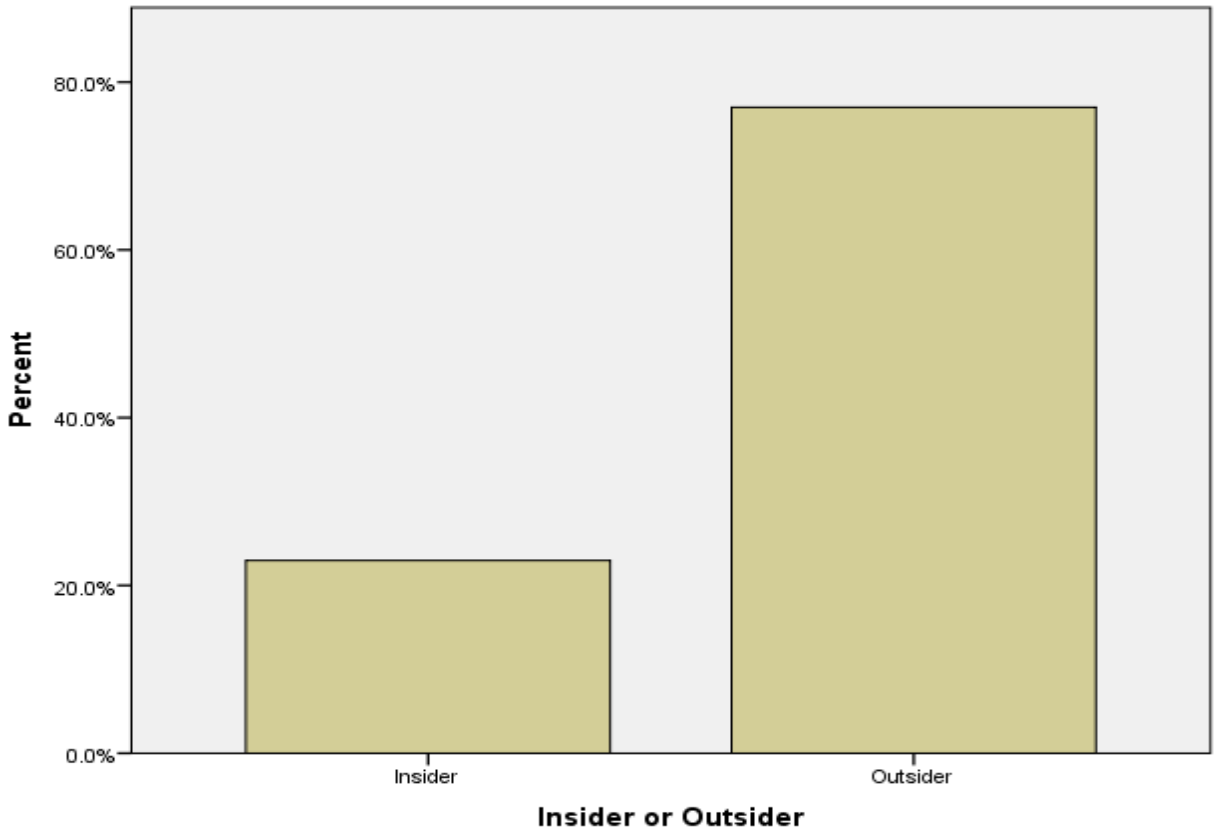

Figure 4. Insider or Outsider

Table 2 presents distibution of the number of perpetrators charged. 65% of the charged cybercrimes were carried out by one perpetrator, 13.3% were by two perpetrators, and 21.7% were by three to ten.

Table 2. Distribution of the Number of Perpetrators Charged

No of Perpetrators		Frequency	Valid Percent
Valid	1	59	65.6
	2	12	13.3
	3	5	5.6
	4	5	5.6
	5	3	3.3
	6	2	2.2
	7	2	2.2
	8	1	1.1
	10	1	1.1
	Total	90	100.0
Missing	System	2	
Total		92	

Table 3 illustrates the profile of the perpetrators with respect to whether they were in the US while committing the crimes or not. 82.6% of the charged cybercrimes were carried out from within the US, 14.1% were from outside of the US, and 3.3% were from both inside and outside of the US. A vast majority of cybercrimes occurred from the U.S. The national origin of the perpetrators may not necessarily be American, but they were in the U.S. when they committed their respective crimes. Cybercrime rings often spread across the world because perpetrators do not need to be in a particular location or even come into contact with each other to commit a cybercrime.

Table 3. Geographical Origin

	Frequency	Percent		
Crime committed from within the US	76	82.6		
Crime committed from outside of the US	13	14.1		
Crime committed from within the US and outside of the US	3	3.3		
Total	92	100.0		

CONCLUSION

This paper focused on analyzing the charged computer and cybercrime cases identifying targets of the crimes and types of interest harmed using the press releases published between 2010 and 2014. The cyber-attack targets included military intelligence, financial data, and intellectual property. They not only affected individuals, but also corporate-level businesses, and government interests. The number of hackers per event varies and has no set number, but yet they tend to move in smaller forces and have no legitimate motives other than to embarrass their targets or exploit them financially. Cyber threats have reached a point where, given enough time, motivation, and funding, a determined adversary will likely be able to penetrate any system that is accessible directly from the Internet.

REFERENCES

Boyle, R., & Panko, R. (2014). *Corporate computer security* (Fourth ed., p. 96).

Davis, H., & Braun, R. (n.d.). Computer Fraud: Analyzing Perpetrators and Methods. Retrieved November 23, 2014.

Feringa, A., Goguen, A., and Stoneburner, G. (2002, July) *NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems. Retrieved from* http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Jones, D. (2014, April 1).*Two U.S. hackers admit to international cyber crime in N.J. court*. Reuters. Retrieved from http://www.reuters.com/article/2014/04/01/usa-crime-cybercrime-idUSL1N0MT23O20140401

Moldovan citizen indicted for Internet Fraud. (13, September 13). Retrieved November 23, 2014, from http://www.justice.gov/usao/nyw/press/press_releases/2013/sept/Vasile_Leu.html

Nakashima, E. & Peterson, A. (2014, June 9). *Report: Cybercrime and espionage costs $445 billion annually*. Washington Post. Retrieved from http://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html

Podgor, Ellen S. "Computer Crime." Encyclopedia of Crime and Justice. 2002. Retrieved September 08, 2015 from Encyclopedia.com: http://www.encyclopedia.com/doc/1G2-3403000048.html

Target Provides Update on Data Breach and Financial Performance | Target Corporate. (2014, January 10). Retrieved November 10, 2014, from http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance

Wagsaff, K. (2014, March 12). The Internet and the World Wide Web Are Not the Same Thing. Retrieved November 24, 2014.