Computer Fraud Challenges and Its Legal Implications

Amber A. Smith-Ditizio
Texas Woman's University, USA

Alan D. Smith
Robert Morris University, USA

INTRODUCTION

Computer Fraud

Computer fraud and hacking attempts have been publicized for more than a century. Although customers only think of computers and smartphones being hacked, there are examples in the early 19th century where phone lines were hacked. Cybercrime is a fast growing area and has drastically increased over the years. Its business model is evolving and the market is profitable for criminals. New activities have emerged as technology advances. Traditionally, consumers and businesses were lax with security as hackers could easily encrypt and infect any technological device. Hence, cybercriminal activities grew rampant in the global economy. Security protection, government involvement, and leading software companies have become strategic partners in combating cybercriminal activities. However, despite all these efforts, cybercrime is still growing. There are many strategic solutions to this growing epidemic, such as investing in anti-virus software and commonsense approaches to password protection. In order to reduce the amount of cybercriminal activity occurring globally, action needs to be taken immediately.

The targets are computers or anything device connected to the Internet, such as tablets or smartphones (Sundarambal, Dhivya, & Anbalagan, 2010). Hackers affect the cybersecurity of large companies, government agencies and regular customers, especially if competitive or personal information is stolen for ransom or extortion purposes. In the majority of incidents, it is relatively simple to trace back to the hacker, as many are nonprofessionals with little experience. However, it has become increasing difficult to catch more sophisticated hackers. Although, if and when they are caught, there are significant penalties that come with hacking and computer fraud, many have argued that these penalties are not severe enough to deter such activities (Beldona & Tsatsoulis, 2010; Mohanty, et al., 2010; Smith, 2007). Some have suggested that such crimes as inevitable as IT systems become increasing complex and globally interconnected (Dharni, 2014; Latha & Suganthi, 2015; Chand, et al., 2015; Han, et al., 2015; Soon, et al., 2015).

Exploring Types of Computer Fraud

To illustrate these trends, Stewart and Shear of SecureWorks™ have examined many hacker markets and found that cybercriminals are increasing their activity of stealing information (Clarke, 2013). Stewart is Dell's SecureWorks™' Director of Malware Research for the Counter Threat Unit (CTU) and independent researcher Shear have done much research into the dark marketplace that is frequented by cybercriminals. There are online tutorials for novice hackers to learn the trade for under US$1. For example, one can access Social Security card numbers, name and address of customers for US$250. Cy-

DOI: 10.4018/978-1-5225-2255-3.ch419

bercriminals can gain control of computers for US$20 to 50. Customers can also hire someone to hack a website for US$100 to 200. However, not everything is cheaper. The price of botnets, spam and malicious software, has increased from US$90 to US$600-1,000. Multiple sellers advertise "satisfaction guaranteed" on the data, which is designed to capture the attention of a potential or practicing hacker. It seems the traditional business model of value-added activities works well in the more hidden and illegal markets as well. However, organizations' drives to understand and anticipate their customers' needs ultimately forces management to connect valuable and vulnerable corporate systems to the general public and, thus, cyberthieves (Daim, Basoglu, & Tanoglu, 2010; Daramola, Oladipupo, & Musa, 2010; Dominic, Goh, Wong, & Chen, 2010; Kapur, Gupta, Jha, & Goyal, 2010; Keramati & Behmanesh, 2010).

Dell and its software SecureWorks™ are well-known and highly respected IT-security providers. Software and management at Dell has been investigating this illegal market for some time. Dell, as a provider of security systems, has in place this particular security software in over 61 countries with 4100 clients and has been providing top of the line service for the past 16 years. Dell SecureWorks™ provides a relatively quick warning to its clients when a cyber-attack is happening. It also provides a prediction of where the cyberattack is coming from and what it is trying to get from the computer. After the security system finds a cyberattack the system then works to get rid of it and tries to prevent the cyberattack from happening again. Counter Threat Platform (CTP) powers Dell SecureWorks™. CTP analyzes a total of 150 billion networks to find any possible threats, generate information, and find any information that could lead to a cyberattack (Alderete & Gutiérrez, 2014). Overall, CTP allows Dell's SecureWorks™ to prevent, detect, respond, and predict.

Cybercrime an industry that has shown double digit growth year after year within the current struggling global economy. Cybercriminal activities have been on the rise and are becoming more profit driven as its business model is evolving and new cybercriminal activities are emerging. Out of dozens of underground markets surveyed by SecureWorks™ researchers, a subsidiary that specializes in cybersecurity and data protection, it was found that business is booming. Not only have prices gone down on many of the services offered, but offerings have expanded as well. From basic hacking offerings to infecting networks of computers with the use of botnets, "underground hackers are monetizing every piece of data they can steal or buy and are continually adding services so other scammers can successfully carry out online and in-person fraud" (Lawrence, 2014). Cybercriminal activity has become a major global problem.

China, for example, tops the list for online crime hotspots with 83% of respondents residing there having been victimized (Bertolucci, 2016). According to the Norton Cybercrime Report ("Cybercrime Report," 2011), 41% do not have an updated security software suite to protect their personal and online data in the U.S. Within this study, more than 65% have claimed that they have fallen victim to viruses and malware attacks, online scams, phishing, social network hacking, credit card fraud, and sexual predation. Many people are uneasy about the safety of online commerce, as they feel that the majority of online criminals operate within countries where prosecution is unlikely. Illegal downloads, digital piracy, and digital harassment are some of the other more common cybercriminal activities committed on a daily basis (Shinder, 2011).

Cybercrime is up 10.4% over the previous year as stated by Kassner (2016). In general, cybercrime has risen over US$1.13 million domestically in the 2014 alone. Web-based attacks, denial of services, malicious insiders, viruses, worms, Trojans, malicious code, phishing and social engineering, malware, stolen devices, and botnets are among the top cybercriminal activities have cost the U.S. and other countries the most money it terms of lost productivity, cybertheft, and counterintelligence efforts. The actual price of cybercriminal