IPRPD
International Journal of Business & Management Studies
ISSN 2694-1430 (Print), 2694-1449 (Online)
Volume 04; Issue no 11: November, 2023
DOI: 10.56734/ijbms.v4n11a6

CYBERCRIME

Jeffrey Everhart[1]

[1]*Assistant Professor, Department of Accountancy, Bemidji State University*

Abstract

First, the paper will define and analyze cybercrime, computer crimes, and internet fraud. Then, the paper will examine how criminals use the Internet to commit crimes anonymously. Lastly, the paper will offer insight into the prevention and how to combat cybercrime, internet fraud, and computer crimes.

Keywords

Computer Crimes, Cybercrime, Internet Fraud

Cybercrime is growing at incredible speeds as most cybercriminals can remain anonymous through the Internet as a tool to commit cybercrime (Kranacher & Riley, 2020). Criminals can set up shop and commit cybercrimes from anywhere in the world, stay unknown, and then sell the information the cybercriminals stole (Kranacher & Riley, 2020). Kranacher and Riley (2020) explain that there are two types of fraudsters: one is known as the first-time fraudster, and the other type is a predator.

What are the differences between the two different types of fraudsters? The first-time fraudster is usually a first-time offender, has no criminal record, is highly educated, is a trusted citizen, and is a good community member (Kranacher & Riley, 2020). The first-time fraudster usually has some financial problem, has intense financial pressure, and rationalizes that the problem can be solved by stealing money (Kranacher & Riley, 2020). The other type of fraudster is the predator, who has committed fraud multiple times over the years and is a repeat fraud offender (Kranacher & Riley, 2020). The predator researches to find a business or organization that will be an easier target to start financially defrauding the organization as soon as they are hired by the organization (Kranacher & Riley, 2020). The predators often start as first-time fraudsters and become financial fraud predators (Kranacher & Riley, 2020).

Cybercrime and the Internet

With the invention of the Internet came the possibility of committing accounting fraud and staying anonymous (Seetharaman et al. (2017). The Internet allows criminals to prey on the weak and elderly, all while staying unknown, working anywhere in the world, and profiting by committing cybercrimes (Seetharaman et al. (2017). Cybercrime involves using computers and the Internet to commit theft, alter computer records, and steal financial information (Seetharaman et al. (2017). There are different types of cyber theft that criminals commit using the Internet. Many cybercrimes are referred to as white-collar crimes, where the illegal offense is related to the theft of confidential information or for financial gain (Seetharaman et al. (2017).

Computer Crimes

Neufeld (2023) explains that there has been a rise in computer crimes in recent years as computer crimes have gotten so out of control that this type of crime has gotten global attention, affecting the entire planet. Computer crimes are when criminals use technology to accomplish a long list of illegal and destructive crimes (Neufeld, 2023). The crimes include identity theft, data theft and breaches, ransomware use, and cyber espionage (Neufeld, 2023).

What are some techniques commonly used to try and prevent or deter computer crimes from happening? Sophisticated technology is aimed to provide protection barriers from computer crime criminals (Neufeld, 2023). Organocations have entire Information Technology departments dedicated and focused on deterring this type of crime from occurring (Neufeld, 2023). Along with barriers to the technology system, organizations also use an array of access authentication systems to try and prevent data breaches and the theft of information (Neufeld, 2023). In the modern-day business environment, ensuring resources are available to combat and prevent computer

crimes is one way to keep these high-tech criminals at bay (Neufeld, 2023). The fraudulent criminals continue to get more sophisticated and tech-savvy in the ways and methods in which computer crimes are committed. Because of this, forensic accountants must be up on the latest technology to prevent this type of crime and combat the growing trend of computer crimes worldwide (Neufeld, 2023).

Internet Fraud

The Internet is a viral tool worldwide, improving production in the modern conventional work office (Peifeng & Wang, 2022). However, there have been some very adverse effects of the Internet, as the Internet has provided a space for criminals to commit internet fraud (Peifeng & Wang, 2022). When Comparing traditional methods of fraud and the newly emerged trend of using the Internet for fraud, one of the significant differences is the ability to commit no-contact and anonymous crimes on a large portion of the population in a concise amount of time (Peifeng & Wang, 2022). The criminals use different internet platforms to commit fraud, such as webchats, SMS, and other telecommunication products tied to the Internet (Peifeng & Wang, 2022).

Internet fraud has created considerable losses to communities and individuals. Over the last ten years, internet fraud has grown between twenty and thirty percent yearly (Peifeng & Wang, 2022). The internet platform has become the technological fraudsters' choice in committing fraud as the fraudsters can stay anonymous, and detectives and other law enforcement agencies have a tough time catching the criminals as their identity is hidden behind their internet computer screen (Peifeng & Wang, 2022). Each year, government statistics tell us that internet fraud is growing alarmingly and that combating it is very tough as the criminals are not in plain sight, making it hard to apprehend them (Peifeng & Wang, 2022). Despite the growing trend of internet fraud, cybercrime, and computer crimes, preventing such crimes is very difficult because of the enormous volume and the difficulty of trying to predict and define early warning signs of such criminal behavior (Peifeng & Wang, 2022). The FBI (2020) also runs into the problem of jurisdiction when cybercrimes are committed, as the question is, who is responsible for prosecuting the criminals?

FBI and Cybercrime

The FBI (2023) website states that with the growing advent of accounting fraud, financial crimes, and cybercrimes, the need for forensic accounting continues to grow to try and prevent these types of crimes from happening. The severe threat of these crimes has become all too common and is growing in sophistication. The FBI continues to enhance the organization's Cyber Division in terms of investigative work and overall capacity to enhance its capabilities to detect breaches in both government organizations and the private sector (FBI, 2023). The FBI continues to train employees and educate them on how to catch these cybercriminals. However, the criminals continue to devise criminal methods to avoid being detected and stay anonymous (FBI, 2023). Cybercrime has become a problem worldwide, and this type of destructive behavior affects everyone worldwide, sometimes directly and, in other cases, indirectly. However, it does affect everyone in some capacity (FBI, 2023).

Conclusion

Modern-day cybercrime perpetrators continue to improve at concealing their fraudulent criminal tracks (Özcan, 2018). Therefore, forensic accountants must continue developing new methods to detect and prevent this ever-revolving white-collar crime (Özcan, 2018). What actions can be taken to reduce cybercrime, computer crime, and internet fraud? One method to combat these types of crimes where the perpetrator is anatomy and hides behind a screen is to have great auditors. The auditor is critical in preventing and detecting computer fraud (Seetharaman et al., 2017). The auditors usually have experience in detecting computer fraud and have the knowledge to specialize in finding and reporting the accounting fraud that has taken place or is going to take place (Seetharaman et al., 2017).

These specialized auditors are called forensic accountants and are responsible for combating accounting fraud, cybercrimes, and computer crimes (Seetharaman et al., 2017). Accounting information systems need to be protected from criminals, and the forensic accountant is the resource that is available to secure the system from information and financial theft (Seetharaman et al., 2017). Lastly, the forensic accountant must effectively collect evidence against the accounting system's perpetrator to stop the fraud and penalize the thief with incarceration and fines (Seetharaman et al., 2017). Reporting cybercrime is also critical to fighting cybercrime and trying to prevent the next person or organization from being scammed by criminals (Grossklags & Bidgoli, 2016). Grossklags and Bidgoli (2016) explain that reporting cybercrime helps with the prevention of future cybercrime as the reporting provides valuable information and educates users of the Internet on what they can do to reduce or mitigate the possibility of being scammed cybercrime, computer fraud, and Internet fraud. The information given in the report to authorities can be used to hopefully prosecute and give some resolution to the person or organization that crime was committed against.

References

FBI. (2023). What we investigate. https://www.fbi.gov/investigate/cyber

Jens Grossklags, & Morvareed Bidgoli. (2016). End user cybercrime reporting: what we know and what we can do to improve it. *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF).*

Kranacher, M., & Riley, R. (2020). Forensic accounting and fraud examination, 2nd ed. John Wiley & Sons: Massachusetts, USA – Chapters 12 & 13.

Neufeld, D. (2023). Computer crime motives: Do we have it right? *Sociology Compass*, 17(4), 1–42. https://doi.org/10.1111/soc4.13077

Özcan, A. (2018). The Use of Beneish Model in Forensic Accounting: *Evidence from Turkey. Journal of Applied Economics & Business Research*, 8(1), 57–67.

Peifeng Ni, & Quanxiu Wang. (2022). Internet and Telecommunication Fraud Prevention Analysis Based on Deep Learning. *Applied Artificial Intelligence*, 36(1), 1–19. https://doi.org/10.1080/08839514.2022.2137630

Seetharaman, A., Patwa, N., & Niranjan, I. (2017). Role of Accountants and Auditors in Mitigating Digital Crimes. *Journal of Applied Economics & Business Research*, 7(1), 1–17.