BOOK CHAPTER | Syndicate Operations

Cyber Fraud and Syndicate Operations

Osa Edosa
Department of Electrical/Electronic Engineering
University of Benin
Benin City, Nigeria
Email: edosa.osa@uniben.edu
Phone: +2348168307508

Abstract

Cyber fraud is the most common and threatening form of fraud which occurs the world over. Since the advent of the third industrial revolution that characterized the rise of computers and the internet, there has been an exponential increase of cyber activities thus allowing fraudsters to hack personal and financial information of unsuspecting victims in a variety of ways. The illegally obtained information can be used to garner personal financial funds by the fraudsters, to fund terrorism, defiantly disrupt daily business activities amongst other vices. This chapter presents a review of Cyber Fraud and how cyber criminals operate. It also provides case studies of some recent occurrences.

Keywords: Cybercrime, Internet, Phishing, Fraud, Data Breach, Syndicate Operations.

Introduction

Computers, computer networks as well as the Internet were realized for the generation, storage and transfer of information in government, academic, corporate as well as other circles. These information are meant to be highly valuable to the right people. The creation of digitized methods for operations have pushed mankind into the twenty first century. However, this thrust includes criminal operations as a significant component (Mujović, 2018). This negative development underlines a relatively recent form of crime known as Cybercrime. Cybercrime is a crime that involves a computer and a network (Moore, 2005; Encyclopedia Britannica, 2021).

The computer may be used in committing the crime, or it may be the target of the cybercrime (Kruse and Heiser, 2002). The effects of cybercrime may be harmful to security and financial health of an individual or group of individuals as the case may be (Bossler and Berenblum, 2019). At the international level, both governmental and non-state actors engage in cybercrimes, such as espionage, financial theft, and other cross-border crimes. Such cybercrimes that cross international borders and often involve the actions of at least one nation-state are sometimes referred to as Cyberwarfare. The harmful effects of the cybercrime menace cannot be overemphasized since many a human endeavour are now being made electronic. According to Warren Buffet, Cybercrime is the "number one problem with mankind" (Buffett, 2021) and "poses real risks to humanity" (Buffett, 2021). Computer or cyber crime encompasses a broad range of activities (Gordon, 2006).

Citation Osa, Edosa (2022). Cyber Fraud and Syndicate Operations. SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series
Book Chapter on Web of Deceit - African Multistakeholders' Perspective on
Online Safety and Associated Correlates Using Multi-Throng Theoretical, Review, Empirical
and Design Approaches. Pp 191 -196. www.isteams.net/bookchapter2022.
DOI https://doi.org/ 10.22624/AIMS/BK2022-P32

The primary effects of cybercrimes are mostly financial as cybercrime can include various types of profit-driven criminal activities such as ransomware, email and internet fraud, identity fraud, as well as attempts to steal financial account, credit card or other types of payment card information (Brush, 2020). Cybercriminals may also target private information, as well as corporate data for theft and resale.

Types Of Cybercrimes

Some specific types of cybercrimes include:

Cyberextortion

These are crimes involving an attack or threat of an attack usually coupled with a demand for money to stop the attack or threat. One popular form of cyberextortion is ransomware attack. In this attack, the attacker gains access to the systems of an organisation and encrypts important documents and files thus making the data inaccessible until a required ransom is paid. The payment method is usually in some form of cryptocurrency, such as bitcoin. A vivid example of cyberextortion was the cyber attack on Sony Pictures of 2014 (Mohanta, 2014).

Cyberterrorism

A cyberterrorist could be described as someone who intimidates or forces a government or an organization to advance his or her political or social standpoints by launching a computer-based attack against computers, networks, or the data contained in these devices. Cyberterrorism can be said to be an act of terrorism committed via the cyberspace or computer resources. A good example of cyberterrorism is a simple propaganda piece on the Internet stating that there will be bomb attacks during the holidays (SentinelOne, 2016).

Identity theft:

This attack occurs when a criminal accesses a computer to glean a user's personal information. This information can further be used to steal the owner's identity or access their banking and credit cards. Identity information is also sold on the dark web.

Cyberespionage

It involves crimes such as hacking into systems or networks to gain access to confidential information owned by a government or some other important organization. These attacks are usually motivated by profit or ideology.

Exit scam

This involves dark web administrators who divert virtual currency that is held in escrow accounts to their personal accounts. As the name goes, it is the digital version of an old crime dubbed the *exit scam*. (Brush, 2020).

Just as other forms of crime have taken an electronic nature so has Fraud giving rise to a recent shade of Fraud known as Cyber Fraud.

Concept of Cyber-Fraud and Syndicate Operations

Cyber fraud is referred to as any dishonest misrepresentation of fact within the computer domain intended to let another do or refrain from doing something which causes loss. It could also be defined as the crime committed via a computer with the intent to corrupt another individual's personal and financial information stored online.

Cyber fraud will therefore result in obtaining a benefit by:

1. **Altering data processes in an unauthorized way.** Little technical expertise is required for this. However, it is a common form of theft by employees who alter data before entry or enter false data, or who enter unauthorized instructions or use unauthorized processes.
2. **Altering, suppressing, destroying, or stealing output.** It involves using electronic means to conceal unauthorized transactions. It is a difficult crime to detect.
3. **Altering or deleting stored data.**

Forms of fraud may be facilitated using computer systems, including financial fraud crimes, bank fraud, carding, identity theft, extortion, and theft of classified information.

Cyberfraud is so popular (and potentially profitable) that well-organized networks of cyber criminals work in collaboration to pull off massive heists over the internet. These criminal groups are comprised of hackers, programmers and other software bandits who combine their techniques and resources to commit major atrocities (Tropina, 2021). They usually take advantage of national jurisdictions that have no proper legal frameworks and technical frameworks to fight cybercrime.

Some High Profile Methods for Cyber Fraud.

Business E-Mail Compromise (BEC).

A sophisticated scam targeting businesses and companies that regularly perform wire transfer payments. It is usually carried out by compromising legitimate business e-mail accounts via social engineering or other computer intrusion techniques in order to carry out unauthorized transfer of funds.

Data Breach

This involves leakage of data from a secure repository to an untrusted environment. Data breaches occur at personal as well as corporate levels.

Denial of Service

It is an illegitimate interruption of an authorized user’s access to a system or network, usually done with malicious intent.

E-Mail Account Compromise

This method is similar to BEC, but targets emails associated with (but not limited to) financial institutions, real estate companies as well as law firms. The compromised emails are thereafter used to request payment to fraudulent accounts.

Recent Trends in Cyber-Fraud And Syndicate Operations

Pandemic-Related Phishing Attacks

Phishing recently became a critical issue at the beginning of the Covid-19 era. Cybercriminals began using the pandemic to create fear and manipulate individuals to provide them access to sensitive information. One major instance in the UK involved elderly people receiving emails and calls that promised them Covid-19 vaccination on condition they provide the data that the malicious email sender or caller requested (Infosec, 2021).

Increase in BEC Attacks

Research data published by Abnormal Security displayed a 200 percent increase in BEC attacks as per invoice or payment fraud from April to May 2020. These cyberattacks targeted businesses that frequently dealt with overseas suppliers and online money exchangers.

The hackers posed as vendors, customers or suppliers and thus could hijack money exchanges and redirect funds to their own accounts.

Hushpuppi Episode

There was the publicized arrest of Nigerian-born, Dubai-based suspected cyberfraudsters Ramon Olorunwa (hushpuppi) and Olalekan Jacob Ponle (Woodberry) by security officials in Dubai and the subsequent extradition to the United States by FBI agents in July 2020. This was based on charges of Business Email Compromise (BEC) scams amounting to hundreds of millions of dollars (Madawo, 2020).

Effects Of Cyber-Fraud and Syndicate Operations On Businesses.

The actual cost of cyberfraud is difficult to assess. However, in 2018, McAfee released a report on the economic impact of cybercrime which estimated the likely annual cost to the global economy at nearly $600 billion, up from $45 billion in the year 2014. Some consequences of cyberfraud in business environments include the following:

- Damages to perception of investors after a security breach can cause a drop in the value of a company.
- The loss of sensitive customer data to attack can result in fines and penalties for companies due to failure in protecting customer data. Businesses may also face legal action over the data breach.
- Damaged brand identity and loss of reputation after a cyberattack undermine customers' trust in a company and the company's ability to keep their financial data safe. Following a cyberattack, firms not only lose current customers, but they also lose the ability to gain new customers.

How To Prevent Cyberfraud in Corporate Environments

Complete eradication of cybercrime may not be possible. However, businesses can reduce their exposure to it by maintaining an effective cybersecurity strategy. This can be realized by a defense-in-depth approach to securing systems, networks and data of the business.
Cyberfraud risks can be reduced via the following steps:

- Develop clear policies and procedures for the business and employees;
- Cybersecurity incident response management strategy to support these policies and procedures;
- Outline the security measures that are in effect;
- Employ two-factor authentication (2FA) applications or use physical security keys;
- Activate 2FA on online accounts as much as possible;
- Verbal verification by finance manager for authenticating requests to send money;
- Create an intrusion detection system (IDS) that flags off external emails with extensions similar to company emails;
- Careful scrutiny of all email requests for transfer of funds to determine if the requests are suspicious;
- Continual training of business employees on cybersecurity policies and procedures;
- Websites and end systems should be updated or patched regularly; and
- Proper data and information back up should be done regularly to reduce damage in case of a cyber attack.

In addition, cyberfraud can also be prevented by encrypting all local hard disks and email platforms by using a virtual private network (VPN) or by using a private and secure domain name system (DNS) server (Brush, 2020).

How To Protect Yourself Against Cybercrime

Anyone who uses the internet should exercise some basic precautions among which include:

1. Use a full-service internet security suite
2. Use strong passwords
3. Keep your software updated
4. Manage your social media settings by keeping private information locked down

5. Strengthen your home network
6. Keep up to date on major security breaches
7. Take measures to help protect yourself against identity theft
8. Guard your personal data especially when accessing the internet on public Wi-Fi. A virtual private network (VPN) can also help to protect online data.

Challenges To Fighting Cyber Fraud

Fighting cybercrime has always been a complex problem due to the number of ICT network users, the transnational nature of the Internet and its decentralised architecture. Cybercriminals, and especially organised criminal groups, have been and probably would always remain several steps ahead of legislators and law enforcement agencies. Countries face the problem of addressing this international problem collectively. Some States just do not have the necessary tools to respond to the activities of the organised cybercriminals, they may lack the technical skills or have legal drawbacks. The development of a common understanding that no country could be safe alone in the global ICT network is very important (Tropina, 2021).

Recommendations

What follows are recommendations:

- There is a need for enhanced cooperation and improved data sharing between law enforcement, computer security incident response teams and private partners.
- In addition to strengthening the current legal frameworks, updating old legislation and harmonizing laws on an international level, what is needed is also the cross-sector cooperation on national level as well as international cooperation in detecting, investigating and preventing e-crimes committed by organised criminal groups.

References

1. Bossler, A. M. and Berenblum, T. (2019). "Introduction: new directions in cybercrime research". Journal of Crime and Justice. 42 (5): 495–499. doi:10.1080/0735648X.2019.1692426. ISSN 0735-648X.
2. Brush, K. (2020). CYBERCRIME. Available at: https://searchsecurity.techtarget.com
3. BUFFETT, 2021. This is 'the number one problem with mankind'". Business Insider.
4. Buffett, W. (2021). 'Cyber poses real risks to humanity'". finance.yahoo.com.
5. BUSINESS WIRE, (2020). Abnormal Security Data Reveals 200 Percent Monthly Increase in Invoice and Payment Fraud Business Email Compromise Attacks. Available at: http://www.businesswire.com.
6. Cloudbric. (2020). Cybersecurity statistics in the first half of 2020. https://v2.cloudbric.com
7. Encyclopedia Britannica "cybercrime | Definition, Statistics, & Examples". Encyclopedia Britannica.
8. Gordon, S. (2006). "On the definition and classification of cybercrime". Journal in Computer Virology. 2: 13–20. doi:10.1007/s11416-006-0015-z. S2CID 3334277.
9. Karimi, F. 2020. “Ray Hushpuppi Is accused of Cyber Crimes in Two Continents”-CNN 2020.
10. Kruse, W.G and Heiser, J.G. (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 978-0-201-70719-9.
11. Leukfeldt, E.R and Holt, T.J. (2019). Examining the Social Organization Practices of Cybercriminals in the Netherlands Online and Offline. International Journal of Offender Therapy and Comparative Criminology, 2019; 0306624X1989588 DOI: 10.1177/0306624X19895886.
12. Madawo, L. (2020). “Hushpuppi’s Lawyer Says FBI ‘kidnapped’ Nigerian Instagrammer from Dubai”. BBC News 2020.

13. Mohanta, A. (2014). "Latest Sony Pictures Breach: A Deadly Cyber Extortion".
14. Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
15. Mujović, V. (2018). Where Does Cybercrime Come From? The Origin & Evolution of Cybercrime, https://Www.Le-Vpn.Com.
16. SentinelOne, (2016) "Cybercriminals Need Shopping Money in 2017, too!". Available at: www.sentinelone.com.
17. Tropina, T. (2021). Cyber Crime and Organized Crime. Available at: unicri.publicinfo@un.org
18. Virgillito, D. (2021). Top 9 Cybercrime Tactics, Techniques and Trends in 2020: A Recap. https://resources.infosecinstitute.com.