Educational Administration: Theory and Practice
2024, 30(5), 40-43
ISSN: 2148-2403
https://kuey.net/

Research Article

A Study On Emerging Financial And Cyber Threats

Dr. P. Shiney[1*], Dr. M. Shanthana Lakshmi[2], Dr. S. Mahadevi[3], Ms. S. Shanthi[4], Dr. K. Rajarajeshwari[5]

[1*]Assistant Professor, School of Commerce Nehru Arts & Science College, Nehru Garden, Thirumalayam Palayam, Coimbatore -641 105, Tamilnadu, India.
[2]Dean, School of Commerce Nehru Arts & Science College, Nehru Garden, Thirumalayam Palayam, Coimbatore -641 105, Tamilnadu, India.
[3,4]Head & Assistant Professor School of Commerce Nehru Arts & Science College, Nehru Garden, Thirumalayam Palayam, Coimbatore -641 105, Tamilnadu, India.
[5]Head & Associate Professor School of Commerce Nehru Arts & Science College, Nehru Garden, Thirumalayam Palayam, Coimbatore -641 105, Tamilnadu, India

Citation: Dr. P. Shiney, et al (2024) A Study On Emerging Financial And Cyber Threats, *Educational Administration: Theory and Practice,* 30(5), 40-43,
Doi: 10.53555/kuey.v30i5.2765

ARTICLE INFO

ABSTRACT

Over the past few decades, cyber security has been a catch-22. In this digital generation, it is of prime importance to secure our information. Unbelievably, the evolving technology has taken all its possible ways to interfere and affect regular life at a high and sophisticated level. The future seems exciting with all its booby traps. As it is the pressing issue of the present day, it is essential that we gather information about the intensity of this graveness. Yet the upcoming technological advancement has created many solutions to prevent the current cyber threats. The purpose of this paper is to address cyber-enabled financial crimes and present solutions to overcome challenges, by maintaining the balance between technology and sustainable living.

Keywords: Cyber Security, Technology, Financial Crime.

INTRODUCTION:

In this era, financial crime and cybersecurity are interdependent terms. Financial crime has become a menace to society. Money laundering, insider trading and forgery are some of them. This paper will delve into the evolution of financial crimes, the introduction of cybercrimes and preventive cyber security methods. There are sources that prove that financial crimesexisted in our world around 4000 years ago. It evolved into cybercrimes. But the intervention of cyber security in the 1970s played a major role in preventing cybercrimes. However, AI intervention in cybercrimes has opened a new horizon for cyber-attackers in financial crimes. By examining the past, analyzing the present, and envisioning the future, we equip ourselves with the knowledge and insights necessary to fortify our defenses, enact effective countermeasures, and ensure the resilience and integrity of financial systems in an age where the digital realm and financial realm intertwine ever more closely.

STATEMENT OF THE PROBLEM:

Within the ever-evolving advanced danger scene, money related violations have never misplaced their significance. The strategies and complexity of cybercrime are quickly advancing with technology. This progressing battle can be unraveled by counterfeit insights that can analyze endless sums of information, identify designs and adjust in genuine time. In expansion to security concerns, the intervention of fake insights in cybercrime moreover raises ethical concerns. To make a more secure computerized world, these advances must be actualized capably and morally, regarding protection rights and human values.

OBJECTIVES OF THE STUDY:

The study has the following subjects:

- To examine the advancement of cyber-enabled financial crimes.
- To examine AI intervention in financial crimes.
- To study various prevention measures to combat financial crimes.
- To evaluate the effectiveness of cybersecurity measures.

SIGNIFICANCE OF THE STUDY:

The present study examines the pivotal role of a secure online environment free of financial offenses. In 2023, the central banks of 114 countries will be in various stages of evaluating the launch of a national digital currency. This consists of 95% of the world's GDP. Also, our nation had more than 30 billion online transactions in 2022, which accounts of ₹149 trillion. So, in this digital era, the prevention of financial crimes holds profound significance for individuals, businesses, nations, and society at large. This paper also establishes various measures and solutions to avert financial crimes.

LIMITATIONS OF THE STUDY:

The limitations faced in doing this paper are as follows:

- **TIME CONSTRAINTS**: Time constraints restrict the researcher to collect more data and thus limiting the study.
- **LIMITED SAMPLE SIZE**: Inability of the researcher, to acquire a standard amount of respondents affects the accuracy of the study.
- **LACK OF RESOURCES**: Insufficiency in data can lead to misinterpretation of conclusion and that being so, averting the study.
- **LACK OF GENERALIZABLITY**: Lack of generalizability means that the findings may not be applicable to other populations or contexts.
- **LACK OF AWARENESS AND EDUCATION**: The failure of the citizens to be on guard against financial conspiracy affects the study.
- **SOPHISTICATED TECHNIQUES**: Cyber criminals usually use advanced techniques like phishing, malware and social engineering. These techniques can be difficult to detect.

CYBER-ENABLED FINANCIAL CRIMES:

Financial crimes are unlawful acts committed by people or organizations for the purpose of obtaining financial gain through dubious means. Around 4000 years ago, in the time of the Bible, there were Hebrew stories of financial crimes.The first documented crime was in England during the 15thcentury.In the upcomingcenturies, small-scale financial crimes will be an everyday occurrence. As time passes, the growth of technologies and the expansive use of cyberspace have also created an easy path for financial crimes to happen. Financial crimes, which have increased in importance in recent years around the world, have a negative impact on both the economy and society. Financial crime is a complicated and constantly changing issue that has to be addressed from several angles. Financial institutions, regulatory organizations, and law enforcement agencies all have a crucial role to play in identifying and stopping financial crimes. Increasing cross-border collaboration, bolstering anti-money laundering rules, and utilizing technology and data analytics to spot suspect activity are all effective ways to combat financial crime.

ANALYSIS:

Incidents	Jan-June 2022	Jan-June 2023	% Increase/ (decrease)
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Malicious code	353	442	25
Cyber Harassment	173	233	35
Content related	10	42	320
Intrusion attempts	55	24	(56)
Denial of services	12	10	(17)
Vulnerability reports	45	11	(76)
Total	5581	5592	

INTERPRETATION:

The above table shows the cyber threats reported in Malaysia from January - June 2021 and 2022. The above comparison clearly states that even though cyber threats are increasing, the measures to control and prevent those crimes have also increased. The percentage of cyber threats in sectors like intrusion, denial of service, and vulnerability reports has decreased tremendously. This shows that the cybersecurity in those areas has improved.

SOLUTIONS:

General solutions to cybercrimes:

- **CREATE STRONG PASSWORDS**

Build complex passwords and change passwords at regular intervals. Also enable multi factor authentication to add another layer of security to the passwords.

- **BLOCK CHAIN TECHNOLOGY**

Decentralised and tamper resistant nature can improve security in financial processes also use block chain technology for auditing purposes. No single authority will have complete control of the systems.

- **REGULAR SECURITY AUDITS**

To know the vulnerability of our systems, frequent vulnerability tests should be done to address the issue proactively. Penetration tests can be done periodically to identify potential weakness

- **CYBER INSURANCE**

Business and individuals can invest in cyber insurance to reduce the impact of the possible cyber attacks, data breaches etc. They will also help in post cyber attack investigation.

- **INCIDENT RESPONSE PLAN**

To recover from the attack immediately we need to draft a response plan to act suddenly after the attack. Also prepare a crisis communication plan to talk to investors and other stakeholders immediately after the attack.

- **THREAT INTELLIGENCE**

Always proactively beware of the emerging cyber threats in our surroundings to draft corresponding counter measures. Constantly update the systems to safeguard them from the upcoming threats.

- **NETWORK SEGMENTATION**

Divide network to various segments to avoid the spreading of the cyber attacks and to prevent unauthorised access to crucial financial data. This will help to reduce the attack consequences in a very considerable rate.

Al driven solutions to cyber crimes:

- **VECTRA Al**

It is a cyber attack response platform which automatically acts when the system is under cyber attack. Take counter measures to prevent the outspread

- **SPLUNK**

Uses Artificial Intelligence and machine learning to predict the possible cyber attacks by studying vast amount of data

- **AI-CHAT BOT**

Artificial intelligence chat-bots can provide instant and more precise information to customers and also detect fraudulent enquires

- **CREDIT RISK ASSESMENT**

It analyses social media activities and other online behaviour of an individual to ascertain the credit risk.

- **SHAPE SECURITY AI**

They helps to verify people who are they claimed to be by analyzing customer behaviour and tracking their previous activities

- **FRAUDULENT DOCUMENT DETECTION**

It is an Al tool used to check legitimacy of the documents. They helps to detect fake signatures and forged images

SUGGESTIONS:

- Be Suspicious.
- Validate the User's Identity.
- Avoid clicking on untrustworthy links.
- Keep the software updated.
- Avoid connecting your computer to any public Internet connection, especially when you're doing any monetary transactions (example: Hotel Wi Fi).

- Do not give away personal information to anyone on the Internet, and be aware of impostors.

CONCLUSION:

Cybercrime has become jeopardy in today's digitally connected world, posing significant risks to individuals, organizations, and governments. The conventional methods of combating cybercrime are proving inadequate in dealing with the evolving tactics employed by cybercriminals. However, emerging a robust framework, thecooperation of mankind with the law and public awareness offers promisingsolutions for cybercrime prevention, detection, and mitigation. To ensure a safe and enjoyable experience over the internet both the User and the Government play a vital role.

REFERENCE:

1. "Timeline of Cyber Incidents Involving Financial Institutions," Carnegie Endowment for International Peace, updated August 2020, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.
2. "About the FinCyber Strategy Project," Carnegie Endowment for International Peace, https://carnegieendowment.org/specialprojects/fincyber/about.
3. House of Commons Treasury Committee, "IT Failures in the Financial Services Sector: Second Report of Session 2019-20," UK House of Commons, October 20, 2019, https://publications.parliament.uk/pa/cm201919/cmselect/cmtreasy/224/224.pdf.
4. "RTGS Renewal Programme," Bank of England, September 29, 2020, https://www.bankofengland.co.uk/payment-and-settlement/rtgs-renewal-programme.