VOLUME 6 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

A STUDY ON ECONOMIC CYBER CRIMES: A RISING THREAT TO FINANCIAL INSTITUTIONS

- S K Aruna Shankari[1] & Vaishali[2]

ABSTRACT:

Economic cyber crime has emerged as one of the most serious threats to the global financial system in the digital age. With the expansion of online banking, mobile payments, and interconnected financial technologies, criminal actors now exploit digital platforms to conduct fraud, extortion, identity theft, and large-scale financial manipulation. This paper examines the growing phenomenon of economic cyber crime and its evolving impact on financial institutions worldwide. It explores the major forms of cyber enabled financial crime, the techniques used by cyber criminals, and the economic, operational, and systemic risks posed to banks and other financial entities. A comprehensive review of existing literature highlights the transformation of cyber crime from individual hacking activities to highly organized transnational criminal enterprises.Through qualitative analysis and documented case evidence, the study demonstrates that economic cyber crime is no longer a technical issue alone, but a fundamental economic and national security concern. The paper concludes with policy recommendations and strategic measures necessary for strengthening cyber resilience in financial institutions.

INTRODUCTION:

The rapid digital transformation of financial services has fundamentally reshaped how money is stored, transferred, and managed in the global economy. Internet banking, mobile payment platforms, automated trading, and digital wallets have enhanced efficiency and financial inclusion. However, this technological progress has also created new opportunities for cyber criminals to exploit financial systems with unprecedented speed and scale.

[1] Student at School of Excellence in Law , The Tamilnadu Dr. Ambedkar Law University
[2] Assistant Professor at School of Excellence in Law , The Tamilnadu Dr. Ambedkar Law University
For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/

Economic cyber crime refers to criminal activities conducted through digital means with the primary aim of obtaining financial gain. These activities include online fraud, identity theft, ransomware attacks, unauthorized fund transfers, market manipulation, and digital money laundering.

Financial institutions have become the primary targets of cyber criminals due to the immense concentration of financial assets, sensitive personal data, and critical infrastructures they manage. Unlike traditional crimes, cybercrime transcends national borders, operates anonymously, and evolves rapidly with technological advancements. A single cyber attack can cause billions of dollars in losses, destabilize markets, and undermine public trust in financial systems. The World Economic Forum consistently ranks cyber crime among the top global risks facing economic stability.[3]

The purpose of this research is to examine the rising threat of economic cyber crime to financial institutions by analyzing its causes, typologies, impacts, and regulatory responses. The paper further evaluates existing cybersecurity frameworks and proposes strategies for risk mitigation. The study is significant because economic cyber crime is no longer an operational nuisance but a systemic threat capable of triggering financial crises if left inadequately addressed.

REVIEW OF LITERATURE:

The study of economic cyber crime has expanded rapidly with the digitalization of financial systems. Scholars from criminology, economics, cyber security, and financial regulation have examined the structure, motivations, impacts, and governance challenges of cyber enabled financial crime. The following review highlights major academic contributions to this field.

1. Ross Anderson et al. (2019)– Measuring the Cost of Cybercrime[4]

Anderson and his colleagues produced one of the most influential economic analyses of cyber crime. Their study challenges the exaggerated global cost figures often cited in policy

[3] World Economic Forum, Global Risks Report 2023 (18th ed. 2023)

[4] Ross Anderson et al., Measuring the Cost of Cyber crime, 2 J. Cyber security 121 (2019).

debates and instead proposes a victim-centered framework for estimating losses. The authors demonstrate that although individual incidents may appear small, their cumulative effect on financial institutions is substantial. They also emphasize that banks bear a disproportionate share of indirect losses through fraud reimbursement, infrastructure investments, and reputational damage. This work is foundational in understanding the economic structure of cyber crime.

2. Michael Levi (2021) – Cyber Fraud and the Financial Sector[5]

Levi's work focuses on the intersection between traditional financial crime and digital fraud. He explains how cyber crime now integrates with money laundering, insider trading, and organized crime networks. The study highlights that financial institutions are no longer just victims but also key gatekeepers in preventing cyber enabled financial crime. Levi concludes that weak internal controls and poor inter bank coordination significantly magnify cyber related financial losses.

3. Dinei Florêncio & Cormac Herley (2018) – The Economics of Cybercrime[4]

Florencio and Herley apply rational choice theory to cyber crime and argue that attackers behave as economic agents who calculate risks and expected returns. Their research reveals that low prosecution rates and cross-border enforcement difficulties make cyber crime against banks highly profitable. They also show that financial institutions, due to their reimbursement obligations, unintentionally absorb much of the economic damage, reducing deterrence for offenders.

4. Nir Kshetri (2019) – Cybercrime and Global Governance[6]

Kshetri analyzes cyber crime from a geopolitical and regulatory perspective. He argues that economic cyber crime thrives because of regulatory fragmentation and uneven cyber security capacity across countries. His research shows that financial institutions operating internationally face elevated risks due to conflicting compliance requirements. Kshetri

[5] Michael Levi, Cyber Fraud and the Financial Sector, 45 Crime, L. & Soc. Change 89 (2021). [4]Dinei Florêncio & Cormac Herley, The Economics of Cybercrime, 16 Info. Sec. Tech. Rep. 116 (2018).
[6] Nir Kshetri, Cybercrime and Global Governance, 32 J. Int'l Pol. Econ. 321 (2019).

stresses the importance of international treaties, financial intelligence sharing, and cyber diplomacy to curb transnational financial cyber crime.

5.**Daniel Nagaratnam et al. (2020) – Ransomware Economics and the Financial Sector**[7]

This study focuses on the rapid growth of ransomware attacks against banks and financial service providers. The authors explain the economic logic behind ransomware, showing how attackers maximize leverage by targeting institutions that cannot tolerate downtime. The research finds that financial institutions increasingly face "double extortion" tactics, where stolen data is used for blackmail even after systems are restored.

6. Susan Brenner (2017) – Cyber crime and the Law[8]

Brenner examines the legal challenges of prosecuting cyber-enabled economic crime. She highlights jurisdictional conflicts, the problem of digital evidence, and the slow pace of international legal cooperation. Her work is particularly significant for financial institutions, as it explains why recovery of stolen digital assets is rare and why regulatory compliance often focuses more on prevention than prosecution.

7. Tyler Moore (2017) – The Economics of Online Crime[9]

Moore's research explores underground cyber crime markets, including the buying and selling of stolen bank credentials, malware kits, and money laundering services. He demonstrates that cyber crime operates as a decentralized marketplace with pricing mechanisms, competition, and customer support. This framework is essential for understanding why attacks on financial institutions remain persistent and adaptive.

[7] Daniel Nagaratnam et al., Ransomware Economics and the Financial Sector, 11 J. Fin. Crime 201 (2020).
[8] Susan W. Brenner, Cyber crime and the Law (Northeastern Univ. Press 2017).
[9] Tyler Moore, The Economics of Online Crime, 12 J. Econ. Persp. 45 (2017).

8. Franklin Allen & Elena Carletti (2020) – Systemic Cyber Risk and the Banking Sector[10]

Allen and Carletti extend cyber crime research into the domain of systemic financial risk. They argue that large-scale cyber attacks on major banks or payment networks could trigger liquidity crises and threaten global financial stability. Their study classifies cyber risk as a new category of systemic risk alongside credit and market risk.

WHAT IS ECONOMIC CYBER CRIME ?

There are three main forms of economic cyber crime:

1. Cyber dependent crimes: Cyber dependent crimes in law rely on networked information and communications technology (ICT), largely via the internet. Without the internet, the offending would not be possible.
2. Cyber enabled crimes: Cyber enabled crimes are facilitated by these same ICT - connected technologies, but are not dependent on them, and therefore can exist in some non cyber form. If the networked technologies were removed, the crime could still take place but locally and more likely on a one-to-one basis. Being cyber enabled allows these crimes to be carried out at scale for less capital and sometimes with fewer criminal staff than would be needed for similar crimes offline.
3. Cyber assisted crimes: Cyber assisted crimes are differentiated from cyber dependent and cyber enabled crimes, and use networked digital technologies (such as mapping applications) in the course of criminal activity which would take place anyway. The nature and volume of criminal activity are essentially unaffected by its involvement (i.e. if the internet involvement was removed, the crimes would be organized in different ways).

Both the cyber dependent and cyber enabled forms of economic cyber crime provide criminals with a globalized reach in a distributed and informational way. If the networked technologies are removed, then the crimes still take place but both victim and perpetrator are much more likely to be located in the same country, or adjacent countries, when crimes are

[10] Franklin Allen & Elena Carletti, Systemic Cyber Risk and the Banking Sector, 35 Brookings J. Econ. Activity 157 (2020).

undertaken offline. The number of victims per criminal attempt is also likely to be lower and the means employed – in person, telephone, advert or letter – can be more amenable to investigation. The cyber element can occur in different forms at any stage, from the planning of a crime through to its execution, to the expenditure and/or laundering of its proceeds. The Crime Triangle theory teaches us that crime is the product of would-be offenders, targets/victims and guardians, including those professionally paid to protect the public or whose routine activities serve to reduce opportunities for particular forms of crime. The virtue of this model is that it is dynamic, and can include insiders (some of whom may need or use ICT to complete their crimes), outsiders, and combinations thereof.

So at any given time, economic cyber crimes are affected by the technologies available, those who are capable and motivated to exploit them and the vulnerabilities of the targets/victims. Some targets are deliberately selected for attacks (known as 'spear-phishing') whereas others are indiscriminately selected in mass attacks.

FORMS OF ECONOMIC CRIMES THROUGH FINANCIAL INSTITUTIONS :

Economic cyber crime manifests in multiple forms, each exploiting different technological and institutional vulnerabilities.

i. Online Banking and Payment Fraud :

This includes unauthorized fund transfers, phishing-basetakeovers, and fraudulent card transactions. Criminals often steal login credentials using social engineering, malware, or data breaches, then rapidly move stolen funds across mule accounts.

ii. Identity Theft and Data Breaches :

Financial institutions store vast quantities of personal and biometric data. When breached, this information is sold in underground markets and used to commit further financial crimes.

iii. Ransomware and Cyber Extortion :

Ransomware attacks involve encrypting institutional systems and demanding payment for restoration. In the financial sector, even short system outages can result in massive market disruptions and liquidity risks.

iv. Market Manipulation and Trading Attacks :

Cyber criminals may manipulate high-frequency trading systems, disseminate false information to influence stock prices, or compromise brokerage platforms to execute illegal trades.

v. Digital Money Laundering :

Cryptocurrencies and decentralized exchanges are increasingly used to launder stolen funds through complex layering mechanisms that hinder tracing and recovery.

TECHNIQUES FOLLOWED BY CYBER CRIMINALS :

Cyber criminals employ a wide range of tactics designed to bypass security controls.

Phishing and Social Engineering	Fraudulent emails,messages,and websites designed to trick users into revealing Credentials.
Malware and Trojans	Software implanted into systems to steal data or provide remote access.
Distributed Denial-of-Service (DDoS)	Used to disrupt banking operations
Insider Attacks	Employees abusing authorized access to facilitate financial theft
Supply Chain Attacks	Compromising third-party vendors to gain indirect access to financial systems

These methods are continuously adapted to defeat new security technologies, making cybercrime a moving and evolving target.

Major Types of Economic Cyber crimes Affecting Financial Institutions

1.Online Banking and Account Takeover Fraud

Nature of the Crime

This involves unauthorized access to customer bank accounts using:

a) Phishing

b) SIM-swap fraud

c) Malware and spyware

d) Credential stuffing

Once access is obtained, funds are transferred to mule accounts.

Economic Impact

i. Direct loss to customers and banks
ii. Mandatory reimbursement by banks
iii. Loss of public confidence
iv. Increased cyber-insurance costs

Case Law :

State Bank of India v. Shreya Gupta[11]

The court held the bank partially liable for customer losses caused by online fraud due to inadequate security mechanisms and poor consumer awareness. This case established institutional responsibility in cyber-financial fraud.

2. Payment Card and ATM Fraud Nature of the Crime :

This includes:

a. ATM skimming

b. Card-not-present (CNP) fraud

c. POS terminal hacking

d. Dark-web sale of stolen card data

[11] (2019) SCC OnLine Del 9321 (India).

Economic Impact :

i. Charge backs and refunds ii.Merchant liability iii.Massive banking losses iv.Cross-border laundering

Case Law:

United States v. Albert Gonzalez (2010)[11]

Gonzalez led a hacking operation that stole over 170 million credit and debit card numbers, causing hundreds of millions in bank losses. He was sentenced to 20 years imprisonment, and the court legally recognized organized card fraud as economic cybercrime.

3.Interbank Transfer and SWIFT Fraud

Nature of the Crime Hackers manipulate:

a) SWIFT messaging systems

b) RTGS and NEFT platforms

c) Cross-border correspondent banking channels **Economic Impact :**

i. Large-value financial theft ii.Disruption of international settlements iii.Loss of trust in payment infrastructure iv.Central bank risk **Case Law :**

Bangladesh Bank v. Federal Reserve Bank of New York (2016)[12]

Cyber criminals issued fraudulent SWIFT messages attempting to steal USD 951 million; USD 81 million was successfully laundered. This case legally established SWIFT fraud as transnational economic cyber crime threatening global banking stability.

4.Ransomware Attacks on Financial Institutions

[11] 647 F.3d 41 (11th Cir. 2010).

[12] No. 17-CV-10654 (S.D.N.Y. 2016).

Nature of the Crime

Ransomware encrypts banking systems and demands payment in cryptocurrency.

Modern attacks also include data theft and blackmail (double extortion).

Economic Impact

a) Operational shutdown of banks

b) Regulatory penalties

c) Customer service disruption

d) Massive recovery costs

Case Law

United States v. Maksim Yakubets (2019)[12]

Yakubets led a global ransomware syndicate causing over USD 100 million in financial sector losses. The US government charged him for banking system cyber extortion, classifying ransomware as organized economic cybercrime.

5.Cryptocurrency and Digital Money Laundering

Nature of the Crime

Stolen funds are laundered through:

e) Cryptocurrency exchanges

f) Mixing and tumbling services

g) Decentralized finance (DeFi) platforms

h) NFT wash trading

[12] No. 19-CR-259 (W.D. Pa. 2019).

Economic Impact

i. Undermines AML and KYC frameworks ii.Enables terrorism financing iii.Makes fund recovery nearly impossible

iv.Weakens regulatory oversight

Case Law

United States v. Ilya Lichtenstein (2022)[13]

The accused laundered over USD 4.5 billion in stolen cryptocurrency, the largest digital asset seizure in U.S. history. The case legally confirmed crypto laundering as full-scale economic cyber crime.

6.Insider-Based Economic Cybercrime

Nature of the Crime This includes:

a) Bank employees leaking credentials

b) Manipulating databases

c) Creating fake accounts

d) Aiding mule networks **Economic Impact :**

i.Direct financial loss ii.Internal trust erosion iii.Severe regulatory sanctions

[13] No. 22-CR-015 (S.D.N.Y. 2022)

Case Law

Cosmos Bank Cyber Fraud Case (India, 2018)[14]

Hackers, with internal assistance, withdrew ₹94 crore in two days using fraudulent ATM and SWIFT transactions across 28 countries. The case highlighted insiderenabled international cyber theft.

7.Stock Market and Algorithmic Trading Manipulation Nature of the Crime :

a) Cybercriminals manipulate:

b) High-frequency trading algorithms

c) Stock price feeds

d) Fake trading volumes

e) Insider trading through hacked data **Economic Impact :**

i. Market instability

ii.Investor confidence loss

iii.Regulatory penalties iv.Billion-dollar volatility **Case Law :**

Securities and Exchange Commission v. Lek Securities (USA, 2017)[15]

The firm was fined for aiding cyber enabled algorithmic stock manipulation, establishing that market hacking is a form of economic cyber crime.

MEASURES TO COMBAT ECONOMIC CYBERCRIMES :

Economic cyber crimes pose a serious threat to financial institutions by undermining financial stability, consumer trust, and national economic security. Due to the transnational, technologically complex, and rapidly evolving nature of cybercrime, traditional crime-control mechanisms are no longer sufficient.A multi-layered strategy combining legal,

[14] FIR No. 0218/2018, Pune Cyber Police Station (India).
[15] No. 17-CV-1789 (S.D.N.Y. 2017).

technological, institutional, and international measures is essential for effective prevention and control.

1. Strengthening the Legal and Regulatory Framework :

A strong legal framework forms the backbone of cyber crime

prevention. Laws must clearly define cyber offences, prescribe stringent punishments, and empower investigative agencies with adequate enforcement powers.

The Information Technology Act, 2000[16] criminalizes hacking, identity

theft, online fraud, data theft, and cheating by personation using digital means.Economiccyber crimes are also prosecuted under the Indian Penal Code, 1860[17], the Prevention of Money Laundering Act, 2002 (PMLA)[18], and the Banking Regulation Act, 1949[19]. However, with the rise of cryptocurrency frauds, deep fake scams, and AI-driven cyber attacks, existing laws require continuous updating.

Special cyber crime courts, fast-track cyber trials, and specialised

cyber prosecutors must be established to ensure speedy justice and deterrence.

2. Strengthening Institutional Cyber security in Financial Institutions :

Financial institutions must treat cyber security as a core governance

obligation rather than a technical support function.

(a) Multi-Factor Authentication (MFA)

Mandatory two-factor or multi-factor authentication for online banking

[16] Information Technology Act, No. 21 of 2000, §§ 43, 66C, 66D (India).

[17] Indian Penal Code, No. 45 of 1860 (India)

[18] Prevention of Money Laundering Act, No. 15 of 2002 (India).

[19] Banking Regulation Act, No. 10 of 1949 (India).

and digital payments significantly reduces account takeover fraud.[4]

(b) Zero-Trust Security Architecture

The zero-trust model assumes no inherent trust in any network user and requires continuous verification. This reduces insider-based cyber fraud and unauthorised access.

(c) Artificial Intelligence-Based Fraud Detection

AI and machine learning systems detect:

i. abnormal transaction patterns
ii.mule accounts iii.SIM-swap fraud
iv.suspicious crypto transfers

These systems enable real-time prevention of fraud before financial loss occurs.

(d) Periodic Cyber Audits and Penetration Testing

Banks must conduct regular vulnerability assessments, penetration testing (VAPT), and cyber security audits to identify weaknesses and prevent systemic breaches.

3. Securing Digital Payment and Banking Infrastructure

Digital payment ecosystems form the primary target of economic cyber criminals. Therefore, securing this infrastructure is vital.

(a) End-to-End Encryption and Tokenization

Encryption protects sensitive banking data during transmission, while tokenization replaces card details with encrypted tokens, preventing card cloning and data theft.

(b) ATM and POS Terminal Security

Banks must deploy:

I. anti-skimming devices

II. EMV chip cards

III. biometric authentication

IV. CCTV surveillance

These measures reduce ATM fraud and POS malware attacks.

(c) SWIFT Security Controls

After the major Bangladesh Bank cyber heist, the SWIFT network introduced strict Customer Security Controls requiring layered authentication and activity monitoring.

4. Regulation of Cryptocurrency and Digital Assets

Cryptocurrencies are widely used for laundering proceeds of economic

Cyber crime due to anonymity and cross-border operability.

(a) Mandatory Licensing of Crypto Exchanges

All virtual asset service providers must be registered with regulators and follow KYC, AML, and transaction reporting obligations.

(b) Blockchain Forensic Monitoring

Advanced block chain tracing tools allow law enforcement agencies to track:

i. suspicious wallet clusters
ii.dark web transactions iii.crypto
mixers iv.ransomware payments

Such tools have strengthened prosecution in major crypto laundering cases.

(c) FATF Compliance

Countries must follow the Financial Action Task Force (FATF)[20] virtual asset guidelines to prevent terror financing and digital money laundering.

5. Strengthening Consumer Protection Mechanisms

Consumers are the most vulnerable targets of cyber fraud. Therefore, public protection is a critical pillar of cyber crime prevention.

(a) Digital Awareness Campaigns

Banks must educate customers on:

I. phishing
II. fake KYC calls
III. SIM-swap fraud
IV. identity theft

Public awareness significantly reduces cyber victimisation.

(b) Mandatory Incident Reporting

Cyber incidents must be reported within fixed timelines to enable quick response. In India, reporting within six hours of detection is mandatory under CERTIn[21] directions.

(c) Customer Liability and Compensation Rules

[20] Virtual Assets and Virtual Asset Service Providers: Guidance for a Risk-Based Approach (2021).
[21] Computer Emergency Response Team–India (CERT-In), Directions under Section 70B of the Information Technology Act, 2000 (2022).

Banks are required to compensate customers for unauthorised electronic

transactions caused due to institutional negligence.This strengthens public confidence in digital banking.

6. Strengthening Law Enforcement and Judicial Infrastructure

Specialisedcyber crime investigation cells, digital forensic laboratories,

and trained cyber police officers are essential for effective enforcement. Digital evidence such as IP logs, malware analysis, transaction trails, and block chain forensics must be legally admissible and scientifically analysed.

7. Strengthening International Cooperation

Economic cybercrimes are inherently transnational in nature. Therefore:

i. Mutual Legal Assistance Treaties (MLATs)
ii.Extradition agreements iii.International cyber task forces iv.Global intelligence sharing platforms

are essential for tracing offenders, freezing digital assets, and securing cross-border prosecutions.

8. Cyber Insurance and Risk Management

Cyber insurance provides financial protection against:

I. ransomware attacks
II. data breaches
III. litigation costs
IV. system restoration expenses

It is now considered a critical component of banking risk management frameworks.

CONCLUSION:

Economic cyber crime has become one of the most dangerous threats to financial stability in the digital age. Combating it requires an integrated approach involving strict legal enforcement, modern cyber security infrastructure, institutional vigilance, consumer education, forensic readiness, and international regulatory cooperation. Without strong preventive mechanisms and swift legal action, cyber criminals will continue exploiting financial systems with devastating economic consequences.

REFERENCES:

1. World Economic Forum, Global Risks Report 2023 (18th ed. 2023).
2. Ross Anderson et al., Measuring the Cost of Cybercrime, 2 J. Cybersecurity 121 (2019).
3. Michael Levi, Cyber Fraud and the Financial Sector, 45 Crime, L. & Soc. Change 89 (2021).
4. Dinei Florêncio & Cormac Herley, The Economics of Cybercrime, 16 Info. Sec. Tech. Rep. 116 (2018).
5. Nir Kshetri, Cybercrime and Global Governance, 32 J. Int'l Pol. Econ. 321 (2019).
6. Daniel Nagaratnam et al., Ransomware Economics and the Financial Sector, 11 J. Fin. Crime 201 (2020).
7. Susan W. Brenner, Cybercrime and the Law (Northeastern Univ. Press 2017).
8. Tyler Moore, The Economics of Online Crime, 12 J. Econ. Persp. 45 (2017).
9. Franklin Allen & Elena Carletti, Systemic Cyber Risk and the Banking Sector, 35 Brookings J. Econ. Activity 157 (2020).
10. State Bank of India v. Shreya Gupta, (2019) SCC OnLine Del 9321 (India).
11. United States v. Albert Gonzalez, 647 F.3d 41 (11th Cir. 2010).
12. Bangladesh Bank v. Federal Reserve Bank of New York, No. 17-CV-10654 (S.D.N.Y. 2016).
13. United States v. Maksim Yakubets, Indictment No. 19-CR-259 (W.D. Pa. 2019).
14. United States v. Ilya Lichtenstein, No. 22-CR-015 (S.D.N.Y. 2022).
15. Cosmos Bank Cyber Fraud Case, FIR No. 0218/2018, Pune Cyber Police Station (India).

16. Securities and Exchange Commission v. Lek Securities Corp., No. 17-CV-1789 (S.D.N.Y. 2017).
17. Information Technology Act, No. 21 of 2000, §§ 43, 66C, 66D (India).
18. Indian Penal Code, No. 45 of 1860 (India).
19. Prevention of Money Laundering Act, No. 15 of 2002 (India).
20. Banking Regulation Act, No. 10 of 1949 (India).
21. Financial Action Task Force, Virtual Assets and Virtual Asset Service Providers: Guidance for a Risk-Based Approach (2021).
22. Computer Emergency Response Team–India (CERT-In), Directions under Section 70B of the Information Technology Act, 2000 (2022).