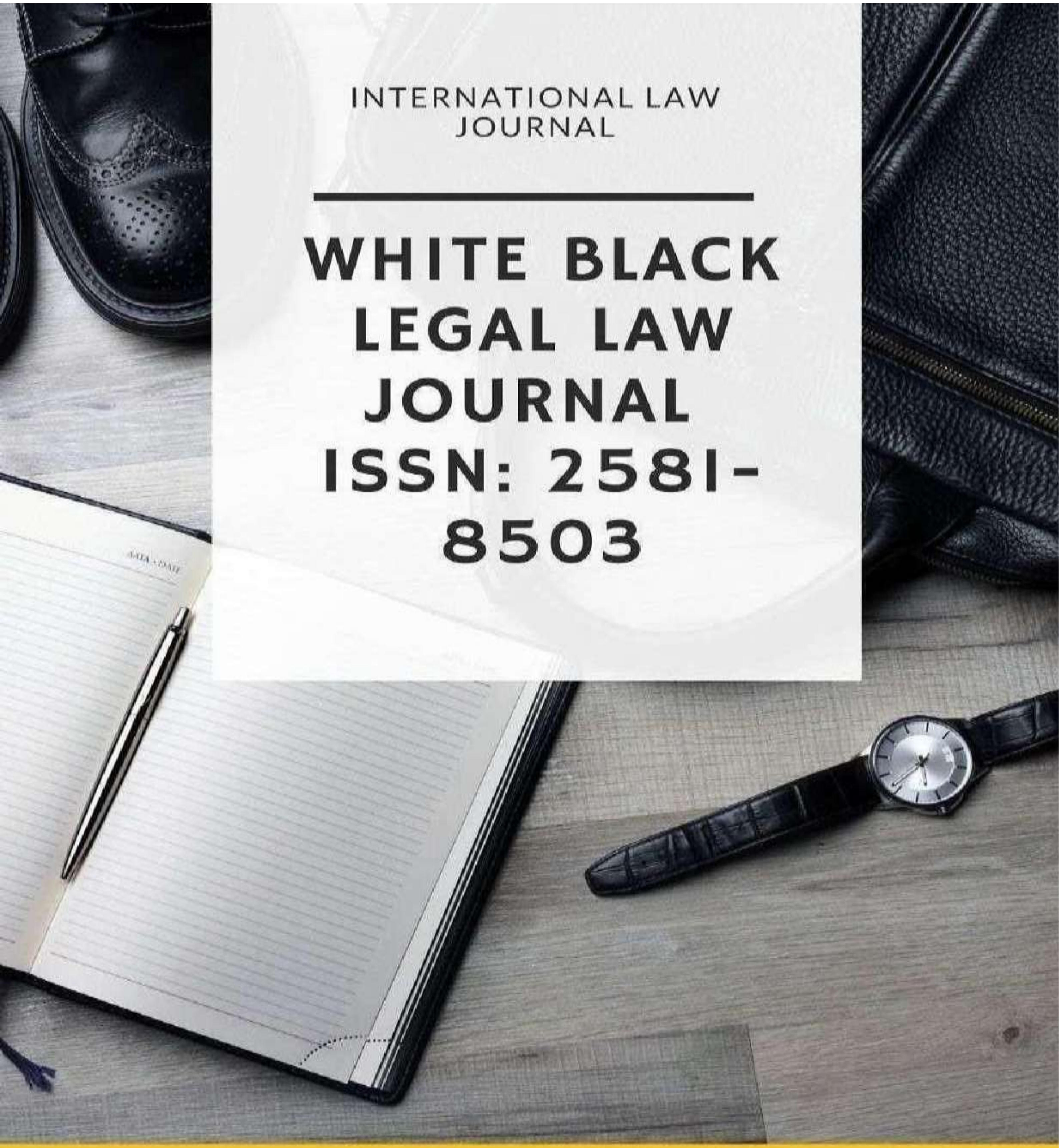

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and
refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

SECURING THE FUTURE OF FINANCE: STRATEGIES FOR PROTECTION AND PREVENTION

AUTHORED BY - CS SIMRANJEET KAUR
Assistant Professor,
Amity University, Mohali,
Research Scholar at Rajiv Gandhi National University of Law

Abstract:

Banking and Financial fraud includes techniques such as phishing, identity theft, card skimming, and malware attacks. All such techniques can lead to substantial financial losses, reputational damage. To mitigate these risks, banking and financial institutions must proactively adopt measures to safeguard customer's privacy and prevent fraudulent activities. Some primary tactics for fraud prevention and protection include the implementation of multi-factor authentication, real-time transaction monitoring, data encryption, employee training on cybersecurity best practices, and collaboration with industry peers to share threat intelligence. Moreover, regulatory compliance with set standards is essential to ensure the safety and privacy of customer information.

By implementing a comprehensive cybersecurity strategy and investing in advanced technologies and employee training, banking and financial institutions can bolster their resilience to cyber fraud and maintain the trust and confidence of their customers. Nonetheless, continuous vigilance and adaptation to emerging threats are paramount to effectively combatting financial fraud in the ever-changing cyber landscape.

Keywords: Banking and Financial Institutions, cybersecurity, cybercriminals, cyber fraud.

INTRODUCTION:

Cybersecurity includes security from cyber-attacks, network security, security from cyber threats, security from hacking, security from password cracking, security from insecure network connections, malicious code or security from malware, firewall security etc.[1] Thus cybersecurity is a mechanism whereby systems, networks and programs are protected from digital attacks. These attacks are usually aimed at accessing sensitive and confidential information for extorting ransom from users via ransom ware and thus disturbing normal business processes. Moreover, with business operations going digital, the threat of cyber-attacks has increased manifold. Effective from 2019 April, the Risk Management Committee of a listed entity which includes banks as well are required by SEBI to discharge function for laying down a framework for identifying the cyber security risks. Additionally, the companies and financial institutions are required to report the cyber security incidents to an agency called Indian computer emergency response team (‘CERT- In’) which is established under section 70 B of Information Technology Act, 2000 and comes under the Ministry of Electronics and Information Technology (‘MEITY’).[2] It is established with an objective of securing Indian cyber space.

Since, the cyber security incidents are so important and material and also relevant for the stakeholders, SEBI vide its notification dated June 14, 2023 inserted regulation 27(2) (ba) in the Listing obligation and disclosure requirement mandating the listed entities to disclose the details of cyber security incidents or breaches or loss of data in its quarterly Corporate Governance report in terms of Regulation 27 (2) effective from July 13, 2023.

In these times of technological innovation and disruption it is, better to be safe than sorry. Without cybersecurity, the Internet of Everything has potential to transform into Internet of threats.

Financial services sector is the foremost engine i.e. the primary driver of economic growth of the country, encompassing wide range of activities such as banking, capital markets, pensions, insurance, etc. The vitality and robustness of this sector are critical in determining the prosperity of a nation's population. It is fair to state that this sector touches the life and stability

[11] Dr Bhagyashree A Deshpande, *Text Book on Cyber Law* (Central law publication, first edition, 2019)

[2] CS Aisha Begum Ansari, *Quarterly Cybersecurity Incident Reporting: SEBI Circular vs. Board Meeting Discussion- An Analysis*155 taxmann.com 77 (2023)

of every individual in our economy. What people deposit in these organization is not just money but aspirations and confidence in the sector to provide security in times of need.

Thus, the strength of this sector is crucial considering high stakes involved. That is why the topic commands heightened importance as these entities of public interest need to take proactively measures to tackle ever-evolving threats.

It is in year 2022, CERT-In handled 1391457 incidents. This included Website intrusion & Malware propagation, Malicious Code, Phishing, Distributed Denial of Service (DDoS) attacks, Website Defacements, Unauthorized Network Scanning/Probing activities, Ransomware attacks, Data Breaches/Leaks and Vulnerable Services.[3]

Drivers behind the rise of cyber attacks in financial service industry

1. The remarkable shift to digital platform from traditional manual processes:

Covid-19 pandemic was one of the factors that led to the digital platform from traditional manual processes. Individuals and businesses embrace digital platform for various transactions and communications, which can attract cybercriminals. Moreover, many people are not aware about the risk associated with the digital transactions eg. Operational risk, security risk, reputational risk, legal risk, transnational risk and various other types of risks.[4]. With proliferation of smart phones, online banking, e- commerce and digital payment systems are becoming increasingly used for daily activities. Moreover, cybercriminals are constantly developing new techniques and strategies to bypass the security measures and thus posing threat to individuals.

2. Emergence of Neobanks leading to disruption of financial markets:

Neobanks are a type of bank that operates digitally. The global neobank market was worth USD 18.6 billion in 2018 and is expected to accelerate at a compounded annual growth rate (CAGR) of around 46.5% between 2019 and 2026, generating around USD 394.6 billion by 2026.[5] India's fifth largest private sector bank – Yes Bank, has partnered with fintech startup NiYO to launch "Yes Bank NiYO Benefits Card" which will help organisations in handling

[3] Government of India, Report: *Enhancing Cyber Security in India* (Ministry of Electronics and Information Technology, 2022)

[4] Talat Fatima, *Cyber Crimes* (Eastern Book Company,2nd edn. 2018)

[5] https://www.pwc.in/industries/financial-services/fintech/fintech-insights/neobanks-and-the-next-banking-revolution.html (Visited on March 3, 2024)

employee benefits and enable employees to claim their benefits easily. However, it is pertinent to note that such banks can be targeted by malware or ransomware attacks, where malicious software is used to compromise systems or disrupt operations. Moreover, cyber attackers can gain access to sensitive customer information.

3. **Incentives to attack financial services sector:** Given that financial sector houses majority of money and that is the primary place where we find the fraudsters. Thus, a direct association with money makes the finance sector relatively vulnerable.

Types of Financial Fraud:

1. Phishing: It is considered to be a common enemy of Internet Banking. It is mainly carried out by e-mail spoofing or instant messaging.[6]Cybercriminals use such tricks to get sensitive information, such as login credentials or financial details. It directs the user to fake website appeared like an authentic one. The term ‘phishing’ was first used in respect of a phishing attack in 1996 when hackers tried to steal American online passwords from the online users.[7] Phishing is a term derived from ‘fishing’ in which the fish catcher puts a bait to catch fishes.[8] It is influenced by phreaking. The word originated in the 1960s and 1970s. it basically means exploration and manipulation of the phone network, by individuals known as "phreaks." These individuals exploited the loopholes in the system to make free phone calls, access restricted received by the user apparently originating from a bank asking the victim to dial a phone number authorised to solve their banking problems. Once the number is dialled the user enters account number and PIN.

   Through various awareness programmes phishing attacks were brought down, but fast-Flux is the newly adopted method used by them to increase the life of a phishing attack which is a Domain Name Server (DNS) technique that utilises a network of compromised computers known as a botnet to hide the origin of the content server often referred to as the “mother ship”.

   Drive-by-downloads is yet another technique used by the fraudsters as Trojans are being used to a higher degree to infect user’s system in a phishing attack.

[6] Tan, Koontorm Center, “Phishing and Spamming via IM (SPIM)”.

[7] White Paper, *Phishing, Vashing and Smishing: Old Threats Present New Risks* (September, October, and November 2009) RSA Monthly Online Fraud Report 1.

[8] White Paper, *Phishing, Vashing and Smishing: Old Threats Present New Risks* (September, October, and November 2009) RSA Monthly Online Fraud Report 1

Spear phishing or whaling is a phishing attack which targets employees or high profiles in a business. It is an attempt to urge to divulge his credentials through a link which contains malware. It is in the form of a keylogger capable of stealing anything the user types in his computer. It becomes hard to detect such attacks as apparently it shows that the e-mail etc comes from a well-known source such as employer.

Vishing: IT is also known as phone phishing; it is exploitation of the user's trust in telephone services where the Caller ID spoofing and complex automated systems are used to commit such crime. Here, list of phone numbers are stolen from financial institutions; such caller than warns the consumer that some malicious activity is detected on their credit card or bank account, hence they should make a call to the bank instantly; the moment the consumer makes the call, the unauthorised number ask the consumer to enter the credit card credentials and number; than such unauthorised individual uses the credentials to fraud the user of card.

Smishing: it is also known as SMS phishing, where a person receives a text message that directs the user to call a phone number to confirm his personal information; such message often ask the consumer to visit a website to confirm his account number, this results in stealing his personal information. [9]

Ransome attack: Hacker encrypts your data and then asks for ransom, i.e. the money to retrieve your data or just prevent him from sharing it publicly on the internet.

2. Identity Theft: Criminals steal personal information of individuals so that they can impersonate individuals and have full access to their accounts and thereby commit fraudulent transactions and activities.
3. Card Skimming: Credit card 'double scan' machines can copy information from magnetic strip of the card and this can help in creating new duplicate card for the account.[10] Thus the cyber criminals use such devices which can capture payment card information at ATMs or point-of-sale terminals, thus enabling unauthorized transactions, Practical Cases: Cyber compromises in the financial sector.

Case 1- **Lazarus Group**: A cybercrime group made up of an unknown number of individuals run by the government of North Korea. Their simple modus operandi, apparently in the financial services world is to prevent a user, from going to a central server where all the data

[9] Talat Fatima, *Cyber Crimes* (Eastern Boom Company, second edition, 2016)

[10] Yogesh Barua, *Frauds and Financial Crimes in Cyberspace* (Dominant Publishers and Distributors ,1st edition, 2005)

is stored, make modifications in the bank balances of accounts, and take out outside the jurisdiction, finally doing an ATM cash out through a mule, so that the Kingpin doesn't get caught.

Case 2- **Magecart Syndicate:** It refers to notorious hacker groups that employ online skimming techniques for the purpose of stealing personal data from e-commerce websites, most commonly - customer details and credit card information on websites that accept online pay. This information is further used for unauthorised transactions.

International Co-operation & broad level measures

Today, cyber-attacks are growing in number, frequency and sophistication. To combat this, enterprise level efforts coordinated with macro level multilateral policy action is needed.

Actions taken

- Australia, Netherlands and the United Kingdom government have already taken the very first step with statements which indicate that cyber-attacks from abroad may be treated as unlawful application of coercion or intervention in the domestic affairs of another country. Basically, cyber threat has been taken to a level where it is treated as a cyber war against one country by another.
- Importance of financial services highlighted at top most global platform when in 2017, the G20 warned that cyber-attacks could undermine security and confidence and endanger financial stability of world economy. In year 2023, the issue was addressed by our Hon'ble Minister of Home Affairs – Shri Amit Shah at G20 summit.
- In India there are bodies like NASSCOM and Data Security Council of India that are playing a very important role in fostering the talent in the startup ecosystem and promoting best practices, lobbying government and the private sector collaboration and cooperation and working together.
- Many years ago, when 2nd factor authentication came for Master and VISA cards, India was the first country to be 100% compliant across the globe and it was because of the mandates that were issued by the Reserve Bank of India. RBI sees this as a systemic risk for the banking system and so it always tries to be ahead of the curve in terms of building controls.

Impact of Financial Fraud:

- Financial Losses: Fraudulent transactions and theft result in significant financial losses to the customers and institutions. E.g. data breach at major retailers, where hackers gained unauthorised access to customers credit card information. Credit card ‘double scan’ machines can copy information from magnetic strip of the card and this can help in creating new duplicate card for the account[11].
- Reputational Damage: Incidents of fraud can finish the reputation of banks and financial institutions, leading to a loss of trust among the stakeholders.
- Legal Consequences: Failure to protect stakeholders’ data and prevent fraud can result in legal consequences and regulatory sanctions.

Strategies/ Best Practices for Fraud Prevention and Protection:

- Multi-Factor Authentication/ Two factor authentication: Implementing multi-factor authentication mechanisms/ two factor authentication adds an extra layer of security to verify users' credentials and prevent unauthorized access. The enterprise dealing with consumer financial accounts should protect their accounts from phishing and other malware attacks through stronger user authentication and transaction verification.[12] Keep up-to-date security patches and update release for operating system; Keep up- to date security and update release for application software; Keep up to date antivirus and antispyware signatures to protect against latest malware spreading in the wild;
- Transaction Monitoring/ Encryption of data: Employing machine learning algorithms to monitor transactions and encryption of data so that it remains safe, even if stolen is an important strategy for prevention of fraud. Enterprises should deploy an enterprise security model that combines intrusion detection, firewall, antivirus and vulnerability management systems for maximum protection against malicious code and other threats;[13]
- Employee Training: Providing regular training to employees on cybersecurity best practices and implementing the two guru mantras: firstly, Zero Trust Principle: never

[11] Yogesh Barua, *Frauds and Financial Crimes in Cyberspace (*Dominant Publishers and Distributors, 1st edition, 2005)

[12] White Paper, *Phishing, Vashing and Smishing: Old Threats Present New Risks* (September, October, and November 2009) RSA Monthly Online Fraud Report 1

[13] White Paper, *Phishing, Vashing and Smishing: Old Threats Present New Risks* (September, October, and November 2009) RSA Monthly Online Fraud Report 1

trust, always verify; secondly, Least Privilege Principle: Only give access to those things which are required.

- No Free Lunch Mindset: Do not click on a link embedded within any potentially suspicious email, especially if the email requests personal information. Instead start a new internet session and type the web address of the link into the address bar to ensure that you are now in the legitimate page;
- The two-fold ways to solve this problem of cyber security:
  1. To be defensive or reactive: It involves applying technology systems and making peace with the fact that in case of rainy days, our organisation is insured and thus building a reaction to it.
  2. To build proactive resilience: This is where we all need to air towards. The approach means that, "we have to learn from each of the cyber security incidents proactively and not wait for those incidents to recur in our own respective organizations." For example, there is a ransom ware attack on an ex-organization and you have lost the data. Then, if we at the board level or as accountants or as Auditors should ask –
     a) What if that incident were to happen in our own respective organizations?
     b) How prepared are we to face and overcome such kinds of challenges?

This is what proactive resiliency all about. We have to:

- Learn from what is happening around
- Share that information with our fellow members or professionals on various platforms
- Then, of course to prepare ourselves as well as our clients to face such kinds of cyber threats

In conclusion, addressing the challenges of banking financial fraud in the cyber world requires a multi-faceted approach that combines technological solutions, employee awareness, regulatory compliance, and collaboration among industry stakeholders. By implementing robust cybersecurity measures and staying vigilant against emerging threats i.e. following g the mantra of proactive resiliency “learn, Share and Prepare” to ensure confidentiality, integrity and availability of the information stored in our systems. By adopting such banking and financial institutions can effectively protect themselves and their customers from cyber fraud.