Insider Led Cyber Fraud in Indian Banking System

Garima Dahiya

Research Scholar (Pursuing Ph. D. in Deptt. of Management Studies from Deenbandhu Chhotu Ram University of Science & Technology, Murthal, Sonipat)
under the guidance/ supervision of Prof. Rajbir Singh

ABSTRACT

Employees, contractors, and other "insiders" pose a significant threat as they have access to their employers' systems and databases and can circumvent security measures through legitimate means. The paper focuses on the threat insiders pose to the banking industry given the surge in online transactions. The research explores the basis of insider frauds viz., human error and rogue employees. The study further states the impact of such crimes in bank. Finally, it concludes with the measures to be taken to mitigate the impact of such crimes.

INTRODUCTION

The surge in number of banks is a positive development as it increases public awareness and access to banking services.However, this rapid expansion has stretched regulators to the hilt, weakened the effect and scope of regulatory oversight and eased the standards of accountability and corporate governance (Ikpefan O. A. and Odularu G.O., 2007).This has made the industry more vulnerable to insider abuses, bad practices, and executive self-indulgences such fraudulent procurement scams, staff deception, earnings manipulation, and the dishonest diversion of bank capital by boards and top management, among other things.(Anya A.O., 2003) states that financial fraud and other economic crimes involve intentional use of deceit, asset theft/ misappropriation by company directors and others in fiduciary positions or an employee, to deprive another of money, property or a legal right, for their own benefit. These fraud acts, not only incapacitate the banks' effective delivery of their economic functions but, also, pile pressure on the nation's scarce foreign exchange resources with no visible economic benefits being transmitted to the productive sector of the economy and the general public.

The RAND reportaddresses insider threat as "malevolent (or possibly inadvertent) actions by an already trusted person with access to sensitive information and information systems" (Anderson R. H. and Brackney R.,2005).The Institute of Internal Auditors (2009) defines fraud as: "Any illegal act characterized by deceit, concealment, or violation of trust. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage." Fraud impacts organizations in several areas including financial, operational, and psychological. One of the most challenging aspects in the Indian banking sector is to make banking transactions free from the electronic crime (Pasricha P. and Mehrotra S., 2014).Over the past 50 years, even sophisticated markets and banking systems have had severe bank collapses and crises due to fraud and scams.

The growing reliance on technology in the current cyber environment, leave organisations vulnerable to the dangers of cybercrime. Some of the largest cybercrimes in recent years have been committed in India, including cases where banks were duped by the illicit activities of their own reliable staff members. One notable instance is Citibank Mphasis BPO becoming a victim of cybercrime and suffering a significant financial loss due to the greed of its own employees. Internal cyber risks stemming from employee misuse of sensitive personal data entrusted to them at work is one of the major concerns of modern information technology society. Employees working for such institutes are more likely to breach the system than outside criminals because they are more knowledgeable about the technical architecture and safety precautions put in place to avoid cybercrimes. Disgruntled employees are another group of people who might commit cybercrimes. They could exploit stolen information to disrupt or lose business. Insider threats pose significant security risks to financial institutions' monetary assets and sensitive consumer data.

Modern banks keep a wealth of personal and financial information about its customers. From Aadhar numbers, PAN numbers, addresses, and cellphone numbers to income tax returns, spending patterns, average monthly expenditure, property registration paperwork, and so on. In sum, as clients, we trust banks with every piece of information we share. However, this may not always be true. Banks, like all other organisations, are vulnerable to insider threats. In the cyber ecosystem, an insider threat is defined as malicious personnel of a business that steal, damage, or expose internal data or systems of the organisation to which they belong. At times, a malicious insider may be solely responsible for the data breach.A total of 5,785 bank employees were charged with fraud in 2015, which came down to 4,360 in 2016. It further fell to 3,804 cases of individual bank frauds in 2017 (“SBI took action against 1,287 officials over fraud in past three years.” 2018)

In December 2019, an incident involving bank staff stealing client data came to light. The Sharmrao Vithal Cooperative (SVC) Bank filed a FIR in Thane's Srinagar police station for criminal breach of trust and data leak against two current employees and one retired employee. This FIR was filed under Section 408 (criminal breach of trust by clerk or servant), Section 109 (punishment for abetment if the act abetted is committed in consequence and no express provision is made for its punishment), and Section 34 (Common intention) of the Indian Penal Code, 1860, as well as Section 43A (Compensation for failure to protect data) and Section 66 (Computer-related offences) of the Information Technology Act, 2000.The bank, which has 198 branches in 10 states, filed the case on December 12, 2019, through its managing director, Ajit Venugopalan. The accused have been named as PS Shinde, RM Satam, and SN Kubal. It is worth noting that the former employee, SN Kubal, was also the general secretary of the employees' union, and he was fired in November 2017 for misbehaviour.In August 2018, the Pune branch of Cosmos bank was drained of Rs 94 crores, in an extremely bold cyberattack. By hacking into the main server, the thieves were able to transfer the money to a bank in Hong Kong. Along with this, the hackers made their way into the ATM server, to gain details of various VISA and Rupay debit cards.

Former and current employees, as well as directors of companies with cruel intents stand for threats to businesses and organizations. This is especially so given the tendency of some groups of individuals to commit illegal acts deliberately for a variety of reasons such as quest to get rich quick, job dissatisfaction, job insecurity, fear of disengagement, hostile working environment and conditions, and/or manipulation by others seeking to exploit access to confidential business information (Omar M., 2015). Insider threats can be in form of fraud, system sabotage, theft of valuable data or information and/or information system assets/network (Cummings A., Lewellen T., Mclntire D., Moore A. P. and Trzeciak R., 2012).As banks adopt IT innovations to improve service delivery, malicious insiders have shifted their focus from loan abuse to electronic payment channels, with a focus on user privilege abuse and theft of personal information (PII). Banks have suffered significant financial losses due to fraudulent actions over time.

Uttar Pradesh cyber police detained techies and a former bank employee in connection with an illicit withdrawal of Rs 145 crore from the Cooperative Bank's account in Lucknow. Another allegation alleges that an Android spyware known as Drinik, which operated under the guise of the Income Tax Department of India, targeted 18 banks in the country. Similarly, a carding website on the dark web called BidenCash rose to prominence after hackers posted the credit card information of over nine million people for free on the site. Data analysis revealed that the majority of compromised cards originated in the United States. However, a large data dump began in India, the United Kingdom, Brazil, Mexico, Turkey, Spain, Italy, and China.

The Indian Banking Finance Services and Insurance (BFSI) sector has been at the forefront of cyber-attacks directed at the Asian area. Even government records show a dramatic rise in attacks on the banking and financial sectors. Between June 2018 and March 2021, India's banks saw 248 successful data breaches by hackers and criminals, the central government informed Parliament on August 2. Among the 248 successful data breaches, 41 were reported by public sector banks, 205 by private sector banks, and two by international banks. CloudSEK, a Singapore-based cyber security business, stated in its Whitepaper that 7.4% of targeted attacks in 2020 were directed against the Indian subcontinent. Whether it is for nationalised banks, cryptocurrency exchanges or wallets, NBFCs, or credit card informationleaks, India has emerged as the newfound hotbed for cyber-attacks in Asia.

LITERATURE REVIEW

(Jeffords R. et al.1992) evaluated 910 instances reported to the "Internal Auditor" between 1981 and 1989 to evaluate the specific risk indicators mentioned in the Treadway Commission Report. Approximately 63% of the 910 cases are classed as internal control concerns. Similarly, (Calderon T. and Green B. P., 1994) conducted an investigation of 114 genuine examples of corporate fraud reported in "Internal Auditor" between 1986 and 1990. The investigation discovered that professional and managerial personnel were involved in 45% of the incidents. In his case study, (Willson R., 2006) looked at the factors that contributed to Barring Bank's failure. Baring Banks' management, financial, and operational controls failed, resulting in the collapse.

According to (Albrecht W. S., 1996), the signs of inadequate internal controls enhance the chance of fraud. Internal control symptoms include a bad control environment, absence of segregation of roles, physical safeguards, independent checks, authorizations, documents and records, overriding existing controls, and an inadequate accounting system.
(Beirstaker J., Brody R. G., and Pacini C., 2005) offered several fraud prevention and detection methods. Various techniques are used to combat fraud, such as policies, telephone hotlines, employee reference checks, vulnerability reviews, vendor contracts, financial ratio analysis, password protection, firewalls, software analysis, and discovery sampling.

(Ganesh A. and Raghurama A., 2008) surveyed 80 executives from Corporation Bank and Karnataka Bank Ltd in India to assess their subordinates' skill improvement before and after similar training programmes. Results showed statistically significant improvement in the 17 highlighted skills. The paired t-test was used for each of the seventeen talents, and all demonstrated statistical significance. In (Khanna A. and Arora B., 2009) conducted a study to identify the causes of bank fraud and install preventive security controls in the Indian banking system. The study tries to evaluate the many causes of bank fraud. According to the findings, bank fraud is primarily caused by inadequate training, overwhelmed staff, competitiveness, and low compliance levels.

(Yang S. and Wang Y., 2011) said authorised insiders (e.g. employees, clients, vendors, contractors, partners, customers) with authorised credentials (username, password, and token) have access to the information system and network, allowing malicious individuals to compromise its confidentiality, integrity, and availability.

(BamraraA. et al. 2013) explored various types of digital assaults and prevention measures in India. The study relied on vital information. The investigation examined 100 cases of digital malfeasance and 50 bank employees. The study examined the methods used by digital fraudsters to target certain banks and found a correlation between general population and private sector banks in various types of digital fraud. The study used measurable methods such as Chi-Square and Karl Pearson's Coefficient of Connection to identify relationships between variables. The study found no significant difference in the techniques used to detect electronic fraud in public or private institutions. The study identified a strong link between gatecrasher recognition and digital assaults.

(Siddique M. I. and Rehman S. 2013) conducted a calculated analysis on various types of savings fraud, including IRS avoidance, digital fraud, and card-related fraud. The study analysed the impact of digital fraud on Indian savings and identified factors such as complex frameworks, human error, lack of evidence, and information instability. They offer preventive ways to control digital wrongdoings, such as adopting new technology and establishing reliable workers and devices.

(Soni R. R. and Soni N., 2013) conducted a comparative analysis of digital fraud in Indian open and private banks. The study relied on data from the Store Bank of India's distribution channels. The study focused on two types of examinations: examining the same segment banks and comparing different area banks. The data was analysed for 27 open area banks (including SBI and its partners, cooperative banks), 14 private sector banks, and 6 remote division banks. The study found that private and external banks have a higher risk of fraud related to e-banking, credit and debit cards, and other online transactions. The main reason for cheating is the lack of innovation in saving methods.

INTERNAL CYBER RISK

Employee actions or inactions provide dangers to businesses for a variety of reasons, including:

Employee human error: This includes accidentally delivering sensitive information or personal data to the incorrect recipient. Furthermore, there is the issue of system misconfiguration, in which sensitive information is not adequately secured, encrypted, or password protected, allowing unauthorised access.

It is also vital to address the loss of gadgets or papers containing sensitive data.In the context of security, human mistake refers to inadvertent activities - or inaction - by staff and users that originate, spread, or allow a security breach to occur. This includes a wide range of acts, from downloading a malware-infected attachment to neglecting to use a strong password, which is one of the reasons it can be tough to solve.

The key to decreasing such hazards is to raise awareness of data security threats through real-world examples and to provide staff with the skills necessary to mitigate them. While it is impossible to totally eliminate human error, it can be significantly minimised via effective staff education and regular training.

A recent government poll found that only 14% of enterprises claimed that they offered cyber security skills training to staff, even though training is more typical in larger organisations.

Types of human error:

- **Skill-based errors**: Slips and lapses are tiny errors that occur when executing familiar jobs and activities. In these circumstances, the end-user is aware of the proper course of action but fails to take it owing to a short lapse, mistake, or neglect. These could occur because the employee is fatigued, not paying attention, is distracted, or has a temporary lack in recollection.
- **Decision-based errors**: Decision-based errors occur when a user makes an incorrect decision. This can be caused by a variety of circumstances, including the user's lack of understanding, insufficient information about the unique situation, or even not recognising that they are making a decision through their inaction.

Examples of human error:

- **Misdelivery**: Sending anything to the wrong recipient is a common vulnerability in corporate data security. According to Verizon's 2018 breach report, misdelivery was the seventh leading cause of cyber security breaches. Many individuals rely on email programmes' auto-suggest features, making it easy for any user to mistakenly send personal information to the wrong person if they aren't vigilant.
  One of the most catastrophic human error-related data breaches occurred when an NHS practice exposed the email addresses (and hence names) of over 800 HIV clinic patients. How did the error occur? The employee sending an email notification to HIV patients unintentionally placed their email addresses into the "to" area rather than the "bcc" field, exposing their information to one another. This is a classic example of a skill-based error, since the employee understood the right thing to do but didn't take the time to double-check that they were doing it correctly.
- **Password Problems:** Humans and passwords just don't get along. The findings from the National Centre for Cyber Security's 2019 report paint a bleak picture: 123456 remains the most used password in the world, with 45% of users using their primary email account password on other services. In addition to not setting strong, unique passwords, untrained users make other password blunders, such as putting passwords on post-it notes on their monitors or sharing them with coworkers.
- **Patching:** Cybercriminals are continuously seeking for new software exploits. When exploits are discovered, software developers work quickly to address the vulnerability and distribute the patch to all users before cyber criminals may compromise new people. This is why it is critical that users install security updates on their computers as soon as they become available. Unfortunately, end users frequently postpone the installation of updates, with disastrous consequences.

The 2017 WannaCry ransomware assault infected hundreds of thousands of systems globally, costing businesses and organisations millions of dollars in damages. However, Microsoft patched the flaw exploited in the attack, called 'EternalBlue', months before the strikes occurred. If the affected computers had just downloaded and implemented the security update, they would not have been infected.

Physical security error: While cyber attacks are the most common cause of data breaches, organisations are also vulnerable to physical dangers. Unauthorised individuals who obtain access to secure locations have the potential to steal or view confidential information and credentials. Physical security failures take many forms, but one of the most common is leaving important documents unattended on workstations, meeting rooms, or even printer output trays. Anyone who gains access to the firm premises can simply pick up the paper, and no one will notice that it has gone missing. Allowing tailgating is another very typical physical security issue. Tailgating occurs when an unauthorised person follows someone through a protected door or barrier, typically by strolling closely behind them.

Rouge employees: In contrast to the previous section, this refers to purposeful wrongdoing by an employee who has access to and/or is knowledgeable with the company's IT systems. For example:In 2018, a Cisco engineer was accused of causing $1.4 million in damages by gaining unauthorised access to the company's cloud infrastructure and deploying malicious code that erased 456 virtual machines used for Cisco's WebEx Teams product.In the United Kingdom, in 2013, an IT auditor at Morrisons Supermarkets committed a data breach by posting almost 100,000 employees' payroll data to the internet after being subjected to unrelated disciplinary proceedings.

Types of Employee Mindset That Encourages Crime:

- **Anonymity**: Employees may believe their online behaviours are untraceable or anonymous, leading to increased risk-taking or reckless behaviour. This sense of invisibility may encourage employees to behave in ways they would not typically do if their identity was known.
- **Entitlement:** Employees who feel underpaid or unappreciated may justify squandering company resources. This could range from squandering business time for personal purposes (i.e., cyberloafing) to outright theft of data or IT resources.
- **Revenge:** Employees who feel wronged by their workplace may resort to cybercrime or deviance as a means of vengeance. This could appear as data theft, sabotage, or the propagation of malware.
- **Thrill-seeking**: Some employees may engage in cybercrime or deviance for the excitement of it, seeing it as a challenge or game. This could result in high-risk actions such as unauthorised access and hacking.

FACTORS WHICH FACILITATE INSIDER THREATS

Lack of awareness: One of the primary reasons why employees pose a security risk is that they are unaware of what they should and should not be doing. They may be ignorant that their devices are connected to an insecure Wi-Fi network, or that they should not be storing client information on a USB. As a business, you should evaluate your internal processes and training. Something the GDPR set out to do: protect personal information. When they are unclear where to begin, having an outside company analyse your processes might be a wonderful way to secure your business. This could include completely examining your processes or obtaining ISO certified to improve company security, personnel expertise, and business credentials with new clients.

Phishing emails: Symantec discovered that 71% of all targeted attacks began with phishing scams. Criminals send emails that appear to be from a respectable organisation and request critical information. Often, these include a link within the email that brings one to a highly convincing, false website with a form where you may enter your information. This information is then delivered directly to the criminals who designed the website, allowing them to sell or utilise your information. They may want passwords, credit card information, or usernames, anything they can sell or use illegally.In 2020, India was ranked third globally for phishing attacks, with over 1.5 million reported incidents, according to a report by security firm.During the height of the pandemic, India saw an almost unbelievable 4000% increase in phishing emails.

Signs of phishing emails:

- Addressing you as "Customer" rather than by your name
- Typing or spelling errors
- The 'From' email address does not appear to be who it says it comes from.
- Please open the links or attachments. If it doesn't appear real, don't click any attachments or links.
- If in doubt, contact the sender.

Using unsecured network: Staff may be unaware of the dangers of using any device, business or personal, on an insecure network. This could be free Wi-Fi at a nearby café or on the train to a business meeting. These connections may not encrypt your data, allowing it to be intercepted and misused. When data is transferred in an unencrypted format, such as plain text, it gives hackers access to potentially sensitive and important information. Accessing emails and social media on an insecure network poses a danger of unwittingly leaking passwords or other personal information. While using a banking app, you risk exposing your bank accounts to crooks who hack the network.

Viruses and malicious software can also spread easily across several devices, creating the framework for DoS or DDoS attacks on websites or networks. More recently, Symantec, a cyber security software vendor, has reported an 8500% surge in currency miner malware, and an unsecured network is one entry point.

- **Storing sensitive data:** Personal or business sensitive information should never be stored on external hard drives, USBs, or printed out for use outside of the office. GDPR regulation has been implemented to ensure that all personal data is properly protected, however having it on a portable device or printed puts it at danger.
- **Installingillegitimate apps and programs:** Every day, thousands of malware-infected programmes are posted to mobile devices, browser extensions, and new programmes. Apps and extensions from reputable sources are continually monitored to ensure they are not harmful, although some do slip through the cracks. These apps can be doing a range of activities in the background of your device, from collecting data and leaking cell numbers, to infecting other devices on the same network.
- **Not updating software:** This is a common reason for leaving your networks and devices vulnerable to hackers. System updates and upgrades are typically performed to not only improve the usability or design of the programme, but also to incorporate new security elements to safeguard it from future attacks. Employees may be unaware that by failing to keep up with system changes, they are leaving themselves vulnerable to attacks. To improve firm security, update any software you use on a regular basis. It can be costly and difficult to break out of this scenario.
- **Lack of cyber security culture:** An institute that does not prioritise cybersecurity may unwittingly encourage criminal and deviant behaviour. Employees may be unaware of the gravity or potential consequences of their conduct in the absence of appropriate policies, training, and awareness programmes.
- **Poor communication:** Employees may not comprehend the need of adhering to cybersecurity protocols if communication inside the organisation is weak, or they may be reluctant to report suspicious behaviour. A culture that values open communication can assist to reduce these dangers.
- **Extended stress environment:** organisationsthat establish and maintain high-stress work conditions may motivate people to behave in ways they would not otherwise. Constant stress can lead to poor decision-making and make employees more likely to commit cybercrime.

IMPACT ON BANKS

- **Technical Risk:** IT infrastructure is a highly valuable target. A breach poses a substantial danger to operational control and data integrity, with significant time, financial, and reputational costs. The resulting operational interruption might cause delays in service delivery for the company, leading to a loss of customer and client confidence**.**

- **Financial risk:** In addition to the expenditures and expenses that are involved in reacting to a cyber-attack (such as the cost of recovering IT systems) there is also business disruption loss or the cost of making a potential ransom payment. Organisations may also face regulatory fines and penalties if a cyber-attack results in a data breach.
- **Litigation Risk:** banks can be found liable by the courts for data breaches of their employees.
- **Reputation Risk**: A cyber breach can potentially harm an organization's brand and lead to a loss of trust in the firm. This is especially true if the breach appears to have been avoidable. According to a poll, 85% of customers are inclined to tell others about their data breach experience.

STEPS FOR EMPLOYERS TO ADOPT MITIGATE RISKS

- **Provide regular cybersecurity training**: Educating your staff on the newest cybersecurity dangers and best practices is critical for engaging them in cybersecurity.
- **Create a cybersecurity culture:** Your company's culture should reflect the fact that cybersecurity is everyone's responsibility. This can involve making cybersecurity a regular topic of discussion and fostering a climate in which, employees feel comfortable asking questions.
- **Set clear expectations:** Make it clear what your cybersecurity policies are and what employees should do to protect company information.
- **Highlight the significance of passwords:** Ensure that staff understand the necessity of secure passwords and provide instructions for setting them. Require staff to utilise multi-factor authentication to protect firm data.
- Require staff to utilise **multi-factor authentication** to protect firm data.
- **Implement access control**s: Limit access to firm data to those who need it, and make sure the staff understands the necessity of keeping their access information secure.
- Encourage employees to **report questionable activities** by providing explicit guidelines on how to do so.
- **Develop a cybersecurity incident response plan:** Have a plan in place for responding to a cybersecurity event, and make sure all staff is informed of it.
- **Reward cybersecurity-conscious behaviour:** Recognising employees who take precautions to secure firm data can go a long way towards inspiring others to do the same.
- **Lead by example.** Finally, as a leader, you must model the cybersecurity behaviour you want to see in your workforce**.**
- **Clarify the business risk:** Leadership must explain the impact of a data breach on the company's financial outcomes, customer connections, and reputation.
- **Align with ideals and culture:** Data protection is not only the duty of IT; it is the responsibility of everyone in a business. Ensure that you have systems in place for employees to express issues, especially during times of corporate upheaval.
- **Employees should be directly involved in the solution development process**: Our analysis revealed that millennials, in particular, are inspired by direct involvement in problem solving, therefore solicit their assistance in developing techniques that would appeal to their peers.
- **Collaborate with the compliance and IT teams:** Technology or compliance training for cyber security should be preceded by awareness efforts that emphasise the business's necessity.

CONCLUSION

But it is not all doom and gloom. Despite the obvious hurdles, organisations are attempting to address the issue of risk from inside. Training individuals and bringing in additional dedicated staff to help enforce security regulations is a natural solution to the problem of employee negligence. And it's the solution that many firms around the world are striving to apply. Having security procedures in place is insufficient. To assist reduce staff carelessness or dangers caused by misinformed workers, the appropriate balance of policy and engagement should be struck.Staff training is crucial for raising awareness and inspiring employees to prioritise cyberthreats and countermeasures, even if it is not part of their job responsibilities. Installing updates, ensuring anti-malware protection is turned on, and correctly maintaining personal passwords should not always be at the bottom of an employee's priority list.

Employee understanding of cybersecurity is a crucial component of every organization's security strategy. Employees who are unaware of the hazards and threats that exist in the internet environment may find it difficult to protect the company's assets and data. Organisations must undertake measures to raise employee awareness of cybersecurity in order to guarantee that staff is knowledgeable and appreciate its importance. Regular training sessions and workshops are one of the most effective ways to raise staff awareness about cybersecurity. These workshops should include security issues such as phishing, malware, data protection, and social engineering. It is critical that these sessions are dynamic and interesting so that employees can learn from them. Organisations should also consider rewarding staff to follow excellent security practices. This can be accomplished through awards, recognition, or even bonus points that can be exchanged for goodies. Organisations can help guarantee that all members of the workforce take security rules seriously by motivating them to obey them.

Finally, organisations should foster an open climate in which employees may communicate security concerns without fear of penalties. This can be accomplished by allowing employees to share their concerns and suggestions with management or other members of the security team. Employers could also consider establishing anonymous feedback polls or forums where employees can voice their opinions and suggestions on security issues without fear of consequences.

To combat cybercrime, it is necessary to address it both before and after the crime occurs. Organisations could consider preventive measures to combat these crimes, such as establishing an internal vigilance system, conducting periodic system reviews by corporate houses, and educating employees about the occurrence of such crimes and the legal consequences of engaging in such offences, such as under the IT Act and the Indian Penal Code. Furthermore, organisations must take steps to limit risks by getting proper insurance coverage against liabilities resulting from cybercrime. However, nothing can replace the necessity for a complete regulation dealing with data protection, data theft, and piracy, which will also result in achieving a "Data Secure Status" for India.

REFERENCES

[1]. Albrecht W.S. (1996). Employee fraud. Internal Auditor, October, p. 26

[2]. Anderson R. H. and Brackney R. (2005 March). “Understanding the insider threat.” RAND Corporation. [Online]. Available: http://www.rand.org/pubs/conf proceedings/CF196.

[3]. Anya, A. O. (2003). Corporate governance as an effective tool for combating financial and economic crimes. The Nigerian Banker, October-December, 32 – 36.

[4]. Bamrara A. Singh G.& Bhatt M. (2013), Cyberattacks and defence strategies in India- An Emperical assessment of Banking Sector. International Journal ofCyber Criminology, Volume 7 issue. 1, p- 49- 61.

[5]. Bierstaker J., Brody R.G. and Pacini, C. (2006). Accountants‟ perception regarding fraud detection and prevention methods. Managerial Auditing Journal, Vol. 21, No. 5, pp 520-535.

[6]. Calderon T. and Green B. P., 1994. Internal fraud leaves its mark: Here’s how to spot, trace and prevent it. National Public Accountant, 39(2): 17-20.

[7]. Cummings A., Lewellen T.,Mclntire D., Moore A. P., and Trzeciak R. (2012). Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector. Carnegie Mellon University USA.

[8]. Ganesh A. and Raghurama A., 2008. Status of training evaluation in commercial bank- a case study. Journal of Social Sciences and Management Sciences, 37(2): 137-158.

[9]. Ikpefan, O. A. &Odularu, G.O. (2007). Using money laundering Act as a tool for monitoring deposits and frauds in the Nigerian banking industry: An empirical approach. The Nigerian Banker, April – June.

[10]. Institute of Internal Auditors (2009). International professional practices framework. USA: The Institute of Internal Auditors.

[11]. Jeffords, R., M.L. Marchant and P.H. Bridendall, 1992. How useful are the tread way risk factors. Internal Auditor, 49(3): 60-61.

[12]. Khanna A. and Arora B. (2009). A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry.International Journal of Business Science and Applied Management, Vol. 4, No. 3

[13]. Omar M. (2015). New Threats and Countermeasures in Digital Crime and Cyber Terrorism. Nawroz University Press, Iraq. 297.

[14]. Pasricha, P. and S. Mehrotra (2014). Electronic crime in Indian banking. Sai Om Journal of Commerce and Management, 1(11): 7-14.

[15]. SBI took action against 1,287 officials over fraud in past three years (2018, Dec 17). Business Today.

[16]. Siddique M. I.& Rehman S. (2011), Impact of Electronic crime in Indian Banking Sector – An Overview. Int. J Busi. Inf. Tech. Vol. 1, No.2, p-159-164.

[17]. Soni R.R. and Soni N. (2013), An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks. Research Journal of Management Sciences. Vol. 2 Issue 7, p- 22-27.

[18]. Willson R., 2006. Understanding the offender/environment dynamics for computer crimes. Information Technology and People, 19(2): 170- 186.

[19]. Yang, S. and Wang, Y. (2011). System Dynamics Based Insider Threats Modelling. International Journal of Network Security and Its Applications (IJNSA), 3(3), 1-13.