SURVEY ON ELECTRONIC FRAUD CASES IN THE BANKING INDUSTRY USING DIGITAL FORENSICS

Atharva Kokate (18BCE0709), Arya Abrol (18BCE0691)
Vellore Institute of Technology, Vellore (2020).

ABSTRACT

As technology advances, criminal minds are evolving and are turning towards new ways of attacking banks and financial institutions. These institutes are now vulnerable to several information security threats. There is a sudden rush in the number of cyber-attacks, causing unrest in institutions. Issues related to legal, regulatory, and privacy compliance are constantly endangering these institutions. Considering the situation, an ideal approach will be to focus on the detection of attack and reduction of cyber security risks across multiple channels. The lack of proper forensic analysis tools and incident management can adversely affect an institution by increasing the downtime and the investigation expenses. Also this results in a lack of evidence collection leading to ineffective investigation. The ability to identify, investigate, and mitigate such security incidents, while ensuring legal and regulatory compliance, has thus become an organizational imperative.

Keywords: Digital Forensics, Cyber Security, Cyber attacks, Banking.

1.1 INTRODUCTION

Banking institutions are facing a challenge with increased incidents of frauds and phishing mails thereby directly affecting their bottom-line and increased cost of compliance. With increased regulatory surveys, banks are under greater pressure to implement best security practices. Compliance is therefore not an option but a necessity. From the report of **Deloitte's India Banking Fraud Survey 2012**, we found that almost 93% of customers of these institutions believe that fraud incidents have increased in the banking industry. Also the survey says that there is more than 10 Lakh of average loss per incident for nearly half of the respondents. Now our focus will be towards exploring the possibility of reducing electronic fraud cases using digital forensics in banking institutions and examining digital technologies being used on the electronic fraud prevention and detection in the banking industry.

1.2 PROBLEM ANALYSIS

1.2.1 UNDERSTANDING PROBLEM BY A CASE STUDY

A hypothetical case study will help in understanding the role of digital forensics in the banking institution:

An employee at Bank A takes a leave of 2 weeks. After he leaves, the bank gets multiple complaints about receiving fraud calls and messages demanding sensitive information. The

bank hires a digital forensic investigator to gather evidence from the employee's personal computer who is suspected by the company. All the information in the PC's disk is collected and conserved using robust procedures. Recovery of several deleted files and data that shows emails sent to users act as evidence against the suspect. The detailed audit and records are given to Bank A, and proper counsels are held with legal advisors from the company, and a police complaint is filed under cyber-security laws.

1.2.2 PURPOSE / OBJECTIVE

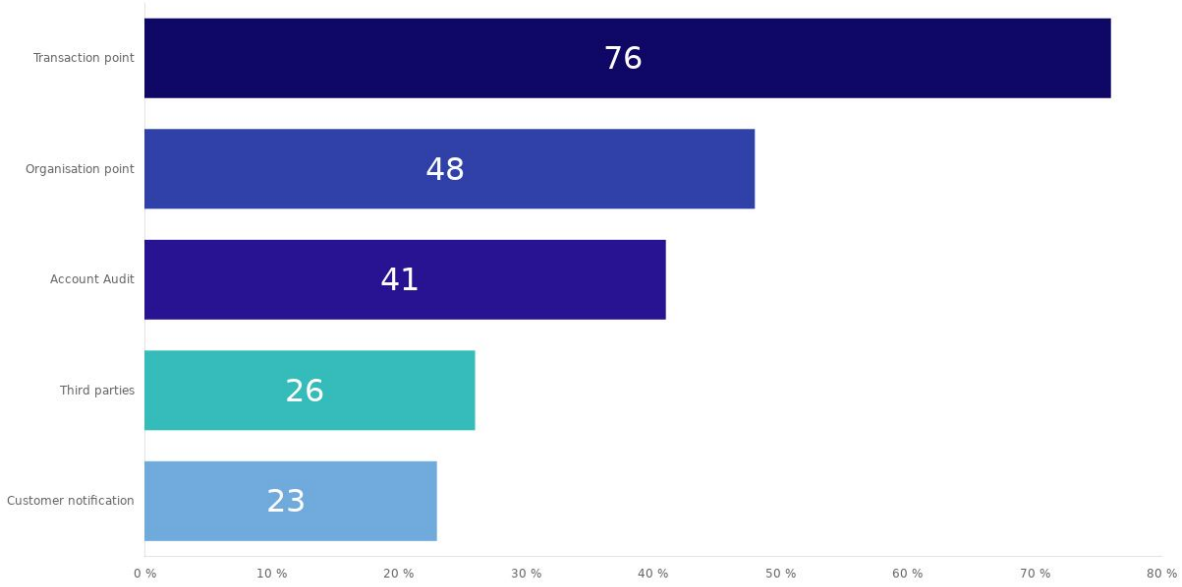
The objective of the survey is to :

- to explore the possibility of reducing electronic fraud cases using digital forensics in the banking industry,
- to examine digital technologies being used on electronic fraud prevention and detection in the banking industry.

1.2.3 FINDINGS

According to a survey (Shewangu Dzomira, 2014):

- A total of 76% of the respondents get to know about frauds from customer notification.
- 48% indicated that they detect fraud at the transaction point
- 41% of the respondents showed that they get to know of the fraud incidents from third party notification.
- 26% of the respondents revealed they learn about fraud incidents using detecting techniques tools
- 23% of the respondents indicated that during account audits or reconciliations that is when they know discover the fraud incident.



Deloitte's (2013) survey found that the major prevention mechanisms are regular training on financial crimes' trends and risks, continuous employees' activities monitoring in high-risk departments, technology solutions, and financial crime control mechanisms.

2.1 METHODOLOGY

After referring to the various studies and researches on the digital forensics tools and technologies for electronic fraud risk management, we are considering the following facts: The study was based on descriptive research. The purpose of descriptive study is to describe the characteristics of phenomena, relations between variables or relationships between phenomena and can be the purpose of qualitative and quantitative studies (Plooy-Cilliers et al, 2014). The descriptive study is popular in research because of its versatility across management disciplines (Cooper & Schindler, 2011). Descriptive research is intended to merely describe a phenomenon and the researcher does not manipulate any variables and makes no effort to determine the relationship between variables (Brink et al., 2012). In this study the use and application of digital forensic tools to combat the risk of e-fraud in the banking industry forms the phenomenon. The primary data was collected on the basis of self-completion questionnaires and interviews administered to various respondents from different banks. According to Bryman & Bell (2003), a self-completion questionnaire, respondents answer questions by completing the questionnaire themselves.

2.2 REFERENCES

1. Shewangu Dzomira (2014) Digital Forensic Technologies as e-fraud risk mitigation tools in the Banking Industry: Evidence from Zimbabwe, Journal Risk governance & control: financial markets & institutions
2. ACI, (2013), Fighting online fraud: An Industry perspective. Vol. 3, www.aciworldwide.com
3. ACL, (2013), Detecting and Preventing Fraud with Data Analytics. www.acl.com
4. ACL, (2014), Fraud Detection Using Data Analytics in the Banking Industry. www.acl.com