INSIDER THREAT PREVENTION IN THE US BANKING SYSTEM

Oghenekome Efijemue[1] Ifunanya Ejimofor[2] and Omoshola Simon Owolabi[3]

[1]Department of Computer Science, Austin Peay State University, Clarksville USA.
[2]Department of History and Philosophy, Austin Peay State University, Clarksville USA.
[3]Department of Data Science, Carolina University

ABSTRACT

Insider threats have been a major problem for the US banking sector in recent years, costing billions of dollars in damages.

To combat this, the implementation of effective cybersecurity measures is essential. This paper investigates the current state of insider threats to banks in the U.S., the associated costs, and the potential measures that can be taken to mitigate this risk. The development of a framework for the adoption of cybersecurity measures within the banking industry is the primary emphasis in order to stop fraud and lessen financial losses. Through a detailed examination of the literature, in-depth interviews with experts in the banking sector, and case studies of existing cybersecurity measures, this paper provides a comprehensive overview of the problem and potential remedies.

Analysis of the research reveals that identity and access management, data encryption, and secure authentication are key components of any cybersecurity strategy. Furthermore, it is recommended that banks increase their technical capabilities and improve their employee awareness and training. The study concludes with a series of suggestions for enhancing banking industry cybersecurity and eventually reducing the danger of insider attacks.

This paper explores the topic of insider threats in the US banking industry and presents cybersecurity measures to prevent fraud. Insider threats from people with access to sensitive data and systems present serious hazards to the banking industry, resulting in monetary losses, reputational harm, and compromised data integrity.

KEYWORDS

Insider threats, banking industry, cybersecurity measures, fraud prevention, authorized access, data protection, encryption, incident response, investigation, regulatory compliance.

1. INTRODUCTION

Insider threats pose a significant and persistent challenge to the cyber-security landscape of the banking industry [1]. These threats, arising from individuals with authorized access to sensitive information and systems, have the potential to cause substantial financial losses, and reputational damage, and compromise the availability, integrity, and privacy of critical data [2]. The banking sector, being a primary target for malicious actors seeking financial gain, faces unique vulnerabilities because of the high volume of valuable assets and the inherent trust placed in its employees [3].

DOI:10.5121/ijsc.2023.14302

The significance of addressing insider threats in the banking industry cannot be overstated. Insider fraud accounted for approximately 16% of all fraud cases reported in the banking and financial services sector [4]. This figure highlights the demand for effective cyber-security controls to protect against such dangers. Furthermore, insider threats can have significant repercussions that damage not just financial institutions but also client confidence in the banking industry as a whole.

The purpose of this paper is to explore and analyze the various cyber-security measures that can be implemented to prevent fraud resulting from insider threats within the US banking industry.

1.1. Understanding Insider Threats

The dangers and weaknesses provided by people who are authorized to access sensitive data, systems, or resources within financial organizations and use that access for dishonest or malevolent motives are known as insider threats in the banking sector [1]. Based on the nature of the insider's actions and goal, these dangers can be divided into many categories.

Malicious insiders are one sort of insider danger. These people purposefully abuse their authorized access for personal advantage, for as by stealing confidential customer information, engaging in fraudulent activity, or destroying systems [2]. Motivations for malicious insiders may include financial incentives, revenge, dissatisfaction with the organization, or involvement in organized crime [3].

Another type of insider threat is the negligent, otherwise known as an unintentional insider. Even while these insiders may not be intentionally trying to compromise security or access sensitive data, their carelessness or actions nonetheless have the potential to do so [1]. Employees who unintentionally reveal passwords, handle sensitive information improperly, or are the targets of social engineering assaults are a few examples.

Insider threats in the banking industry exhibit certain motivations and characteristics. Motivations can range from financial gain and personal enrichment to revenge, ideological beliefs, or coercion by external parties [2]. Insider threats are driven solely by financial motives; some insiders may have non-financial motivations, such as political or ideological agendas.

Characteristics of insider threats often include a level of trust and access to sensitive information or systems, making it easier for them to execute their malicious activities undetected [1]. Insider threats may exploit their knowledge of internal processes, weaknesses in security controls, or gaps in monitoring and detection mechanisms. They may also display altered behaviors, such as more frequent access to sensitive information, odd working hours, or attempts to get around security precautions [3].

1.2. Related Work

Several previous works have delved into the domain of insider threats and mitigation strategies in the context of the banking industry. In this section, we will review and critique a selection of notable works to gain insights and build upon existing research.

Silowash et al. (2012) authored the "Common Sense Guide to Mitigating Insider Threats," which provides a comprehensive and widely recognized framework for organizations to address insider threats effectively. The manual offers helpful tactics and recommendations for averting, detecting, and dealing with insider threats. While the work offers valuable insights, it is important to note that it was published almost a decade ago, and the threat landscape may have evolved since then, necessitating the inclusion of more recent studies.

Harris (2020) presented the "Insider Threat Mitigation Guide" published by the Cybersecurity and Infrastructure Security Agency (CISA). This guide focuses on addressing insider threats across various sectors, including the financial industry. It offers actionable steps and recommendations to improve organizations' resilience against insider threats. Although the guide is a recent publication and provides relevant insights, it predominantly addresses insider threats from a broader perspective, and specific nuances related to the banking industry may require further investigation.

Saydaliev et al. (2022) explored financial inclusion, financial innovation, and macroeconomic stability, contributing to the broader discussion on financial industry advancements. While the study is pertinent to the banking sector's developments, it does not directly address insider threats or cybersecurity concerns, making it less applicable to this paper's focus.

Vinogradov (2020) published an article discussing the definition, detection, and prevention of insider threats. Although it offers a concise overview of insider threats and detection mechanisms, the work is from a vendor perspective and lacks the comprehensive depth provided by research studies or guides from recognized institutions.

Ekran (2022) presented "7 Best Practices for Banking and Financial Cybersecurity Compliance," which outlines cybersecurity practices specifically tailored to the banking sector. While the work is focused on compliance, it provides valuable insights into security measures that could be adapted to mitigate insider threats. However, it primarily addresses external cybersecurity compliance rather than internal threats posed by insiders.

These works provide a foundation for understanding and addressing insider threats in the banking industry. However, future research could focus on more recent and sector-specific studies to develop a holistic and up-to-date approach to insider threat mitigation in the dynamic cybersecurity landscape. However, this paper focuses on the US banking system with some strategies (for the prevention of fraud and insider threats) discussed as well as case studies and lessons drawn from them.

2. FRAMEWORK FOR REGULATION AND COMPLIANCE

The US banking sector is governed by strict regulations that are intended to protect against insider threats and foster cyber-security resilience. Subsequently, I shall provide an overview of relevant regulations and standards, compliance requirements, and the role of regulatory bodies and industry organizations in addressing insider threats.

i. The Gramm-Leach-Bliley Act (GLBA) is a crucial regulation that avails financial institutions the opportunity to protect the privacy and security of customer information [2]. Under GLBA, banks must establish safeguards to protect against anticipated threats, including insider threats, and implement measures to detect and prevent unauthorized entry to, or use of customer data [5]. Compliance with GLBA is essential in preventing insider threats and maintaining customer trust.

ii. The Sarbanes-Oxley Act (SOX) also plays a significant role in addressing insider threats within the banking industry. SOX requires publicly traded companies, including certain banking institutions, to establish internal controls and procedures for financial reporting [1]. These controls aim to detect and prevent fraudulent activities, including insider fraud. Compliance with SOX ensures that banks have adequate measures in place to address insider threats and mitigate the risk of financial fraud.

In addition to specific regulations, industry standards provide guidance on cyber-security practices and insider threat prevention. The Payment Card Industry Data Security Standard is a universally acknowledged standard that applies to banks and other organisations that process payment card transactions [2]. PCI DSS mandates the implementation of security controls to protect cardholder data, including measures to prevent insider threats, such as access control, monitoring, and regular vulnerability assessments.

Compliance requirements for preventing insider threats involve various aspects of cyber-security. To limit and oversee employee access to sensitive data and systems, financial institutions must set up effective access controls, such as separation of duties, least privilege, and role-based access control [5]. Regular monitoring and auditing of employee activities, including log reviews and anomaly detection, are necessary to identify suspicious behavior or unauthorized access [1].

Regarding insider risks in the banking sector, regulatory agencies and industry groups are key. The Federal Deposit Insurance Corporation (FDIC) is a key regulatory body that oversees and enforces compliance with regulations pertaining to cyber-security and insider threat prevention [3]. These bodies provide guidance, conduct examinations, and enforce penalties for non-compliance.

Industry organizations such as the Financial Services Information Sharing and Analysis Centre (FS-ISAC) also contribute to addressing insider threats. The FS-ISAC platform allows financial institutions to collaborate and share information to improve their cyber-security resilience and response capabilities [2]. Through information sharing and collaboration, industry organizations facilitate the identification and mitigation of insider threats.

3. INSIDER THREAT DETECTION AND PREVENTION

Effective detection and prevention of insider threats in the banking industry require a multi-layered approach encompassing various strategies and measures, which are expanded as follows:

3.1. Employee Screening and Background Checks

Employee screening and background checks play a vital role in mitigating insider threats by identifying potential risks during the hiring process. In-depth background checks, which confirm job history, educational credentials, and criminal records, can aid in locating people with a history of dishonest or malevolent behavior [2]. By establishing a robust screening process, banks can reduce the likelihood of hiring individuals who may pose insider threat risks.

3.2. Management of Privileged Users and Access Controls

To prevent unauthorized access and reduce the potential harm caused by insider threats, it is essential to implement adequate access controls and privileged user management. Role-based access controls (RBAC), least privilege principles, and separation of duties should be enforced to ensure that employees only gain access to the required resources necessary for their job responsibilities [1]. Privileged accounts, such as system administrators, should be tightly controlled and monitored to minimize the risk of insider abuse [3].

3.3. Monitoring and Auditing Systems

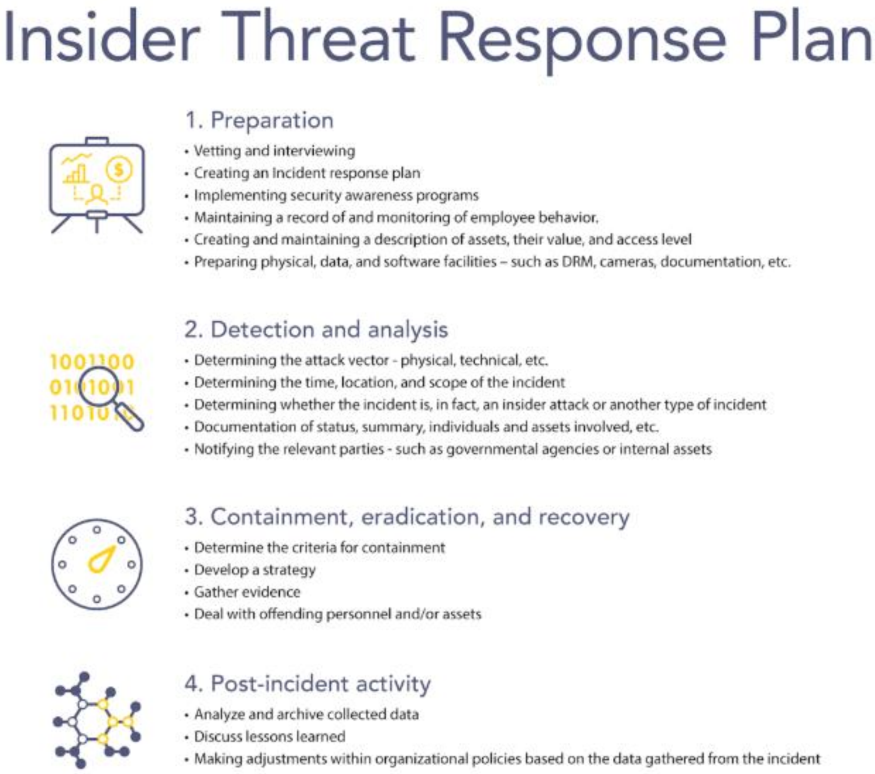
Continuous monitoring and auditing systems are essential for detecting suspicious activities and identifying insider threats promptly. These systems should include logging and auditing mechanisms that capture user activities, system events, and network traffic [5]. Regular review and analysis of logs enable the identification of anomalous behavior and potential indicators of insider threats. Real-time monitoring solutions can provide alerts for unusual or unauthorized activities, enabling swift response and mitigation [2].

3.4. User Behaviour Analytics and Anomaly Detection

User behavior analytics (UBA) and anomaly detection technologies leverage machine learning and statistical analysis to identify patterns and anomalies in user activities. By establishing baseline behavior profiles, these systems can detect deviations from normal behavior, indicating potential insider threats [1]. UBA tools can analyze various factors, such as access patterns, data transfer volumes, and system interaction, to identify unfriendly activities and generate alerts for further investigation [3].

3.5. Employee Training and Awareness Programmes

For the purpose of fostering a strong security culture and giving staff the information they need to identify and disclose possible insider threats, comprehensive training, and awareness programs are essential. Training should cover subjects such as social engineering awareness, data protection, secure password practices, and the consequences of insider threats [5].



Insider Threat Response Plan

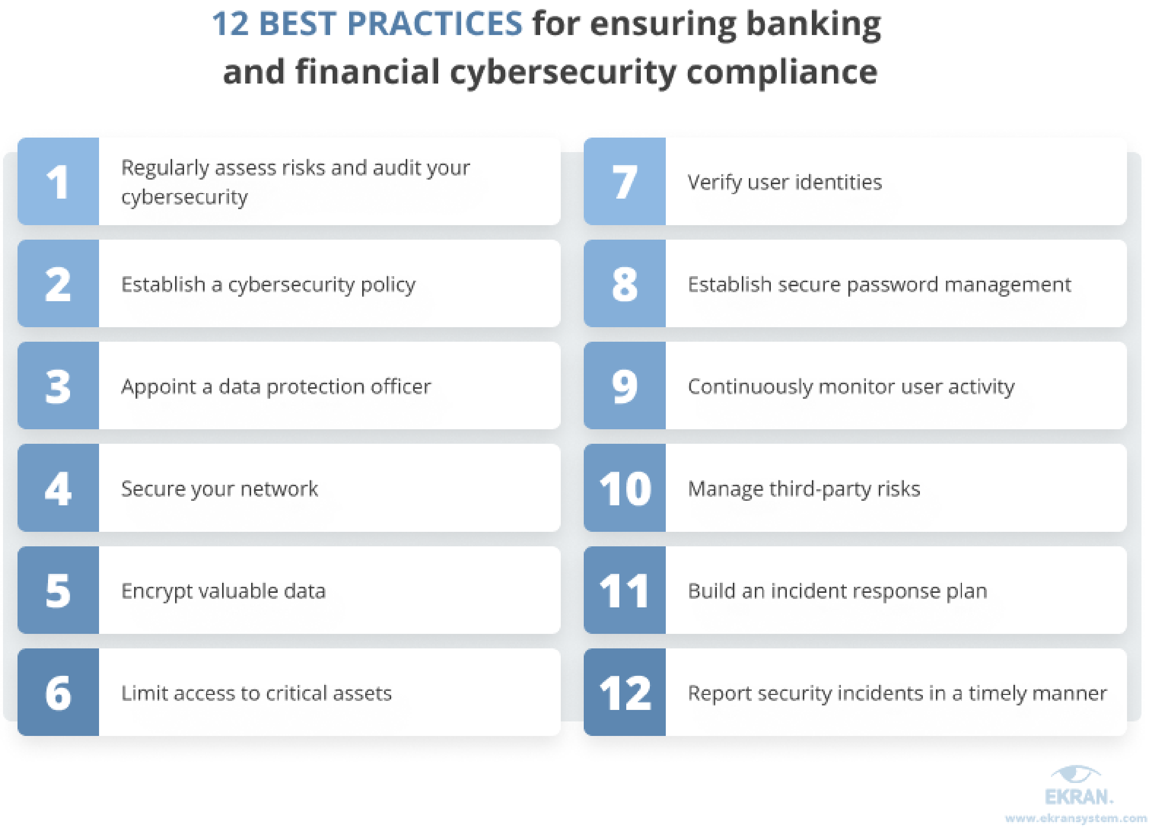
1. Preparation
- Vetting and interviewing
- Creating an Incident response plan
- Implementing security awareness programs
- Maintaining a record of and monitoring of employee behavior.
- Creating and maintaining a description of assets, their value, and access level
- Preparing physical, data, and software facilities – such as DRM, cameras, documentation, etc.

2. Detection and analysis
- Determining the attack vector - physical, technical, etc.
- Determining the time, location, and scope of the incident
- Determining whether the incident is, in fact, an insider attack or another type of incident
- Documentation of status, summary, individuals and assets involved, etc.
- Notifying the relevant parties - such as governmental agencies or internal assets

3. Containment, eradication, and recovery
- Determine the criteria for containment
- Develop a strategy
- Gather evidence
- Deal with offending personnel and/or assets

4. Post-incident activity
- Analyze and archive collected data
- Discuss lessons learned
- Making adjustments within organizational policies based on the data gathered from the incident

Figure 1: Insider threat response plan [6]



12 BEST PRACTICES for ensuring banking and financial cybersecurity compliance

1. Regularly assess risks and audit your cybersecurity
2. Establish a cybersecurity policy
3. Appoint a data protection officer
4. Secure your network
5. Encrypt valuable data
6. Limit access to critical assets
7. Verify user identities
8. Establish secure password management
9. Continuously monitor user activity
10. Manage third-party risks
11. Build an incident response plan
12. Report security incidents in a timely manner

EKRAN.
www.ekransystem.com

Figure 2: Best Practices for Ensuring Banking and Financial Cybersecurity Compliance: [7]

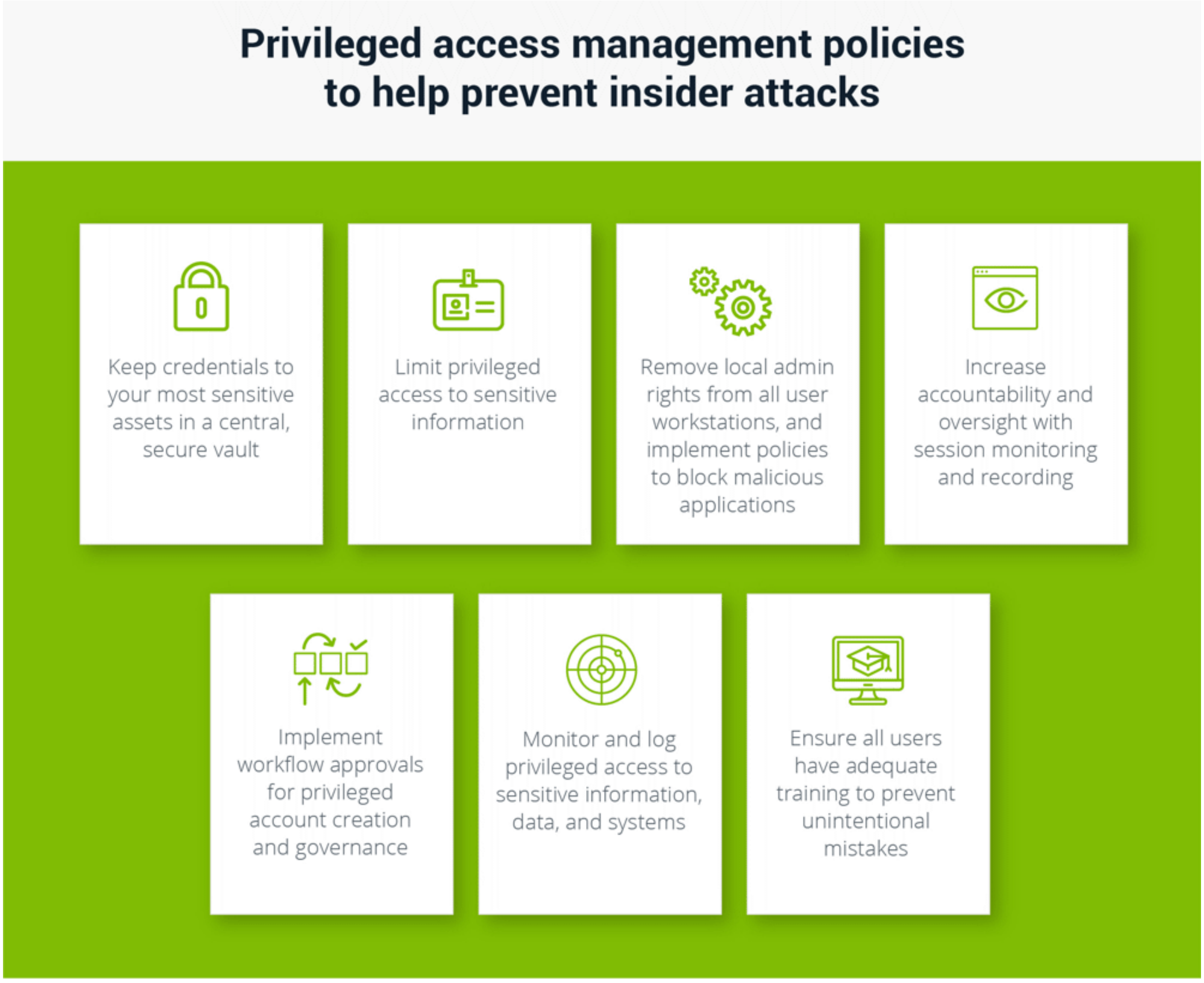
Regular awareness campaigns, simulated phishing exercises, and security reminders help reinforce good security practices and create a vigilant workforce [2].

4. Encryption and Data Protection

In order to stop insider threats in the banking sector, data protection is essential. It's essential to protect sensitive data from unauthorized access, modification, or disclosure in order to reduce the dangers brought on by insider threats. This sub-section explores the importance of data protection, encryption techniques, best practices, secure storage and transmission of sensitive information, as well as the role of data loss prevention (DLP) solutions.

4.1. Data Protection's Importance for Preventing Insider Threats

Since data protection strives to secure sensitive information from unauthorized access and misuse, it is crucial for mitigating insider threats. By implementing strong data protection measures, banks can minimize the potential impact of insider threats, including the unauthorized disclosure or theft of sensitive customer data [2]. Protecting data at rest, in transit, and in use is crucial to maintaining the confidentiality, integrity, and availability of critical information.



Privileged access management policies to help prevent insider attacks

Keep credentials to your most sensitive assets in a central, secure vault

Limit privileged access to sensitive information

Remove local admin rights from all user workstations, and implement policies to block malicious applications

Increase accountability and oversight with session monitoring and recording

Implement workflow approvals for privileged account creation and governance

Monitor and log privileged access to sensitive information, data, and systems

Ensure all users have adequate training to prevent unintentional mistakes

Figure 3: Privileged access management policies to help prevent insider attacks [8]

4.2. Encryption Techniques and Best Practices

Encryption has an important function in securing sensitive data and preventing unauthorized access. To safeguard data both at rest and in transit, American banks should implement strong encryption methods like Advanced Encryption Standard (AES) or RSA [1].

The best practices include utilizing powerful encryption algorithms to secure critical files, databases, and communication channels and making sure that encryption keys are managed properly [3]. Even if unauthorized parties manage to have access to the data, encryption helps make it unreadable and useless to them.

4.3. Secure Storage and Transmission of Sensitive Information

Secure storage and transmission of sensitive information are crucial components of data protection. Banks should employ secure storage solutions, such as secure databases or encrypted file systems, to protect sensitive data from insider threats [5]. Data communication between computers should be encrypted using secure transmission protocols like Transport Layer Security (TLS) or Secure File Transfer Protocol (SFTP) [2]. Secure storage and transmission practices help prevent unauthorized access or interception of sensitive information.

5. RESPONSE TO AN INCIDENT AND INVESTIGATION

Addressing insider threats in the banking sector requires effective incident response and investigation. Insider threat situations are easier to spot, manage, and lessen in impact with a strong incident response strategy and efficient investigative procedures. Subsequently, I shall explain the key aspects of incident response and investigation, including the importance of incident response, the incident response lifecycle, and the role of investigations in understanding and preventing insider threats. [9].

5.1. Importance of Incident Response

Incident response is crucial for effectively managing and mitigating the impact of insider threat incidents. Organizations can respond quickly, contain the issue, and reduce possible harm with the use of an incident response strategy that is well stated. Timely detection and response can help prevent the escalation of insider threats, limit the scope of the compromise, and reduce the impact on sensitive data and systems [10]. An effective incident response program enhances the resilience of the organization and aids in maintaining customer trust.

5.2. Crisis Management Lifecycle

There are varying stages in the incident response lifecycle, including planning, identification and analysis, containment, eradication, recovery, and lessons learned. During the preparation phase, organizations establish an incident response team, define roles and responsibilities, and develop an incident response plan [11]. The detection and analysis phase involves monitoring systems for suspicious activities, analyzing alerts, and investigating potential incidents. Once an incident is confirmed, organizations move to the containment phase, where they isolate affected systems, limit access, and implement measures to prevent further damage [10]. The eradication phase involves removing the threat, restoring systems to a secure state, and implementing security patches or updates. The recovery phase focuses on restoring normal operations and conducting post-incident analysis. The incident's lessons are recorded, and required adjustments are made to policies, procedures, and security measures [11].

5.3. Role of Investigations

Investigations play a crucial role in understanding the root causes of insider threats, identifying responsible individuals, and gathering evidence for potential legal or disciplinary actions. Investigations help determine the motive, scope, and impact of the insider threat incident. They involve forensic analysis of digital evidence, including logs, system snapshots, and network traffic, to reconstruct the sequence of events and identify the actions taken by the insider [10]. Investigations may also involve interviews with employees, review of access logs, and collaboration with law enforcement agencies when necessary. To reduce the risk of future insider threats, preventative measures are developed using the knowledge gathered from investigations, such as better security controls, personnel training, and policy upgrades [11].

6. STRATEGIES FOR MINIMISING INSIDER THREATS

Organizations, like those in the American banking sector, have a difficult and continuous problem when attempting to mitigate insider threats. To secure sensitive data, defend vital systems, and keep customers' confidence, it is essential to deploy insider threat mitigation measures effectively. These are the strategies to mitigate insider threat:

i. **Privileged Access Management:** Privileged access management (PAM) is a critical strategy for mitigating insider threats. PAM focuses on controlling and monitoring privileged user access to sensitive systems and data. Organizations may lessen the danger of insider exploitation by setting strict access restrictions, upholding the concept of least privilege, and routinely assessing and removing unneeded rights [12]. PAM solutions provide centralized management of privileged accounts, enforce strong authentication mechanisms, and enable session monitoring and recording to detect and respond to suspicious activities. [13].

ii. **Security Awareness Programs**: Comprehensive security awareness programs are essential for mitigating insider threats. These initiatives inform staff members of the dangers and repercussions of insider threats, offer instructions on spotting and reporting suspicious activity, and encourage a security-conscious and responsible culture [14]. Training sessions, simulated phishing exercises, and regular communication help employees understand their role in preventing insider threats and reinforce good security practices [19].

iii. **Incident Response**: A well-defined incident response plan is critical for the effective mitigation of insider threats. In order to respond to events involving insider threats, organizations should build an organized and documented incident response strategy that includes roles, responsibilities, and processes. The plan should encompass the detection, containment, eradication, recovery, and lessons learned from incidents [2]. Rapid response, containment, and mitigation measures help minimize the impact of insider threat incidents and prevent their recurrence.

iv. **Continuous Monitoring**: Continuous monitoring is a proactive strategy to detect and mitigate insider threats in real time. It involves the use of security technologies to keep an eye on user activity, network traffic, and data transfers [1]. These technologies include Security Information and Event Management systems, User and Entity Behaviour Analytics (UEBA), and data loss prevention (DLP) solutions. Continuous monitoring enables businesses to see unusual behavior, uncover insider risks early on, and take fast action to stop unauthorized activity or data breaches.

v. **External Collaborations**: Collaboration with external entities, such as industry associations, law enforcement agencies, and information-sharing communities, plays a key role in mitigating insider threats. Information-sharing programs like the Financial Services Information Sharing and Analysis Centre (FS-ISAC) make it easier for sector players to share threat intelligence, best practices, and lessons learned [5]. Collaboration with law enforcement agencies can aid in investigations and legal actions against insider threats.

7. CASE STUDIES AND LESSONS LEARNED

By analyzing these cases, organizations (especially the banking sector in the United States of America) can gain a holistic understanding of the vulnerabilities and risks associated with insider threats and develop effective prevention and mitigation strategies.

7.1. Société Générale Rogue Trader Incident

One notable case is the Société Générale rogue trader incident in 2008, where a trader named Jérôme Kerviel caused substantial financial losses amounting to billions of dollars through unauthorized trades [1]. This incident demonstrated the value of putting in place strong access restrictions, a system of segregated roles, and monitoring tools to find and stop unauthorized acts by privileged insiders. Lessons learned from this case emphasized the need for comprehensive risk management frameworks and controls to minimize the risk of rogue traders.

7.2. Bangladesh Bank Cyber Heist

The Bangladesh Bank cyber heist in 2016 involved the compromise of the bank's SWIFT messaging system, leading to the attempted theft of $1 billion [15]. This incident demonstrated the need of putting in place robust authentication controls, network segmentation, and intrusion detection systems to safeguard crucial infrastructure and guard against unauthorized access to payment systems. It emphasized the significance of effective communication procedures and incident response plans to enable a prompt and coordinated reaction to lessen the consequences of such occurrences.

7.3. Capital One Data Breach

Millions of people's sensitive financial information and customer data were made publicly available due to the Capital One data breach in 2019 [16]. This instance served as a reminder of the need of putting in place strong data protection measures, such as encrypting sensitive data while it is in transit and at rest and maintaining tight access restrictions to prevent unauthorized access to important databases. It emphasized the necessity for ongoing surveillance and anomaly detection systems to spot and address ominous behaviors that could be signs of insider threats [17].

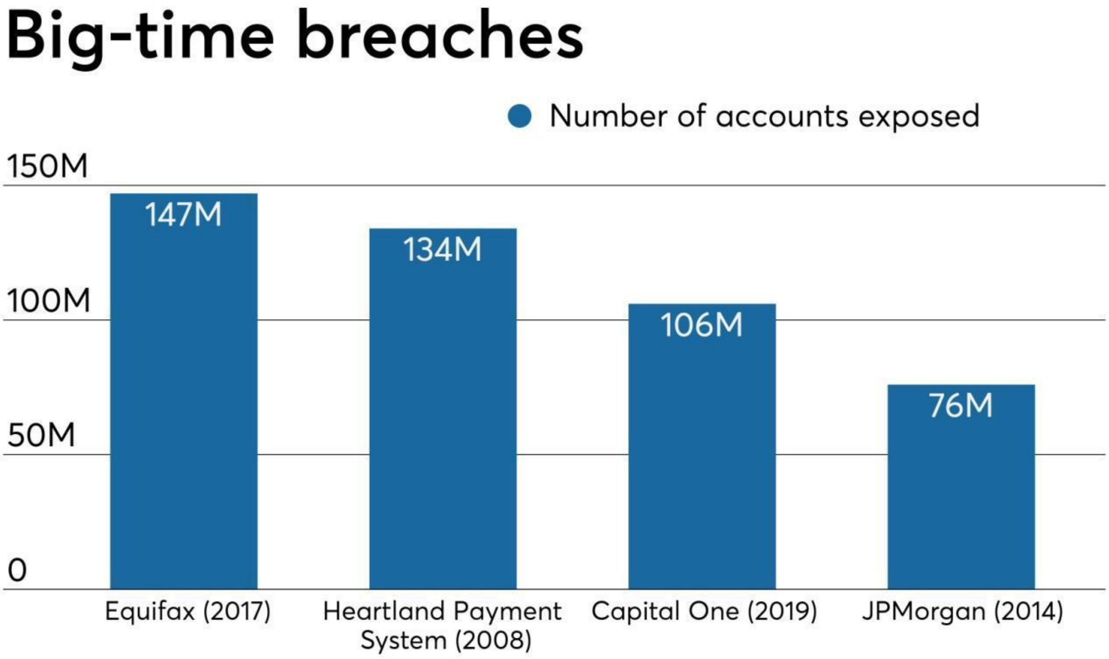


Figure 4: Big-time breaches [18]

As seen in Figure 4, about 106 million credit card applicants' data was stolen during Capital One's data breach, comprising data from contact information and addresses to credit scores and payment records. However, because the breach was discovered very promptly, the exposed data was most likely not used to steal consumer identities. Furthermore, the software issue that was capitalized in the attack was found through the bank's responsible disclosure procedure [18].

The implementation of a comprehensive strategy for insider threat prevention, including strong access restrictions, ongoing monitoring, incident response preparation, and staff awareness programs, is stressed by the lessons learned from these case studies. By incorporating these lessons into their cyber-security strategies, organizations in the banking industry can enhance their resilience and minimize the impact of insider threats.

8. Conclusion

Since authorized people have access to sensitive data and systems, insider threats pose serious vulnerabilities to the US banking industry's cyber-security environment. Due to the high value of assets and confidence in personnel, the banking sector has particular vulnerabilities and is a potential target for hostile actors. To address these threats, the sector has to implement various measures such as regulatory compliance, employee screening, access controls, monitoring systems, and training programs. Data protection, encryption, incident response, and investigation play crucial roles in preventing and mitigating insider threats. The US banking industry might safeguard sensitive information, defend crucial systems, and preserve client trust by using these techniques.

Through regulatory compliance, robust security measures, employee awareness programs, and incident response readiness, the sector should strive to mitigate the risks associated with insider threats. By continually enhancing its defenses and leveraging technologies, the US banking industry can strengthen its resilience and ensure the integrity and security of the financial ecosystem.

References

[1] Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T.J. and Flynn, L., 2012. Common sense guide to mitigating insider threats 4th edition. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

[2] Securities and Exchange Commission, Office of Compliance Inspections and Examinations, “National Exam Program Risk Alert, Cybersecurity Examinations” (April 15, 2014), https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf

[3] Harris, S., 2020. Insider threat mitigation guide. Cybersecurity and Infrastructure Security Agency, Tech. Rep.https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf

[4] ACFE (Association of Certified Fraud Examiners), 2020. Report to the nations: 2020 global study on occupational fraud and abuse. Retrieved from [https://www.acfe.com/fraud-resources/report-to-the-nations-archive]

[5] Saydaliev, H.B., Kamzabek, T., Kasimov, I., Chin, L. and Haldarov, Z., 2022. Financial inclusion, financial innovation, and macroeconomic stability. In Innovative Finance for Technological Progress (pp. 27-45). Routledge.

[6] Vinogradov I., 2020. What is an Insider Threat? How to define, detect and stop an insider threat. Logpoint. Retrieved from: https://www.logpoint.com/en/blog/insider-threat/

[7] Ekran. 2022. 7 Best Practices for Banking and Financial Cybersecurity Compliance. Retrieved from: https://www.ekransystem.com/en/blog/banking-and-financial-cyber-security-compliance

[8] Smith C., (n.d.). How can you prevent insider threats when none of your insiders are actually “inside”? Delinea. Retrieved from: https://delinea.com/blog/insider-threats-in-cyber-security

[9] Tu, M., Spoa-Harty, K. and Xiao, L., 2015. Data Loss Prevention Management and Control: Inside Activity Incident Monitoring, Identification, and Tracking in Healthcare Enterprise Environments. Journal of Digital Forensics, Security and Law, 10(1), p.3.

[10] Vormetric, (2015). Insider Threat Report, available at https://enterprise-encryption.vormetric.com/rs/vormetric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf

[11] Ismaila, I. and Mustafa S, Z., 2020. Digital Forensics and Incident Response.

[12] Shaw, E.D. and Stock, H.V., 2011. Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall. White Paper, Symantec, Mountain View, CA.

[13] Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T. and Rogers, S., 2005. Insider threat study: Computer system sabotage in critical infrastructure sectors. National Threat Assessment Ctr Washington Dc.

[14] Sinclair, S., Smith, S.W., Trudeau, S., Johnson, M.E. and Portera, A., 2008. Information risk in financial institutions: Field study and research roadmap. In Enterprise Applications and Services in the Finance Industry: 3rd International Workshop, FinanceCom 2007, Montreal, Canada, December 8, 2007. Revised Papers 3 (pp. 165-180). Springer Berlin Heidelberg.

[15] Pfleeger, S.L., Predd, J.B., Hunker, J. and Bulford, C., 2009. Insiders behaving badly: Addressing bad actors and their actions. IEEE transactions on information forensics and security, 5(1), pp.169-179.

[16] Novaes Neto, N., Madnick, S., de Paula, M.G. and Malara Borges, N., 2020. A case study of the capital one data breach. Stuart E. and Moraes G. de Paula, Anchises and Malara Borges, Natasha, A Case Study of the Capital One Data Breach (January 1, 2020).

[17] Trzeciak, R. and Costa, D., 2020. Building Out an Insider Threat Program. Carnegie Mellon University.

[18] Crosman P., 2019. Capital One’s data breach was bad. It could’ve been worse. American Banker. Retrieved from: https://www.americanbanker.com/news/capital-ones-data-breach-was-bad-it-couldve-been-worse

[19] Obunadike, Callistus & Efijemue, Oghenekome & Taiwo, Esther & Kizor, Somto & Olisah, Somtobe & Ejimofor, Ifunanya. (2023). Cybersecurity Strategies For Safeguarding Customers Data and Preventing Financial Fraud in the United States Financial Sectors. International Journal of Soft Computing. Vol. 14, No.3. 10.5121/ijsc.2023.14301.