Tamjeed Journal of Business Information Technology (BIT)

Volume 1(1): 2024, Page 10-18

The Impact of Information Security on Employees in the Human Resources Department of Banks

Nizar N. Romman[1,*]

[1] Master of Business Administration, Business School, University of Bedfordshire, Luton, United Kingdom; nezarrumman@gmail.com

***** Correspondence: Nizar N. Romman; nezarrumman@gmail.com

Abstract: The evolution of technology and digitalization worldwide has a significant impact on the digital transformation in banking services, with a focus on progress and security. This impact is particularly evident in the targeting of digital customer data, necessitating advanced measures to ensure security. This study addresses the impact of information security on employees in the banking sector, especially in human resource management, highlighting the influence of human resource management on the information security team within the banking sector. The study also underscores the importance of training and development in the field of information security and protection, as well as the need to enhance communication between relevant departments. The research follows a methodology that analyzes secondary data to interpret the expected impact on building and developing human resource management in the banking sector. The research emphasizes the potential contribution of information security to enhancing the digital security environment and increasing customer confidence in digital transactions, opening up opportunities for advanced digital banking services.The research indicates that information security is an essential part of the development and training phase in human resource management, emphasizing the necessity of engaging with relevant departments to address technical issues that may affect customer trust. Additionally, the research highlights the importance of the role of human resource management in developing financial services and providing technical solutions for banking services.

Keywords: Information Security; Employees; Human Resources Department; Banks

1. Introduction

The instances of electronic crimes targeting bank customers have seen a rise, with an increasing number of unauthorized attempts to access customer user panels or financial wallets. Moreover, electronic attacks on banks with the aim of breaching customer data have become more prevalent. This research specifically aims to bolster the information security system within the banking sector, with a focus on the role of human resources management [1].

In the banking context, human resources management endeavors to provide guidance to the technical and administrative departments. The primary goal is to foster a secure environment that safeguards customer data privacy, preventing its unauthorized exposure to external entities. The staff works closely with technical and administrative teams to cultivate a culture of security and privacy within the bank. By providing comprehensive training and guidance, Human Resources aims to equip employees with the knowledge and skills needed to safeguard customer data effectively. This not only enhances the overall security posture of the bank but also ensures that customer privacy is upheld to the highest standards [2,3].

Moreover, investing in employee training and development in the realm of cybersecurity not only mitigates risks but also has positive cascading effects. By improving employee competence and awareness, we can enhance the quality of the services and customer support. This, in turn, leads to faster and more inclusive deployment of banking services, ultimately benefiting the customers and the organization as a whole [1].

Furthermore, addressing these security gaps is not only essential for protecting customer data but also for maintaining employee performance and satisfaction. By proactively addressing security concerns and providing necessary support and resources, we can prevent negative impacts on employee evaluations and career progression. By placing a significant emphasis on training and guidance within the human resources department and fostering communication with information security management, employee performance can be enhanced. This strategic approach will contribute to the improvement of user data security and protection in the banking industry. Consequently, the realm of user data security and protection will witness tangible improvement, fostering a safer and more resilient banking ecosystem [1,3]. In our study, the research question, the technology and development in the field of cybersecurity and gaps continuously and where we look at employees in the banking sector to develop their security skills and training in this area as well as the integration of information security staff with human resources staff works to develop in the area of dealing with customers, customers face periodic problems in the financial transfer sector [1]. The use of financial technology depends on many characteristics of the use of applications that help and guide customers in facilitating obtaining quality service, including the combination of the information security department and human resources will contribute to a qualitative transfer. This contributes to the development of the internal system and strengthens the management of banks this helps in measuring the efficiency of the human resources department through the client and through the effectiveness in the management of dealing with cybercrimes that occur in the banking department through dealing with the client [2]. This is the need to ask what is the impact of information security on employees in the human resources department of banks.

The objective of the study is to examine the impact of information security output on employees in the Human Resources department its impact on employees through its impact on the financial sector in customer service and see the gap through the development or interest of employees. Increasing the security capacity in the information security sector by either merging the two sections or increasing the system in the department so that all sections of the banks need to be protected and developed continuously and that will help in the end to develop the human resources department and improve the performance and quality of the user. Considering the existence of privacy and security as a strong factor in building information security and threats that can pose to the client and affect confidence in the banking sector, it is followed by increasing the internal system of privacy in banks and protecting the financial sector and help improve administrative and financial performance. The importance of the information security sector in the banking sector helps in improving performance and increasing confidence, increasing the training of employees in the human resources sector in training mainly on dealing with cybercrimes that seriously affect the banking system, During the strengthening of the privacy and security of the customer in the bank sector, increase the capacity and security strength to face cybercrime and deal with it in the banking sector either with the client or within the bank system that helps to deal with the information and human.

Resources departments in dealing with the client and save the misappropriation of either the portfolio or theft of files of interest to the staff.

In addressing the literature gap, the research specifically targets the information security system within the human resources department. It explores threats to customer information and their potential impact on the internal system of the bank, as well as customer confidence regarding privacy. The studies included in this research aim to bridge these gaps in the banking sector, with a particular focus on the human resources sector's development.

The analysis within this research emphasizes the contribution of various studies to bridging the identified gaps. It specifically highlights the role of staff skill development and customer protection from threats in enhancing the human resources sector. Overall, the research aims to circulate

comprehensive studies that contribute to the advancement of the human resources sector in addressing cybersecurity challenges within the banking sector.

2. Literature review

Literary review on the subject which is divided into information security, human resources, and the banking sector. Information security is a system that helps to protect personal data from theft [3] and works to preserve the value of the person's information from threats. Employees and develop their functional skills which are due to the best of the company. [4]. The banking sector in terms of human resources and linking it in information security contributes to support the banking sector by protecting the user from threats through customer data and also contributes to the maintenance of the internal system of the bank. The bank is a financial sector that assists in customer service, financial mobility, and economic growth [5].In this study, we examine the information security of the human resources department and its impact on other departments in a bank, results in an interactive effect through the development of a tool to deal with customers of the banking sector and user protection and development in the renaissance of the human resources department, it will give results of improvement in the features and services provided by the banking system, as well as in the services provided to the customer, and an increase in the quality of the services provided [6]. This contributes to the development of the internal security system of the bank in increasing its impact on the information protection systems [7].

Study examined the impact of information security on financial services and security threats to the banking sector, the information technology department of the banks works on the security of data and private information in employees and customers and works to protect against attacks that are considered cyber-crimes. (HR data security: 5 questions to ask your IT department today'2017) Theft is one of the most dangerous threats to the banking sector because the client's confidence in the bank to save his data and the banking sector works so that in order not to cause financial loss, an electronic cloud that keeps the customer and his data and also provide a firewall for files and archived and these security measures, which are estimated annually sums of money prevent new loopholes and keep the bank safe from any cyber-attacks that harm the bank[8].

However, the security environment in the human resources sector and the customer environment, the cooperation of the human resources department, and its enhancement in information security makes the client's association in additions and banking transactions stronger, [9] which helps to build confidence in the customer in financial services, which works to preserve the property information with the customer [10].

According to several academic studies, training HR staff on cybersecurity in the banking sector technology has several advantages over, it is considered that human resources employees have a great role in the security of information and data protection and that contributes to their training to strengthen their practical skills in this area has become an employee penetration easy to hackers and if they penetrate one of the company will affect the existing data as it became with ransomware The employees in the bank will contribute to increasing the internal security strength of the company and also needs the security awareness of the banking client in order to develop strategies in case of risk and security of the bank data[10,11].

3. Methodology

The systematic literature review is chosen to answer the research question and objectives and so follow a specific methodology in a protocol or specific plans in the databases to see references literature and identify references on the type of information that is of interest to the research and within a time frame helps the research of the strategies of the references. Research methods and research analysis of literature references that contribute to linking research to the objectives [12].

In the research design, the systematic reviews are linked with the objectives of the research on the subject of information security and its impact on human resources staff in the banking sector. It was through the selection of secondary data and qualitative and empirical data from researches

that were used in the databases of Ebsco databases and Emerald. Search for journals in a period of time in which research is available that supports the objectives. Systematic reviews have contributed to the ease of searching for studies that were related to the research objectives and also to the accuracy of the data through the collection of literature that was supportive of the research objectives, the literature references part of the clarification of objectives through information security in the banking sector, which also contributed to the studies that develop human resources through training staff, which contributes to increase the internal system and customer service and strengthen confidence between customers and employees has contributed literature references to show the amount of data The secondary work facilitated the creation and linking of achievement objectives.

Studies conducted through the protocol focused on methodology were explored using secondary databases due to challenges in conducting primary research. This approach facilitated access to a wide array of quantitative data, streamlining the search for relevant literary references. The diverse range of research under examination was connected to the study's objectives, aiding in research selection and analysis.

The methodology and criteria for conducting searches hinge on various factors, including the timeframe and the nature of the topic under consideration. As part of the established conditions for accurate topic exploration, the initial steps involve navigating database sites and selecting either a basic or advanced search option. The advanced search relies on keywords to refine results, allowing for the specification of timeframes and article types such as magazines, scientific research, or books. Furthermore, the selection can be narrowed down to particular countries or geographic locations where research has been conducted, along with the option to focus on specific sectors like HR or banking. These protocol steps facilitate the precise and comprehensive extraction of research results, ensuring their suitability for further study and analysis.

A systematic approach was undertaken to search for keywords, encompassing primary, secondary, and specific data. Initially, detailed searches were conducted focusing on primary keywords such as "information security," followed by "human resources staff," and "banks." The search scope did not confine itself to any particular region, ensuring a comprehensive exploration of relevant data. Employing the advanced search feature on the Ebsco site, a meticulous examination was conducted, yielding comprehensive information within the Emerald database. Notably, the search yielded results pertinent to the research question, particularly in the domain of information security within banking institutions. This methodical approach facilitated the extraction of substantial information, underscoring the efficacy of employing targeted keywords within database search engines to streamline the information retrieval process for researchers.

3.1. Accessibility and Resources

The search was based on the keys that followed the method in the search protocol and the words that were searched were "information security," "employees," "human resources," and "banks," covering the period from 2000 to 2019. This timeframe encapsulates major milestones such as the proliferation of the rise of cyber threats, and advancements in data protection laws. By encompassing these years, the search captures a comprehensive overview of the contextual factors influencing the research topic, and the selected timeframe provides a substantial pool of data for analysis while avoiding potential data gaps or outdated information. Research studies and academic literature published within this period offer a rich source of information to support the research objectives, and this period was applied to the Ebsco databases and Emerald and geolocation selection were Available to all the country to know more than magazines and scientific sites and interest in the search for the ad Allocated sector, which was the banks at the beginning of the selection of journals of scientific databases were selected initially 30 scientific journals were talking mostly about information security in banks and became excluded scientific journals that do not specialize in HR and the integration of the department of human resources in information security in customer service has become 13 scientific journals selected from databases that were within the search protocol that helps in the development of research and methodology of systematic reviews facilitated the search process with the protocol.

Table 1. Methodological studies

TOPICS	AUTHOR	PUBLICATION DATE	DATABASE	RELEVANCE
Perceived Security Threats of Computerized Accounting Information Systems in the Egyptian Banking Industry	Abu-Musa, A. A.	2006	Ebsco	Relevant
The Impact of Human Resource Accounting Information System	Alam, J. and Hasan, M	2016	Ebsco	Relevant
The future of HR and information capability	Brockbank, W. et al	2018	Ebsco	Relevant
People analytics and the rise of HR	DiClaudio, M	2019	Ebsco	Relevant
Cyber security is too important to be left to the IT department	KIRTON, H	2017	Ebsco	Relevant
Business performance and customer relationship management	Lee, C.-H. et al	2010	Ebsco	Relevant
Cybercrime: an emerging threat to the banking sector	Malik, MS & Islam, U	2019	Ebsco	Relevant
Professional Monitor', SC Magazine: For IT Security Professionals (UK Edition), p. 82	Moretti, A	2007	Ebsco	Relevant
Bank Tech Expertise in Short Supply', Bank Systems & Technology	Nelson, K.	2004	Ebsco	Relevant
The global market for cloud security and vulnerability technologies	PR Newswire	2017	Ebsco	Relevant
THE HUMAN STAIN. (cover story)', Bank Systems & Technology	Schneider, I.	2004	Ebsco	Relevant
The Impact and Interaction Effect of HR and IT Applications on the Performance of Customer Relationship Management in the Banking	Yu-Chiang Wang & Yi-Feng Yang	2005	Ebsco	Relevant
Examining customers' continuance intentions towards internet banking usage	Ofori, K., Boateng, H., Okoe, A.	2017	Emerald	Relevant

4. Analysis of Studies and Data in Research

The analysis of research studies is contingent upon several key factors, notably the methodological framework utilized and the specific methodologies employed in the development of literature reviews. This analysis focuses on investigating the ramifications of information security in banking institutions, with a particular emphasis on its implications for human resources personnel. The initial phase involves navigating through databases using predefined protocols, facilitating the identification of pertinent studies. Search criteria include parameters such as time frame and subject specificity. The initial steps involve selecting search options, either basic or advanced. This systematic approach ensures the retrieval of comprehensive research results aligned with the study's objectives. Key terms like "information security," "human resources staff," and "banks" are systematically deployed, complemented by secondary and specific data searches. The search scope remains broad to encompass diverse regions, enabling a thorough exploration of relevant data. Leveraging advanced search functionalities within platforms such as Ebsco facilitates meticulous examination and comprehensive data extraction, as evidenced by the findings from the Emerald database. This systematic approach underscores the effectiveness of targeted keyword utilization within database search engines and enhances the relevance of extracted data to the research question at hand.

4.1. The impact of information security on the banking sector in human resources

The security of information and its impact on the banking sector depends on the employees and the impact on the relationship and trust of customers in a bank, and the HR department is the effective separation between the bank and the characteristics of information security so that it contributes to influence on employees and customers and the financial sector. Financial problems are faced by protecting the personal information of users and bank customers, we will discuss in the analysis of research that was positive and negative in support of the research sector, which relates to the objectives of the research by addressing and discussing research that affected the bank sector through information securit [13].

4.2. Positive impact of information security on the banking sector

The following topics: (The Impact of Human Resource Accounting Information System), (The future of HR and information capability), (People analytics and the rise of HR), (Cyber security is too important to be left to the IT department), (Business performance and customer relationship management),(Professional Monitor', SC Magazine: For IT Security Professionals (UK Edition), p. 82),(Bank Tech Expertise in Short Supply', Bank Systems & Technology),(The global market for cloud security and vulnerability technologies),(The Impact and Interaction Effect of HR and IT Applications on the Performance of Customer Relationship Management in the Banking),(Examining customers' continuance intentions towards internet banking usage). One of the positives related to the induction of information security in the banking sector, which talks about the high rate and increased information security in banks through the development of human resources staff and development and also the integration of two sections with each other in order to become a cooperation between the two sections and also interest customers to the banks [5,6]. Their personal and financial rights and the removal of any risks that can be posed by the client during his calculations and increases the confidence of the client in the banking sector of the services provided in the field of information security and protection, which leads to increase the internal system and security at the bank in terms of human resources this helps to protect the financial files of the banks [14,15].

4.3. Negative Impact of information cybercrime on the banking Sector

The topics discussed include the emerging threat of cybercrime in the banking sector, perceived security threats in computerized accounting systems within the Egyptian banking industry, and the broader implications of these threats. These topics highlight the direct impact of electronic

crimes, theft, and customer targeting, which banks are addressing by enhancing their information security departments in collaboration with other departments, such as human resources. This collaborative effort aims to mitigate customer risks through awareness, training on data protection, and system development. The effectiveness of these measures is reflected in service provision and the protection of internal banking files, emphasizing the importance of comprehensive employee awareness across departments to prevent cybercrime-related losses and maintain customer trust [16,17].

4.4. *Security challenges in the electronic banking sector*

In light of the age of digital technology and development in information protection, the banking sector has become a target for electronic crimes, and the crimes that the customer may be exposed to include electronic fraud, malware, data hacking, and credit card fraud. These targeted activities cause losses to financial institutions and customers [18,19].

In terms of the impact on financial services, there is a loss of trust between customers and banking institutions, which negatively affects commercial relations and is reflected in a reduction in the use of banks' electronic services, which will lead to high costs in solving cybercrime problems, and this will lead to an increase in the operational costs of the banking sector to provide protection [19]. More on information and also awareness among its customers. The central operational department in the bank will be the information protection and security department. The human resources department will also contribute to training employees and linking them with the information security department [20].

The impact that will be on the electronic environment will lead to a delay in the technical development of financial services due to the entire operational department's focus on electronic security and information protection, as well as reducing trust, which reduces users' concerns about private information and its safety, which will negatively affect their reliance on digital financial services [18].

Banks and financial institutions face major challenges in ensuring cybersecurity and protecting the digital environment. To enhance trust and ensure the sustainability of digital financial services, training, and developing employees within the information security department is crucial for ensuring that they are equipped with the necessary skills and knowledge to effectively protect the bank's digital assets [4]. This can involve providing specialized training in areas such as cybersecurity protocols, threat detection, and incident response. Furthermore, investing in the continuous professional development of these employees through certifications, workshops, and seminars can keep them updated on the latest trends and technologies in the rapidly evolving field of cybersecurity [8]. Additionally, fostering collaboration and communication between the information security department and other relevant departments such as IT, risk management, and operations is essential for a holistic approach to cybersecurity. This can be achieved through regular cross-departmental meetings and the establishment of clear communication channels. By linking these departments together and ensuring alignment with the overarching goals, banks can create a unified approach to cybersecurity that effectively mitigates risks and strengthens the overall digital services environment [20].

5. Conclusions

The ongoing evolution of technology and digitalization globally has profoundly impacted the banking sector, particularly in terms of both progress and security. This transformation underscores the critical need for robust measures to safeguard digital customer data. This study delves into the nexus between information security and human resource management within banking. It emphasizes the pivotal role of human resource management in bolstering the effectiveness of information security teams and highlights the significance of training and development initiatives in fortifying information security measures. Moreover, the study underscores the necessity for improved communication between relevant departments to address technical challenges and uphold customer trust

in digital transactions. By integrating information security into the fabric of human resource management practices, banks can enhance the digital security landscape and cultivate customer confidence, thereby fostering the advancement of digital banking services.

6. Recommendation

Recommendations stemming from extensive literature reviews and research inquiries highlight the critical importance of information security in the banking sector. It is strongly recommended that banks invest in comprehensive training programs to foster a culture of information security awareness among employees. Prioritizing the safeguarding of personal and financial data not only enhances customer relationships but also fosters trust in the institution. The human resources department plays a central role in implementing these measures and should actively promote data protection awareness throughout the bank.

Recognizing the pivotal role of HR management in addressing information security challenges is paramount. Emphasizing the significance of HR practices in optimizing the efficiency of the information security team and fortifying the overall security framework is essential. This involves prioritizing training and development initiatives tailored to equip employees with the necessary skills and knowledge to mitigate risks effectively.

Furthermore, enhancing communication channels between relevant departments, particularly between HR and the information security teams, is crucial. Collaborative efforts are vital for promptly addressing technical issues and upholding customer trust. By fostering synergy among departments, banks can effectively navigate evolving security threats and maintain a resilient security posture.

References

1. Alam, J. and Hasan, M. (2016) 'The Impact of Human Resource Accounting Information System (Hrais) on Human Resource Management Practices of the Banking Sector in Bangladesh', UTCC International Journal of Business & Economics, 8(2), pp. 79–90.
2. Brockbank, W., Ulrich, D.,. Kryscynski, D. G., & Ulrich, M. (2018). The future of HR and information capability. Strategic. H R Review, 17(1), 3-10.
3. People Management, pp. 42–44.
4. Schneider, I. (2004) 'THE HUMAN STAIN. (cover story)', Bank Systems & Technology, 41(1), pp. 22–27.
5. Abu-Musa, A. A. (2006) 'Perceived Security Threats of Computerized Accounting Information Systems in the Egyptian Banking Industry', Journal of Information Systems, 20(1), pp. 187–203.
6. Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. Authorea Preprints.
7. Mezioud, B., & Smai, A. (2016). The Cybercrimes on Financial and Banking Services: The Challenges and Treatment.
8. Kovalchuk, O., Shynkaryk, M., & Masonkova, M. (2021). Econometric models for estimating the financial effect of cybercrimes. In 2021 11th International Conference on Advanced Computer Information Technologies (ACIT) (pp. 381-384). IEEE.
9. Nelson, K. (2004) 'Bank Tech Expertise in Short Supply', Bank Systems & Technology, 41(5), p. 14.
10. SynergySynergy, H. (2019). How Your HR Department Can Improve Information Security and Prevent Data Loss - Synergy.
11. Pecb.com. (2019). Information Security in Banks and Financial Institutions.
12. Chao-Hsiung Lee , Shaio Yan Huang , F. Barry Barnes & Li Kao (2010) Business performance and customer relationship management: The effect of IT, organisational contingency and business process on Taiwanese manufacturers, Total Quality Management & Business Excellence, 21:1, 43-65, DOI: 10.1080/14783360903492595
13. Yu-Chiang Wang & Yi-Feng Yang (2015), 'The Impact and Interaction Effect of HR and IT Applications on the Performance of Customer Relationship Management in the Banking Industry: An Empirical Study of Five Taiwanese Banks', Information Resources Management Journal, vol. 28, no. 3, pp. 29–41.
14. PR Newswire (2017) 'The global market for cloud security and vulnerability technologies reached $4.6 billion in 2016. The market should reach $5.3 billion in 2017 and $10.1 billion by 2022, increasing at a compound annual growth rate (CAGR) of 13.9% from 2017 to 2022', PR Newswire US, 2 November.
15. Emerald.com. (2019). Examining customers' continuance intentions towards internet banking usage | Emerald Insight.
16. KIRTON, H. (2017) 'Cyber security is too important to be left to the IT department: As hackers increasingly exploit human vulnerability, HR has a vital role to play - not least in ensuring businesses have the technical talent to fight back', People Management, pp. 42–44.
17. Malik, MS & Islam, U (2019), 'Cybercrime: an emerging threat to the banking sector of Pakistan', Journal of Financial Crime, vol. 26, no. 1, pp. 50–60.
18. Abu-Musa, A. A. (2006) 'Perceived Security Threats of Computerized Accounting Information Systems in the Egyptian Banking Industry', Journal of Information Systems, 20(1), pp. 187–203.
19. DiClaudio, M. (2019) 'People analytics and the rise of HR: how data, analytics and emerging technology can transform human resources (HR) into a profit center', Strategic HR Review, 18(2), pp. 42–46.
20. Moretti, A. (2007) 'Professional Monitor', SC Magazine: For IT Security Professionals (UK Edition), p. 82.