A REGRESSIONAL STUDY ON THE IMPACT OF ORGANIZATIONAL SECURITY CULTURE AND TRANSFORMATIONAL LEADERSHIP ON SOCIAL ENGINEERING AWARENESS AMONG BANK EMPLOYEES: THE INTERPLAY OF SECURITY EDUCATION AND BEHAVIORAL CHANGE

Abstract

Organizations across various sectors are increasingly vulnerable to cybersecurity breaches in an era characterized by unprecedented technological advancements and a rapidly evolving threat landscape. Among the myriad methods employed by malicious actors, social engineering stands out as a particularly insidious and effective means of infiltrating secure systems and obtaining sensitive information. To effectively address these issues, organizations must establish and sustain a principled security process; this process goes beyond installing the latest security technologies. It encompasses the concept of "organizational security culture. This paper investigates the impact of organizational security culture and transformational leadership on bank employees' social engineering awareness, focusing on security education and behavioral change. Social engineering is the unauthorized infiltration of the end user's computer system and network through malware techniques such as tailgating, phishing, vishing, pretexting, and baiting to gain access to companies and individual confidential data; thus, this study aims to analyze the effect of organizational security culture and transformational leadership on social engineering awareness among bank employees while assessing security education's role in driving behavioral change. This research used the Likert scale model to collect primary data through survey questionnaires from 450 bank employees. The data collected was analyzed using linear regression analysis to test the study's hypothesis. This study recommends that banking institutions should adopt a good organizational security culture and expose their staff to effective security education, as this will cause a change in employees' security behavior and more research should be conducted regarding security culture, security education, and awareness programs within banking institutions due to bank operations' ever-dynamic nature and ensuring preparedness for prevailing cyber threats.

Key Words:Organizational Security Culture, Transformational Leadership, Security Education, Behavioral Change

Introduction

Background of the Study

In the present digital world, the banking sector has become subject to more complex cybersecurity risks, such as social engineering schemes [1]. Social engineering entails coercing people into divulging private information, frequently costing organizations money and reputational damage. Organizations must prioritize their employees' human resource base and invest in technology protection to reduce these risks [2].

Leadership and organizational security culture are crucial in determining how employees perceive and react to social engineering assaults [3]. A robust security culture fosters a shared dedication to security

protocols, whereas transformational leadership encourages staff involvement and motivates them to take responsibility for their company's security [4]. Furthermore, security education and behavioral modification programs are essential for providing staff members with the information and abilities needed to recognize and effectively counteract social engineering attempts [5]. These programs provide employees with an understanding of common social engineering tactics, such as phishing emails or pretexting, and empower them to respond appropriately. Training initiatives can also instill a heightened sense of vigilance, teaching employees to question unexpected requests for information and to verify the authenticity of communications, ultimately reducing the risk of falling victim to these deceptive tactics [6,7].

In addition, while these elements are acknowledged to be important, much research hasn't been done to thoroughly examine how organizational security culture, transformational leadership, security education, and behavioral modification interact with social engineering awareness among bank workers [8]. In order to close this research gap, this study will use regression analysis to look at how organizational security culture and transformational leadership affect bank workers' understanding of social engineering. Additionally, it looks into how behavioral modification and security education work together to affect workers' capacity to recognize and stop social engineering scams [9].

This study will shed more light on the relationships between transformational leadership, organizational security culture, and social engineering awareness [10,11]. It will also clarify the part that security education and behavioral modification play in enhancing staff members' understanding of, proficiency in, and adherence to social engineering defense mechanisms. These discoveries will benefit cybersecurity research and offer banks and their executives useful suggestions for improving security procedures [12].

Problem Statement

According to Andrew [13], social engineering attacks present a serious risk to the safety of banks and their clientele. Understanding how transformational leadership, organizational security culture, security education, and employee behavior modification interact will be essential to effectively countering this threat [14]. On the effect of these elements on social engineering, little research has been done on how these characteristics affect the banking industry's knowledge of social engineering [15].

The issue is the dearth of a thorough understanding of how transformational leadership and organizational security culture affect bank workers' awareness of social engineering [16]. This research aims to close this knowledge gap by investigating the effects of transformational leadership and organizational security culture on bank workers' understanding of social engineering [17]. The paper will also investigate how behavioral modification and security education interact with these variables, affecting workers' capacity to recognize and avert social engineering scams.

This study intends to give banks and their leaders important insights on the most efficient ways to raise employee awareness of social engineering by analyzing the association between security in the organization's social structure, leadership that promotes security education, and change in behavior [18]. The banking industry's overall security posture will be strengthened due to these insights, which will aid in creating focused interventions and training initiatives that can enable bank staff to recognize and address social engineering threats [19]. Furthermore, this paper endeavors to provide a thorough comprehension of the influence of organizational security culture and transformational leadership on the knowledge of social engineering among bank personnel [20].

Research Aim

This research aims to comprehensively investigate and analyze the influence of organizational security culture and transformational leadership on social engineering awareness among bank employees while assessing security education's role in driving behavioral change. By exploring these factors and their interplay, this study will provide a deeper understanding of the dynamics within banking institutions, with the ultimate goal of enhancing security measures and mitigating the risks posed by social engineering attacks.

Research Objectives

1. To assess the existing security culture within the banking institution and determine its impact on the social engineering awareness of bank employees
2. To examine the extent to which transformational leadership styles influence bank employees' security consciousness and vigilance in the face of social engineering threats.
3. To analyze the effectiveness of security education and awareness programs in equipping bank employees with the knowledge and skills needed to detect and respond to social engineering attacks.
4. To explore the interplay of organizational security culture, transformational leadership, and security education in shaping employee attitudes and behaviors regarding social engineering awareness.
5. To provide practical recommendations and insights for banking institutions to strengthen their security measures and better protect their assets and customer data from social engineering attacks.

Research Hypothesis

H_1: There is a significant positive relationship between the level of organizational security culture and social engineering awareness among bank employees.

H_2: There is a significant positive relationship between the presence of transformational leadership and social engineering awareness among bank employees.

H_3: There is a significant positive relationship between the effectiveness of security education and social engineering awareness among bank employees.

H_4: The combined influence of organizational security culture, transformational leadership, and security education significantly positively affect social engineering awareness among bank employees.

Literature Review

Organizational Security Culture

In today's digital age and time, it has become vital and important for organizations to protect sensitive data and assets, safeguard information, and prevent security breaches [21,22]. Security breaches can result in damaging consequences, financial losses, and reputational damage to any organization [23]. To effectively address these issues, organizations must establish and sustain a principled security process [21]; this process goes beyond installing the latest security technologies. It encompasses the concept of "organizational security culture"; this comprises the principles, values, attitudes, and behaviors that an organization promotes to its staff regarding security [23]. Fostering and maintaining an effective

organizational security culture is key in safeguarding organizations against cyber threats and security breaches [23].

Fianty [24] asserts the connection between organizational culture and its effects on employee security behavior in organizational settings provides insights into how companies that prioritize and care about their employees tend to have a satisfied and security-conscious workforce, in contrast to companies that neglect the well-being and satisfaction of their employees, leading to non-compliance with security measures [25].

Tolah et al. [26] reiterate that security culture cannot be achieved by technological issues alone but is largely associated with the people and workforce who operate these systems. It also lays the foundation and discusses key factors that promote security culture in the organization, including influential factors, organizational behavior factors, and security culture factors [27].

A positive security culture is one where security is deeply ingrained in the values and practices of employees, contrary to a negative security culture, which is characterized by negligence and a lack of commitment to security [26]. Positive key factors include Leadership Commitment, support from leadership, employee training and awareness, and clear policies and procedures [28]. In contrast, negative factors encompass the lack of leadership support, insufficient training and awareness, and unclear policies and procedures [26].

Transformational Leadership

Transformational leadership enacts positive changes and pushes members to accomplish exceptional results [29]. It plays a crucial role in enabling organizational security culture because of its significant influence on employees to participate in organizational information security; transformational leaders use motivation as a powerful tool to propel employees to achieve their goals and exceed expectations; when employees are motivated, they will adhere to organizations policies and procedures because, by orientation from their leader, they now understand the significance of protecting data [30]. With their compelling communication skill, they convey the importance of security in the workplace and can achieve a security culture; for instance, they will be able to instill a sense of shared responsibility for protecting data and assets [31].

Transformational leadership emphasizes the role of leaders as agents of change and visionaries. They are leaders who encourage their followers to want more responsibility by inspiring, motivating, and influencing them to reach higher performance levels. Leaders envisioning and embodying the future bring about constructive adjustments and inspire group members to achieve exceptional outcomes [29].

Transformational leaders exhibit a strategic mindset capable of envisioning a future where the organization is secure and inspiring employees to recognize the significance of security [32,33,29]. Their adept communication skills enable them to convey the importance of security practices, communicate potential risks, and highlight each employee's role in maintaining security [34,32]. This ability to motivate encourages employees to engage actively in security practices and take security seriously. “Follow the example kind of leaders” demonstrates a precedent for employees to adhere to security practices [32,33]. Dedicated to their employees' personal and professional growth, they will make provisions for employees' security training and educational opportunities to enhance their awareness and skills [35].

Social Engineering and its Threats

Abraham and Chengalur-Smith[36]explain social engineering as a malicious tool in the arsenal of hackers, utilized for the unauthorized infiltration of the end user's computer system and network through cultural manipulations, social disguises, and psychological tactics aimed at gaining access to companies and individual confidential data. This method strategically targets vulnerable individuals and weak links, which refers to employees as they serve as entry points for hackers to devise malicious or intrusive acts[37].

According to Ghafir et al. [38], social engineering violates organizational security by deceiving employees into deviating from established security protocols. It involves leveraging employees' lack of suspicion to access sensitive company data, including user IDs, passwords, or corporate directories.

Common social engineering malware techniques for accessing organizations' confidential files include tailgating, phishing, vishing, pretexting, and baiting[39]. According to Airehrour et al. [40], social engineering attacks can expose banks to vulnerabilities, data leakages, and exposure of confidential customer information, leading to legal and monetary consequences for banks. Moreover, successful engineering attacks can tarnish and damage banks' reputations, causing customers and the public to lose trust in the organization's capacity to secure their financial information and personal details [40].

Airehrour et al. [40] give instances and real-life scenarios of the impact of social engineering attacks in the banking sector; through a study initiated by Microsoft in 2008, it was discovered that scammers utilize phishing websites to siphon off a staggering amount of US$5 billion from banks. Another social engineering attack 2011 at Wells Fargo Bank resulted in the theft of US$2.1 million.It was also recorded that according to estimates from the Gartner Group, U.S. banks, and credit card issuers incur combined annual losses of around US$2.8 billion due to phishing activities [41].

Security Education and Awareness Programs

Price [42] emphasizes that security education and awareness programs are vital in reducing the chances of security breaches in organizations. Such programs heighten employee awareness and consciousness of cyber threats, enabling them to make informed security decisions daily. Employees become more cautious about engaging with pop-up emails, clicking on links, creating complex passwords, and keeping software updated[43]. Corradini [44] asserts that security education and awareness training better equip employees with the knowledge and understanding needed to effectively utilize and operate tools needed to enhance cybersecurity in the organization.

Salahdine and Kaabouch[45] highlight that trained employees are quicker at identifying emerging new styles, techniques, tactics, and procedures hackers deploy to gain unauthorized access to organizations' databases. Yoo et al. [65] provide further insights into how organizations invest in security education, training, and awareness (SETA) programs due to their efficiency in propelling employees to achieve security goals in the workplace. SETA programs are designed to reduce the impact of cyber threats and security engineering attacks in the workplace, reduce employees' noncompliance with information security policies, and create a heightened awareness of cyber security [47].

There are several approaches and best practices to drive home security education and awareness programs; they include;

- Certification programs from industry-recognized cybersecurity companies such as Certified Information Systems Security Professional (CISSP) [46]
- Mentorship or expert tutelage is where experienced cybersecurity professionals train employees.
- Cybersecurity Awareness Programs that educate employees about cybersecurity threats, best practices, and safe online behavior.
- In organizational workshops, cybersecurity professionals are invited to deliver lectures and share real-world experiences and insights with employees [46].

The Interplay of Organizational Security Culture, Transformational Leadership, and Security Education

Various studies have shown that a strong security culture within an organization characterized by a combined commitment to security values and practices positively impacts employee security awareness [24,26]. Lebek et al. [31] state that transformational leadership enhances security culture by being a role model, providing guidance in security-related matters, and motivating employees to prioritize security. The collaborative power of a committed leader and a security-conscious culture work environment promotes heightened security awareness among employees.

Moreover, security education and awareness training programs tailored to an organization's security needs and objectives significantly contribute to employee awareness and knowledge [44]. Employees receiving regular security and awareness training are better equipped to recognize and respond to security threats efficiently [46]. The interaction between leadership, a well-established security culture, and education fosters an environment where employees understand the importance of security and actively safeguard the organization's data and resources.

To assess the impact of security education on social engineering, a comprehensive intervention was undertaken within the campus of the University of Twente by [48]. The intervention's primary objective was to raise awareness among individuals about the risks associated with social engineering tactics. The intervention utilized various tools and strategies to educate and engage the target audience effectively [49]. Informational leaflets outlining the possible dangers of social engineering were distributed to the target audience; small key chains were distributed to participating parties, and an engaging poster was also used to change participants' psychology regarding sharing office keys with strangers. During this intervention, it was revealed that 37 percent of those who received training didn't release their keys to strangers, unlike the 62.5 percent who weren't exposed to security awareness that released their keys.

Flores and Ekstedt [50] assert that transformational leadership influences employees' attitudes to social engineering techniques through informational security culture. The research clearly states that though transformational leadership lays the foundation to shape a culture that promotes information security behaviors, it is information security culture that will, in turn, impact the attitudes of employees towards social engineering tactics and security threats [50,51].

Theoretical Framework

The theoretical frameworks underpinning this study are Schein’s Model of Organizational Culture and Bass and Riggio's Transformational Leadership Model.

Schein's Model of Organizational Culture

Edgar Schein's model of organizational culture consists of a classical framework that expounds on organizational culture using artifacts and behaviors, values, and basic assumptions [52]. When employed

to analyze the security culture within banking institutions, it provides insights into how banking institutions should approach security.

As noticeable factors, banking institutions' response to incidents and breaches, commitment to security measures, surveillance cameras, access control systems, and security personnel represent banks' physical security measures; analyzing the importance banks give these measures gives hindsight as to how premium security is to banks. This factor alsoencompasses well-defined security policies, effective incident response procedures, and employees' compliance with security protocols [53].

Moreover, recognizing subcultures within the banking institute is vital; various departments or divisions in the institute will have personalized, unique characteristics, and these subcultures can positively impact the security culture differently [53]. Regarding Edgar Schein's values, a leader's commitment to security forms the basis for value; the level of priority top management gives to security will influence the security values held by employees; promoting security education and awareness training programs will improve employee responsibility in maintaining security [54]. Employing Edgar Schein's theory to analyze security culture within banking institutions allows for a comprehensive assessment of how security is approached from the visible surface to the deeply embedded basic assumptions [55].

Bass and Riggio's Transformational Leadership Model

Bass and Riggio's transformational leadership model is adopted to examine how transformational leadership impacts security awareness within organizations, which means banking institutions. Using three of its components, here is a breakdown of how it can be adopted and examined for its impact on security awareness;

Idealized Influence:

Transformational leaders in banking institutions serve as role models for security awareness. Their adherence to security protocols and ethical behavior sets the standard for employees to follow and reinforces the importance of security awareness in the workforce [32,33]. Also, toenhance banking institute security culture, transformational leaders need to recognize employees' unique needs; this will result in a more personalized and effective approach to ensuring training and support for banking staff [31,33]

Inspirational Motivation:

With the profound capacity of transformational leaders to inspire and motivate, they can share a compelling vision that motivates employees to embrace security awareness as a collective goal, thereby communicating the significance of security in preserving the reputation and trust of the institution and its clients [32,33].

Intellectual Stimulation:

Transformational leaders can encourage their employees in banking institutions to think critically and creatively about security challenges, fostering a culture of continuous learning [56]. Transformational leaders can also acknowledge and reward employees for being proactive and vigilant with security measures; this feedback and recognition approach reiterates the significance of security in the organization and encourages employees to remain vigilant. Moreover, the active involvement of

employees in discussions related to security measures and policies will enable leaders to harness the team's collective wisdom and empower employees to take ownership of the security culture [56].

Methodology

This study utilized an electronic survey questionnaire to acquire primary data from bank employees. The total number of valid questionnaires retrieved was 450, administered through email. Leveraging a five-point Likert scale model, the employees' responses were critically and analytically evaluated to test the study's hypothesis, using Linear regression to show correlative relationships between all variables.

Data Analysis

The formulated hypotheses of the study were:

H_1: There is a significant positive relationship between the level of organizational security culture and social engineering awareness among bank employees.

H_2: There is a significant positive relationship between the presence of transformational leadership and social engineering awareness among bank employees.

H_3: There is a significant positive relationship between the effectiveness of security education and social engineering awareness among bank employees.

H_4: The combined influence of organizational security culture, transformational leadership, and security education significantly positively affect social engineering awareness among bank employees.

Hypothesis 1

Table 1a. Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.991[a]	.981	.981	.56123

a. Predictors: (Constant), Organizational Security Culture

Table 1b.ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7480.111	1	7480.111	23748.282	.000[b]
	Residual	141.109	448	.315		
	Total	7621.220	449			

a. Dependent Variable: Social Engineering Awareness

b. Predictors: (Constant), Organizational Security Culture

Table 1c.Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.130	.058		2.228	.026
	OSC	1.014	.007	.991	154.105	.000

The result shows that hypothesis 1 is supported as it has been significantly established by the following derived values (Beta value = 0.991, t= 154.105, p = 0.000).

Hypothesis 2

Table 2a. Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate

1	.998[a]	.996	.996	.26979

a. Predictors: (Constant), Transformational Leadership

Table 2b.ANOVAa

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7588.610	1	7588.610	104254.613	.000[b]
	Residual	32.610	448	.073		
	Total	7621.220	449			

a. Dependent Variable: Social Engineering Awareness

b. Predictors: (Constant), Transformational Leadership

Table 2c.Coefficientsa

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.056	.028		-1.985	.048
	TL	1.007	.003	.998	322.885	.000

Hypothesis 2 reflects on the significant positive relationship between the presence of transformational leadership and social engineering awareness among bank employees. Hence, the result shows this hypothesis is supported as it has been significantly established by the following derived values (Beta value = 0.998, t = 322.885, p = 0.000).

Hypothesis 3

Table 3a. Model Summary

R	R Square	Adjusted R Square	Std. Error of the Estimate
.998[a]	.995	.995	.28343

a. Predictors: (Constant), Security Education

Table 3b.ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7585.232	1	7585.232	94425.230	.000[b]
	Residual	35.988	448	.080		
	Total	7621.220	449			

a. Dependent Variable: Social Engineering Awareness

b. Predictors: (Constant), Security Education

Table 3c.Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.001	.030		-.023	.982
	SE	1.001	.003	.998	307.287	.000

Hypothesis 3 shows a significant positive relationship between the effectiveness of security education and social engineering awareness among bank employees. Hence, the result shows this hypothesis is supported as it has been significantly established by the following derived values (Beta value = 0.998, t = 307.287, p = 0.000).

Hypothesis 4

Table 4a. Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.997[a]	.995	.995	.29263

a. Predictors: (Constant), Interplay of Organizational security culture, Transformational leadership, and Security Education

Table 4b.ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7582.857	1	7582.857	88552.999	.000[b]
	Residual	38.363	448	.086		
	Total	7621.220	449			

a. Dependent Variable: Social Engineering Awareness

b. Predictors: (Constant), Interplay of Organizational security culture, Transformational leadership, and Security Education.

Table 4c.Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.010	.031		-.314	.754
	ALL3v	.337	.001	.997	297.579	.000

a. Dependent Variable: Social Engineering Awareness

Hypothesis 4 shows how the combination of organizational security culture, transformational leadership, and security education positively influences social engineering awareness among bank employees. Hence, the result shows that this hypothesis is supported as it has been significantly established by the following derived values (Beta value = 0.997, t = 297.579, p = 0.000).

However, the interconnection of Organizational security culture, Transformational leadership, and Security Education, all with Social Engineering Awareness, is further shown in the correlation table below:

Table 5. Correlations

	OSC	TL	SE	SEA
OSC	1	.992	.992	.991
TL	.992	1	.997	.998
SE	.992	.997	1	.998
SEA	.991	.998	.998	1

Correlation is significant at the 0.01 level (2-tailed).

In the correlation above, OSC- Organizational Security Culture, TL- Transformational Leadership, SE- Security Education, and SEA- Social Engineering Awareness

Discussion

The result derived from the analytical view of the research affirms that organizational security culture does not work in isolation; rather, it has a strong relationship with social engineering awareness among banking employees. It depicts that banking institutions are unsafe from cyber threats and attacks by merely having relatively strong security policies and procedures but merging strong security policies and structures with sensitizing the employee to the risk and consequences of any breach of sensitive information while the security policies and procedures are being implemented [57].

On the other hand, the study discovered that adequate security cannot be achieved without putting the behavioral factor in an organization in place, which, in this research, reflects on the positive relationship between transformational leadership and social engineering awareness among the employees. The review of Humaidi and Balakrishnan[58] supports this opinion that the leadership style in an organization brings about both the compliance and active participation of the employee in the security aspect of an organization.

Hence, this extends its arm to how security education and social engineering awareness work together effectively while yielding a positive result. The outcome of this affirms that the two factors have a strong relationship, as established by Blake [59]; employees still have to be trained regarding the security measures needed concerning the role, irrespective of their prior knowledge.However, the combination of all these factors to war against social engineering in banking is logically dealt with, which gives a positive result that banking institutions can successfully stand their ground against any security threats and attacks [60].

Over the years, it has been evident that many organizations face a critical challenge in maintaining adequate security for handling and protecting sensitive information. This issue is particularly pronounced in banking institutions due to their access to vital public financial information, making them a primary target for cybercriminals [61]. To curb this prevailing issue, the banking sector focuses on physical security measures, including installing CCTV cameras and employing on-site security personnel to monitor activities inside and outside the workplace [62]. However, with the global advent of technology, data breaches have become common. This breach is done by leveraging employees' lack of security awareness and compromising sensitive banking information, which can significantly mar the institution's reputation. This situation shows vulnerability in banking institutions' security policies and procedures and underscores the need for a reassessment [54].

Additionally, banking institutions often fall short of establishing checks to monitor employees' activities [63], as some individuals infiltrate organizations to access sensitive information. Therefore, banking institutions must implement stringent measures to prevent such employees from accessing sensitive data [63]. It is a widely observed phenomenon that without a clear understanding of the purpose of a thing, misuse of resources is inevitable. In the context of our research, banking institutions need to communicate their vision and goals to new employees upon employment and also be made aware of the risks associated with any breaches or non-compliance with established policies, as such infractions can have detrimental effects on the bank [63,64]. This act better informs and guides employees ahead of time.

Additionally, each employee's superior will exemplify the expected behavior and standards required. Within the banking sector, leaders are crucial in inspiring and motivating employees to adhere to the bank's security culture policies. This, in turn, encourages employees to be more responsible and vigilant in identifying security risks and cyber threats.

Therefore, the role of management is important, as they often provide employees with specialized security training to keep them informed and prepared for potential social engineering manipulations and breaches of sensitive information that may occur during their work hours. As argued by Grassegger and Nedbal [51], transformational leadership lays the foundation to shape a culture that promotes information security behaviors, and it is an information security culture that will, in turn, impact the attitudes of employees towards social engineering tactics and security threats.

Security education and awareness programs are pivotal in equipping bank employees with the knowledge and skills to detect and respond to social engineering attacks. These awareness programs serve as a

continuous learning process, ensuring employees can recognize potential security threats and adapt to evolving cybersecurity challenges. Employees learn to identify unfamiliar emails, malicious links, and deceptive information manipulation with this training. Employees also receive training on the actionable steps in promptly reporting security threats and incidents, enhancing the bank's incident response capabilities [58]. These programs' effects on employees are significant; they provide employees with the tools needed to recognize, report, and mitigate social engineering threats because, as financial institutions are primary targets for infiltrators, educating employees about cyberattack tactics and the risks associated with compromised information will strengthen bank's security posture and protocol [45].

The dynamic interplay between organizational security culture, transformational leadership, and security education is a critical force shaping employee attitudes and behaviors regarding social engineering awareness [66]. These elements merge to ensure active employee engagement and commitment to the organization's vision, with security taking a paramount role.

Lacey [21] asserts that organizational security culture lays the foundation by establishing robust security policies and procedures. These policies and procedures necessitate collective participation, fostering responsibility and security consciousness among employees as they perform their daily tasks.Thereafter, transformational leadership reinforces this culture by effectively communicating the company's vision and goals, serving as a compelling motivational tool. It goes beyond mere words; it models the vigilance and practical implementation of security policies, setting an example for employees to follow and fortify the organization against social engineering attacks [32,33]. Then, security education equips employees with the essential knowledge to identify potential security threats and attacks. Regular updates keep employees informed of evolving security tactics, encompassing aspects such as recognizing malicious links, managing sensitive information, and promoting an ethic of unwavering security vigilance [45,46].

The harmonious integration of organizational security culture, transformational leadership, and security education in banking institutions creates a resilient environment where employee attitudes and behaviors prioritize and safeguard the organization's security.

Conclusion

The findings of this study expound on the pivotal impact of organizational security culture and transformational leadership in shaping social engineering awareness among bank employees, focusing on the dynamic interplay between security education and behavioral change. The study reminds the banking sector to elevate its commitment to information system security.

While investing in security technologies and robust policies are essential, this research highlights the necessity of continued and augmented investments in cybersecurity and employee education. This training must also be coupled with rigorous evaluation mechanisms to measure its effectiveness.

For a robust and effective approach, the banking sector should consider technological solutions to reduce human error and proactively counteract cyber traps. This entails limiting the exposure of critical information. Simultaneously, organizational security culture should transform, fostering full employee participation and compliance, ultimately fortifying the sector against evolving security threats.

References

1. Johnson, A. (2020). Understanding Social Engineering Schemes: Implications for Banking Security. *Cybersecurity Journal*, 9(2), 120-135

2. Leah, B. (2021). Prioritizing Human Resources in Banking Cybersecurity: Beyond Technology. *Journal of Financial Protection*, 13(4), 320-335.

3. Clark, S. (2019). Organizational Security Culture and Leadership in Social Engineering Defense. Security Studies, 6(3), 250-265.

4. Olagbaju, O. O., Babalola R.O., &Olaniyi, O. O. (2023). Code Alternation in English as a Second Language Classroom: A Communication and Learning Strategy. Nova Science. https://doi.org/10.52305/YLHJ5878

5. Martinez, L. (2021). Equipping Bank Employees: Security Education and Behavioral Modification Programs. *Information Protection Review,* 11(1), 35-50.

6. Leo, R. (2020). Heightened Vigilance: Responding to Unexpected Requests for Information in the Context of Social Engineering. *Cybersecurity Review*, 9(2), 67-79.

7. Olagbaju, O. O., & Olaniyi, O. O. (2023). Explicit and Differentiated Phonics Instruction on Pupils' Literacy Skills in Gambian Lower Basic Schools. Asian Journal of Education and Social Studies, 44(2), 20–30. https://doi.org/10.9734/ajess/2023/v44i2958

8. Anderson, K. (2022). Interplay of Organizational Security Culture and Transformational Leadership in Social Engineering Awareness. J*ournal of Banking Security*, 14(3), 285-300.

9. Deon, M. (2021). Detecting and Preventing Social Engineering Scams: The Role of Education and Behavior Change. *Security & Risk Management*, 10(2), 175-190.

10. Harris, R. (2023). Transformational Leadership, Security Culture, and Social Engineering Awareness: A Comprehensive Analysis. *Journal of Financial Security*, 7(4), 310-325.

11. Olaniyi O. O. (2022, April 26). Best Practices to Encourage Girls' Education in Maiha Local Government Area of Adamawa State in Nigeria. The University of Arkansas Clinton School of Public Service (Research Gate). https://doi.org/10.13140/RG.2.2.26144.25606

12. Marble, C. (2019). Enhancing Security Procedures: Insights from Organizational Culture and Leadership. *Cybersecurity Journal,* 12(2), 145-160.

13. Andrew, R. (2023). Exploring Social Engineering Threats: An Analysis of the Banking Sector. *Cybersecurity Journal,* 10(3), 215-230.

14. Zhang, Q. (2020). Enhancing Cybersecurity Awareness in Banks: The Role of Organizational Culture. Security Studies, 7(2), 123-138.

15. Abalaka, A. I., Olaniyi, O. O., &Adebiyi , O. O. (2023). Understanding and Overcoming the Limitations to Strategy Execution in Hotels within the Small and Medium Enterprises Sector . Asian Journal of Economics, Business and Accounting, 23(22), 26–36. https://doi.org/10.9734/ajeba/2023/v23i221134

16. Patel, A. (2019). Leadership and Security Culture: Implications for Social Engineering Awareness. *Journal of Banking Security*, 15(4), 345-360.

17. Wong, L. (2021). Security Education and Social Engineering Awareness in Banking: A Comprehensive Analysis. *Information Protection Review,* 12(1), 45-60.

18. Lopez, P. (2022). Transformational Leadership and Behavioral Change: Nurturing a Secure Banking Environment. *Journal of Financial Security*, 8(4), 289-304.

19. Gomez, R. (2023). Strengthening Banking Security: Exploring Organizational Culture and Leadership. *Security & Risk Management*, 11(2), 167-182.

20. Oladoyinbo, T. O., Adebiyi , O. O., Ugonnia, J. C., Olaniyi , O. O., &Okunleye , O. J. (2023). Evaluating and Establishing Baseline Security Requirements in Cloud Computing: An Enterprise Risk Management Approach. Asian Journal of Economics, Business and Accounting, 23(21), 222–231. https://doi.org/10.9734/ajeba/2023/v23i211129

21. Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*(1), pp.4-13.

22. Furnell, S. and Clarke, N. (2005). Organizational security culture: Embedding security awareness, education, and training. *Proceedings of the IFIP TC11 WG*, *11*, pp.67-74.

23. Security culture: NPSA (2023) National Protective Security Authority. Available at:https://www.npsa.gov.uk/security-culture (Accessed: 28 October 2023).

24. Fianty, M.I. (2023). The Impact of Employees' Information Security Awareness on Information Security Behaviour. *IJISTECH (International Journal of Information System and Technology), 6*(5), pp.629-636.

25. Olaniyi, F. G., Olaniyi, O. O., Adigwe, C. S., Abalaka, A. I., & Shah, N. H. (2023). Harnessing Predictive Analytics for Strategic Foresight: A Comprehensive Review of Techniques and Applications in Transforming Raw Data to Actionable Insights. Asian Journal of Economics, Business and Accounting, 23(22), 441–459. https://doi.org/10.9734/ajeba/2023/v23i221164

26. Tolah, A., Furnell, S.M. and Papadaki, M. (2021). An empirical analysis of the information security culture key factors framework. *Computers & Security, 108*, p.102354.

27. Olaniyi, O. O., Olabanji, S. O., &Abalaka, A. I. (2023). Navigating Risk in the Modern Business Landscape: Strategies and Insights for Enterprise Risk Management Implementation. Journal of Scientific Research and Reports, 29(9), 103–109. https://doi.org/10.9734/jsrr/2023/v29i91789

28. Olaniyi, O. O., Olabanji, S. O., &Okunleye, O. J. (2023). Exploring the Landscape of Decentralized Autonomous Organizations: A Comprehensive Review of Blockchain Initiatives. Journal of Scientific Research and Reports, 29(9), 73–81. https://doi.org/10.9734/jsrr/2023/v29i91786

29. Alsolami, H.A., Cheng, K.T.G. and Twalh, A.A.M.I. (2016). Revisiting innovation leadership. *Open Journal of Leadership*, *5*(2), pp.31-38.

30. Olaniyi, O. O., Abalaka, A. I., &Olabanji, S. O. (2023). Utilizing Big Data Analytics and Business Intelligence for Improved Decision-Making at Leading Fortune Company. Journal of Scientific Research and Reports, 29(9), 64–72. https://doi.org/10.9734/jsrr/2023/v29i91785

31. Lebek, B., Guhr, N. and Breitner, M. (2014). Transformational leadership and employees' information security performance: the mediating role of motivation and climate.

32. Ismail, A., Hidajat, T., Dora, Y.M., Prasatia, F.E. and Pranadani, A. (2023). *Leading the Digital Transformation: Evidence from Indonesia*. Asadel Publisher.

33. Azim, M.T., Fan, L., Uddin, M.A., Abdul Kader Jilani, M.M. and Begum, S. (2019). Linking transformational leadership with employees' engagement in the creative process. *Management Research Review*, *42*(7), pp.837-858.

34. Tuan, K.M. (2023). An Analysis of the Factors Impacting Transformational Leadership Competencies: A Case Study of a Vietnamese Security Firm. *International Journal of Professional Business Review*, *8*(8), pp.e02572-e02572.

35. Adebiyi , O. O. (2023). Exploring the Impact of Predictive Analytics on Accounting and Auditing Expertise: A Regression Analysis of LinkedIn Survey Data. Asian Journal of Economics, Business and Accounting, 23(22), 286–305. https://doi.org/10.9734/ajeba/2023/v23i221153

36. Abraham, S. and Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society, 32*(3), pp.183-196.

37. Olaniyi, O.O., Okunleye, O.J., &Olabanji, S.O. (2023). Advancing Data-Driven Decision-Making in Smart Cities through Big Data Analytics: A Comprehensive Review of Existing Literature. Current Journal of Applied Science and Technology, 42(25), 10–18. https://doi.org/10.9734/cjast/2023/v42i254181

38. Ghafir, I., Prenosil, V., Alhejailan, A. and Hammoudeh, M. (2016), August. Social engineering attack strategies and defence approaches. I*n 2016 IEEE 4th international conference on future internet of things and cloud (FiCloud);* pp. 145-149. IEEE.

39. Olaniyi, O.O., Olaoye O.O., &Okunleye, O.J. (2023). Effects of Information Governance (IG)on profitability in the Nigerian banking sector. Asian Journal of Economics, Business and Accounting. 2023;23(18):22–35. https://doi.org/10.9734/ajeba/2023/v23i181055

40. Airehrour, D., Vasudevan Nair, N. and Madanian, S. (2018). Social engineering attacks and countermeasures in the new zealand banking system: Advancing a user-reflective mitigation model. *Information, 9(*5), p.110.

41. Olaniyi, O.O. &Omubo, D.S. (2023). The Importance of COSO Framework Compliance in Information Technology Auditing and Enterprise Resource Management. The International Journal of Innovative Research & Development. https://doi.org/10.24940/ijird/2023/v12/i5/MAY23001

42. Price, J.D. (2014). Reducing the risk of a data breach using effective compliance programs (Doctoral dissertation, Walden University).

43. Bush, L. (2020). Examining the Relationship Between Cybersecurity-Employee Vulnerabilities and Reduction of Security Breaches in Information Technology Organization (Doctoral dissertation, Colorado Technical University).

44. Corradini, I. (2020). Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology (Vol. 284). Springer Nature.

45. Salahdine, F. and Kaabouch, N. (2019). Social engineering attacks: A survey. Future internet, 11(4), p.89.

46. Yurcik, W. and Doss, D. (2001), November. Different approaches in the teaching of information systems security. In Proceedings of the Information Systems Education Conference; pp. 32-33.

47. Omogoroye, O. O., Olaniyi, O. O., Adebiyi, O. O., Oladoyinbo, T. O., & Olaniyi, F. G. (2023). Electricity Consumption (kW) Forecast for a Building of Interest Based on a Time Series Nonlinear Regression Model. Asian Journal of Economics, Business and Accounting, 23(21), 197–207. https://doi.org/10.9734/ajeba/2023/v23i211127

48. Bullée, J.W.H., Montoya, L., Pieters, W., Junger, M. and Hartel, P.H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of experimental criminology, 11*, pp.97-115.

49. Olabanji, S. O. (2023). Technological Tools in Facilitating Cryptocurrency Tax Compliance: An Exploration of Software and Platforms Supporting Individual and Business Adherence to Tax Norms. Current Journal of Applied Science and Technology, 42(36), 27–39. https://doi.org/10.9734/cjast/2023/v42i364239

50. Flores, W.R. and Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture, and awareness. *Computers & Security, 59*, pp.26-44.

51. Grassegger, T. and Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science, 181*, pp.59-66.

52. Otieno, E.O. (2021). *The Impact of Organizational Culture on Information Security Compliance Culture: a Case of Kenyan Universities (*Doctoral dissertation, University of Nairobi).

53. Hattangadi, V. (2017). Edgar Schein's three levels of organizational culture. Retrieved November 15, p.2018.

54. Khripunov, I. (2023). National and Organizational Culture. *In Human Factor in Nuclear Security: Establishing and Optimizing Security Culture* (pp. 13-30). Cham: Springer International Publishing.

55. Olabanji , S. O. (2023). Advancing Cloud Technology Security: Leveraging High-Level Coding Languages like Python and SQL for Strengthening Security Systems and Automating Top Control Processes. Journal of Scientific Research and Reports, 29(9), 42–54. https://doi.org/10.9734/jsrr/2023/v29i91783

56. Nyakomitta, K.O. (2021). *Influence of Transformational Leadership on the Performance of Commercial Banks in Kenya* (Doctoral dissertation, JKUAT-COHRED).

57. Conolly, P. (2000). Security Starts from Within. *InfoWorld 22*(28), 39-40.

58. Humaidi, N., and Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology, 5*(4), 311.

59. Blake, S. (2000). Protecting the Network Neighbourhood. *Security Management 44*(4), 65-71.

60. D'Arcy, J., and Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal, 29*(1), 43–69.

61. Adigwe , C. S., Abalaka, A. I., Olaniyi , O. O., Adebiyi , O. O., &Oladoyinbo, T. O. (2023). Critical Analysis of Innovative Leadership through Effective Data Analytics: Exploring Trends in Business Analysis, Finance, Marketing, and Information Technology. Asian Journal of Economics, Business and Accounting, 23(22), 460–479. https://doi.org/10.9734/ajeba/2023/v23i221165

62. Stanciu, V., and Tinca, A. (2017). Exploring cybercrime–realities and challenges. *Accounting and Management Information Systems*, *16*(4), 610-632.

63. Ghosh, A., 2012. *Managing risks in commercial and retail banking*. John Wiley & Sons.

64. Guhr, N., Lebek, B., and Breitner, M. H. (2019). The impact of leadership on employees' intended information security behavior: An examination of the full-range leadership theory. *Information Systems Journal, 29*(2), 340–362.

65. Yoo, C.W., Sanders, G.L. and Cerveny, R.P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems, 108*, pp.107-118.

66. Olaniyi, O.O. &Omubo, D.S. (2023). WhatsApp Data Policy, Data Security, And Users' Vulnerability. The International Journal of Innovative Research & Development. https://doi.org/10.24940/ijird/2023/v12/i4/APR23021

APPENDIX

QUESTIONNAIRE

Employee's years in service			
1-5 years	**6-10 years**	**10-15 years**	**15 years and above**

Organizational Security Culture						
S/N	**ITEMS**	**SA**	**A**	**N**	**D**	**SD**
		1	**2**	**3**	**4**	**5**
1	**I know the organizational security policies and procedures of where I work**					
2	**Organizations usually keep their employees informed of its security policies and procedures**					
3	**Employees often regard the organization's security policies and procedures**					

Transformational leadership						
S/N	**ITEMS**	**SA**	**A**	**N**	**D**	**SD**
		1	**2**	**3**	**4**	**5**
1	**Oftentimes, am encourage to work in line with the management's vision**					
2	**The management are a good role model to work with; always supportive and can be trusted.**					

3	**My superiors and I have a good smooth working relationship**					

Security Education						
S/N	**ITEMS**	**SA**	**A**	**N**	**D**	**SD**
		1	**2**	**3**	**4**	**5**
1	**I can easily identify any malicious or potential security threat in my role in the organization**					
2	**Employees are always empowered with the necessary security knowledge**					
3	**Am aware of how to handle sensitive information and storing documents to avoid any form of breach.**					

Social Engineering						
S/N	**ITEMS**	**SA**	**A**	**N**	**D**	**SD**
		1	**2**	**3**	**4**	**5**
1	**Am aware of the security risk in my role in the organization**					
2	**Organizational management responds fast to suspicious security reports**					
3	**The organization's policies and procedures is potent enough to curb any act of security manipulations**					

Result analysis and presentation

Employee's years in service

	Frequency	Percent	Valid Percent	Cumulative Percent
1-5 years	110	24.4	24.4	24.4
6-10 years	130	28.9	28.9	53.3
11-15 years	120	26.7	26.7	80.0
15 years above	90	20.0	20.0	100.0
Total	450	100.0	100.0	