DISCOVERY

The role of Self-Efficacy in effective strategies to promote secure behavior among employees in Tanzania's public authorities: A case of Tanzania Communication Regulatory Authority (TCRA)

Itonge Julius[1], **Kenneth Mlelwa**[2]

To Cite:
Julius I, Mlelwa K. The role of Self-Efficacy in effective strategies to promote secure behavior among employees in Tanzania's public authorities: A case of Tanzania Communication Regulatory Authority (TCRA). *Discovery* 2023; 59: e119d1362
doi: https://doi.org/10.54905/disssi.v59i333.e119d1362

Author Affiliation:
[1]Department of Informatics, Institute of Accountancy Arusha, Arusha, Tanzania, Email: itojr04@gmail.com, ORCID: 0000-0002-4483-8740
[2]Head of ICT Department, The Mwalimu Nyerere Memorial Academy, Dar es Salaam, Tanzania

Peer-Review History
Received: 16 August 2023
Reviewed & Revised: 19/August/2023 to 24/October/2023
Accepted: 28 October 2023
Published: 01 November 2023

Peer-Review Model
External peer-review was done through double-blind method.

Discovery
pISSN 2278–5469; eISSN 2278–5450

ABSTRACT

The increasing reliance on information systems in public authorities in Tanzania has heightened the importance of ensuring secure behavior among employees to safeguard sensitive data and protect against potential threats. However, promoting secure behavior remains challenging for organizations, leading to vulnerabilities in their information systems. This study explored self-efficacy (SE) in effective strategies to promote secure employee behavior toward information systems in Tanzania's public authorities, using the Tanzania Communication Regulatory Authority (TCRA), Dar es Salaam, as a case study. This study uses A Social Cognitive Theory as a guiding theory. Findings indicated that employees' performance of secure behavior is affected by the low level of SE since more employees seemed to have doubts about their confidence level in undertaking security-related tasks. The study recommends the improvement in the current security awareness programs that should find a way to focus on the SE of employees to improve their confidence in performing secure behavior and also on the development of clear security guidelines that are user-friendly to employees to make them understand what the importance of them adhering to security guidelines and policies and hence feel comfortable executing them. This study recommended more research on public and private organizations to add to the body of knowledge on improving strategies to promote secure employee behavior.

Keywords: Secure behavior, self-efficacy, information systems, employees' confidence, social cognitive theory

DISCOVERY
SCIENTIFIC SOCIETY

1. INTRODUCTION

One of the main contributing elements to the security of the information system is the behavior of employees (Anwar et al., 2017). The perspectives and actions of employees can either add to or hinder the security of the information system from different threats (Sasu, 2014). Research has shown that employees have shifting perspectives and behaviors toward information system security, and different variables, like their level of security awareness, their role in the organization, and their own beliefs and values, affect their behavior (Grassegger and Nedbal, 2021). Ayereby et al., (2018) stated that employees are the weakest point in information security and the primary cause of security vulnerabilities, either because they engage in unethical behavior at work that jeopardizes organizational information security or because they give computer hackers access to their organization's computers, making them vulnerable to attack or hacking.

Despite the importance of employee behavior in ensuring the information system's security, organizations still need to work on encouraging secure conduct among employees (Grassegger and Nedbal, 2021). However, this is because security education and awareness could be more effective at encouraging secure conduct, and there needs to be more knowledge about the elements that affect employee behavior. As a result, businesses struggle to create strategies that effectively encourage secure behavior and defend the information system against various threats. Empirical studies based on behavioral theories have been carried out to explore the persistent phenomenon of employees disobeying information security regulations (Njenga, 2016). Examples include General Deterrence Theory (GDT) D'Arcy and Herath, (2011), Neutralization Theory Skowronek, (2022), and Self-Determination Theory (SDT) (Frank and Kohn, 2023).

Social Cognitive Theory (SCT), developed by Albert Bandura, (1986) describes the influence of individual experiences, the actions of others, and environmental factors on individual health behaviors. Through the perspective of SCT, this study intends to research how people's self-efficacy beliefs shape their impression of information security threats and impact their judgment concerning secure behavior. According to research, most organizations have information security policies, but employees routinely and intentionally violate or disregard them (Njenga, 2016). Posey and Shoss, (2022) reports indicated that user violations of information security policies accounted for more than half of all information security breaches.

Studies have shown that the lack of understanding of the factors influencing employees' behavior is a significant barrier to developing effective strategies to promote secure behavior (Siponen et al., 2014). A similar problem affects Tanzania's electronic government information systems, as almost all information systems are vulnerable to attacks due to the rising frequency of information security threats (Dewa and Zlotnikova, 2014). Therefore, this study aimed to assess the role of self-efficacy in effective strategies to promote secure behavior among employees in Tanzania's public authorities to determine the influence of high confidence in performing security-related tasks.

Literature Review

According to studies Liao et al., (2021), Rashid et al., (2019), employees' attitudes and behaviors toward information system security vary. While some personnel are highly aware of safety issues and take aggressive measures to protect the information system, others must be aware of them and respect safety precautions (Kim and Park, 2019). Numerous factors, including an employee's level of safety awareness, their position within the company, and their traits and convictions, impact how they behave (Humphreys and Liao, 2020). Employees' adoption of secure behavior toward information systems depends significantly on self-efficacy, an essential concept in social cognitive theory. Self-efficacy is the degree to which a person believes they can carry out a behavior successfully.

Employees' self-efficacy in information security might affect their drive, judgment, and general success in adopting and upholding secure behaviors (Hajloo, 2014). Self-efficacy refers to an employee's belief in their ability to adopt secure behaviors and safeguard confidential data and systems (Rhee et al., 2009). self-efficacy, in several ways, influences employees' adoption of secure behavior. According to Barni et al., (2019), employees who have greater levels of self-efficacy are more self-assured in their abilities to carry out security-related tasks, take the initiative to adopt secure behaviors, persist with it once they do, and believe that security issues are possible to manage. However, the studies reviewed have not focused on the public authorities in Tanzania, especially the Tanzania Communication Regulatory Authority (TCRA). In this manner, this study aimed to understand the factors affecting effective strategies to promote secure employee behavior toward information systems in public authorities in Tanzania.

2. MATERIAL AND METHODS

The study was conducted at the Tanzania Communication Regulatory Authority (TCRA) Dar es Salaam, using a mixed-method research approach, which helped the researcher gain an in-depth understanding of the influence of SE in promoting secure behavior among employees. A total of 79 respondents from employees were employed in the study using probability and non-probability sampling techniques. Purposive sampling was applied to select respondents based on their role in the organizations, and simple random sampling was applied to select different individuals in their respective departments. The collected data was analyzed using descriptive statistics, correlation, and multiple linear regression analysis with the help of Statistical Package for Social Sciences (SPSS) software.

3. RESULTS

Table 1 shows the reliability test and the measure of internal consistency of the instruments employed in the study. Using Cronbach Alpha, Table 1 demonstrates that the reliability of the instruments was good according to Cronbach Alpha's scale, which explains that the reliability is excellent when the Cronbach alpha is between 0.9 – 1, good when between 0.8 – 0.9, and acceptable when between 0.7 – 0.8.

Table 1 Reliability Test

Variables	Number of Items	Cronbach alpha	Internal consistency
Self-efficacy	8	0.832	Good

Table 2 shows the demographic characteristics of the respondents where gender (male=63.3%, and female=36.7%), age of the respondents (<30 years=11.4%, 30-50 years=66.9%, and +50 years=19%), position of the respondents (leadership=16.5%, Technical (ICT) =22.8%, and Normal user=60.8%) and the work experience of the respondents (<5 years=7.6%, 5 - 10 years=48.1%, and +10 years=43.0%). These findings explain that male respondents were many compared to female respondents, most of the respondents propagated in the age group of 30 to 50 years of age, with normal user position of the respondents took up most of the respondents, but also the work experience of most of the respondents lie between 5 to 10 years of experience.

Table 2 Demographic characteristics of the respondents

Category	Variable	Frequency	Percent
Gender	Male	50	63.3%
	Female	29	36.7%
Age	<30 years	9	11.4%
	30 – 50 years	55	66.9%
	50 + years	15	19%
Position	Leadership	13	16.5%
	Technical (ICT)	18	22.8%
	Normal user	48	60.8%
Experience	<5 years	7	7.6%
	5 – 10 years	38	48.1%
	10+ years	34	43.0%

Table 3 shows the statistical data of the findings that effective use of security measures to protect sensitive information (min=2, max=5, mean=3.25 and STD=0.707), successful application of security best practices in the daily task (min=2, max=4, mean=3.04, and STD=0.759), also employees' consistency in following security protocols when accessing sensitive data (min=2, max=5, mean=3.18 and STD=0.694). It also revealed confidence in securely storing and transmitting confidential information (min=2, max=5, mean=3.08 and STD=0.656).

There was also an assessment of the risk associated with sharing information with colleagues or third parties (min=2, max=5, mean=3.24, and STD=0.720). Other responses show confidence in applying security training and guidelines in work tasks by (min=2, max=5, mean=3.27, and STD=0.614). On the other hand, to positively influence colleagues to adopt secure behavior is shown by

(min=2, max=5 mean=3.05 and STD=0.714), as the confidence in encouraging colleagues toward reporting security incidents promptly by (min=2, max=5, mean=3.04, and STD=0.694).

Table 3 The role of SE in effective strategies to promote secure behavior

Descriptive statistics on the role of SE in effective strategies to promote secure behavior among employees	*N*	*Min*	*Max*	*Mean*	*Std. D*
Effectively use of security measures to protect sensitive information.	79	2	5	3.25	.707
Successfully application of security best practices in daily tasks.	79	2	4	3.04	.759
Consistency in following security protocols when accessing sensitive data.	79	2	5	3.18	.694
Confidence in the ability to securely store and transmit confidential information.	79	2	5	3.08	.656
Assessment of the risk associated with sharing information with colleagues.	79	2	5	3.24	.720
Confidence in the ability to apply security training and guidelines in work tasks	79	2	5	3.27	.6.14
Positively influence colleagues to adopt secure behavior	79	2	5	3.05	.714
Confidence in encouraging colleagues to report security incidents promptly	79	2	5	3.04	.694
Valid N (listwise)	79	-	-	-	-

Regression analysis

Table 4 shows the model summary's coefficient of determination (R2), which explains 47.6% of the independent variable. This result suggests that the independent variable, self-efficacy, explains only 47.6% of the secure behavior among employees toward the information systems; hence, the coefficient of determination is statistically significant.

Table 4 Model Summary

R	R2	Adjusted R2	Std. Error of the Estimate
.690	.476	.453	.594

Table 5 shows the degree of freedom with a df numerator of 1 and a df denominator of 23 with a computed F value of 20.882 and a p-value of 0.000, less than 0.001. This output demonstrates the statistical significance of the overall regression model and its suitability to explain how the independent variable chosen impacts employees' secure behavior.

Table 5 ANOVAa Test

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	1.815	1	1.815	20.882	.000b
Residual	1.999	23	.087	-	-
Total	3.814	24			

Table 6 shows that Self-efficacy significantly predicted employees' secure behavior toward information systems, F (1, 23) =20.882, p<0.001, which means that employees' self-efficacy can play a significant role in influencing secure behavior (b=0.61, *p*<0.001). The output depicts that self-efficacy directly affects the secure behavior toward information systems.

Table 6 Coefficientsa

	Unstandardized Coefficients		Standardized Coefficients		
Model	B	Std. Error	Beta	t	Sig
(Constant)	2.629	0.132	-	19.940	0.000
SE	0.61	0.013	0.690	4.570	0.000

4. DISCUSSION

The researcher measured respondents' confidence in performing secure behavior using the five-point Likert scale. The findings showed that despite most respondents seeming to be unsure about their confidence when performing secure behavior toward information systems, a substantial number of responses showed confidence in their ability to perform secure behavior. Previous studies show that employees with higher levels of self-efficacy feel more confident in their ability to perform security-related tasks, take the initiative to adopt secure behavior, and persist in adopting secure behavior (Rhee et al., 2009; Hajloo, 2014). It is crucial to improve the employees' confidence in performing secure behavior, as people with high levels of self-efficacy are more confident in undertaking secure behavior practices toward information systems.

5. CONCLUSION

This study showed a significant relationship between employees' self-efficacy and secure behavior toward information systems. Based on the findings of this study, employee's confidence to perform secure behavior is of great importance. Therefore, it is high time for public authorities to improve the security awareness programs to make sure they are also focusing on advancing the confidence of employees in performing numerous security-related tasks by showing them the importance of doing so using real-life examples to make them more comfortable and well understand what they are required to do to preserve the information systems security. The current study mainly focused on assessing the role of self-efficacy in effective strategies to promote secure behavior among employees toward information systems in public authorities.

More research needs to be done in this area as the challenges of dealing with the human element in security are changing rapidly with the increase in numerous security threats. Further studies may consider researching other public and private organizations, as this study focused on only one public authority due to time limitations and resources. There is still a need to research this topic using other theories based on human behavior, like the General Deterrence Theory (GDT), theory of planned behavior, Self-determination Theory (SDT), and Protection Motivation Theory (PMT), to explore the problem from an in-depth perspective and come up with the actionable results.

Acknowledgments

I am deeply grateful to almighty God for his blessings during this work. I want to thank all those who have supported me in this research journey. I sincerely appreciate my supervisor, Dr Mlelwa, for his invaluable guidance, encouragement, and support throughout the development of this dissertation. I would also like to acknowledge the contributions of the Tanzania Communication Regulatory Authority (TCRA), who have provided valuable insights and support to help make this research a reality. All participants agreed to participate in this study. Finally, this research would not have been possible without the support and encouragement of all those involved. I am genuinely grateful for the contributions and unwavering support they have given.

Author's contribution

Itonge Julius: Student, Researcher

Kenneth Mlelwa: Research supervisor, Lecturer

Informed consent

Not applicable.

Ethical approval

Not applicable.

Conflicts of interests

The authors declare that there are no conflicts of interests.

Funding

The study has not received any external funding.

Data and materials availability

All data associated with this study are present in the paper.

REFERENCES AND NOTES

1. Anwar M, He W, Ash I, Yuan X, Li L, Xu L. Gender difference and employees' cybersecurity behaviors. Comput Human Behav 2017; 69:437–443. doi: 10.1016/j.chb.2016.12.040
2. Ayereby MP Marius, Committee R, Chairperson C, Management A, Faculty DS, Member C. Walden University 2018.
3. Bandura A. Social foundations of thought and action. Upper Saddle River, NJ: Prentice Hall, 1986.
4. Barni D, Danioni F, Benevene P. Teachers' Self-Efficacy: The Role of Personal Values and Motivations for Teaching. Front Psychol 2019; 10:1645. doi: 10.3389/fpsyg.2019.01645
5. D'Arcy J, Herath T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. Eur J Inf Syst 2011; 20(6):643–658. doi: 10.1057/ejis.2011.23
6. Dewa M, Zlotnikova I. Current Status of e-Government Services in Tanzania: A Security Perspective. ACSIJ 2014; 3(3): 9.
7. Frank M, Kohn V. Understanding extra-role security behaviors: An integration of self-determination theory and construal level theory. Comput Secur 2023; 132:103386. doi: 10.1016/J.COSE.2023.103386
8. Grassegger T, Nedbal D. The role of employees' information security awareness on the intention to resist social engineering. Procedia Comput Sci 2021; 181:59–66. doi: 10.1016/j.procs.2021.01.103
9. Hajloo N. Relationships between self-efficacy, self-esteem and procrastination in undergraduate psychology students. Iran J Psychiatry Behav Sci 2014; 8(3):42–9.
10. Humphreys J, Liao T. The role of employee perceptions and attitudes in workplace cybersecurity. Comput Secur 2020; 91: 101713.
11. Kim Y, Park S. A study on the effects of information security awareness on the security behavior of employees in the financial sector. Sustainability 2019; 11:2754.
12. Liao C, Yang Y, Li J, Li J. How do social media promote knowledge sharing? A meta-analysis of antecedents and consequences. Inf Manag 2021; 58:103370.
13. Njenga K. Information Systems Security Policy Violation: Systematic Literature Review on Behavior Threats by Internal Agents. CONF-IRM 2016 Proc 2016; 39.
14. Posey C, Shoss M. Research: Why Employees Violate Cybersecurity Policies. Harvard Business Review 2022.
15. Rashid T, Aslam B, Abro AH. A critical review of the security threats, attacks, and vulnerabilities of internet of things (IoT). Int J Adv Comput Sci Appl 2019; 10:197–206.
16. Rhee HS, Kim C, Ryu YU. Self-efficacy in information security: Its influence on end users' information security practice behavior. Comput Secur 2009; 28(8):816–826. doi: 10.1016/j.cose.2009.05.008
17. Sasu A. MASTER'S THESIS. Human Threats to Information Security by Employees in an Organisation 2014.
18. Siponen M, Adam MM, Pahnila S. Employees' adherence to information security policies: An exploratory field study. Inf Manag 2014; 51(2):217–224.
19. Skowronek SE. DENIAL: A conceptual framework to improve honesty nudges. Curr Opin Psychol 2022; 48:101456. doi: 10.1016/j.copsyc.2022.101456