JPM Jurnal Prima Manajemen E-ISSN : 3123-7266

Measuring Multi-Channel IT Security Awareness Effectiveness in Strengthening Cybersecurity Culture at Bank XYZ

Naufalarizqa Ramadha Meisa Putra
Teknik Informatika, Fakultas Teknik, Universitas Satya Negara Indonesia,
Jakarta, Indonesia
naufalarizqa@usni.ac.id

Abstract
Information security awareness is a critical determinant in mitigating human-related cybersecurity risks within the banking sector. This study evaluates the implementation and effectiveness of the IT Security Awareness program conducted by Bank XYZ throughout 2025. The program adopted a multi-channel delivery model encompassing newsletters, flyers, desktop wallpapers, monthly quizzes, e-learning modules, and webinars. A descriptive quantitative and qualitative approach was employed using participation statistics, learning outcomes, and employee engagement trends obtained from internal organizational systems. The findings reveal that interactive awareness media substantially outperform passive content in terms of employee engagement. The e-learning module reached 14,810 employees (88.86% of the total workforce) with a completion rate of 99.68%. Monthly quizzes achieved an average participation of 3,520 employees, with a peak of 5,123 participants in November 2025. In contrast, webinar participation remained comparatively low at 413 employees. These results indicate that continuous, interactive, and context-driven awareness initiatives significantly enhance employee cybersecurity awareness. This study contributes empirical evidence for the design of sustainable, data-driven IT security awareness programs in large banking institutions.

Keywords: IT Security Awareness; Cybersecurity; Employee Engagement; Security Risk.

1. INTRODUCTION

Information security is an essential component in ensuring operational continuity and public trust in banking institutions. The massive digital transformation in the banking sector has increased reliance on information systems and expanded the surface area for cyberattacks. Several studies have shown that most security incidents are triggered by human factors, either through negligence, lack of awareness, or a lack of understanding of cyber threats.

Bank XYZ, as a national banking institution, manages large volumes of financial data and sensitive information. In this context, technical controls such as firewalls and endpoint security need to be complemented by increased security awareness at the individual level. The IT Security Awareness program is a strategic element within the information security governance framework to shape employee security behaviors sustainably.

In 2025, Bank XYZ implemented a structured and ongoing IT Security Awareness program through various media. However, the effectiveness of this program needs to be empirically evaluated based on implementation data. This study aims to evaluate the

Article info
Received 22 Januari 2026
Revised 26 Januari 2026
Accepted 31 Januari 2026
Available Online 1 Februari 2026
naufalarizqa@usni.ac.id

achievement, level of employee engagement, and effectiveness of each awareness media used.

2. LITERATURE REVIEW

2.1 Security Awareness and Human Factors

Security awareness is generally defined as an individual's level of understanding of information security risks and organizational policies, as well as the ability to implement appropriate security practices in the context of daily operations. Several studies have shown that awareness is not only related to knowledge but also includes attitude and behavior as key determinants of preventive action against information security incidents.

The human factor is consistently cited as the weakest link in information security systems. Industry surveys indicate that the majority of cyber incidents are caused by human errors, social engineering, or non-compliance with internal security policies. Consequently, organizations need to implement learning-based interventions and behavior change as strategic components of a defense-in-depth system.

2.2 Security Awareness in the Banking Sector

Banking institutions operate in an environment with higher levels of risk and compliance requirements than the non-financial sector. Cyber threats targeting this sector include data theft, transaction manipulation, ransomware-based extortion, and advanced social engineering attacks that utilize impersonation, fraud, or business email compromise.

Security awareness programs in the banking sector should ideally be continuous, adaptive to the evolving threat landscape, and based on actual risks relevant to the organization's business processes. Furthermore, effective programs are generally complemented by evaluation tools and implementation controls to measure the level of behavioral change, the effectiveness of learning, and the contribution to reducing potential incidents.

2.3 Awareness Program Evaluation

Awareness program evaluation is conducted using both quantitative and qualitative approaches to generate a holistic interpretation. The quantitative approach can include indicators of participation, completion rates, test or quiz scores, and frequency of content consumption. Meanwhile, the qualitative approach focuses on the relevance of the material to the organizational context, the consistency of security messages, the credibility of the material, and participants' perceptions of the program's benefits and impact on their daily work. The integration of these two approaches is expected to provide a picture not only of the technical effectiveness of the learning program, but also of its implications for security culture within banking organizations.

3. METHODOLOGY

This research used a descriptive method with both quantitative and qualitative approaches. The descriptive method was chosen to provide an objective representation of the implementation, achievements, and challenges of the security awareness program during the observation period.

3.1 Data Sources

Data for this study were obtained from four main sources:

1) The IT Security Awareness Quiz System
   Served as a source of learning evaluation data, including scores, pass rates, and participant engagement.
2) Bank XYZ's internal e-learning platform

Used to obtain information on participation, module completion, and the intensity of digital-based material consumption.

3) Webinar Data Recapitulation
Provided quantitative data on the number of participants, attendance duration, interaction dynamics, and participation trends in online sessions.

4) Awareness Content Distribution Report
Used to map the reach and intensity of content distribution, including infographics, educational videos, and digital campaign materials.

3.2 Analysis Techniques

The analysis techniques were conducted in three main stages:

1) Content distribution analysis by media type
This stage assesses the proportion of learning media use (e.g., videos, articles, quizzes, webinars, and infographics) and its relationship to participant consumption patterns.

2) Analysis of participation levels and learning outcomes
This stage involves measuring engagement metrics (participation, attendance, module completion) and learning outcomes (quiz scores, score improvement, or conceptual understanding).

3) Identification of monthly engagement trends
This stage observes changes in participant engagement levels over time to map patterns, consistencies, and factors driving fluctuations.

4) Qualitative interpretation of quantitative findings
This stage aims to explain the context, meaning, and implications of the numerical data, including organizational, operational, and behavioral factors that influence the success of the awareness program.

4. RESULTS AND DISCUSSION

4.1 Quantitative Analysis

4.1.1 Awareness Content (Program Output)

Table 4.1 Distribution of IT Security Awareness content of Bank XYZ (2025)

No	Content Type	Amount	Percentage
1	Flyer	18	40.9%
2	Newsletter	12	27.3%
3	Quiz	12	27.3%
4	Desktop Wallpaper	4	9.1%
5	E --learning	1	2.3%
6	Webinar	1	2.3%
	Total	44	100%

Source: (Bank XYZ, 2025)

Component interactive (quizzes, e-learning, webinars) = 31.8% of total content, the rest nature passive (flyers, newsletters, wallpapers)

4.1.2 Scope and Outcomes of E-learning

Table 4.2 Summary of IT Security Awareness E-learning performance (2025)

Information	Mark
Total employees (data coverage)	16,667
Employee do	14,810
Employees Not yet do	1,857
Passed	14,763
Not pass	47
Average value	80.73
Participation	88.86%
Graduation rate	99.68%

Source: (Bank XYZ, 2025)

E-learning reach majority employees (88.86%) and very high completion (99.68%) with average value of 80.73, indicating effectiveness instrument mandatory and structured.

4.1.3 Monthly Quiz Participation and Results

Table 4.3 Recap of participation & results of the IT Security Awareness Quiz (2025)

Month	Participant	% of Total Employees	Average value	Not pass
January	3,326	19.96%	98.2	8
February	2,924	17.55%	99.2	10
March	3,255	19.53%	99.4	3
April	3,538	21.23%	96.5	22
Mei	2.996	17.98%	97.1	36
June	3.756	22.53%	95.8	72
July	3.411	20.47%	96.3	17
Agustus	3.195	19.17%	99.1	4
September	3.239	19.43%	98.8	13
October	3.020	18.12%	97.2	10
November	5.123	30,73%	97,7	50
Desember	3.844	22,53%	97,5	26

Source: (Bank XYZ, 2025)

Based on results data processing in Table 4.3, total participation for One year reached 41,627 participants. The average participation monthly totaling 3,468.92 participants with median value 3,290.5 participants. Deviation standard amounting to 594.17 resulting in coefficient variation (CV) of about 17.13%, which indicates level variation participation inter-monthly is in the category moderate. Peak participation happened in the month November with 5,123 participants, while level participation lowest recorded in the month February with 2,924 participants. In total overall, range variation participation reached 2,199 participants, indicating existence quite a fluctuation significant in distribution involvement participant throughout year.

4.1.4 Webinar Participation

Table 4.4 Summary of Webinar participation

Parameter	Mark
Total participant	413
Number of groups/regions	25

Source: (Bank XYZ, 2025)

Table 4.5 Distribution of participants by group/region (Top-10)

Ranking	Group/Region	Participant	Share (%)
1	Financing Center Group	191	46.25
2	Financing Operations Group	62	15.01
3	Surabaya Region	33	7.99
4	Kalimantan Region	16	3.87
5	Aceh Region	14	3.39
6	SME & Micro Risk Group	14	3.39
7	Jakarta Region 2	13	3.15
8	Semarang Region	11	2.66
9	Medan Region	10	2.42
10	Bandung Region	9	2.18

Source: (Bank XYZ, 2025)

Distribution participant webinar across 25 groups/regions and share (%) is calculated against a total of 413 participants.

4.2 Qualitative Analysis

4.2.1 Program Strengths

a) Consistency & continuity

The program is carried out regularly throughout year with approach multi-channel (newsletter, flyer, wallpaper, monthly quiz, e-learning, webinar), building reinforcement and maintenance top-of-mind issue security information.

b) Instrument interactive superior

E-learning (88.86% participation, 99.68% pass rate) and quizzes (±3,469 participants / month) resulted in engagement tall at a time provide metric measurable for evaluation.

c) Relevance material as driver

Surge (5,123 participants) was consistent with topic Highly contextual Banking Cybercrime for XYZ Bank audience.

4.2.2 Main Challenges

a) Coverage webinar limited

Only 413 participants participated so that need format innovation (e.g. live polls, studies) cases, extended Q&A) and orchestration invitation unit - based engagement low for increase reach.

b) The impact of passive media difficult measurable

Flyers and wallpapers No own indicator individual participation so that need proxy KPI (impressions, open/click, wallpaper adoption) so that you can assessed his contribution.

c) Variation inter-monthly

February become lowest (2,924) because indication sensitivity to timing (seasonal / capacity) business) and power pull topic as well as importance content calendar adaptive.

4.2.3 Managerial Implications

a) Keep it up channel interactive as bone back (e-learning and monthly quiz) and set a participation target per unit for equality.

b) Repositioning the webinar with schedule at peak availability, use an interactive format, and do micro-campaign to historical units low his participation.

c) Measure passive media with proxy metrics standardized so that decisions content more based evidence (evidence-based).

5. CONCLUSIONS

The 2025 IT Security Awareness Program implemented by Bank XYZ demonstrated substantial effectiveness in enhancing organizational security culture, particularly in terms of employee awareness and engagement. The program employed a multichannel instructional framework; however, e-learning modules and structured assessments emerged as the most successful components, delivering broad participation and rigorous evaluation outcomes. E-learning achieved an 88.86% participation rate and a 99.68% pass rate, indicating not only high accessibility but also strong assimilation of key security competencies among employees. These findings suggest that self-paced digital learning is particularly well-suited to the operational characteristics and regulatory demands of the banking sector.

Conversely, the webinar component, although offering value through synchronous interaction and contextual discussion, exhibited lower engagement and demonstrated the need for refinement in delivery format, scheduling alignment, and promotional strategies. The comparative performance between channels highlights the importance of selecting pedagogical modalities that align with employee workflows and learning preferences.

Overall, the results underscore that the sustainability of an information security awareness program depends on three critical pillars: program continuity, topical relevance aligned with evolving cyber threats, and robust, quantifiable performance metrics. These elements form the basis of an adaptive and resilient security awareness framework that supports compliance obligations and strengthens cyber risk mitigation within the financial services industry.

REFERENCES

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society.* https://doi.org/10.48550/arXiv.1901.02672

Bank XYZ. (2026). *Laporan Pelaksanaan IT Security Awareness Tahun 2025*. Dokumen internal.

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity, 8*(1). https://doi.org/10.1093/cybsec/tyac006

Colwill, K. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report, 14*(4), 186–196.

Da Veiga, A. (2019). Achieving a security culture. In *Cybersecurity Education for Awareness and Compliance*. IGI Global. https://doi.org/10.4018/978-1-5225-7847-5.CH005

ENISA. (2019). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. European Union Agency for Cybersecurity.

Furnell, S., & Clarke, N. (2007). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 26*(6), 404–409.

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cyber behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Haney, J., & Lutters, W. (2020). Security awareness training for the workforce: Moving beyond "check-the-box" compliance. *IEEE Computer Magazine, 53*(10). https://doi.org/10.1109/MC.2020.3001959

Hinsz, V. B. (2025). Motivating cybersecurity behaviors: A beyond reasoned action conceptualization. *Organizational Cybersecurity Journal: Practice, Process & People, 5*(1), 60–78. https://doi.org/10.1108/OCJ-08-2023-0015

ISO. (2022). *ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*. International Organization for Standardization.

Kambourakis, N. F., Gritzalis, S., & Parkin, C. (2019). Evaluating information security awareness programs: A critical review. *Information & Computer Security, 27*(2), 237–258.

National Institute of Standards and Technology. (2003). *NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program*. NIST.

Orehek, Š., & Petrič, G. (2021). A systematic review of scales for measuring information security culture. *Information and Computer Security, 29*(1), 133–158. https://doi.org/10.1108/ICS-12-2019-0140

Parsons, S., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267–270.

Sumner, A., Yuan, X., Anwar, M., & McBride, M. (2022). Examining factors impacting the effectiveness of anti-phishing trainings. *Journal of Computer Information Systems, 62*(5), 975–997. https://doi.org/10.1080/08874417.2021.1955638

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2018). Analyzing information security awareness through social dimensions. *Information Systems Management, 35*(3), 263–280.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Verizon. (2024). *Data Breach Investigations Report*. Verizon Enterprise.