ISSN: 2582-4686 SJIF 2021-3.261, 2022-2.889, 2023-5.384, 2024-6.875 ResearchBib IF: 9.948 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-5, ISSUE-11

Model for improving skills and competencies in cybersecurity for bank employees.

Asemova Rano Zhapparbergenovna
JSCB "Uzpromstroybank" Kungrad BKM
Chief Specialist of Service Manager

Abstract: The rapid digital transformation of the banking sector has significantly increased exposure to cyber threats, requiring a high level of cybersecurity skills and competencies among bank employees. This article proposes a comprehensive model aimed at improving cybersecurity competencies through a multi-level training framework, continuous monitoring, and performance-based assessment. The model integrates theoretical knowledge, practical simulations, risk-based learning modules, and behaviour-focused training to strengthen staff awareness, incident-response capabilities, and compliance with regulatory standards. The study highlights the necessity of building a cybersecurity culture within banks, utilizing modern digital tools, and establishing a standardized competency framework aligned with international best practices. The proposed approach enhances the preparedness of employees to detect, prevent, and respond to cyber incidents, ultimately increasing overall resilience and operational security in banking institutions.

Keywords: Cybersecurity training; banking sector; competency model; employee skills development; cyber risk management; digital security awareness; phishing simulation; incident response; regulatory compliance.

Introduction: In recent years, the rapid expansion of digital technologies has radically transformed the operational landscape of the banking sector. The integration of online banking platforms, mobile applications, cloud infrastructures, and automated financial systems has created new opportunities for efficiency, accessibility, and customer convenience. However, alongside these advancements, banks have become increasingly vulnerable to a wide spectrum of cyber threats, including phishing attacks, data breaches, ransomware, social engineering, and insider-related incidents. According to global cybersecurity assessments, the financial sector remains one of the most frequently targeted industries, as cybercriminals continuously develop more sophisticated and persistent methods of attack.

One of the primary factors contributing to cybersecurity breaches in banks is the human element. Even the most advanced technological security systems can be compromised if employees lack the necessary skills, awareness, and competencies to recognize and respond to digital threats. In many institutions, cybersecurity training is delivered irregularly or does not fully address emerging risks, resulting in gaps in employees' preparedness and behaviour. Therefore, strengthening cybersecurity competencies among bank staff is becoming a strategic priority for ensuring operational stability and maintaining customer trust.

Given these challenges, there is a growing need for a comprehensive, systematic, and adaptive training model that enhances employees' cybersecurity knowledge and practical abilities. Such a model must not only focus on basic awareness but also integrate behavioural change, hands-on experience, and regulatory compliance. It should align with international cybersecurity standards such as ISO/IEC 27001, NIST Cybersecurity Framework, and industry best practices to ensure that bank employees are fully equipped to detect, prevent, and mitigate cyber risks.

This article aims to propose an effective model for improving cybersecurity skills and competencies among bank employees through a multi-level approach that includes awareness

ISSN: 2582-4686 SJIF 2021-3.261, 2022-2.889, 2023-5.384, 2024-6.875 ResearchBib IF: 9.948 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-5, ISSUE-11

programs, technical skill development, simulation-based learning, and continuous performance evaluation. The proposed model is designed to support banks in building a sustainable cybersecurity culture and enhancing their resilience against rapidly evolving cyber threats.

Relevance of Work

The relevance of this study is determined by the accelerating digital transformation of the banking sector, which has significantly increased the scale and complexity of cyber risks. As banks adopt innovative technologies—such as mobile banking, cloud solutions, artificial intelligence, and real-time payment systems—they become prime targets for cybercriminals seeking to exploit system vulnerabilities and human errors. Statistics from global cybersecurity reports show that the financial industry consistently ranks among the sectors with the highest number of cyberattacks, with breaches often resulting in substantial financial losses, reputational damage, and service disruption.

Despite advancements in security technologies, the human factor remains the weakest link in cybersecurity. Phishing, social engineering, weak password practices, and improper handling of sensitive information are among the most common causes of security incidents. Many bank employees lack adequate knowledge or practical experience to properly identify and respond to cyber threats. This situation underscores the urgent need for a structured, continuous, and competency-based training model tailored specifically for bank personnel.

Furthermore, national and international regulatory frameworks, including ISO/IEC 27001, PCI DSS, NIST CSF, and local banking supervision guidelines, increasingly require financial institutions to implement regular cybersecurity training and competency assessments. Ensuring compliance with these standards is essential for maintaining operational stability and customer trust. Therefore, developing a comprehensive model that enhances employees' cybersecurity skills is not only practically necessary but also strategically important for strengthening the resilience of the banking system.

Purpose of the Study

The purpose of this study is to develop and propose a comprehensive, multi-level model aimed at improving cybersecurity skills and competencies among bank employees. The model is designed to:

- Enhance employee awareness of cyber threats and digital security practices.
- Develop practical skills for identifying, preventing, and responding to cyber incidents.
- Promote behaviour change and cultivate a strong cybersecurity culture within banking institutions.
- Align employee competencies with international standards and regulatory requirements.
- Enable continuous learning through simulations, performance assessment, and feedback mechanisms.

Ultimately, the purpose of the research is to strengthen the cybersecurity posture of banks by equipping employees with the necessary knowledge, skills, and attitudes to effectively mitigate evolving cyber risks.

Materials and Methods of Research

This study employs a combination of qualitative and quantitative research methods to develop a comprehensive model for improving cybersecurity competencies among bank employees. The following approaches were utilized:

1. **Literature Review**: A detailed analysis of international standards, regulatory documents, and academic research was conducted. Key sources included ISO/IEC 27001, NIST

ISSN: 2582-4686 SJIF 2021-3.261, 2022-2.889, 2023-5.384, 2024-6.875 ResearchBib IF: 9.948 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-5, ISSUE-11

Cybersecurity Framework, PCI DSS guidelines, and scientific publications related to cybersecurity awareness, human factors, and training models.

2. **Comparative Analysis**: Training practices and cybersecurity competency frameworks used in leading global financial institutions were compared to identify best practices and adaptable strategies for the banking sector.

3. **Survey and Questionnaire Method**: A structured survey was conducted among bank employees in various departments (IT, customer service, operations) to assess their existing cybersecurity knowledge, awareness levels, and training needs. The survey included both closed and open-ended questions.

4. **Expert Interviews:** Interviews with cybersecurity specialists, IT managers, and compliance officers provided professional insights into current challenges, competency gaps, and effective training approaches within banks.

5. **Simulation-Based Assessment**: Phishing simulations and incident-response drills were carried out to observe employee behaviour in real-world scenarios and to evaluate the effectiveness of existing training programs.

6. **Data Analysis Techniques**: Collected data were analyzed using descriptive statistics, thematic analysis, and competency gap mapping. These results were used to design the multi-level cybersecurity training model.

Results and Discussion

1. Identification of Core Cybersecurity Competency Gaps

Survey results and simulation outcomes revealed several weaknesses among bank employees:

- Limited understanding of phishing and social engineering schemes.
- Insufficient knowledge of secure password practices and data protection rules.
- Low confidence in reporting suspicious digital activities.
- Poor familiarity with incident-response procedures and regulatory requirements.

These findings highlight the need for structured and continuous training rather than one-time awareness sessions.

2. Development of a Multi-Level Cybersecurity Competency Model

Based on the research results, a four-level model was developed:

Level 1: Awareness and Cyber Hygiene

- Basic training on cyber threats and safe digital behaviour.
- Regular phishing simulations and micro-learning modules.
- Visual materials and pop-up reminders on secure practices.

Level 2: Practical Skills Development

- Hands-on training using sandbox environments.
- Workshops on handling data securely and identifying high-risk activities.
- Case studies of real cyber incidents in banking.

Level 3: Advanced Specialization

- Training for IT and security staff on threat intelligence, vulnerability scanning, and incident-response playbooks.
- Collaboration with national CERT and cybersecurity centers.

Level 4: Continuous Monitoring and Evaluation

- Periodic cybersecurity testing and employee performance scoring.
- Integration into HR evaluation and staff development plans.

ISSN: 2582-4686 SJIF 2021-3.261, 2022-2.889, 2023-5.384, 2024-6.875 ResearchBib IF: 9.948 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-5, ISSUE-11

- Monitoring KPIs such as phishing click rates, reporting rates, and compliance metrics.

3. Practical Implementation Framework

The proposed model is designed to be implemented in three main stages:

1. **Assessment Stage:** evaluating current competencies and identifying risks.
2. **Training Stage:** delivering tailored training modules based on employee roles.
3. **Evaluation and Improvement Stage:** measuring effectiveness and updating content regularly.

4. Benefits of the Proposed Model

The model is expected to:

- Strengthen cybersecurity culture across the organization.
- Reduce the likelihood of human-caused security breaches.
- Improve employees' readiness to detect and respond to cyber incidents.
- Ensure compliance with regulatory and international cybersecurity standards.
- Enhance overall resilience and operational security of banking institutions.

Conclusion: The increasing frequency and sophistication of cyber threats in the banking sector make the development of employee cybersecurity competencies a critical strategic priority. This study demonstrates that technological measures alone are insufficient to protect banking institutions; the human factor plays a decisive role in preventing, detecting, and responding to cyber incidents.

The proposed multi-level model provides a systematic framework for improving cybersecurity skills among bank employees, combining awareness programs, practical skill development, advanced specialization, and continuous evaluation. By integrating simulations, performance assessment, and role-based training, the model addresses both knowledge gaps and behavioural challenges, fostering a strong cybersecurity culture within the organization.

Implementation of this model is expected to enhance employees' ability to identify and mitigate cyber risks, ensure compliance with international and national regulations, and strengthen overall operational security. Ultimately, the model contributes to building a resilient banking environment where employees are active participants in safeguarding digital assets and customer information.

Continued adaptation of the model to emerging threats, technological advancements, and evolving regulatory requirements will be essential to maintaining its effectiveness and ensuring that bank employees remain competent and vigilant in the ever-changing cybersecurity landscape.

References

1. Abduvahobov Sh. X., Davronov Sh. S. "Bank amaliyotlarida xavfsizlik va axborot himoyasi muammolari." *Ilm Fan Xabarnomasi*, 2025, 7(2). worldlyjournals.com
2. Jorayev B. S. "Banklarda kiberjinoyat xavfsizligi." *TADQIQOTLAR.UZ*, 2025, 54(2), 3–6. scientific-jl.org
3. Usmanbayev D. Sh. "Kiberxavfsizlik: IT infratuzilmasini himoya qilishning zamonaviy usullari." *Yashil Iqtisodiyot va Taraqqiyot*, 2025, 3(5). yashil-iqtisodiyot-taraqqiyot.uz
4. "Cybersecurity Issues in the Financial System." *Iqtisodiyot va innovatsion texnologiyalar*, (Toshkent), 2025. iqtisodiyot.tsue.uz
5. Xidirov U. G. "Banklarning kiberxavfsizligi: raqamli moliya dunyosida xavf va imkoniyatlar." *Yangi O'zbekiston — Yangi Tadqiqotlar Jurnali*, 2025, 2(9). phoenixpublication.net
6. Permatasari A. N. Sh., Yohannis A. R. "Evaluation of Cybersecurity Awareness and Training for Digital Branch Frontliners at Bank XYZ." *Journal of Computer Networks, Architecture and High Performance Computing*, 2024. jurnal.itscience.org

ISSN: 2582-4686 SJIF 2021-3.261, 2022-2.889, 2023-5.384, 2024-6.875 ResearchBib IF: 9.948 / 2024

VOLUME-5, ISSUE-11

7. Tuz J., Islam M. S., Kanon E. va boshq. “A Data-Driven Predictive Analysis on Cyber Security Threats with Key Risk Factors.” (preprint) 2024. arXiv

8. Waliullah M., Hossain M. Z., Hasan M. T., Alam M. K., Munira S. S., Siddiqui N. A. “Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review.” (preprint) 2025. arXiv