Evaluation of the SAAT Cybersecurity Awareness Model in a Nuclear Regulatory Authority

Samo Tomažič
Slovenian Nuclear Safety Administration
Litostrojska 54
1000 Ljubljana, Slovenia

Blaž Markelj
Faculty of Criminal Justice and Security
Kotnikova 8
1000 Ljubljana, Slovenia

ABSTRACT
The human factor remains one of the most significant vulnerabilities in cybersecurity, particularly in high-consequence environments such as the nuclear sector, where a single inappropriate action may compromise critical systems, cause financial damage, or undermine institutional credibility. To address this risk, the Slovenian Nuclear Safety Administration (SNSA) has maintained a structured information security awareness programme since 2011. Building on this foundation, the SAAT model (Systematic Approach to Awareness Training) was developed as an integrated framework that combines awareness, training, and testing into a continuous and adaptive process aimed at strengthening cybersecurity culture and mitigating human-related cyber risks.

This paper presents a longitudinal evaluation of SAAT implementation between 2020 and 2025, based on controlled phishing simulations and systematic observation of employee behaviour. Using a descriptive and observational methodology, the study analyses how the type, timing, and frequency of awareness activities influence phishing susceptibility, reporting behaviour, and overall vigilance.

The results indicate that awareness levels decline when reinforcement intervals are prolonged, increasing user interaction with phishing content. Conversely, regularly delivered and well-balanced awareness interventions significantly reduce risky behaviour while maintaining or improving reporting rates. The findings confirm that cybersecurity awareness must be treated as a continuous, carefully calibrated process. Excessive frequency, however, may lead to awareness fatigue, highlighting the need for optimised implementation strategies in critical infrastructure organisations.

Keywords
Cybersecurity awareness, phishing simulation, human factor, nuclear sector, security culture

1. INTRODUCTION
Cybersecurity incidents increasingly exploit the human element rather than technical vulnerabilities, making user behaviour one of the most critical factors in an organisation's security posture [1]. This challenge is particularly pronounced in high-consequence environments such as the nuclear sector, where successful cyber-attacks may have far-reaching safety, financial, and reputational consequences [2][3]. Despite significant investments in technical controls, human actions – such as clicking malicious links, mishandling sensitive information, or failing to report suspicious activity – remain a persistent source of cyber risk [4] [5].

In response to this challenge, cybersecurity awareness programmes have become a widely adopted preventive measure across critical infrastructure sectors. However, many awareness initiatives are implemented as isolated or periodic activities, often lacking systematic structure, empirical evaluation, and long-term sustainability [6][7]. As a result, organisations frequently struggle to assess whether awareness efforts translate into durable behavioural change or merely short-lived improvements in user knowledge.

This issue is further compounded in highly regulated organisations, such as nuclear facilities or competent authorities, where cybersecurity is a supporting function rather than a core operational mission [8]. In such environments, awareness activities must be carefully balanced to maintain employee vigilance without overburdening staff or detracting from primary responsibilities. Excessive or poorly timed interventions may lead to awareness fatigue, disengagement, or resistance, undermining the very objectives they are intended to achieve.

The SNSA has addressed these challenges by establishing and continuously maintaining an information security awareness programme since 2011. Building on more than a decade of institutional experience, the programme was further developed into a structured and empirically evaluated framework beginning in 2020. This evolution led to the development of the SAAT model, which integrates awareness, training, and testing into a continuous, adaptive, and measurable process.

The objective of this paper is to present the design, implementation, and longitudinal evaluation of the SAAT model based on real-world operational data collected between 2020 and 2025. Using controlled phishing simulations and systematic observation of employee behaviour, the study examines how the type, frequency, and timing of awareness activities influence susceptibility to social engineering attacks, reporting behaviour, and overall cybersecurity vigilance.

By providing empirical evidence from a nuclear regulatory environment, this paper contributes practical insights into the optimisation of cybersecurity awareness programmes. The findings support the view that awareness is not a one-time intervention but a dynamic process that must be continuously reinforced, carefully calibrated, and aligned with organisational context and mission priorities.

2. METHODOLOGY
This study employed descriptive and observational research to develop and empirically evaluate the SAAT model. The descriptive approach included a review of legislation, standards, and guidance related to nuclear cybersecurity and security culture, while observational research enabled systematic observation of employee behaviour, awareness levels, and responses to various awareness interventions over time [9]. This approach is particularly appropriate in regulated,

high-consequence environments where experimental manipulation is limited.

The research combined qualitative and quantitative methods, including:

- observation of employee behaviour during awareness sessions, applied training, and exercises;
- analysis of controlled phishing simulation results and training feedback; and
- comparison of behavioural outcomes across different types, frequencies, and timings of awareness activities.

The study was conducted at the SNSA and included all employees.

2.1 Awareness Activities and Phishing Simulations

Awareness activities were systematically planned within an annual programme and varied in form and intensity. Controlled phishing simulations were conducted periodically between 2020 and 2025, reflecting realistic attack techniques such as malicious links, infected attachments, USB drives, SMS messages and requests for sensitive information.

Key metrics included interaction rates with phishing content, reporting rates, and repeated susceptibility patterns. The intervals between awareness activities and phishing tests were intentionally varied to assess behavioural reinforcement and awareness decay over time.

2.2 Data Collection, Analysis, and Limitations

Data were collected over five years using quantitative phishing test results and qualitative observations from training activities. Descriptive statistical analysis identified trends and relationships between activity frequency, timing, and user behaviour, including indicators of improved vigilance or awareness fatigue.

Due to its descriptive nature, the study does not establish strict causality, and findings are specific to the organisational and regulatory context of SNSA. Nevertheless, the longitudinal design and real-world operational setting provide strong practical relevance for organisations in critical infrastructure sectors.

In addition to qualitative observations, descriptive statistical measures, including annual reporting rates, phishing interaction rates, percentage changes, and longitudinal trend analysis, were used to support the interpretation of behavioural changes over the study period.

3. RESULTS

This research examines the long-term implementation and effectiveness of a SAAT programme at the SNSA. The study employs a longitudinal design spanning multiple years, beginning in 2020, and focuses on the relationship between systematically delivered awareness activities and measurable employee cybersecurity behaviour. The research was prompted by internal observations that earlier awareness initiatives, although present since 2013, were conducted irregularly, lacked defined execution criteria, and did not provide sufficient empirical data to support objective evaluation [11].

To address these shortcomings, SNSA introduced a comprehensive SAAT framework that integrates awareness, formal training, practical exercises, visual reinforcement, and phishing tests into a unified and adaptive process. All activities were designed to be repeatable, mandatory, and periodically reinforced, while remaining flexible enough to respond to changing threat landscapes, organisational conditions, and operational constraints. Particular attention was given to the timing and sequencing of activities, as well as their cumulative impact on employee behaviour over extended periods.

3.1 Objectives

The primary objective of the research was to establish a sustainable and systematic approach to information and cybersecurity awareness that would result in observable and measurable behavioural change among employees. Rather than focusing solely on knowledge acquisition, the research aimed to influence day-to-day decision-making and risk perception in routine work activities.

A key objective was to evaluate how different types of awareness-related interventions interact over time, and how the frequency and temporal spacing of these interventions affect their overall effectiveness. The research specifically sought to determine whether regular reinforcement through diverse activities could mitigate the well-documented decay of awareness that occurs when training is delivered infrequently. Another objective was to identify practical limits to the frequency of awareness activities, including the risk of employee fatigue and disengagement, particularly in a highly specialised regulatory organisation where cybersecurity is a supporting function rather than the primary mission.

Finally, the research aimed to generate an empirical basis for optimising awareness programme design, including the selection of activity types, their content, and their periodicity, in a manner that supports organisational resilience without negatively affecting core regulatory responsibilities.

3.2 SAAT Framework

The SAAT framework was implemented as a continuous and iterative process starting in 2020. Awareness activities formed the baseline of the framework and were conducted throughout the year using short, targeted communications to maintain cybersecurity visibility in everyday work contexts. These communications included brief emails highlighting current attack techniques, summaries of recent cyber incidents relevant to public administration or critical infrastructure, and reminders of secure behaviour related to email use, authentication practices, and handling sensitive information. Awareness messages were intentionally concise and focused on a single topic to reduce cognitive overload and increase retention. The timing of these messages was influenced by contextual factors such as holiday periods, increased remote work, or known peaks in phishing campaigns.

3.3 Overview of Awareness Activities and Phishing Simulations (2020–2025)

Table 1 presents phishing test results from 2020 to 2025.

Table 1. Phishing tests results

	YEAR				
	2021	**2022**	**2023**	**2024**	**2025**
Fraud method	e-mail	e-mail	SMS	USB drive	e-mail
Number of employees	43	40	10	28	42

Number of fraud reports	10	14	5	12	25
Percentage of fraud reports (%)	23,26	35,00	50,00	42,86	59,52
Number of employees who fell for the scam	5	0	0	3	3
Percentage of employees who fell for the scam (%)	11,63	0,00	0,00	10,71	7,14

Phishing simulations conducted during the study period produced the following recorded outcomes:

- 2021 (Email phishing): 43 employees received the simulated email; 10 reports and 5 clicks were recorded.
- 2022 (Email phishing): 40 employees received the simulated email; 14 reports and 0 clicks were recorded.
- 2023 (SMS phishing): 10 employees received the simulated message; 5 reports and 0 clicks were recorded.
- 2024 (USB-based phishing): 28 employees were exposed to the simulation; 12 reports and 3 device insertions were recorded.
- 2025 (Email phishing): 42 employees received the simulated email; 25 reports and 3 clicks were recorded.

Several behavioural trends emerge from the longitudinal observations.

First, employee susceptibility to phishing attacks decreased over time. The click rate fell from 11.63% in 2021 to 0% in 2022 and 2023, before slightly increasing during the USB simulation (10.71%) and declining again to 7.14% in 2025.

Second, reporting behaviour improved continuously throughout the observation period. The reporting rate increased from 23.26% in 2021 to almost 60% in 2025, indicating growing employee confidence in identifying and reporting suspicious activities.

Third, the type of phishing simulation influenced user behaviour. SMS phishing generated no successful compromises despite involving fewer participants, whereas USB-based attacks produced higher interaction rates despite previous awareness activities, suggesting that physical attack vectors remain less familiar to users than email-based attacks.

Finally, periods following multiple awareness activities consistently resulted in lower phishing susceptibility than periods preceded by extended awareness gaps.

Table 2 provides an overview of awareness activities and phishing simulations conducted during the study period.

The table shows the timing and type of activities across calendar years and highlights intervals with limited or no awareness interventions.

Legend for Table 2 is as follows:

Activity
No-Activity
Perfect score on Phishing Test
Negative score on Phishing Test

Table 2. SAAT model activities

Year/ Month		Activity
2020	6	Basic Awareness on Information Security
	7	
	8	
	9	Training on Secure Remote Work
	10	
	11	
	12	
2021	1	
	2	
	3	
	4	
	5	Phishing test - E-mail
	6	Training on Secure Email Practices
	7	
	8	
	9	Flyer on Phishing Techniques
	10	
	11	
	12	Basic Awareness on Information Security
2022	1	
	2	
	3	Interactive Riddle Exercise on Information Security, Received by all Employees over E-mail
	4	
	5	International exercise KiVA[2022]
	6	
	7	
	8	
	9	Phishing test - E-mail
	10	Training on Office Information Security
	11	
	12	
2023	1	
	2	Interactive Riddle Exercise on Information Security, Received by all Employees over E-mail
	3	
	4	Training on Information Security and Cybersecurity
	5	
	6	Flyer on Strong Passwords
	7	
	8	
	9	Phishing test -SMS
	10	Crossword Exercise on Information Security, Received by all Employees over E-mail
	11	
	12	
2024	1	Basic awareness on Information Security
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	Phishing test - USB drive
	10	
	11	
	12	
2025	1	
	2	
	3	Training on Information Security and Cybersecurity
	4	
	5	Flyer on Information Security Culture
	6	
	7	

8	
9	
10	
11	
12	**Phishing test - E-mail**

Formal awareness and training sessions constituted the structured educational component of the framework and were conducted periodically. Training was mandatory for all employees and was also included in the onboarding process for newly employed staff. The training content was developed specifically for the SNSA environment and addressed both general cybersecurity principles and organisation-specific risks. Sessions covered the secure use of information systems, identification of phishing and social engineering indicators, password hygiene, authentication mechanisms, secure remote work practices, and clearly defined procedures for reporting suspicious emails and incidents. To ensure comprehensive participation, each session was repeated when necessary, and employees who were absent were required to attend follow-up sessions. Observations during early cycles indicated a high level of self-perceived competence among employees, reinforcing the need for objective evaluation mechanisms.

Practical hands-on, table-top, and online exercises were introduced to translate theoretical knowledge into behavioural competence. These exercises were typically conducted after sessions and focused on realistic decision-making scenarios. Employees were exposed to real and simulated phishing emails and guided through the process of identifying subtle indicators of malicious intent. Group discussions explored how time pressure, authority cues, and contextual relevance influence user decisions. Scenario-based exercises demonstrated how seemingly minor user actions, such as clicking on a link or opening an attachment, could escalate into significant organisational consequences. In addition, lightweight interactive activities, such as riddles and crosswords distributed via email, reinforced key concepts in an informal and engaging manner, allowing frequent reinforcement without significant disruption to daily work.

Visual awareness materials complemented digital activities and maintained continuous exposure to cybersecurity messages. Flyers and posters were placed in common areas and designed to be visually engaging while conveying concise and actionable messages. Their content was periodically updated to reflect current threat trends, such as phishing techniques or password-related risks, and aligned with ongoing awareness campaigns to ensure coherence across communication channels.

Phishing tests were the primary evaluation tool within the SAAT framework and were conducted once per year. These controlled simulations were designed to realistically reflect contemporary phishing tactics and varied in complexity, urgency, visual quality, and contextual relevance to the organisation. For each test, the number of recipients was recorded alongside the number of users who fell victim to the phishing test and the number of reports submitted by employees. The phishing tests were not conducted as isolated assessments but were integrated into the broader awareness cycle, with their results directly informing the design and timing of subsequent awareness activities, training content, and exercises.

Table 3 summarizes the principal behavioural patterns observed during the five-year implementation of the SAAT framework. Rather than representing results from controlled experimental groups, the table synthesizes longitudinal observations collected during successive awareness activities and phishing simulations. The findings indicate that employee behaviour was strongly influenced by the timing of awareness interventions. Regular reinforcement was associated with higher reporting rates and lower phishing susceptibility, whereas prolonged periods without awareness activities resulted in increased interaction with phishing content. Conversely, overly frequent awareness interventions occasionally generated employee dissatisfaction, suggesting that awareness programmes should balance reinforcement with organisational workload to avoid awareness fatigue.

Table 3. Relationship between Awareness Frequency and Observed Behavioural Outcomes

Awareness frequency	Observed employee behaviour	Impact on cybersecurity awareness
Regular reinforcement (approximately every 2–4 months)	Higher phishing reporting rates, lower interaction with phishing content, consistent vigilance	Awareness remained high and phishing susceptibility was minimised
Moderate intervals (approximately 4–6 months)	Stable reporting behaviour with slight reduction in vigilance	Awareness remained acceptable but showed early signs of behavioural decay
Extended intervals (more than 6 months)	Increased interaction with phishing content despite previous training	Awareness declined over time, indicating the need for periodic reinforcement
Excessively frequent awareness activities	Employee feedback indicated reduced engagement and occasional dissatisfaction	Risk of awareness fatigue and reduced effectiveness of awareness activities

3.4 Observed Behavioural Outcomes

The behavioural observations summarized in Table 3 are supported by the quantitative results presented in Table 1 and the chronological implementation of awareness activities shown in Table 2. Across the five-year study period, phishing simulations captured employee responses in terms of interaction with phishing content and reporting behaviour. Together, these results demonstrate that both the frequency and timing of awareness interventions influenced employee cybersecurity behaviour.

3.5 Descriptive Statistical Analysis

To complement the qualitative observations, descriptive statistical analysis was performed using the phishing simulation results presented in Table 1. The average phishing reporting rate across the five-year observation period was 42.13%, while the average employee interaction rate with phishing content was 5.90%.

Reporting behaviour demonstrated an overall positive trend throughout the study period, increasing from 23.26% in 2021 to 59.52% in 2025, representing an increase from 23.26% to 59.52% (approximately 156% relative improvement). During the same period, phishing susceptibility decreased from 11.63% to 7.14%, corresponding to an overall reduction of approximately 39%, despite the introduction of different phishing techniques of varying complexity.

The longitudinal observations further indicate that periods following multiple awareness activities generally corresponded with higher reporting rates and lower phishing interaction rates. Although the limited sample size does not permit statistically significant inferential analysis, the observed trends are consistent with the hypothesis that systematic and continuous awareness activities contribute to improved cybersecurity behaviour.

Figure 1 illustrates the inverse relationship between phishing reporting rates and successful phishing interactions over time. As employee reporting behaviour increased, successful interactions with phishing content generally decreased, suggesting that improved awareness contributes to enhanced organisational resilience against social engineering attacks.

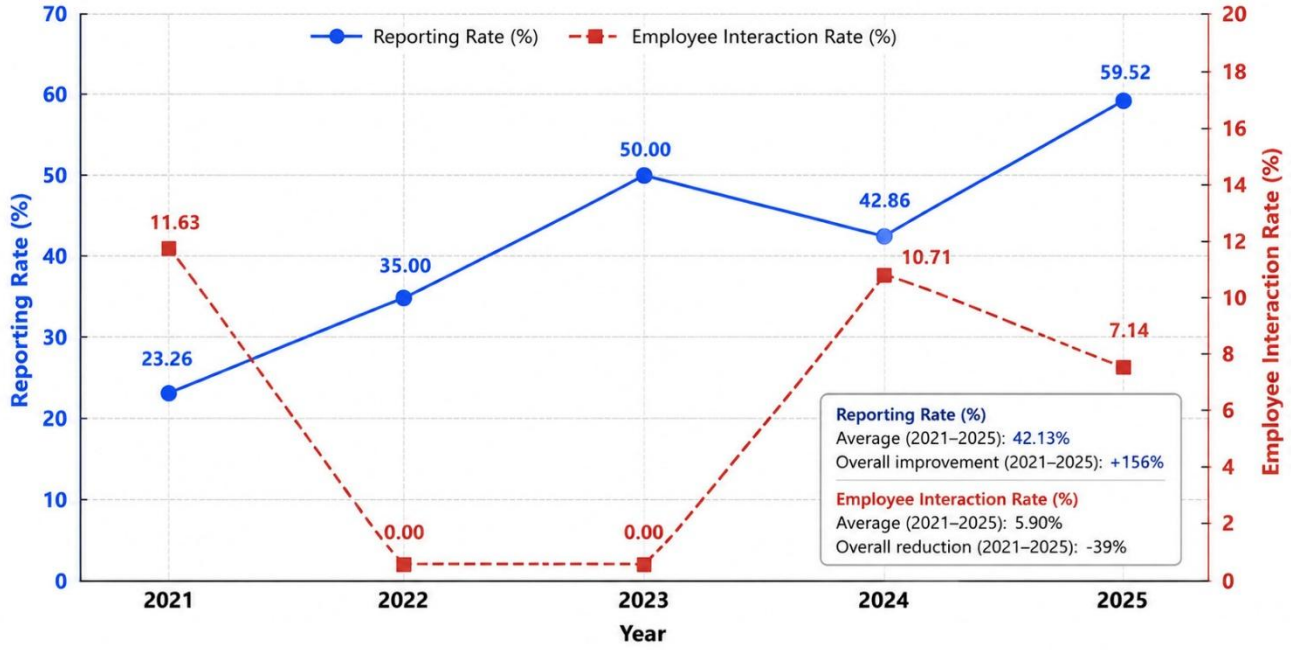

Fig 1: Trends in phishing reporting rate and employee interaction rate during phishing simulations (2021–2025)

4. DISCUSSION

This section interprets the results in relation to the study objective of developing a sustainable and effective cybersecurity awareness approach suitable for a nuclear regulatory organisation. The discussion examines the relationship between the frequency of awareness activities, employee behaviour, and organisational constraints, and considers the broader implications of the findings.

4.1 Awareness Reinforcement and Behavioural Decay

The results show that employee cybersecurity vigilance depends on time and is influenced by the interval between awareness interventions. Periods exceeding approximately six months without awareness-related activities were associated with reduced attentiveness to social engineering indicators in phishing simulations. These findings are consistent with established research indicating that security awareness diminishes over time if not periodically reinforced [1][6].

In contrast, simulations conducted after periods of regular reinforcement – approximately every three months – showed reduced or eliminated successful interaction with phishing content. Regular exposure to diverse awareness inputs appeared to maintain familiarity with attack techniques and reinforce secure decision-making in routine work activities.

4.2 Effectiveness of a Multi-Modal Awareness Approach

The findings suggest that combining multiple activity types within a single framework enhances the effectiveness of awareness [5]. Awareness messages, formal training, practical exercises, visual materials, and phishing simulations each addressed different aspects of user behaviour and risk perception. Awareness and training sessions provided foundational knowledge, while practical exercises and phishing simulations translated this knowledge into behavioural competence. Visual and lightweight interactive activities enabled frequent reinforcement without significant operational disruption.

The integration of phishing simulations as both an evaluation and feedback mechanism proved particularly valuable. Simulation results informed the timing and content of subsequent awareness activities, allowing the programme to adapt to observed behavioural trends and emerging threats [12].

An additional observation concerns the different employee responses to individual phishing techniques. Although only one USB-based phishing simulation was conducted during the study period, it resulted in a higher interaction rate than the email- and SMS-based simulations. This suggests that employees primarily associate cybersecurity threats with electronic communication channels, whereas physical media may receive less attention despite representing a recognised attack vector in critical infrastructure environments. While this observation should be interpreted cautiously, it highlights the importance of maintaining diversity within awareness programmes by incorporating multiple phishing scenarios rather than focusing predominantly on email-based attacks.

4.3 Organizational Constraints and Awareness Fatigue

While regular reinforcement improved behavioural outcomes, the results also revealed practical limits to the frequency of

awareness activities. Employee feedback indicated dissatisfaction when awareness interventions were perceived as excessive or intrusive. In a nuclear regulatory environment, where cybersecurity supports rather than defines the organisational mission, overly frequent activities risk competing with core regulatory responsibilities.

These findings highlight awareness fatigue as a critical consideration in programme design. An optimal awareness strategy must balance sufficient reinforcement to sustain vigilance with respect for organisational workload and mission priorities.

4.4 Implications for Critical Infrastructure Organizations

The SAAT model shows that cybersecurity awareness is most effective when implemented as a continuous and adaptive process, rather than as isolated events. For organisations in critical infrastructure sectors, especially those operating in highly regulated environments, the results highlight the importance of tailoring awareness programmes to the organisational context, threat landscape, and human factors [10][13].

The longitudinal nature of the study provides empirical support for adopting structured awareness cycles with defined evaluation mechanisms. Although the findings are based on a single organisation, the SAAT model offers a transferable framework that can be adapted by other regulators and operators seeking to strengthen cybersecurity culture while minimising operational burden.

4.5 Limitations and Future Research

This study was conducted within a single nuclear regulatory authority, and the results may be influenced by organisational size, culture, and regulatory context. The descriptive research design does not establish causal relationships between specific interventions and behavioural outcomes. Future research could extend this work by applying the SAAT model across multiple organisations, incorporating comparative analysis, or integrating additional quantitative measures of long-term behavioural change.

5. CONCLUSION

This study presents the development, implementation, and longitudinal evaluation of the SAAT model at the SNSA. The findings demonstrate that cybersecurity awareness in a nuclear regulatory environment cannot rely on isolated or ad hoc initiatives [7]. Instead, it requires a structured, continuous, and adaptive framework that systematically integrates awareness activities, formal training, practical exercises, and controlled phishing simulations.

The longitudinal results, supported by descriptive statistical analysis, confirm that employee vigilance is time-sensitive and that systematic awareness reinforcement contributes to measurable improvements in employee cybersecurity behaviour. Extended intervals without reinforcement were associated with increased interaction with phishing content, whereas regularly scheduled and diversified awareness interventions reduced susceptibility and supported stable reporting behaviour. These findings reinforce the principle that behavioural change in cybersecurity depends not only on knowledge acquisition but also on sustained reinforcement and contextual relevance.

The study also identified practical constraints related to awareness fatigue and organisational workload. In highly specialised regulatory environments, cybersecurity represents a supporting function, and awareness programmes must therefore be carefully calibrated to avoid excessive burden on core mission activities. An optimal strategy balances sufficient reinforcement to maintain vigilance with proportionality in frequency and delivery methods.

Although the research was conducted within a single regulatory authority and does not establish strict causality, the longitudinal real-world data provide valuable empirical insight. The SAAT model offers a transferable framework for critical infrastructure organisations seeking to strengthen cybersecurity culture while maintaining operational effectiveness [14][15]. Future research could further validate the model across different institutional contexts and incorporate comparative or experimental methodologies to deepen understanding of long-term behavioural dynamics.

6. REFERENCES

[1] Tomažič, S. (2026). Kibernetska varnost: Koncepti in pristopi k zaščiti kritične infrastrukture – jedrski sektor. Univerza Alma Mater Europaea.

[2] International Atomic Energy Agency (Ur.). (2021a). Computer security for nuclear security: Implementation guide. International Atomic Energy Agency.

[3] International Atomic Energy Agency (Ur.). (2021b). Computer security techniques for nuclear facilities: Technical guidance. International Atomic Energy Agency.

[4] Lee, K., & Lim, J. (2016). The reality and response of cyber threats to critical infrastructure: A case study of the cyber-terror attack on the Korea Hydro & Nuclear Power Co., Ltd. KSII Transactions on Internet and Information Systems, 10(2), 24. https://doi.org/http://dx.doi.org/10.3837/tiis.2016.02.023

[5] Joint Task Force Interagency Working Group. (2020). Security and Privacy Controls for Information Systems and Organizations (Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

[6] Tomažič, S., Mertik, M., & Šeruga, T. (2023). Systematic Approach to Awareness Training at Slovenian Nuclear Safety Administration. International Journal of Computer Applications, 185(3), 30–36. https://doi.org/10.5120/ijca2023922686

[7] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29; str. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

[8] Office for Nuclear Regulation. (2022). Security Assessment Principles for the Civil Nuclear Industry. Office for Nuclear Regulation. http://www.onr.org.uk/syaps/index.htm

[9] Joint Task Force Transformation Initiative. (2018). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (NIST SP 800-37r2; str. NIST SP 800-37r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2

[10] International Atomic Energy Agency. (2018). Computer Security of Instrumentation and Control Systems at Nuclear Facilities: Technical Guidance. IAEA.

[11] International Atomic Energy Agency. (2016). Conducting

computer security assessments at nuclear facilities. International Atomic Energy Agency.

[12] Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST SP 800-61r3; str. NIST SP 800-61r3). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-61r3

[13] International Atomic Energy Agency. (2025). Information and Computer Security for Activities Involving Radioactive Material and for Associated Facilities. International Atomic Energy Agency.

[14] Nuclear Energy Institute. (2024). Cyber Security Plan for Nuclear Power Reactors (NEI 08-09 [Revision 7]). Nuclear Energy Institute.

[15] Boyens, J. M. (2024). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161r1-Upd1; str. NIST SP 800-161r1-upd1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1-upd1