Prioritizing Persona Attributes and Organizational Barriers in Cybersecurity Awareness: An AHP Analysis*

Daria Levaniuk*, Bilal Naqvi and Antti Knutas

LUT University, Yliopistonkatu 34, 53850 Lappeenranta, Finland

Abstract

Organizations often face challenges in implementing personalized cybersecurity awareness strategies. While several factors contribute to the state of the art, implementing intervention strategies to overcome these challenges requires significant effort and cost. Therefore, this study adopts the Analytic Hierarchy Process (AHP) method to prioritize the most critical factors influencing personalized cybersecurity awareness strategies, including the persona attributes that affect the way individuals interpret and interact with cybersecurity. The research is grounded in data from 16 semi-structured interviews conducted across the industry. Drawing on interviews, the study ranks 13 persona attributes and 11 organizational challenges to bridge the gap between existing barriers in current practices and the implementation of personas for addressing employee security behavior. The findings were prioritized by an expert panel of 10 participants using the AHP analysis. As an outcome, the authors suggest the cyber persona design as a solution for overcoming barriers, based on analysis results, and recommendations for persona-based personalization, enabling effective training and enhancing awareness of emerging cybersecurity threats.

Keywords

Analytic Hierarchy Process, Cybersecurity awareness, Persona, Organizational barriers, Human factors

1. Introduction

Cybersecurity threats, including social engineering attacks, are experiencing considerable growth, making employees' behavior one of the major risks for organizations [1]. The complexity of emerging threats requires human readiness to recognize the risks, respond promptly, and avoid mistakes, which can lead to company data leakages and data breaches. Companies have started to explore how a better understanding of potential security incidents and preventive measures can help mitigate human error [2, 3]. Therefore, the focus of organizations is changing from only the technical side to human-centered approaches.

Several studies present the human-centric approaches in cybersecurity addressing human factors [4], including preferred learning styles, cognitive abilities, and motivation for designing effective training and reducing human errors [5]. Prior research also highlights the need for implementing targeted strategies to improve employees' understanding of emerging threats and their reaction in different situations, proposing different personalization frameworks [6], and behavior-driven approaches [5].

Despite this, the current situation shows that the policies and security awareness training still remain too generic and broad, and the prioritization of human attributes is underexplored in the cybersecurity context [7]. Organizations continue to face difficulties transitioning from a "one-size-fits-all" approach to personalized frameworks and strategies [6]. Prior research highlights obstacles to implementing personalization as a preventive mechanism for cyber attacks and human errors, including a lack of resources [1], a considerable amount of work to cover a diverse range of employees, and the complexity of creating personalization strategies.

Our paper proposes a personalization approach incorporating a persona development for creating individual educational paths, analysis of human behavior characteristics, and mitigating organizational barriers. Personas group individuals by common attributes to enable target strategies. While existing

TKTP 2026: Annual Doctoral Symposium of Computer Science, 8.—9.6.2026 Turku, Finland

*Corresponding author D. Levaniuk

Daria.Levaniuk@lut.fi (D. Levaniuk); Syed.Naqvi@lut.fi (B. Naqvi); Antti.Knutas@lut.fi (A. Knutas)

0000-0002-9043-3568 (D. Levaniuk); 0000-0001-5271-5604 (B. Naqvi); 0000-0002-6953-0021 (A. Knutas)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

published 2026-11-02

CEUR-WS.org/Vol-4309/paper04.pdf

literature [8] implements persona in cybersecurity content, this study focuses on identifying the most important components in persona design, extending the traditional attributes with psychological factors, security competencies, cognitive characteristics, and behavioral aspects.

Our research aims to examine how cybersecurity awareness campaigns can be optimized through the Analytic Hierarchy Process (AHP) analysis of personal attributes and challenges in the organizational context.

To achieve this goal, the research questions are structured as follows:

RQ1: Which challenges have the greatest impact on implementing personalized cybersecurity awareness and training programs?

RQ2: Which human attributes impact personalization in security awareness design?

Our study contributes a quantitative prioritization of attributes for cyber personas to existing knowledge. Therefore, it demonstrates the value of psychological and cognitive aspects, which play a crucial role in cybersecurity incidents and human error, and emphasizes persona design as a practical tool to overcome identified organizational barriers. The results of the AHP analysis provide a foundation for creating more effective cybersecurity awareness strategies and developing user-centered policies.

The paper structure consists of several sections. Section 2 presents related work describing already existing research on human-centered cybersecurity and implications of AHP in the cybersecurity area. Research method and study setup are explained in Section 3. Section 4 presents outcomes of ranking organizational challenges and prioritization for the persona creation process. Section 5 discusses existing research compared to the received findings and potential implications. Section 6 describes threats to validity. The conclusion with outcomes of the study is highlighted in Section 7.

2. Related work

2.1. The human element in cybersecurity resilience

Current cyber threats often focus on social engineering attacks and phishing simulations, indicating the human element as an integral part of cybersecurity, shaping organizational risks [5]. Recent studies emphasize the important role of human behavior, cognitive abilities, and psychological patterns in building cybersecurity resilience and mitigating vulnerabilities [2, 9]. The Theory of Planned Behavior (TPB), proposed by Ajzen [10], explains that attributes, subjective norms, and perceived behavioral control determine compliance intentions. Additionally, the Protection Motivation Theory (PMT), introduced by Rogers [11], suggests that self-efficacy and threat appraisals are core cognitive drivers shaping protective security behavior.

Several studies [12, 13] grounded in these theories demonstrate that employee behavior is influenced by a variety of organizational, individual, and cognitive factors. Thus, the environment, including organizational culture and leadership support, acts as a subjective norm and establishes security standards and perceptions [13]. At the individual level, factors such as motivation and awareness of risks influence self-efficacy and compliance behavior [14]. These theories provide a foundation that gives a clear explanation of root causes in human behavior and highlights the need for personalization in cybersecurity.

2.2. Personalization in security awareness

Although cybersecurity strategies primarily rely on advanced digital tools and security measures, there is a need to integrate both technical and human-centered approaches. Existing literature, considering the organizational context, presents personalized security awareness frameworks and strategies emphasizing individual differences, cognitive abilities, and behavior patterns [15, 6].

While, as highlighted in studies [16, 17], a better understanding of human factors improves employee compliance and strengthens security awareness training, organizations still follow a ”one-size-fits-all” approach, and lack personalization [6]. Employee diversity, financial and resource limitations, and infrastructure capabilities limit the personalization process in organizations [18, 19].

Despite the availability of methods and understanding of the importance of human factors in cybersecurity resilience, existing literature does not reflect on how attributes should be prioritized for effective development of personalized awareness strategies and how to mitigate challenges during implementation.

2.3. Persona in cybersecurity

Some studies [20, 21] show how to incorporate persona in cybersecurity as a Human-Centered Interaction (HCI) tool for identifying the needs, motivations, and vulnerabilities of a diverse group of end-users, attackers, developers, and others. Persona descriptions for cybersecurity are used in multiple ways to link understanding of potential users with designing user-friendly systems while also supporting the creation of scenarios of possible attacks, security features, and system or human vulnerabilities[22]. Different persona types and their implications in various cybersecurity areas are presented in the literature review [8]. Therefore, personas reflect individual characteristics and simultaneously act as anonymous, archetypal representatives of a group of employees, simplifying privacy issues. A persona-based approach provides a scalable tool for security awareness campaigns, reducing the workload involved in creating individual learning plans while ensuring personalized security interventions.

2.4. Analytic Hierarchy Process (AHP) implications and research gap

The Analytic Hierarchy Process (AHP) method is commonly used to rank criteria for achieving sufficient approaches [23]. The application of AHP is widely used in software engineering for prioritizing software requirements, evaluating usability features [24], and comparing software tools [25]. At the same time, this approach is also adopted in cybersecurity risk management [26] and threat assessment [14]. Although the AHP was applied in the usability context, no research has been conducted on prioritizing persona attributes. This makes AHP a suitable approach for systematically prioritizing both persona attributes and organizational challenges.

To sum up, previous studies have described how companies can incorporate human-oriented approaches and frameworks in policy design, learning strategies, and targeted attack simulations, yet there is a lack of connection between these suggested strategies and the reasons why companies have struggled with them, as well as how to overcome these challenges. Our study demonstrates the potential of using personas by addressing organizational barriers to personalization and identifying the key attributes for cybersecurity personas to enhance security mechanisms, policy design, and security awareness campaigns.

3. Research method and study setup

3.1. Research method

The Analytic Hierarchy Process (AHP) is a systematic multi-criteria decision-making method presented by Saaty T.L.[27]. This method provides a structural representation for complex decision problems involving human factors. AHP demonstrates a clear way of comparing qualitative findings for identifying the most important elements. In this study, we use AHP for a pairwise comparison to assign weights and evaluate the identified organizational challenges to personalization and the individual factors impacting cybersecurity persona in terms of effective security awareness training. Personal attributes include psychological, behavioral, and demographic components, which are usually difficult to compare directly.

Stage 1. As input, we conducted 16 semi-structured interviews in previous work. From the interview data, the barriers to personalization in the security awareness context were identified, which formed a baseline with an empirical foundation for our analysis. These barriers were divided into 6 categories, including operational resource limitations, organizational constraints, limited expertise, market perception, behavioral and motivational challenges, and individual differences. More details about the

interview protocol, participant description, and code book can be found in the online repository (see Supplementary materials).

Stage 2. Before the AHP assessment, the model of hierarchy was developed. The hierarchical structure of organizational challenges was designed by the authors and based on findings from semi-structured interviews, and identified key barriers. As for persona attributes, the hierarchy was derived from a synthesis of existing cybersecurity personas [8] and complemented by interview insights regarding individual characteristics that act as barriers to secure behavior. As a part of this phase, we provided a dimensional taxonomy and divided all categories of existing barriers into organizational and individual dimensions. The organizational dimension includes Operational resource limitations, Organizational constraints, Limited expertise, and Market perception categories that are influenced by environment, organizational structure, and cybersecurity culture. Additionally, Individual differences themselves are connected to both dimensions, emphasizing the challenge of personalizing cybersecurity due to the varied backgrounds, roles, and skills of employees. In contrast, Individual dimension comes from specific Individual differences as an attribute for persona design and Behavioral and Motivational challenges.

These categories are used for designing schemes (hierarchies). Each scheme consists of 3 levels: Goal (Level 0), Criteria (Level 1), and Sub-Criteria (Level 2). The AHP weighting identifies the rank of criteria and sub-criteria. To answer RQ1, we developed the design scheme presented in Figure 1. The goal of the organizational challenges assessment is to prioritize the key challenges that impact effective personalization. This can be achieved by using pairwise comparison of 3 criteria: "Operational Scarcity", "Strategic Knowledge Gap", and "Systemic fragmentation" - to discover which factors influence cybersecurity resilience and employees' security and privacy compliance. Each criterion is further divided into sub-criteria. For instance, operational scarcity has time constraints or a lack of expertise as a sub-criterion.

Table 1
Personalization challenges prioritization design schema

Goal (Level 0)	Criteria (Level 1)	Sub-criteria (Level 2)
Personalization Challenges Prioritization	Operational Scarcity	Time Constraints
		Staff Capacity Limitations
		Lack of Expertise
		Financial Limits
		Limitations of Technical Measures
	Strategic Knowledge Gap	Privacy & Ethics Concerns
		Low Management Priority
		Dynamic Complexity of Content Updates
	Systemic Fragmentation	Complicated Policies
		Disorganized Training
		Cross-Functional Ambiguity

The goal of persona attributes prioritization (RQ2) is to identify persona attributes for behavior-change and engagement strategies. In AHP prioritization, we included both demographic and role-based characteristics, which are often explicitly mentioned in existing literature [8], but also strengthened the scope of attributes by adding specific categories such as psychological and cognitive drivers, technical security competence, behavioral, and risk factors. Firstly, due to the complexity of identifying, analyzing, and creating cybersecurity personas for a diverse range of employees, it lies with security experts or IT departments in the organization. Secondly, diversity of employees, such as different cultural backgrounds or preferred learning styles, differences in tech-literacy levels, acts as individual components for the AHP method and prioritization of attributes for implementing the persona approach.

Stage 3. The AHP assessment provides weights for 11 challenges and 13 attributes to bridge the gap between existing barriers in current practices and the way of persona implementation for addressing

Table 2
Persona attributes prioritization design schema

Goal (Level 0)	Criteria (Level 1)	Sub-criteria (Level 2)
Persona Attributes Prioritization	Structural and Demographic Context	Age Role and Function Work Experience Cultural Background Accessibility Needs
	Psychological and Cognitive Drivers	Cognitive Workload Risk Perception Resistance to Change Motivation Preferred Learning Styles Engagement
	Technical and Security Competence	Technical Literacy Level Digital Security Knowledge & Skills
	Behavioral and Risk Factors	Behavioral Habits Risk Profile

employees' security behavior. The assessment of criteria was conducted using a web-based Analytic Hierarchy Process tool [23]. In the analytical process, each criterion is compared in pairs of each category and sub-category, and evaluated by importance on a 1 - 9 scale (1- Equal Importance, 3- Moderate importance, 5- Strong importance, 7- Very strong importance, 9- Extreme importance). These comparisons form reciprocal matrices, from which local priority weights are derived using an eigenvector-based method. The system then aggregates the local weights by multiplying sub-criterion weights with their corresponding parent criteria weights, resulting in global priorities that indicate the relative importance of each sub-criterion with respect to the main goal.

To ensure logical consistency during analysis, AHP-OS validates results using a Consistency Ratio (CR) in each expert session as a standard AHP measure used to assess the consistency of expert judgments. A higher CR indicates lower consistency in pairwise comparisons. The CR is calculated for each participant and for each decision node to ensure both local and global consistency of judgments. Consequently, the tool uses an accepted threshold of $CR \leq 0.1$, meaning only responses with an acceptable level of logical consistency are included in the final analysis. The outcome of the pair-wise comparison is analyzed at the last step, and strategic mitigation through macro-personalization. Macro-personalization is the application of persona in cybersecurity awareness training.

3.2. Study setup

To conduct an AHP assessment, we organized an on-site workshop with an expert panel to increase the effectiveness of participants' engagement and bridge the gap between qualitative insights and quantitative prioritization.

The expert panel included 10 academic experts with industry experience and knowledge of the security fundamentals, as well as expertise in human-centered design. Before the workshop activity, participants were informed about the consent form and the confidentiality and data protection details. The decision-making activity was facilitated by the authors and guided participants through the process, explaining the theoretical background, problem statement, empirical findings from interview data, the AHP method mechanics, and the objectives of the research. After the theoretical grounding, the evaluation phase began. Firstly, we explained the importance of organizational challenges and the goal of the hierarchy. Secondly, we presented a case for evaluating personal attributes as the most critical for persona creation for security awareness programs, educational courses, and training programs. For both hierarchies, we provided vocabulary to define the terminology used in the assessment, alongside

practitioner context from interviews.

4. Findings

4.1. Organizational Challenges Evaluation

Based on findings from initial interviews, 11 organizational barriers to personalization and effective training were evaluated. An analysis was performed based on expert knowledge and experience, and prioritization of challenges considered three dimensions: operational scarcity, strategic knowledge gap, and systemic fragmentation. The final results are shown in Figure 1. The CR for the pairwise comparison matrix was 0.05 for the group results, which is lower than 0.1 and meets the requirement for the logical consistency of expert opinions. The findings indicate that the strategic knowledge gap has the most significant impact on implementing personalization in cybersecurity (weight:0.508), followed by operational scarcity (weight:0.308) and systematic fragmentation (weight:0.184).

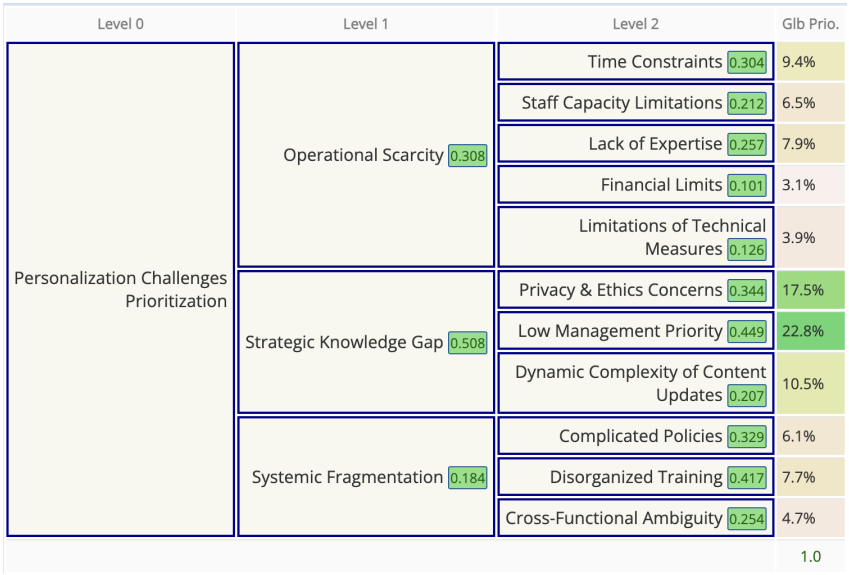


Figure 1: Hierarchical prioritization of organizational challenges

The study highlights organizational barriers to personalization caused, in the first place, by strategic rather than operational limitations. The analysis outcomes reveal that operational capacity, including staff, time, and expertise, is not as highly significant as it might appear. Therefore, the result of AHP analysis shows the Low management priority has the highest global priority (22.8%), and is reflected by experts as the biggest challenge in the hierarchy. The dominance of this criterion shows that the leadership and authority priority as a foundation is significantly important for starting work on specific problem-solving, rather than operational availability, and that barriers do not always lie with technical or resource limitations. Low management priority may limit budget, task priorities alignment, and goal planning, which in turn affects organizational constraints. Thus, there should be reinforcement of the authorities' awareness and strategic alignment towards personalization. Otherwise, without support from top management, it would not be possible.

Nowadays, privacy and ethics concerns are becoming more prevalent in society, ranking second place in this study (17.5%). Personalization tools are developed to increase employee engagement and enhance their security awareness. Often, it involves implementing individual paths and features, including adopting strategies based on personal data, behavior analytics, personal characteristics profiles, and a history of activity. While this approach demonstrates more effective outcomes, it includes work with personal data and requires organizations to be responsible for processing sensitive data and comply with data protection policies, raising privacy and ethical considerations. Furthermore, new systems and

software functionality allow the implementation of AI features, addressing further ethical concerns, and requiring appropriate policies for working with sensitive personal data. The dynamic complexity of content updates (10.5%) presents a concern of keeping up-to-date awareness systems with evolving information about emerging threats. Simultaneously maintaining thousands of individual learning paths makes it difficult to update materials dynamically and continuously.

Nevertheless, operational scarcity as a secondary barrier category (weight:0.308) has meaningful sub-criteria with the highest priority for time constraints (9.4%), lack of expertise (7.9%), and staff capacity limitations (6.5%). In fact, the design of individual learning paths or personalized materials, considering accessibility features, different preferred learning styles, and archetypes of individuals requires time for processing a huge amount of complicated data, knowledge, and understanding of people's behavior, and the way how employees interact with systems. This shows that operational-level challenges primarily impact the implementation stage, rather than determining whether personalization campaigns are initiated. Limitations with finances (3.1%) and technical measures (3.9%) were classified as less impactful challenges.

Accordingly to the experts' opinion, systemic fragmentation with weight 0.184 represents a minor barrier and is the least challenging aspect faced by security practitioners. Disorganized training (7.7%), complicated policies (6.1%), and cross-functional ambiguity (4.7%), in experts' opinions, can be overcome more easily than solving the resource gap and lack of leadership support, which stops effective personalization.

While operational scarcity (time, staff, expertise) and systematic fragmentation (disorganized training, complicated policies) are present, these barriers do not play a role as root causes. The results of AHP analysis indicate the dominance of strategic-level challenges and emphasize that the problem starts at the decision-making level rather than the implementation stage. Therefore, solutions should target managerial alignment rather than resources, as it outweighs operational and fragmentation constraints.

4.2. Personal attributes evaluation

In accordance with the organizational challenges analysis, 13 persona attributes were evaluated and prioritized. For the persona attributes, the analysis included 4 categories: Structural and demographic context, Psychological and cognitive drivers, Technical and Security competence, and Behavioral and risk factors (Figure 2).

While the common persona attributes in software engineering are categorized as structural and demographic context, the persona attributes analysis reveals the significant importance of considering technical and security competence (weight:0.337), and psychological and cognitive drivers (weight:0.302) in personalization security awareness design. Especially, digital security knowledge and skills with 22.6% of global priority qualified is the most efficient way to deal with personalized security awareness. Thus, it is important to understand what employees are actually aware of rather than relying on their background, position title, or security behavior. Technical literacy level (11.2%) seems to experts as a second necessary attribute that describes employees and their abilities to deal with technologies. A basic understanding of how systems work may help to understand the complexity of training they can handle.

Although Figure 2 shows that experts rank psychological and cognitive drivers with high weight (weight:0.302), such as motivation (6.4%), resistance to change (5.8%), risk perception (5.4%), almost as high as technical and security competences attributes. This shows that experts had different opinions on exactly which sub-criteria are the most important, which is confirmed by a low consistency ratio.

In contrast, behavioral and risk factors have opposite results and show lower weight (weight:0.201) and a high consistency ratio. This can happen because of the fewer sub-criteria in the section and agreement between experts that behavioral habits (13.5%) show obvious dominance compared to risk profile (7.5%) in the context of development of security awareness campaigns.

Contrary to the traditional approach, the common components of a persona description presented in a structural and demographic context are ranked by an expert panel as lower in priority (weight: 0.151) for persona profiling in the cybersecurity context. Such attributes, role and function (4.8%), accessibility

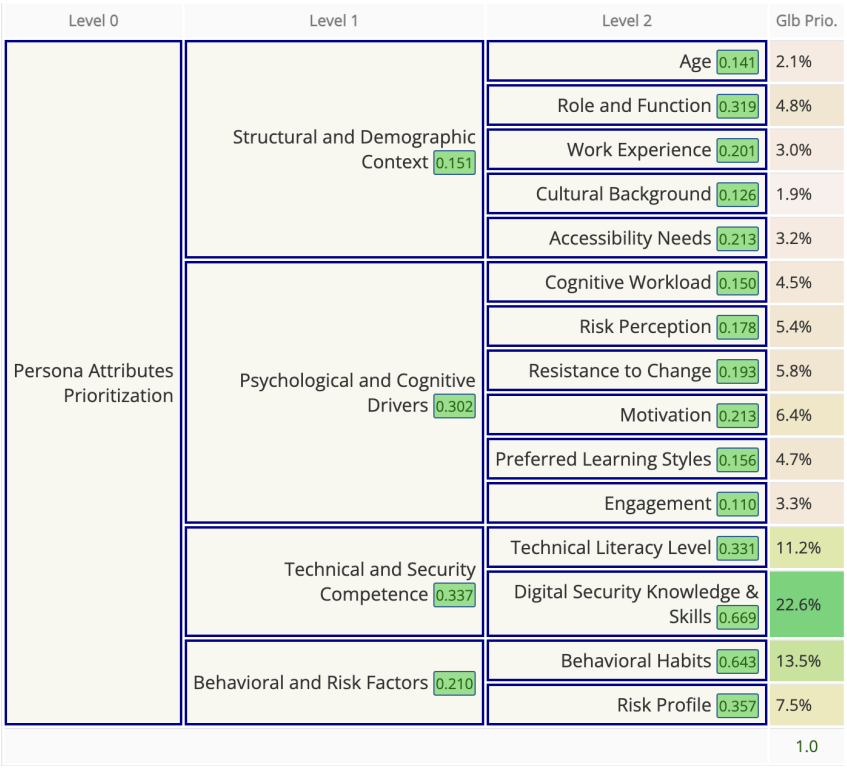


Figure 2: Hierarchical prioritization of persona attributes

needs (3.2%), and work experience (3.0%), still can bring overall understanding of the representative group as a persona in line with age (2.1%) and cultural background (1.9%).

4.3. Reliability metrics

The overall AHP-OS group consensus for organizational challenges is 50.9%, and for persona attributes prioritization is 52.8% (Table 3). The group consensus for both analyses showed a 50-55% consistency ratio despite high individual consistency (CR $\leq$ 0.1), which means that while experts' opinions were consistent, the group opinions varied differently, which emphasizes the complicated nature between socio-human and technical-cybersecurity aspects. Nevertheless, the results of the analysis highlight the primary barrier, the strategic knowledge gap, and technical and security competence with psychological and cognitive drivers as the most important individual attributes for persona creation.

Table 3
Breakdown of Consistency Ratio (CR) and Group Consensus (Gr.Cons.) by levels

Level 0 (Goal)	Level 1 (Category)	CR (%)	Gr.Cons. (%)
Personalization Challenges Prioritization	Operational Scarcity	0.9%	61.5%
	Strategic Knowledge Gap	2.7%	51.0%
	Systemic Fragmentation	3.4%	53.5%
	Overall average	**5.1%**	**50.9% (Low)**
Persona Attributes Prioritization	Structural and Demographic Context	3.6%	57.6%
	Psychological and Cognitive Drivers	2.1%	56.3%
	Technical and Security Competence	0.0%	58.2%
	Behavioral and Risk Factors	0.0%	58.5%
	Overall average	**2.6%**	**52.8% (Low)**

5. Discussion

While organizations acknowledge the value of human-centered approaches, the budget and resource capacity are often perceived as limiting factors for implementation. The findings emphasize that challenges to implement personalization are not only caused by operational and technical barriers, but primarily, a root cause is strategic-level gaps. The experts perceive that the biggest challenge is a lack of support and awareness of top management. This demonstrates that organizations often focus only on compliance with international standards like ISO 27001 and NIST [28], leaving personalization as a last priority. As a result, limited awareness and senior management prioritizing technical vulnerabilities over human-centered risks block the transition from a ”one-size-fits-all” approach to effective information security and lead to failure. Compared to the existing literature [6, 15], where the studies focus on adaptive learning training and personalization frameworks, our study provides insights into what the critical challenges are that organizations struggle with.

Moreover, the AHP analysis results extend the prior research and reveal that psychological and cognitive drivers significantly impact security behavior. The study demonstrates, in the real world, that the description of structural and demographic characteristics, such as job title, age, and work experience, does not reflect actual knowledge about cybersecurity threats and preventive mechanisms. The study outcomes prove that the human aspect remains a complicated and unpredictable variable. At the same time, low group consistency of experts' opinions demonstrates that utilization of different persona attributes can vary, depending on the cyber persona implementation context. For instance, technical competencies or motivation have more influence in security awareness training, while risk profile behavior can be the priority in case of threat analysis scenarios and preventive measures.

These results are in line with behavioral and motivation theories from related work. For instance, the dominance of attributes like digital security knowledge and skills, as well as technical literacy level and risk perception, shape the self-efficacy of employees and threat appraisal. This strengthens the belief in the ability to secure actions and knowledge of how to act with cyber security threats, supported in PMT theory [11]. Motivation, as one of the important drivers, leads employees to actually perform a security behavior and forms security intentions within the organization, as presented in TPB theory [10].

The presented results contribute by presenting a structured foundation for designing security awareness strategies in organizations. Identified barriers can support the decision-making process in strategic planning, while prioritized attributes can be utilized for guiding training campaigns. Furthermore, for the practical implications, persona can be considered as a tool for identifying target needs of employees, while creating macro-personalization for addressing organizational barriers, reducing complexity with privacy and ethics concerns. Thus, personas represent a group of employees with similar characteristics without marking sensitive personal data, instead showing the patterns of security behavior and learning preferences. Developing a few personas can neglect the huge manual work from security professionals and the need to update thousands of individual plans, and address the dynamic complexity of content updates.

The global priority values produced by AHP-OS may be influenced by the number of sub-criteria in the hierarchical structure due to the normalization process. This structural effect should be considered when interpreting the results. Although the barriers and personal attributes were identified through empirical interviews with security professionals, the results were evaluated by an expert panel that included industry-experienced participants. As a result, the findings may still reflect domain-specific knowledge and not fully cover the general patterns of the real-world state. To address this, the results of the study could be extended through further validation with security professionals from the industry.

6. Threats to validity

Participants were informed about the primary goal of the AHP analysis process and the context of prioritization. They were also provided with the AHP-OS manual, which helped to improve their understanding and thereby supported construct validity [29]. Moreover, for each sub-criterion, participants

were provided with a vocabulary list including clear definitions and practitioner context derived from interview data [30]. Before the workshop, the AHP hierarchies and the AHP-OS software tool were pilot-tested with a research group to validate the clarity of the criteria. Individual and group Consistency Ratios (CR ≤ 0.1) were used to ensure the logical consistency of pairwise judgments. However, the group consensus ratio was around 50%, indicating a variety of opinions among experts regarding prioritization across criteria. To address internal validity, the workshop was facilitated by the research team to minimize subjective influence related to the context, and all pairwise comparisons were completed individually without discussion in an expert panel.

As for external validity, the expert panel consisted of a small sample size (n = 10) and domain-specific participants, which may have influenced the final results. While the prioritized criteria demonstrated a clear pattern of agreement among experts, variation emerged at the sub-criteria level, reflecting the subjective nature of expert-based AHP evaluations.

7. Conclusion

Our study presented the AHP analysis, which integrates technical and socio-human phenomena by evaluating 11 organizational challenges and 13 personal attributes, thereby bridging the gap between identified barriers. The findings reveal a strategic knowledge gap (0.508) as the prior barrier on the way to personalization. Precisely, the low management priority is a primary bottleneck (22.8%), showing that the implementation of personalized training is a more strategic barrier rather than operational resource limitation. The study emphasizes the increasing awareness of leadership and bridging the gap between goals and operational availability for the implementation of personalized strategies.

While there are various characteristics of persona, technical and security competence (0.337) as well as psychological and cognitive drivers (0.302), according to experts' opinion, play a crucial role in creating effective cybersecurity awareness campaigns. Based on technical literacy level, digital security knowledge, and skills, the target education can be improved, including different levels of training, for example, for tech- savvy or non-tech-savvy employees. Motivation, resistance to change, and risk perception provide the basics for behavior analytics and help to develop encouraging mechanisms, flexible schedules, and understand the nature behind the employees' actions to prevent human errors and insider threats. The lower consensus (52.8%) of psychological and cognitive attributes reflects the socio-human complexity of employee security behavior. While experts agree on the importance of behavioral and risk factor attributes, their results demonstrate inconsistencies within the category by attributes. This suggests that persona design has a dynamic nature and requires a flexible approach.

Compared to prior work, which discusses the shift from a "one-size-fits-all" approach to target personalization strategies, our study contributes to existing knowledge by evaluating weights and identifying key important parameters influencing security awareness. Additionally, the study suggests that the concept of persona can mitigate several organizational barriers through the macro-personalization approach. By utilizing a cyber persona as a representative group of employees with similar characteristics, organizations can reduce workload for analyzing each individual and optimize resource allocation while still providing targeted education. This allows for differentiated training paths, such as varying information density for tech-savvy versus non-tech-savvy cohorts, effectively preventing human error and insider threats through data-driven user modeling. Personas address privacy and ethics concerns by utilizing not a persona description and data, but a collective image with group-based behavior patterns. By implementing macro-personalization, the changes can be targeted to the specific personas' gap rather than re-designing the entire awareness programs, reducing the dynamic complexity of content updates.

While hierarchies were evaluated by an expert panel with industry experience and basic knowledge of cybersecurity and HCI design, future work can include empirical validation of AHP analysis results, including a wider group of security practitioners. Furthermore, the study can explore the use of AI decision-support systems to enhance automation in the personalization processes. It can serve persona creation analysis based on identified critical attributes and generate individual phishing simulations,

develop user-friendly policies, or create individual learning paths. Combining AHP results and AI-powered tools, the organizations can benefit by moving towards personalization and risk mitigation related to human errors.

Supplementary materials

A preprint of the interview paper and detailed AHP analysis results are available at https://figshare.com/s/d4bd0b60f3609558b43d.

Declaration on Generative AI

During the preparation of this work, the authors used Gemini (Google) and Grammarly in order to: grammar and spelling check, polish language structures, and assist with LaTeX template formatting of figures and tables. After using these tools, the authors reviewed and edited the content as needed and take responsibility for the publication's content.

References

[1] M. Bada, J. R. Nurse, Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (smes), Information & Computer Security 27 (2019) 393–410.

[2] K. Khadka, A. B. Ullah, Human factors in cybersecurity: an interdisciplinary review and framework proposal: K. khadka, ab ullah, International Journal of Information Security 24 (2025) 119.

[3] L. Peca, D. Tsurcanu, Reducing cyber risk through a human–centred approach, Journal of Engineering Science (2025) 18–31.

[4] M. Trstenjak, A. Benešova, T. Opetuk, H. Cajner, Human factors and ergonomics in industry 5.0—a systematic literature review, Applied Sciences 15 (2025) 2123.

[5] A. Pollini, T. C. Callari, A. Tedeschi, D. Ruscio, L. Save, F. Chiarugi, D. Guerri, Leveraging human factors in cybersecurity: an integrated methodological approach, Cognition, Technology & Work 24 (2022) 371–390.

[6] S. Alotaibi, S. Furnell, Y. He, Towards a framework for the personalization of cybersecurity awareness, in: International Symposium on Human Aspects of Information Security and Assurance, Springer, 2023, pp. 143–153.

[7] M. Alshaikh, S. B. Maynard, A. Ahmad, S. Chang, An exploratory study of current information security training and awareness practices in organizations, Information & Computer Security 26 (2018) 70–90. doi:10.1108/ICS-08-2016-0058.

[8] A. R. Asadi, Y. Zhang, H. Said, What do personas say about privacy & security: a systematic literature review through human-ai collaboration, Journal of Ambient Intelligence and Humanized Computing 16 (2025) 1175–1190.

[9] R. A. Alsharida, B. A. S. Al-rimy, M. Al-Emran, A. Zainal, A systematic review of multi perspectives on human cybersecurity behavior, Technology in society 73 (2023) 102258.

[10] I. Ajzen, The theory of planned behavior, Organizational behavior and human decision processes 50 (1991) 179–211.

[11] D. L. Floyd, S. Prentice-Dunn, R. W. Rogers, A meta-analysis of research on protection motivation theory, Journal of applied social psychology 30 (2000) 407–429.

[12] A. T. Lo'ai, F. Muheidat, Factors that motivate defense against social engineering attacks across organizations, Procedia Computer Science 224 (2023) 75–82.

[13] A.-T. Delso-Vicente, L. Diaz-Marcos, O. Aguado-Tevar, M. G. de Blanes-Sebastián, Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity, Future Business Journal 11 (2025) 28.

[14] H.-y. S. Tsai, M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon, S. R. Cotten, Understanding online safety behaviors: A protection motivation theory perspective, Computers & Security 59 (2016) 138–150.

[15] P. Basnet, I. Nepal, R. Khan, Towards security awareness enhancement using dynamic and adaptive behavior learning models, in: 2025 IEEE World AI IoT Congress (AIIoT), IEEE, 2025, pp. 0636–0639.
[16] S. M. Kennison, E. Chan-Tin, Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors, Frontiers in Psychology 11 (2020) 546546.
[17] Z. Przymus, K. Małagocka, K. Przybyszewski, The human factor in cybersecurity: from risk profiles to resilience, Procedia Computer Science 246 (2024) 1437–1445.
[18] T. Mashiane, Z. Dlamini, T. Mahlangu, A rollout strategy for cybersecurity awareness campaigns, in: Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS 2019), Stellenbosch, South Africa, 2019, pp. 243–250.
[19] S. Akter, M. R. Uddin, S. Sajib, W. J. T. Lee, K. Michael, M. A. Hossain, Reconceptualizing cybersecurity awareness capability in the data-driven digital economy, Annals of operations research 350 (2025) 673–698.
[20] B. J. Jansen, J. O. Salminen, S.-g. Jung, Data-driven personas for enhanced user understanding: Combining empathy with rationality for better insights to analytics, Data and Information Management 4 (2020) 1–17.
[21] D. Ki-Aries, S. Faily, Persona-centred information security awareness, Computers & security 70 (2017) 663–674.
[22] A. Atzeni, C. Cameroni, S. Faily, J. Lyle, I. Fléchais, Here's johnny: a methodology for developing attacker personas, in: 2011 Sixth International Conference on Availability, Reliability and Security, IEEE, 2011, pp. 722–727.
[23] K. D. Goepel, Implementation of an online software tool for the analytic hierarchy process (ahp-os), International journal of the analytic hierarchy process 10 (2018). URL: https://doi.org/10.13033/ijahp.v10i3.590.
[24] Z. Liu, Evaluating digitalized visualization interfaces: Integrating visual design elements and analytic hierarchy process, International Journal of Human–Computer Interaction 41 (2025) 5731–5760.
[25] R. Dorado, A. Gómez-Moreno, E. Torres-Jiménez, E. López-Alba, An ahp application to select software for engineering education, Computer Applications in Engineering Education 22 (2014) 200–208.
[26] F. R. Moreira, E. D. Canedo, R. R. Nunes, A. L. M. Serrano, C. J. B. Abbas, M. L. P. Júnior, F. L. L. de Mendonça, Cybersecurity risk assessment through analytic hierarchy process: Integrating multicriteria and sensitivity analysis., in: ICEIS (2), 2025, pp. 117–128.
[27] T. L. Saaty, Decision making with the analytic hierarchy process, International journal of services sciences 1 (2008) 83–98.
[28] A. Tsohou, S. Kokolakis, C. Lambrinoudakis, S. Gritzalis, A security standards' framework to facilitate best practices' awareness and conformity, Information Management & Computer Security 18 (2010) 350–365.
[29] C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, A. Wesslén, Experimentation in Software Engineering, Kluwer Academic Publishers, 2000.
[30] P. Ralph, et al., Empirical standards for software engineering research, https://www2.sigsoft.org/EmpiricalStandards/, 2020. Accessed: 2026-04-14.