

www.jpis.az

Development of a conceptual model for assessing personal information security culture

Rasmiyya Mahmudova

Institute of Information Technology, Baku, Azerbaijan

rasmahmudova@gmail.com

orcid.org/0000-0002-5816-9373

ARTICLE INFO

<https://doi.org/10.25045/jpis.v17.i1.08>

Article history:

Received 01 September 2025

Received in revised form

05 November 2025

Accepted 15 January 2026

Keywords:

Information security
Human factor
Security behavior
Information security culture
assessment methods
Social engineering risks
Security policy

ABSTRACT

The rapid expansion of the digital environment has led to an increase in information security risks, thereby necessitating the formation of an information security culture at both organizational and individual levels. In this article, existing approaches for assessing information security culture are systematically analyzed. The main objective of the research is to determine the adequacy of these approaches in terms of measuring not only the organizational level but also the knowledge, attitudes, and behaviors of individuals regarding information security. The article researches the main characteristics, application areas, and limitations of existing methods in a comparative manner. As a result of the analysis, it has been determined that most existing models are oriented toward assessing information security culture from the perspective of organizational structure and management. In these approaches, the human factor is mostly evaluated as the weak link in the security chain, and the measurement of values, motivations, and behaviors at the individual level is not sufficiently covered. In order to fill this gap, the article proposes a conceptual model for assessing personal information security culture. The model presents a multi-level approach that integrates an individual's knowledge, values, risk perception, sense of responsibility, and behavioral habits related to information security. The proposed conceptual model creates an opportunity to understand the individual's decision-making process and behavioral motivation regarding information security, as well as to more deeply assess the impact of personal culture on the organizational security environment.

1. Introduction

Information security is a concept of vital importance at the individual, organizational, and societal levels in the modern era. Alongside the rapid development of digital technologies, the protection of information resources has become increasingly critical. Technical measures alone are insufficient in this field; the human factor and human behavior are key elements that determine the effectiveness of security strategies. Information Security Culture (ISC) encompasses an individual's knowledge, attitudes, and behaviors, the management and policy mechanisms of an organization, as well as the general level of digital

literacy in society. At the individual level, this culture represents a person's approach to personal data, conscious behavior, and preparedness against technological risks. At the organizational level, security culture pertains to employees' adherence to codes of conduct, the implementation of information security policies, and risk management. At the societal level, ISC is formed through digital awareness, legislative initiatives, and public behavioral norms. The interaction between these three levels plays a decisive role in shaping the overall security environment.

Assessing ISC is essential for identifying existing gaps in this field and formulating

development strategies. Various models and methods are designed to perform this assessment. Among these models, maturity frameworks, empirically-based approaches, and survey-based measurement tools are widely applied. Simultaneously, quantitative and qualitative approaches complement each other among these methods. Surveys, focus groups, interviews, and behavioral analyses serve as the primary assessment tools in this area. The application of each method must be context-appropriate and serve the purpose of the assessment. In scientific literature, models such as the Cybersecurity Culture Measurement Framework (CCMF) and the Information Security Culture Framework (ISCF) provide effective frameworks for analyzing individual and organizational behaviors. These models enable complex assessment by considering the human factor, the technological environment, and the organizational structure. At the same time, survey-based measurement tools are extensively used to measure individual security behaviors and knowledge levels. However, the reliability and suitability of these tools remain a subject of research.

ISC is significant for creating a healthy security environment not only at the individual level but also at the organizational and societal levels. Education, training, and awareness-raising processes play a major role in the formation of this culture (Aliguliyev & Mahmudova, 2010). The application of correct behavioral rules during people's contact with digital technologies makes them more informed and security-conscious. Otherwise, the resilience of society weakens in the face of new risks and threats brought by technological developments. Ensuring security in the digital world depends not only on technical measures but is also linked to social and cultural values on both individual and organizational planes. For this purpose, increasing digital literacy and security knowledge is essential. The study of this issue requires cooperation among specialists from various fields; in particular, the experience of professionals working in the field of information security plays a crucial role. Strengthening information security culture is also associated with the implementation of legislative reforms. The legislative framework can become a foundation that supports the security policies of organizations and encourages people's secure behaviors. Furthermore, considering the human factor in the process of improving digital security forms the basis of success in this field. For this

reason, research continuously seeks new methods and approaches to develop ISC more effectively and to ensure preparedness against future threats.

2. Related work

Information security is not merely a set of technical measures but a process closely linked to human behavior and organizational values. Consequently, the concept of "Information Security Culture" has gained significant importance in modern management and security research. Information security should be approached not only from a technological perspective but as a complex structure that encompasses social and organizational factors (Mahmudova & Dashdamirova, 2021). Simply forming ISC is insufficient; it is also crucial to measure its effectiveness, resilience, and impact. The lack of measurement mechanisms causes ISC to remain at a conceptual level and limits its use as a decision-making and development tool in organizational management. Over the last decade, several psychometric scales and measurement tools aimed at assessing ISC have been proposed, and their diversity indicates a demand for standardization in this field (Orehek & Petrič, 2021).

The primary significance of measuring ISC lies in enabling organizations to objectively identify risks arising from the human factor. Employees' knowledge, attitudes, and behaviors are the main sources of security breaches, and measuring these factors shows management where risks are concentrated. Through these measurements, organizations obtain concrete data regarding employees' compliance with security rules, their knowledge levels, normative expectations, and values (Parsons et al., 2017). Such information allows for the identification of risky behavior patterns, recognition of areas requiring intervention, and more effective planning of training programs (Phillips et al., 2009). The European Union Agency for Network and Information Security (ENISA) recommends the systematic measurement of ISC to assess and improve the human factor in organizations (ENISA, 2018).

A key point here is the contribution of measurement results to the decision-making process. These results help management allocate resources more purposefully by evaluating the effectiveness of security policies and training programs (Parsons et al., 2017). This simultaneously ensures resource optimization and administrative transparency within the

organization (Da Veiga & Eloff, 2010). Furthermore, measurements serve as a baseline for tracking changes. In other words, after diagnosing the initial state of ISC, it becomes possible to comparatively assess the impact of subsequent interventions, providing continuous monitoring of security culture development (Phillips et al., 2009). Systematic measurements strengthen the identification of internal risks because certain behavioral patterns can reveal potential threats in advance (Orehek & Petrič, 2021; Da Veiga & Eloff, 2010). Thus, measurements evolve from passive monitoring into a predictive management tool.

Information Security Culture (ISC) is a system of behaviors, values, and beliefs directed toward protecting information assets within organizations and societies. This culture encompasses individuals' levels of security knowledge, their attitudes toward technological risks, and the degree of adherence to security protocols in daily work processes. To establish a robust ISC, an organization's strategic documents, internal policies, and observable behavioral patterns must be examined comprehensively (Phillips & Moore, 2023). Awareness campaigns, regular training, and the promotion of exemplary behavior by leadership play a vital role in the development of ISC within organizations. For a healthy security culture to flourish, it is essential not only to implement rules but also to ensure that these rules are internalized and executed through intrinsic motivation (Sasse et al., 2007).

Recently, ISC has become a field of increasing interest for both researchers and practitioners. Several models have been developed to assess security culture in organizations. The Information Security Culture Assessment (ISCA) tool, presented by Da Veiga and Martins, was validated using factor analysis, demonstrating the reliability of assessing ISC through questionnaires (Da Veiga & Martins, 2007). Their 2015 study assessed ISC in several organizations within the financial sector and found that security culture improved through interventions such as training and policy applications. Another significant study by Orehek and Petrič conducted a systematic review of ISC assessment tools, comparing 19 different instruments. The results indicated that while most of these tools cover factors like knowledge, behavioral compliance, and policy adherence, they can vary based on the specific context of the organization (Orehek & Petrič, 2020).

Various studies (e.g., Alnatheer et al., 2012; Alfawaz, 2011; Mahmudova, 2023) have emphasized the importance of integrating both technical and non-technical aspects in ISC assessment, including organizational culture, the role of leadership, and the effectiveness of information security training. An interesting finding is that the type of organizational culture (e.g., clan, adhocracy, market, hierarchy) influences the effectiveness of ISC policies. Alongside these traditional approaches, recent scientific research seeks more objective and continuous methods for assessing ISC. Considering the subjectivity of survey-based assessments and their potential divergence from real-world behaviors, researchers are proposing new models based on data analysis from technical systems (McCormac et al., 2017). This approach allows for measuring how individuals actually behave in the work process rather than what they think about security. Studies show that data from sources such as user behavior analytics, security log analysis, and phishing simulation results provide more accurate information about the actual state of the culture.

In parallel with technological development, the scale and complexity of cyber threats continue to grow. In this context, assessing the level of ISC is essential for organizations' risk management and security strategies. Existing research shows that a unified and standardized methodology for measuring ISC does not exist. Most approaches rely on technical indicators or behavioral models and are primarily oriented toward assessing ISC at the organizational level. However, the security behaviors and culture of individual users are also of critical importance in the modern cyber environment. The 2021 report by the Information Systems Audit and Control Association (ISACA) notes that "no matter how advanced security technologies are, individual behaviors can undermine the stability of these systems."

Azerbaijan's digital economy and technological infrastructure are developing rapidly; however, cyber threats are increasing alongside this growth. While attention to cybersecurity has increased in both government agencies and the private sector, technical measures alone are insufficient. In this regard, the human factor is of great importance in managing cybersecurity risks. The "Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027," approved by Decree No. 4060 of the President of the Republic of Azerbaijan, specifically emphasizes the importance

of forming security awareness amid the country's increasing integration into digital systems. In this context, considering the human factor is paramount for ensuring long-term resilience in cybersecurity (Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027, 2023).

The complexity of the modern digital ecosystem and the personalized nature of cyber threats necessitate a reassessment of ISC. While most existing studies investigate ISC within an organizational framework and the context of employee compliance with corporate policy, individuals' behavioral motivations and personal risk perceptions as independent information subjects have been overlooked. Given that the human factor remains the most critical link in the cybersecurity chain, developing new scientific-methodological approaches for measuring security habits at the individual level is of high relevance.

The objective of the study is to develop a conceptual model that, based on a systematic analysis of existing approaches to information security culture assessment, enables the measurement of ISC not only at the organizational level but also at the individual level. This model integrates an individual's knowledge of cyber threats, risk perception, psychosocial motivation, and actual security behaviors within a unified framework.

Problem Statement. Existing approaches primarily focus on assessing information security culture at the organizational level and treat the human factor as the weakest link in the security chain. However, individuals' knowledge of cyber threats, risk perception, psychosocial motivation, and actual security behaviors are neither adequately measured nor evaluated. Consequently, the systematic study and assessment of information security culture at the individual level is hindered.

In this regard, the main issue addressed in the study is the development of a conceptual model that ensures the systematic assessment of information security culture at the individual level.

3. Materials and methods

3.1. Theoretical Foundations and Context of ISC

The assessment of ISC is not limited to empirical surveys and organizational frameworks. In this process, theoretical models derived from social psychology play a crucial role in explaining

and predicting individual behaviors. These models allow for a deeper understanding of the human factor and complement practical assessment methods.

Knowledge–Attitude–Behavior (KAB) Model.

This approach suggests that an individual's security behavior passes through three stages: the acquisition of knowledge, the formation of an attitude based on that knowledge, and finally, its transformation into behavior. The KAB model is noted for its simplicity; however, the "KAB gap" problem exists: even if people know the importance of security rules, they do not always apply them (Nguyen & Le, 2024; Vilander, 2021).

Theory of Planned Behavior (TPB). Proposed by Ajzen, this theory emphasizes intention as the primary determinant of behavior. Intention is formed by three factors: attitude toward the behavior, subjective norms, and perceived behavioral control (Ajzen, 1991). Research indicates that TPB is highly effective in explaining employees' intentions to comply with security policies (Bulgurcu et al., 2010).

Protection Motivation Theory (PMT).

Introduced by Rogers, this theory explains individuals' security behaviors based on threat appraisal and coping appraisal (Rogers, 1975). Threat appraisal depends on how an individual perceives the severity of the risk and the probability of exposure to it. Perceiving the risk as highly dangerous and real increases protection motivation. Coping appraisal, on the other hand, is formed based on the perceived efficacy of the proposed protective measure, the costs associated with implementing this measure, and the individual's self-efficacy in their ability to carry out the measure. Johnston and Warkentin show that PMT has strong explanatory power in understanding why individuals follow or ignore security recommendations (Johnston & Warkentin, 2010).

3.2. Problem solution

The problem addressed is that existing approaches do not sufficiently measure the information security culture of individuals. Since current methodologies view the human factor merely as an implementer of organizational information security policies and a "weak link," they fail to fully encompass individual intrinsic motivation and personal risk perception. To solve this problem, a "person-centered" conceptual model is proposed, distinguishing it from the

"organization-centered" approaches typically used in ISC assessment.

Within the framework of the proposed conceptual model, the solution to the problem is built upon the following methodological innovations:

- **Compensating for the Knowledge–Attitude–Behavior Gap:** To address the issue of individuals failing to comply with security rules despite knowing them, "Risk Perception" and "Psychosocial Motivation" factors have been integrated into the model. These components act as catalysts that explain the disconnect between knowledge levels and real-world behavior.
- **Hierarchical Assessment Structure:** The model assesses an individual's ISC level across six interrelated dimensions: basic knowledge, technical skills, risk assessment, decision-making, motivation, and actual behavioral habits. This structure allows for characterizing an individual's security profile through both quantitative and qualitative indicators.
- **Recognition of the Individual as an "Active Defense Resource":** As a way to solve the problem, the individual is recognized not just as a rule-follower, but as a subjective decision-making element of the information security system. By highlighting the individual's ethical values and sense of responsibility, this approach serves to create a more resilient security environment within the organization.

3.3. Analysis and classification of existing approaches to ISC assessment

ISC is recognized as a key factor in risk management, as the human factor remains the weakest link. An analysis of existing ISC assessment models and methods shows that they have evolved from simple surveys to complex, multidimensional, and behavior-based approaches. In the scientific literature, various models and methods have been proposed for measuring ISC. These can generally be classified into three main groups: qualitative, quantitative, and mixed methods.

3.3.1. Quantitative models

These models primarily seek to statistically measure different aspects of information security culture (ISC) through surveys (questionnaires).

Information Security Culture Assessment (ISCA) Model: Proposed by Da Veiga and Eloff,

this model is a widely used tool for measuring organizational ISC (Da Veiga and Eloff, 2010). The model employs a survey questionnaire to assess employees' behaviors and attitudes toward security across multiple dimensions. These dimensions typically include areas such as 'information security policy,' 'management commitment,' 'security awareness,' and 'incident response.' The results enable the identification of organizational strengths and weaknesses.

Cybersecurity Culture Framework: This framework focuses on the psychological factors that shape culture. The model seeks to predict the behaviors of individuals and groups by measuring their attitudes, subjective norms, perceived control, and self-efficacy (Parsons et al., 2017).

Human Aspects of Information Security Questionnaire (HAIS-Q) Model: This model is used to assess ISC at both the individual and organizational levels (Parson et al., 2014). Using a structured questionnaire consisting of 63 items, the model measures the components of knowledge, attitude, and behavior. These components are evaluated across subdomains such as password security, email usage, internet behavior, mobile device use, social media activity, and information sharing. Owing to its psychometric-based approach, the HAIS-Q model is widely used for predicting individual security behaviors.

3.3.2. Qualitative methods

These methods focus not on numerical indicators but on understanding the essence of culture, its values, and the organizational context. They enable researchers to comprehend the motivations, beliefs, and social relationships underlying employees' security-related behaviors. Therefore, qualitative methods, in addition to quantitative measurements, help to achieve a deeper understanding of an organization's security culture.

Interviews and focus groups: In-depth interviews or focus group discussions conducted with employees and managers help reveal their perceptions of security, the challenges they face, and their actual attitudes toward existing policies. This method is highly effective for answering the 'why' question (Schlienger & Teufel, 2003). The data obtained from such interviews can also be useful for assessing factors such as leadership style, communication culture, and levels of trust within the organization. Focus groups, in turn,

allow for the identification of differences in security approaches across departments.

Observation and scenario analysis: Direct observations by the researcher in the workplace or monitoring employees' responses to specific security scenarios (e.g., a simulated phishing attack) can provide more objective data than written responses. This method shows how employees actually behave in real situations, that is, how they apply training and policies in their daily work. For example, during phishing simulations, it can be observed in which cases employees respond to suspicious emails and in which cases they immediately report the incident. This enables the researcher to examine the practical aspects of security behaviors and the moments when 'culture is translated into behavior' (Morić, 2025; Petrič, 2025; Schwab, 2025).

3.3.3. Maturity models

These models assess an organization's information security culture (ISC) along a defined scale (typically a five-level scale). Each level reflects the degree to which the organization's culture has evolved and become institutionalized. Such models classify an organization's ISC level from 'non-existent' or 'initial' through 'repeatable,' 'defined,' and 'managed,' and ultimately to 'optimized' (Al-Hogail, 2015). This provides organizations with a clear roadmap for understanding their current state and for progressing to the next level.

As can be seen, each of these models has its own strengths and weaknesses and addresses different aspects of ISC assessment. The table presented below compares the key indicators, measurement tools, advantages, and limitations of various ISC assessment models and approaches.

Table 1. Comparison of Information Security Culture (ISC) Assessment Models

Model / Approach	Key Indicators	Measurement Tools	Advantages	Limitations
ISCA Model	Knowledge, attitude, policy compliance, management commitment	Surveys, questionnaires	Structured, widely applied at the organizational level	Based on subjective responses
HAIQ model	Knowledge, attitude, behavior (password usage, e-mail, internet, mobile devices, social media)	A questionnaire comprising 63 items	A questionnaire comprising 63 items	The survey is extensive and time-consuming
Phishing Simulations and Observation	Real behavior, incident response, risk perception	Simulated attacks, observation	Objective results, measures real-world behavior	Potential ethical and privacy concerns
Maturity Models	ISC maturity levels (initial → optimized)	5-level assessment frameworks	Provides a roadmap, allows tracking of organizational growth	Does not cover the individual level
Qualitative Methods	Security values, motivation, social relations	Interviews, focus groups	Deep insight, uncovers underlying motives	Subjectivity, high time and resource requirements

3.3.4. Synthesis of findings and identified Gaps in current Models

While existing models for assessing ISC offer diverse approaches, significant methodological and practical limitations emerge during their implementation. These constraints impact the reliability, generalizability, and applicability of the assessment results.

Quantitative models, particularly ISCA and HAIQ, measure knowledge, attitude, and behavior components through structured surveys. However, the primary weakness of these approaches is their susceptibility to subjectivity and the risk of social desirability bias. Researchers note that these models often capture only the surface-level manifestations of organizational

culture, failing to account for deeper behavioral motivations (Ruhwanya & Ophoff, 2020).

While qualitative methods, such as interviews and observations, are beneficial for uncovering the social and psychological aspects of security culture, they impose high demands in terms of time and resources. Furthermore, the difficulty of implementing these methods on a large scale and the fact that the objectivity of the results depends on the researcher's interpretation are highlighted as significant challenges (Govender et al., 2020).

Maturity models provide useful frameworks for determining the ISC level of an organization but fail to encompass individual behaviors and psychological factors. This creates a gap, particularly in evaluating individual security awareness and motivation. The ENISA (2018) report high-

lights that these models measure culture primarily at the structural and policy levels, proving insufficient for analyzing behavior at the individual level.

Furthermore, a systematic review by Orehek and Petrič analyzed 19 different assessment tools and found that while most are applicable within specific contexts, a standardized and universal approach is lacking. This is due to the diverse cultural, sectoral, and risk profiles of different organizations (Orehek & Petrič, 2021).

Recent research indicates that assessment methods based on data collected from technical systems (e.g., phishing simulations and user behavior analytics) yield more objective results. However, these methods may also raise ethical and privacy concerns and may not be feasible for implementation in every organization.

These analyses suggest that the application of multidimensional and integrative approaches for assessing ISC is more appropriate. Such an approach enables a more accurate and objective analysis of security behaviors at both the individual and organizational levels, laying the groundwork for the formulation of more effective security strategies in the future.

3.3.5. Proposed Conceptual Model of Individual Information Security Culture

An analysis of the existing literature reveals that current scientific approaches to ISC are predominantly organization-centric (Schneider, 2000). According to this perspective, the primary goal of ISC is to protect the organization's information resources, where the human factor is often evaluated merely as a component that either creates or mitigates risk. In this context, culture functions as a tool to ensure that individuals comply with security policies within the organization. The human factor is largely perceived as the "weakest link," and Security Awareness Training (SAT) serves to reduce this vulnerability (Siponen & Willison, 2009).

However, this approach frequently relegates the individual to the background. In the modern information environment, the individual is an independent information subject directly exposed to various cyber threats and risks. The dynamic development of digital society necessitates considering the active participation of individual users in information flows and the close link between their personal well-being and information security. This approach is supported by research indicating that awareness, proper

digital behavior, and responsible internet use play a decisive role in shaping individual information security (Aliguliyev et al., 2014). From this perspective, forming a culture oriented toward individual information security requires the conscious and purposeful management of personal data, passwords, online activities, social media behavior, and cybersecurity habits. Thus, ISC should be viewed not only as a normative mechanism applied within an organization but also as an integral part of social responsibility, knowledge, and behavioral culture at the individual level.

While the organization-centric approach to ISC is significantly important, we believe it does not sufficiently explain the personal risks, individual behavioral motivations, and actual security behaviors of the individual as a separate security object. Consequently, there is a need to develop a culture of Individual ISC. The proposed approach evaluates the individual not as a passive subject who merely follows rules, but as a primary resource and an active participant in the information security system.

Within the scope of this study, Individual ISC is proposed as a conceptual model with a hierarchical structure. The model consists of six interrelated components based on the knowledge – assessment–motivation–behavior sequence. At the base level of the model are the fundamental components - Cybersecurity Awareness and Technical Knowledge and Skills - which enable the individual to recognize risks and build the potential for technological self-protection.

At the next stage, the **Risk Assessment and Decision-Making** component allows the individual to interpret acquired knowledge in specific situations and make behavioral choices corresponding to the risk level. At this stage, the decision-making process relies not only on rational calculations but also on the individual's personal values and risk perception.

The Psychosocial Motivation and Responsibility component acts as the primary internal mechanism facilitating the transition to behavior and ensures the sustainability of security practices. Meanwhile, the Privacy and Protection of Personal Interests component serves as a normative and ethical framework, exerting a transversal influence across all stages and reinforcing the individual's legal and moral responsibility.

The interaction of these components culminates in **Security Behaviors** at the top level

of the model. This component encompasses practical actions such as password management, software updates, data backup, and responses to suspicious incidents, serving as the model's primary empirically measurable outcome variable.

Thus, the presented Individual ISC conceptual model can be applied for the

comprehensive assessment of ISC at the individual level, independent of the organizational context, while also being linked with ISC indicators used at the organizational level. The hierarchical structure and inter-component relationships of the model are reflected in its graphical representation (fig. 1).

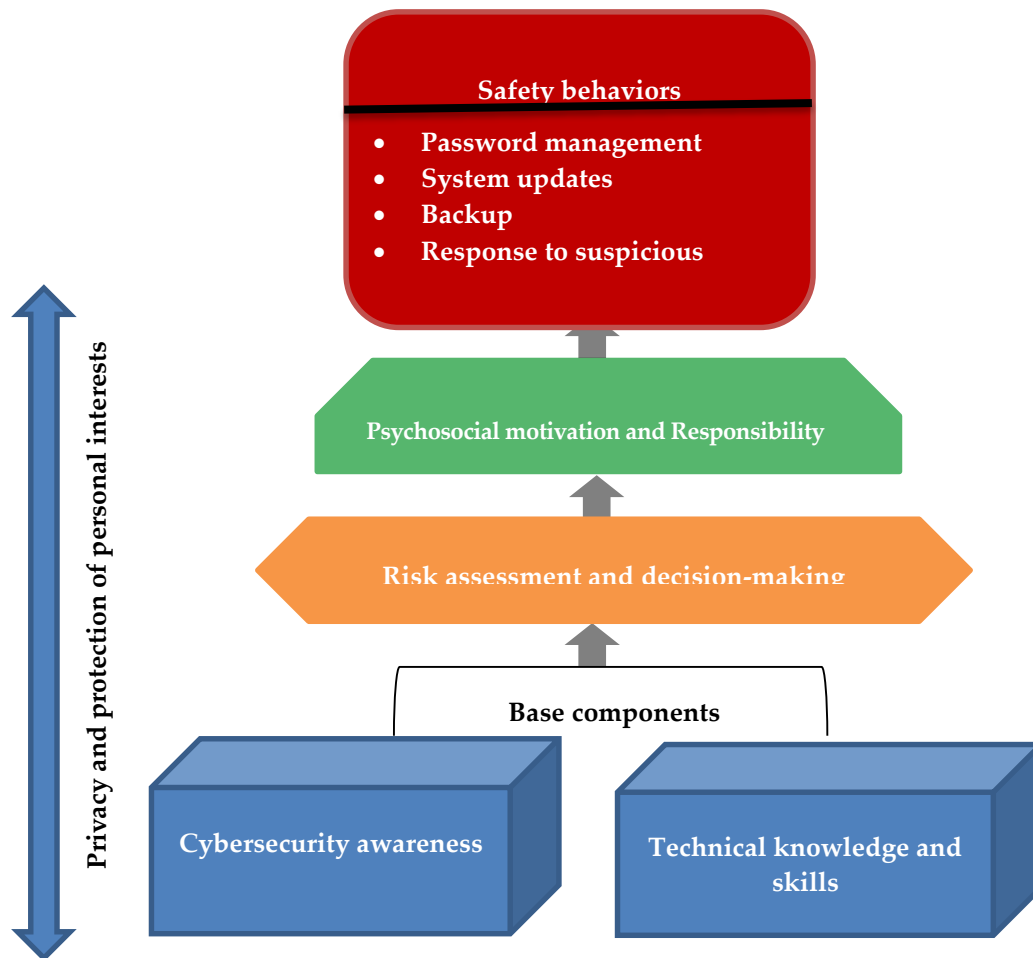


Fig. 1. Conceptual Model of an Individual's Information Security Culture

This approach aligns with the principles outlined in the resolution 'Creation of a global culture of cybersecurity' (A/RES/57/239), adopted by the UN General Assembly in 2002. The resolution emphasizes key values such as individual responsibility, technological literacy, raising awareness, and adherence to ethical norms as primary directions for fostering a culture of cybersecurity (UN, 2002).

4. Discussion

The systematic review conducted in this study demonstrates that the primary gap in assessing ISC is the difficulty of measuring the **intention-behavior gap** at the individual level. While existing quantitative models (e.g., HAIS-Q, ISCA)

effectively measure knowledge and attitudes, they face limitations in reliably predicting individuals' actual behavior, as they rely predominantly on subjective survey data. Similarly, maturity models evaluate organizational policies but do not delve into the depths of individual motivation.

The proposed six-component conceptual model of **Individual ISC** is designed to address these limitations. The model initially covers knowledge and skills (Cyber-threat awareness, Technical knowledge). However, the most critical aspect is the inclusion of psychological factors such as **Risk Assessment** and **Psychosocial Motivation**. In alignment with the core principles of the **Theory of Planned Behavior (TPB)** and **Protection Motivation Theory (PMT)**, these two components act as powerful moderators that

activate an individual's internal sense of responsibility and risk consciousness.

Another fundamental advantage of the model is the presentation of **Security Behaviors** as a distinct outcome measure. This approach necessitates a mixed-methods methodology that allows for the use of objective data (e.g., phishing simulations, password update frequency via system logs) alongside subjective data (surveys) during the assessment. This integrative approach serves as a gold standard for obtaining more reliable and robust results in ISC research. Ultimately, the model offers a strategic framework that enables organizations to measure how effectively security training (knowledge) translates into an individual's daily habits (behavior).

4.1. Socio-Political and Economic Significance of the Model

The proposed Individual ISC model transcends the boundaries of individual behavior and acts as a strategic engine ensuring the resilience of the modern digital ecosystem. The implementation of the model holds fundamental importance in the following three macro-level directions:

- **Social Target: Formation of Digital Trust.** The sustainability of social relations and economic exchange in a digital society depends on individuals' trust in the technological environment. By developing "digital hygiene" habits among users, the Individual ISC model builds collective resilience against cyber-fraud. Individual ISC also acts as a protective barrier ensuring the psychological and social safety of individuals in the digital sphere. Particularly in protecting school-aged children from internet addiction and online threats, the formation of personal awareness and behavioral culture is of critical importance (Aliguliyev et al., 2014). Dutton (2017) notes that cybersecurity culture is not merely technical protection but also a form of social capital that enhances digital participation by strengthening the sense of personal safety in the online environment. This approach serves to preserve social well-being during the society's digital transformation process.
- **Political Target: National Cyber-Resilience and Sovereignty.** In modern public administration, cybersecurity strategies cannot be considered effective without a citizen component. The proposed model elevates the citizen from the status of a "passive user" to an

"active defender." This is a crucial factor in ensuring the state's cyber-sovereignty and political stability, particularly during mass cyber-attacks and disinformation campaigns. As emphasized in UN Resolution **A/RES/57/239 (2002)**, building a global culture of cybersecurity relies directly on the principles of individual responsibility and awareness, which constitute an internal component of national security.

- **Economic Target: Minimizing Cyber-Losses and Cost Optimization.** Global economic losses resulting from cybercrime are fueled by security gaps at the individual level. Ensuring the security of personal data reduces economic damages such as identity theft, phishing attacks, and personal data breaches. Implementing the Individual ISC model allows both the public and private sectors to transfer "reactive" expenditures—aimed at remediating the consequences of cyber-incidents—into "proactive" protection (education and habit development).

5. Conclusion

Against the backdrop of the rapid expansion of the digital environment, the adequate and reliable assessment of individual users' Information Security Culture has become critically important. Through a systematic review of existing ISC models, this article has determined that the primary shortcomings stem from organization-centric approaches and subjective measurement methods.

The main contribution of this research is the proposal of a six-component conceptual model of **Individual ISC**, which successfully integrates "knowledge," "psychological motivation," and "behavior" elements. The model's focus on internal factors such as "risk assessment" and "sense of responsibility" establishes a universal framework for measuring the cybersecurity culture of both organizational employees and independent individuals. This approach confirms the necessity of a **mixed-methods methodology** (the synthesis of objective and subjective data) to overcome the problem of subjectivity in ISC research.

Future research should focus on developing a completely new, objective assessment instrument (survey tool) based on the proposed model and conducting its empirical validation across diverse user groups in real-world settings. This will

provide an accurate, evidence-based tool for determining the effectiveness of ISC programs.

Acknowledgments

I would like to express my sincere gratitude to Academician Rasim Alguliyev for his invaluable scientific advice and guidance in defining the research topic

References

- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Alfawaz, S. (2011). Information security culture: A behaviour compliance conceptual framework. *Information Management & Computer Security*, 19(4), 296–310. <https://doi.org/10.1108/09685221111173064>
- AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49, 567–575. <https://doi.org/10.1016/j.chb.2015.03.054>
- Alguliyev, R.M., Mahmudova R.Sh. (2010). Information Culture: its Essence Problems of Formation and Ways of Solution. *Problems of information society*, no. 1, 14-22.
- Aliguliev R.M. Mahmudova R.Sh., Mahmudov R.Sh. (2014). Voprosy zashchity detey shkol'nogo vozrasta ot internet-zavisimosti [Issues of protecting school-age children from Internet addiction]. *Dstantsionnoye i virtual'noye obucheniye [Distance and virtual education]*, No. 5. Pp. 97–107 (in Russian).
- Alnatheer, M., Chan, T., & Nelson, K. (2012). Information security culture: A behavior compliance conceptual framework. *International Journal of Computer Science and Information Security*, 10(3), 1–8. <https://www.ijcsis.org/papers/Vol10No3/1.pdf>
- Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023-2027, <https://e-qanun.az/framework/55045>, August 28, 2023. (In Azerbaijani)
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548. <https://doi.org/10.2307/25750690>
- Cano, J. J. (2021). Organizational culture for information security: A systemic perspective. *ISACA Journal*, 3. <https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/organizational-culture-for-information-security>
- Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196–207. <https://doi.org/10.1016/j.cose.2009.09.002>
- Da Veiga, A., & Martins, N. (2007). Information security culture assessment: An instrument and validation. *Proceedings of the 2007 Information Security for South Africa Conference (ISSA 2007)*. Johannesburg, South Africa: IEEE. <https://doi.org/10.1109/ISSA.2007.147>
- ENISA. (2018). Cyber security culture in organisations. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations>
- Dutton, W. H. (2017). *Fostering a Cyber Security Culture: Insights from a Global Cybersecurity Capacity Centre*. Global Cyber Security Capacity Centre, University of Oxford.
- Govender, S. G., Kritzinger, E., & Loock, M. (2020). A framework for the assessment of information security risk, the reduction of information security cost and the sustainability of information security culture. In *IFIP AICT*, 580. Springer.
- Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549–566. <https://doi.org/10.2307/25750691>
- Mahmudova, R. (2023). Problems of evaluating the organization's information security culture. *Problems of Information Society*, 14(1), 66–74.
- Mahmudova, R. Sh. (2023). Cyber-physical systems: Security problems and issues of personnel information security culture. *International Journal of Education and Management Engineering*, 13(2), 18-26. <https://doi.org/10.5815/ijeme.2023.02.03>
- Mahmudova, R.S., Dashdamirova, K.G. (2021). Analysis of information security problems in the information society environment. *Problems of Information Society*, 2, 83-94.
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151–156. <https://doi.org/10.1016/j.chb.2016.11.065>
- Morić, D., Roncevic, N., & Petric, G. (2023). Understanding information security behavior: A social and cognitive perspective. *Information & Computer Security*, 31(4), 567–584. <https://doi.org/10.1108/ICS-03-2023-0045>
- Nguyen, B. H., & Le, H. N. Q. (2024). Investigation on information security awareness based on KAB model: The moderating role of age and education level. *Information & Computer Security*, 32(5), 598–612. <https://doi.org/10.1108/ICS-09-2023-0152>
- Orehek, Š., & Petrič, G. (2021). A systematic review of scales for measuring information security culture. *Information & Computer Security*, 29(1), 133–158. <https://doi.org/10.1108/ICS-12-2019-0140>
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. <https://doi.org/10.1016/j.cose.2013.12.003>
- Parsons, K., Calic, D., Pattinson, M., Butavicius, M., & McCormac, A. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66, 40–51. <https://doi.org/10.1016/j.cose.2017.01.004>
- Petrič, G., & Orehek, Š. (2022). Exploring organizational factors influencing information security culture. *Computers & Security*, 116, 102651. <https://doi.org/10.1016/j.cose.2022.102651>
- Phillips, J., Brummel, B., Aurigemma, S., & Moore, T. (2009). Information security culture: A look ahead at measurement methods. Retrieved from <https://tylermoore.utulsa.edu/asc23phillips.pdf>
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
- Ruhwanya, Z., & Ophoff, J. (2020). Critical analysis of information security culture definitions. In *HAISA 2020 (IFIP AICT)*, 593. Springer.
- Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—A human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3), 122–131. <https://doi.org/10.1023/A:1011902718709>
- Schwab, K. (2020). *The Global Competitiveness Report 2020*. World Economic Forum. <https://www.weforum.org/reports/the-global-competitiveness-report-2020>

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

<https://doi.org/10.1016/j.im.2009.03.009>

United Nations General Assembly. (2002). Creation of a global culture of cybersecurity (A/RES/57/239). New York, NY: United Nations. <https://digitallibrary.un.org/record/482184>

Vilander, J. (2021). Bridging the knowing–doing gap: The role of attitude in information security awareness (Master’s thesis). University of Jyväskylä.

How to cite: Rasmiyya Mahmudova (2026). Development of a conceptual model for assessing personal information security culture. *Problems of Information Society*, 1, 70–80. <https://doi.org/10.25045/jpis.v17.i1.08>