COMPREHENSIVE REVIEW OF DEMOGRAPHIC, PHYCHOLOGICAL AND TECHNICAL FACTORS SHAPING INFORMATION SECURITY BEHAVIOUR IN CYBERSPACE

SHUTING, H.[1] – RAHMAN, A. L. A. R.[2*] – HUSSAIN, H.[1]

[1] *College of Computing, Informatics and Mathematics, Universiti Teknologi MARA (UITM), Selangor, Malaysia.*

[2] *College of Computing, Informatics and Mathematics, Universiti Teknologi MARA (UITM) Kedah Branch, Kedah, Malaysia.*

**Corresponding author*
e-mail: ablative[at]uitm.edu.my

(Received 08th August 2025; revised 02nd November 2025; accepted 10th November 2025)

Abstract. In this age of cyberspace, the heightened level of cyber threats sophistication and complexity has made information security an issue of paramount concern. Despite the significant advancement in security technology, human factors are the weakest link in cybersecurity. Human security behavior is influenced by various distinct determinants, but existing research is still dispersed, tending to examine demographic, psychological, and technical factors individually rather than in an integrated framework. This paper reviews the interaction of these factors with individual information security behavior. Most importantly, it reviews how demographic (age, gender, education) influences security awareness and compliance, psychological factors (personality, mental health, cognitive skills) affect security decision-making, and technical expertise promotes or inhibits secure practice. The review employs a Scopus artificial intelligence-based literature mining technique for identifying past research and provides data-driven summary of such relationships. Exploration result state that demographic factors have impacts on security behavior. The youth generation, while being technically capable, is more apt to risk behaviors, whereas the elderly act with more caution with lower technical capabilities. Gender differences are also present with women demonstrating less confidence in security technical tasks. Higher education is linked with improved security practices. Conscientiousness and emotional stability are positively related to security policy adherence, while impulsiveness and neuroticism lead to security violations. Additionally, while technical proficiency enhances security behavior, overconfidence in proficiency can lead to complacency.

Keywords: *information security behavior, cybersecurity awareness, demographic and psychological factors, technical proficiency in security, AI-driven literature analysis*

Introduction

In the era of the internet, information security has become the topmost concern with cyber threats changing in terms of their complexity and sophistication. With growing use of digital media for organizational, financial, and individual transactions, it is important to foster secure behavior among users. Information security behavior comprises behaviors by the users to protect their online assets, such as the use of strong passwords, protection against phishing, and adherence to cybersecurity policies (Haeussinger and Kranz, 2013). Irrespective of technological advancements, human beings continue to be the weakest link in cybersecurity, and hence it is necessary to know more about determinants of security behaviors. Several studies have confirmed that security behavior is determined by a variety of determinants, including demographic factors, psychological tendencies, and technical proficiency (McCormac et al., 2017; Pattinson et al., 2015). However, the literature on these determinants is

fragmented, with each factor being addressed in isolation from the others rather than as part of an integrated system. Knowing how demographic variables (education, gender, age), psychological characteristics (personality, cognitive capacity, mental state), and technical expertise impact security behavior can shed light on the problem holistically.

The increased levels of cyberattacks indicate a new problem: individuals are likely to neglect safe practice despite comprehending cybersecurity vulnerabilities (He and Zhang, 2019). The predicament suggests that disseminating security policies and awareness programs may not be the solution. Rather, it would be required to look deeper into the impact of behavioral drivers that inform security decision-making. Security behaviors have been analyzed technically and organizationally in prior literature, but there is a lack of understanding of individual-level factors, and especially how they combine. Earlier research has been utilized to examine the impact of demographics on security behavior. Research has shown that the elderly are more paranoid but less technologically adept, while the young possess more digital expertise but may be more likely to indulge in security threats. Gender differences still exist, with women generally having lower faith in technical security actions (McGill and Thompson, 2021). Also, there has been a correlation between education level and better security practices because more education is linked with greater awareness and risk-avoidant behavior (Candiwan et al., 2023).

In psychology, personality traits such as conscientiousness and agreeableness have been linked to greater security policy adherence. Conversely, neurotic and impulsive individuals are more prone to security offenses (Al-Hamad et al., 2025). Psychological health factors, including anxiety and stress, have also been linked to reduced security compliance. Also, cognitive models like Fogg Behavior Model show that motivation and competence are determinants in security compliance (Dontamsetti and Narayanan, 2009). Technically, the more technical expertise one has, the safer the habits are, but overconfidence also leads to unsafe behavior (Pattinson et al., 2015). ISA training has been found to enhance compliance, but it is successful only if it depends on individual cognitive attributes (Haeussinger and Kranz, 2013). While existing research is useful, there are still some areas to be covered. Firstly, less research integrates demographic, psychological, and technical variables in an analysis framework for security behavior. Secondly, a lot of the research has relied on self-report measures, which may not be a good measure of security practice. Thirdly, cultural and social determinants of security behavior remain little studied (Berthevas, 2021). Closing these gaps can contribute to a greater understanding of individual information security behavior.

This review aims to: (1) Explore the role of demographic factors (age, sex, education) on information security behavior; (2) Explore the role of psychological traits, including personality and mental health, on information security behavior; (3) Explore the role of technical knowledge and competence on information security behavior; (4) Explore the connection of the information security behavior theme with their sub theme such as technical factors, psychological factors, and demographics factors (*Figure 1*).

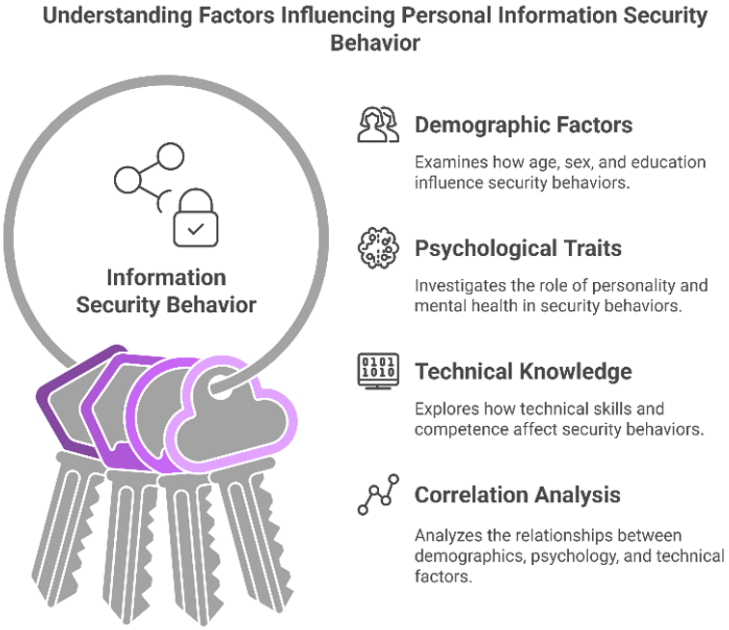

Figure 1. *Objectives of review.*

Materials and Methods

This review employs a Scopus AI-driven in-depth approach to explore the demographic, psychological, and technical factors that influence an individual's information security behavior. The approach is centered on data extraction through Scopus AI-driven literature mining.

Scopus AI-driven literature mining

The explore begins with a critical review of the literature using Scopus AI to extract and analyze existing research on demographic, psychological, and technical variables influencing information security behavior at an individual level. A specific search query was formulated with Boolean operators for searching relevant literature: (1) Demographic variables: ("demographics" OR "age" OR "gender" OR "education") AND ("individual information security behavior" OR "cybersecurity"); (2) Psychological traits: ("Psychology" OR "personality" OR "mental health") AND ("individual information security behavior" OR "cybersecurity awareness"); (3) Technical capabilities: ("technical skills" OR "security awareness" OR "digital literacy") AND ("cyber risk management" OR "data protection") (*Figure 2*).

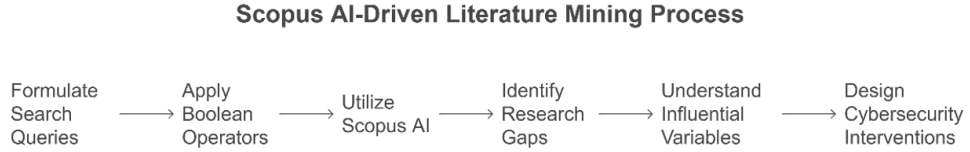

Figure 2. *Scopus AI driven literature mining process.*

Scopus AI was utilized to construct a robotically prepared analysis of influential study subjects, networks of citation, and ongoing trends. The strategy was in a position

to recognize gaps within literature as well as what psychological, demographic, and technical variables have an impact on information security behavior of humans. Through the application of Scopus AI-assisted literature search, the current study can provide an enriched multi-faceted comprehension of determinants of personal information security behavior. Results will inform site-specific intervention design to promote cybersecurity awareness and compliance across user groups.

Results and Discussion

Explore the role of demographic factors (gender, education, age) on an individual's information security behavior

Demographic factors like age, gender, and education affect an individual's information security behavior to a great extent. The gender factor has been found to be linked with differences in security and privacy behavior and that, on average, females have lower technical security behavior compared to males (McGill and Thompson, 2021). Variance is explained by variations in self-efficacy, perceived threat, or cyber security training exposure. Additionally, cultural explanations underpin the security behavior variance origins, as seen in cross-cultural research among Arab and European cultures wherein Arabs reported marginally higher security intentions compared to Europeans (Al-Hamad et al., 2024). Such conclusions reveal that demographic context, at both societal and cultural levels, significantly affects the manner in which individuals address information security. Age has also been ascertained to be a determining individual information security behaviour, such that younger individuals would be expected to be more flexible at security processes given their experience and proficiency with virtual technology. Their aging counterparts develop stalwart security behaviour due to observed heightened risk sensitivity (Gratian et al., 2018).

The variation in security behavior by age indicates the need for age-specific customization of security awareness programs such that interventions target the relative challenge and experience of every age group. In addition to this, research indicates demographic variables account for 5%–23% of explained variance in cybersecurity behavior intentions, which implies the need to address security decision-making individual differences (McCormac et al., 2017). Educational attainment significantly influences cybersecurity behavior and awareness. Individuals with higher education, particularly those with technical education, exhibit improved security behavior due to heightened awareness of cybersecurity concepts and threat mitigation strategies (Parsons et al., 2014). Conversely, individuals with minimal or no formal education or those without technical backgrounds can find even basic security practices too hard to adhere to, thus making them easier targets for cyber threats. Information security awareness (ISA) is also linked to institutional support and training opportunities, highlighting the role of training programs in cultivating more secure behaviors (Haeussinger and Kranz, 2013). All these results demand particular security education programs considering various educational levels. The combination of demographic variables with psychological traits also has an impact on individual information security behavior.

Those with advanced education, especially technical education, show better security behavior because of increased awareness of cybersecurity principles and mitigation of threats (Parsons et al., 2014). On the other hand, those with little or no formal education or no technical background can find even elementary security practices too difficult to

follow and hence are easy targets for cyber attacks. Information security awareness (ISA) is further associated with training opportunities and institutional support, where training programs are identified to instill more secure behavior (Haeussinger and Kranz, 2013). All of these findings call for specific security education programs taking into account different educational levels. The interaction between demographic variables and psychological characteristics also affects information security behavior of an individual. Personality traits of conscientiousness, agreeableness, and emotional stability have also been found to affect security awareness and compliance (McCormac et al., 2017). Some gender difference in risk-taking predisposition may also explain some of the variation in security behavior since female participants had lower scores on risk acceptance in the internet context, which led to restraint in online conduct (McGill and Thompson, 2021). The interplay between psychological and demographic factors emphasizes the complexity of security behavior, and interventions need to be developed to affect intrinsic as well as extrinsic determinants.

Generally, demographic factors have a direct impact on the information security behavior of an individual, and these include age, gender, and education as key factors that influence security awareness and compliance. Young individuals are flexible but conservative, while older individuals are security-conscious but deficient in knowledge about new threats. Gendered differences portray security engagement at different levels, and therefore gender-sensitive approaches toward educating individuals on cybersecurity are in need. Moreover, education level influences technical ability and security behavior, reinforcing the need for affordable and accessible security training. From these demographic considerations, organizations and policymakers can develop targeted cybersecurity practices that meet the different needs of users, resulting in overall better security behavior.

Explore the role of psychological traits, including personality and mental health, on individual information security behavior

The role of psychological traits, including personality and mental well-being, on human information security behavior is portrayed in the majority of studies. Personality traits like conscientiousness, agreeableness, emotional stability, and risk-taking tendency are portrayed to play a significant role in information security awareness and compliance (McCormac et al., 2017). High scorers on conscientiousness will be likely to follow security protocols scrupulously, while high-risk takers will be likely to practice behavior that puts them at risk of being exposed to cyber-attacks (Gratian et al., 2018). The results are suggestive of designing personalized security awareness training on varied personalities with the possibility of greater adherence to security best practices. Mental states have a considerable effect on information security behavior. Anxiety and stress were discovered to influence security case decision-making in a way that security practice is avoided or handled with overcaution (Dontamsetti and Narayanan, 2008). Conversely, individuals under cognitive overload are more susceptible to phishing and social engineering attacks due to worse judgment and attention to detail (Kießling et al., 2021). This is to note that businesses must integrate mental health practices in cybersecurity training so as to mitigate the threats of psychological stressor elements.

Apart from that, motivation and decision style also influence security behavior. Rational decision-makers will assess risks accordingly and adhere to security policy, whereas impulsive will disregard security warnings for the sake of convenience (Gratian

et al., 2018). Fogg Behavior Model (FBM) puts the emphasis on motivation to improve security compliance since, by boosting user motivation via gamification and reward mechanisms, security behavior can be maximized (Kießling et al., 2021). Organizations should then create interventions that boost user motivation towards active safe practice. Demographics and culture further cross with personality types to influence security behavior. To further demonstrate, evidence indicates Arab participants with somewhat more elevated scores in security behavior intent than Europeans according to supposedly cultural attitudes towards aversion to risk and submission according to Al-Hamad et al. (2024). There have also been some gender variations noted, with women respondents indicating lower technical-demand security behavior levels (McGill and Thompson, 2021). They illustrate the need for tailored cybersecurity training programs that consider the unique concerns of different demographic segments.

Lastly, personality, mental well-being, and decision style are also determinants of information security behavior. These results of psychological and demographic construct interactions suggest that maybe there is not one single one-size-fits-all security solution. Adaptive security awareness training with varying styles by varying psychological and demographic types must be examined in future research in trying to increase overall cybersecurity resilience. By incorporating psychological understanding into training and security policy, organizations can then establish a more successful security culture that is best able to thwart human vulnerabilities.

Explore the role of technical proficiency and awareness on individual information security behavior

The technical skill and sensitivity impact on security behavior in relation to personal information is a multifaceted phenomenon affected by various demographic, psychological, as well as technical variables. Technical skills have most frequently been associated with the ability of a user to identify and respond to cybersecurity threats effectively. Studies have proven security behavior to differ according to gender since female participants invested less in security activities that called for technical skills compared to their male peers (McGill and Thompson, 2021). Security behavior intention also proves to differ according to cross-cultural differences, as proven in a comparison of Arab and European cultures where Arab participants showed slightly higher security behavior intention (Al-Hamad et al., 2024). These results show that capability and technical proficiency are not merely shaped by education and training but also by root demographic factors.

Psychological traits, including cognitive style and personality, influence people's behaviors towards information security. Researchers have discovered that people who are highly conscientious, emotionally stable, and cautious are likely to learn secure behavior (McCormac et al., 2017). Learning security awareness is also explained by conscious competence model, categorizing people into four quadrants based on consciousness and competence (Dontamsetti and Narayanan, 2009). This model implies that the awareness programs need to be fragmented in order to meet different levels of user experience so that effective security compliance may be achieved. Even decision-making orientations, i.e., rational or intuitive orientations, have been discovered to have high correlation with security behavior intentions, which is an indication of the impact of psychological tendencies on cybersecurity compliance (Gratian et al., 2018).

Organizational security culture and organizational policy are also primary determinants of security behavior at the individual level from a technical point of view.

ISA is most affected by institutional and environmental determinants, to which security policy contributes significantly along with individual awareness of information systems (Haeussinger and Kranz, 2013). Robust security culture in organizations ensures better adherence to security procedures since employees will more willingly engage in secure practice when they view cybersecurity as a collective responsibility (Parsons et al., 2014). Experiential practice and best practice of security technology compelled through training programmes result in better technical competence and security-conscious behaviour.

Besides, the interaction of psychological, demographic, and technical factors emphasizes the multidimensionality of cybersecurity behavior. The Fogg Behavior Model (FBM) suggests that capability, motivation, and triggers affect security behavior and demands security interventions that can affect both technical and psychological capability (Kießling et al., 2021). Prompt workgroup influence on security decision-making is also significant, as peer and manager relationships influence an individual's likelihood of following security procedures. Thus, teamwork and user-centered security programs can enhance awareness and technical skills.

Lastly, the findings favor technical skills and knowledge as key predictors of user information security behavior, which are moderated by demographic characteristics, psychological makeup, and technical pressure. One can significantly improve cybersecurity behavior by addressing such determinants comprehensively by focused training programs, security awareness programs, and robust security cultures. Future studies need to study the longitudinal effect of security training interventions and emerging drivers of technology advancement on user security behavior.

Explore the connection of the information security behavior theme with their sub theme such as technical factors, psychological factors and demographics factors

The graph provides a theoretical model of Information Security Behavior by categorizing its determinants into three broad categories: Technical Factors, Psychological Factors, and Demographic Factors. There are some elements in each of these categories that contribute towards determining the information security approach of a person or an organization. (1) Technical Factors encompass critical items such as Cyber-Security, Privacy by Design, Security Awareness, and Information Security Education. They shed light on the significance of technology, organized security practices, and learning activities to improve cybersecurity procedures; (2) Psychological Factors focus on psychological facets of individuals' behavior such as Risk-taking Behaviors and Personality Traits. It emphasizes the psychological factors that contribute to affecting decision-making and compliance with security practices; (3) Demographic Factors entail factoring in items like Equity and Gender Differences and understanding how individuals' demographics might influence security-related behavior and knowledge. This model illustrates a broader view of information security behavior in that it balances technical, psychological, and demographic elements to bring about a greater understanding of the ways in which security practice and awareness can be shaped across populations (*Figure 3*).

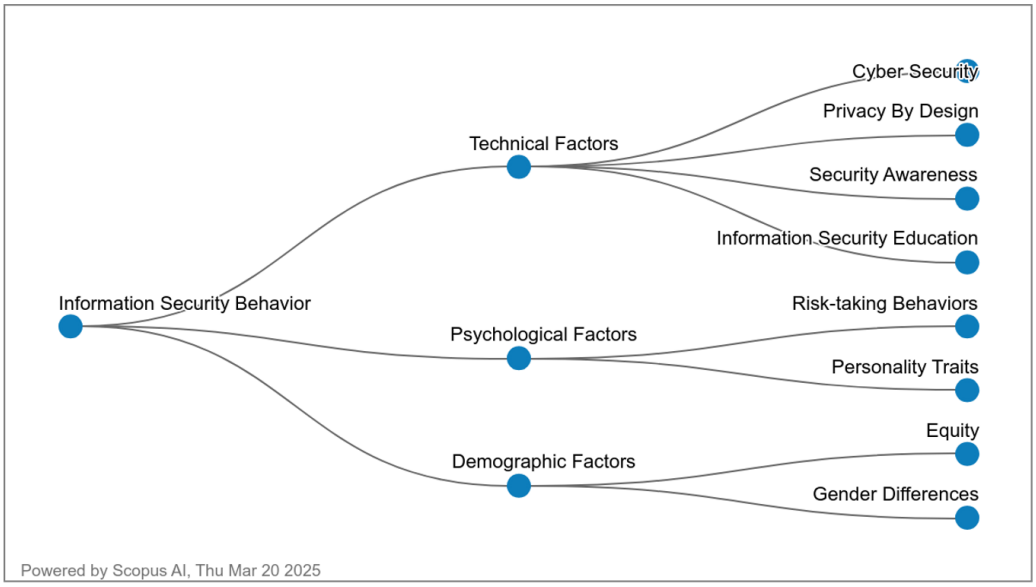

Figure 3. *Concept maps of information security behaviour provide by scopus AI.*

Linkages between information security behavior, technical factors, and cybersecurity

Information security behavior is a great influencer of cybersecurity effectiveness since it determines the way individuals and organizations protect digital material. Security behavior is influenced by technological, psychological, as well as demographic aspects. The intersection of these aspects determines security compliance, awareness, as well as adherence to cybersecurity policies. Lack of compliance from staff with regard to security policy is one of the primary influencers of cyber infringement, and the importance of inculcating secure behavior explains why (Abdalla et al., 2021). Since companies rely increasingly on technology to secure their systems, identifying how technical concerns affect cybersecurity practices is essential. Technical issues contribute to a significant impact in shaping information security behavior through the provision of adequate tools, protocols, and infrastructures to safeguard digital areas. Security awareness, information security training, and privacy-by-design ideas enhance the capabilities of individuals in embracing safe habits. At the university level, user cybersecurity behavior is defined based on skills, knowledge, compliance behavior, and access to safe technologies (Latih and Zin, 2024). Without proper technical controls and training, users can form unsafe behaviors that expose systems to cyber attacks. Therefore, investment in technical training and security awareness can close the policy-practice gap so that users develop secure habits.

Cybersecurity, as a result of strong information security behavior, is dependent on human and technical factors. The implementation of cybersecurity practices is driven by perceived ease of use, perceived benefits, and security perception (Abdalla et al., 2021). In the workplace, information security climate and employee training are significant in enhancing cybersecurity behavior, where individuals understand the seriousness of threats and the efficacy of defenses (Chongrui et al., 2021). Without structured cybersecurity guidelines, even well-intentioned users can inadvertently compromise security, which indicates the need for technical support and continuous instruction. To put it in general terms, information security behavior is a multifaceted phenomenon induced by technical, psychological, and demographic drivers. Technical drivers such as

security awareness, education, and privacy-specific products enable users to acquire the skills and the knowledge necessary for cybersecurity. The technical drivers, however, must be complemented by a better security culture, which considers psychological traits and demographic differences. By reconciling both these perspectives, individuals and organizations can better enhance cybersecurity strategies, overcome security risks, and establish the digital community as a more secure place.

Linkages between information security behavior, technical factors, and privacy by design

Behavior information security is the foundation of protecting digital assets since it prescribes how individuals and organizations interact with security controls. Technical requirements, such as security engineering design, training, and awareness, determine the level at which users interact with privacy-protection practices, for instance, Privacy by Design (PbD). PbD is a new practice of privacy protection that integrates security in systems from the onset and not as an afterthought (Cavoukian, 2012). But the effectiveness of PbD is based on the information security behavior of people, particularly security mechanism-aware system designers and engineers. Their adoption of PbD principles hinges on technical proficiency, expertise, and organizational incentives (Bu et al., 2020). Technical issues are at the core of PbD adoption and implementation. Education, security training, and compliance policy that enable engineers and system designers to clearly understand why it is important to build privacy controls into technology (Bu et al., 2021) are lacking. However, from evidence, there are no guidelines for applying PbD, thus making it difficult for engineers to apply it (Bu et al., 2020). Gaining any specified framework, the use of PbD tends to be one-way, based primarily on individual practice and firm policies. Therefore, making PbD technical guidelines mandatory and enhancing engineering education in protecting privacy can prompt security behavior and build safer cyber spaces.

Privacy by Design is also vulnerable to psychological factors, primarily attitudes and beliefs of information system (IS) engineers. Evidence has shown that their effort expectancies and social influence play an important role in shaping their intention to apply PbD principles in system design (Bu et al., 2021). Engineers who perceive PbD as difficult or complicated to implement are less compliant, whereas engineers who receive organizational support and encouragement have greater compliance. This is a reflection of the need for a good security culture where PbD is viewed as a desirable and feasible practice rather than as a regulatory stipulation. Furthermore, organizations may use motivation techniques such as training and reward to motivate IS engineers to follow PbD principles. Demographic circumstances also influence PbD uptake by pre-conditioning security habits among different user groups, including professional experience, education level, and cultural identity, which are some of the drivers of the way individuals view and apply privacy controls (Bu et al., 2020). Engineers with high information security exposure, for instance, will be susceptible to applications of PbD principles more than their non-exposed counterparts. Both gender inequality and work equality contribute to security behavior with technical education disparities and leadership access influencing privacy protection decision-making. These demographic differences are potentially correctable by special training and comprehensive policy enabling more pervasive adoption of PbD.

In short, information security behavior, technicalities, and Privacy by Design are all dependent on each other in determining the overall efficacy of cybersecurity controls.

Organizational technical training, awareness, and policy all help in promoting safe behavior for PbD adoption. Psychological factors such as effort expectancy and ease of use also play their role in PbD adoption by IS engineers. Furthermore, the demographic traits like inclusivity of work environment and career history influence security behavior differences. Controlling these factors in an integrated manner, organizations can facilitate protection of privacy and enhance resilience in cybersecurity.

Linkages between information security behavior, technical factors, and security awareness

Information security behavior involves how people and organizations respond to security controls in order to protect digital assets. It is influenced by several factors, including technical competence, psychological beliefs, and demographics. Security awareness has a critical role to play in shaping information security behavior because individuals with greater levels of awareness use safer behavior (Hassanzadeh et al., 2014). However, traditional security awareness measures are improving at a slower rate than computerized security controls, making people the cybersecurity defense's weakest point (Stewart and Lacey, 2012). To what extent technical elements such as security policies, training programs, and governance functions help in helping people make intelligent security choices measures the efficiency of security awareness schemes. Technological features stand at the forefront of raising information security awareness and affecting safe behavior. Companies that have formal security divisions, employ coordinating committees, and spread security information within internal channels significantly raise employees' awareness of security (Flores and Ekstedt, 2015). Moreover, integration of technical and non-technical measures, e.g., security training courses, simulated phishing, and real-time security alerts, can assist in safe habits in users (Tanrıverdi and Metin, 2017). However, technical solutions are insufficient; they need to be complemented by behavioral reinforcement measures to encourage good security behavior. Without adequate technical guidance, users will either not perceive security threats or make security procedures so complex that it is too burdensome to follow.

Demographic factors, such as gender, occupation, and profession, play a significant role in security behavior and awareness. IT professionals have been found to have higher security awareness due to their exposure to security controls, while non-technical staff may not be able to understand security requirements (Hassanzadeh et al., 2014). Second, variations in security awareness levels by gender have also been observed with men being more confident about their security know-how compared to women despite having equal exposure to security measures (Kruger et al., 2011). Redress of these imbalances through special awareness campaigns will increase bridging gaps in security knowledge while all user communities acquire skills that make them secure in practice. Psychological factors also have an impact on security behavior, as the attitude and perception of users will decide how they respond to security controls. If the employees perceive security procedures as being too restrictive or inconvenient, they will be inclined to bypass them, even though they know about the risks (Stewart and Lacey, 2012). Conversely, organizations which ensure positive security culture, when employees believe they are motivated to report security threats and participate in security training, are more engaged in secure practices (Flores and Ekstedt, 2015). Security awareness campaigns emphasizing organizational and individual benefits of

cybersecurity, rather than just reminding the users of compliance, are proven to maximize the motivation of the users to comply with security protocols.

In summary, information security behavior is moderated by technical, demographics, and psychological factors, all of which have security awareness acting as a critical mediator. Technical measures such as governance frameworks and security training make awareness stronger but demographic and psychological differences affect the perception and realization of security practice by individuals. Organizations need to implement holistic practices that integrate technical measures with behavior and culture-based reinforcements to further security behaviors. By closing gaps in know-how and providing easy-to-use security tips, institutions and firms can contribute to the digital world being safer.

Linkages between information security behavior, technical factors, and information security education

Information security behavior is a concept that can be applied to refer to the behavior and decision-making of an individual towards cybersecurity routines based on various factors, including technical factors and also education. Information security education will be an influential factor in developing security behavior by offering training and experience in the form of detecting and discouraging cyber attacks to individuals. Studies indicate that learning security information through the internet is very effective in improving security behavior compared to the traditional offline approach because it is an interactive and adaptive learning system (Park and Chai, 2020). However, despite increased emphasis on security education, most computer programs are not comprehensive with full security training, which impacts the cybersecurity preparedness of graduates (Mabece et al., 2017). Closing the gaps has to be achieved through systems-based approaches that connect education and technical solutions to facilitate good security behavior. Technical conditions play an important role in information security behavior by offering the infrastructure and technology needed to enable individuals to practice secure behavior. Ease of use, performance, reliability, and the functioning of a security system affect individuals' knowledge of security measures and their adoption (Abdalla et al., 2021). Security measures will be bypassed by users whenever systems become difficult to use or hinder secure processes. Additionally, security training is effective because there are technology resources such as real-time threat simulation, interactive cybersecurity training exercises, and hands-on training modules. Hence, organizations and institutions have to balance technical security controls with education programs in order to instill an active security culture in users.

Demographic factors such as gender and education are components that play a role in affecting information security behavior and its interaction with technicalities and education. Women, particularly those familiar with online security education, were said to have cautious security behavior compared to men (Park and Chai, 2020). Also, it is argued that computer science students would be more security conscious, but the level of marginalization of computer science in security education has raised doubts about their readiness (Mabece et al., 2017). These variations are the basis for advocating for some security learning approaches based on different levels of prior experience, knowledge, and demographic characteristics to attain full security awareness. Psychological constructs like self-efficacy, perceived usefulness, and subjective norms are the most important variables of the most important considerations in influencing security behavior and how it correlates with education and technical considerations.

Individuals who believe that they can apply security measures will be likely to exhibit secure behavior (Abdalla et al., 2021). Furthermore, perceived usefulness of security education and peer or institution policy also significantly influence intent to abide by security guidelines. For enhanced security education effectiveness, psychological potential must be supplemented with technical capability so that people will see security measures as necessary and attainable in their everyday lives.

Finally, security behavior depends on how education collides with technicalities, demographics, and psychology. The more awareness and preparedness the security education increases, the operates in accordance with the extent of supportive technical infrastructure and the psychological acceptability of the user towards security controls. Organisations and institutions must develop balanced strategies with technical security attributes and tailor-made education schemes to empower cybersecurity behaviors in the long term. Eliminating demographic differences and psychological discrepancies will also boost security awareness and set up active support of security systems.

Linkages between information security behavior, psychological factors, and risk-taking behaviors

Information security behavior is influenced by a complex interplay of psychological factors and individual risk-taking tendencies. Psychological models such as the Theory of Planned Behavior (TPB) and Protection Motivation Theory (PMT) assume that the perceived vulnerability to risk and response cost of an individual have a significant influence on their security behavior (Alam et al., 2025). Individuals who perceive themselves to be at risk of cyber attack and view security measures as useful are going to engage in protective behaviors. Individuals who do not perceive themselves to be competent at risk avoidance or view security procedures as invasive are going to engage in risk-taking behaviors, putting themselves at possible security compromise. These psychosocial concepts guide the need for the development of security awareness programs that address individual risk appraisal and the utility of following security procedures.

Psychological variables such as security risk attitudes, personality, and cognitive biases also play a part in influencing the risk behavior of an individual in cyber space. Conscientious individuals will exhibit secure security behaviors, while impulsive individuals will exhibit risky behaviors (Uffen et al., 2012). Risk perception is also a function of information security threat perception. There is evidence to indicate that the framing of risks has the capability to affect security decisions and successful communication approaches may actually turn behavior risky around (Pattinson and Anderson, 2007). Evidence consequently points towards psychological interventions such as behaviorally anchored security training and nudges for reducing risky security behavior. Demographics such as gender, age, and IT skills influence security behavior and risk-taking tendency as well. Young people and those with greater IT skills have been observed to take more security risks since they overestimate themselves in terms of being able to handle threats (Alohali et al., 2018). In addition, studies have found that women tend to be security conscious in their actions more than men, an occurrence which can be justified on the basis of differences in security awareness and risk perception (Pattinson and Anderson, 2007).

Such population differences underscore the need for targeted security education programs that factor in differences in psychological predispositions and user attributes. Cognitive processes such as habituation, prior experience, and feedback mechanisms

also play an important role in influencing security behavior in the long term. Not only short-term risk perception, but secure behavior is also influenced by process memory models, which suggest that individuals learn from their prior security experiences and develop automatic responses to behaviors (Vedadi and Warkentin, 2018). If safe behavior is rewarded with positive reinforcement, then the users will be more likely to continue with safe behavior. If there are no direct consequences for unsafe behavior, complacency is likely to be fostered. This highlights the importance of continuous security training and real-time feedback mechanisms to encourage safe security behavior.

In short, security information behavior is all about risk-taking behavior and psychological issues. Security threat perceptions, cognitive biases, and personality are what guide them to apply defensive or aggressive methods. Computer skills and demographics also play a part in determining security decisions, whereas cognitive processes govern long-term security behaviors. Trainers and organizations need to integrate psychological knowledge into security training to build more secure behavior, use outstanding risk communication practices, and keep on providing feedback in order to create secure behavior. A multi-component model that includes these elements can reduce risk-taking behaviors and overall cybersecurity resilience.

Linkages between information security behavior, psychological factors, and personality traits

The overlap of personality, psychological testing, and information security behavior is an important research area that predicts how people act securely or insecurely in cybersecurity. Personality characteristics on the Five-Factor Model (FFM) of conscientiousness, neuroticism, openness, agreeableness, and extraversion directly affect users' compliance with security controls and regulations (Uffen et al., 2012). For instance, conscientious non-attentive will adhere to security procedures to the letter for others, and high neurotic will be security routine enforcers through fearfulness, e.g., frequent password changing or never using non-technology devices. Or, openness to experience can also result in risk behavior in cyber security where they experiment with new technology and, in the process, exposing themselves to security threats (Uffen et al., 2012).

Psychological factors such as response efficacy, self-efficacy, and perceived risk also play a role in influencing the information security behavior of an individual. Research has shown that individuals who feel highly vulnerable to cyber attacks are most likely to participate in security protective behaviors (Alam et al., 2025). Similarly, self-efficacy, a capability belief to implement security measures, plays a role in the decision of whether to use security tools like two-factor authentication or encryption software. Response efficacy, that is, having the belief that a security measure works, also influences decision; if an individual doesn't believe something will protect them, they will ignore security recommendations (Al-Hamad et al., 2024). Personality traits intersect with these psychological factors to define risk-taking behavior in information security. For example, highly agreeable people have a tendency to prioritize social relationships over security matters and are thus susceptible to social engineering attacks. Similarly, highly extraverted people have a tendency to expose more about themselves on the internet, making them more susceptible. Compared to this, high conscientiousness individuals have a greater probability of being vigilant in their behaviors, taking good care to execute best practices regarding cybersecurity. With

these results come the necessity to provide customized security awareness training and consider various profiles of personality.

Demographic factors such as gender, age, culture, and education also contribute to security behavior through moderation of psychological factors and personality traits. It is theorized that youth, being more technologically aware, tend to be more risk-taking when it comes to security than older adults with conservative mindsets (Al-Hamad et al., 2024). There are also gender differences, where women are more likely to show increased security compliance through increased risk aversion, whereas men are more likely to undertake experimental or risk-taking behavior online. There are also cultural differences, where individuals from collectivist cultures are more likely to tap into communal security procedures, whereas individualist cultures might emphasize personal responsibility (Al-Hamad et al., 2024). Cross-influence of technical variables, psychological variables, and personality requires that information security behavior be dealt with an interdisciplinary approach. Context-specific security interventions need to be designed by organizations that leverage research in psychology, e.g., by tailoring security messages based on the user's personality or by using behavior nudges to impose secure behavior (Uffen et al., 2012). By integrating these characteristics, cybersecurity training programs can be optimized for utmost prevention of security attacks and adaptability to changing cognitive and behavioral inclinations of users.

Linkages between information security behavior, demographic factors, and equity

Information security behavior, demographics, and equity are central to explaining how population segments engage with cybersecurity practices. Demographic attributes like age, gender, educational level, and cultural orientation significantly influence the likelihood of an individual adopting secure behavior. The same demographic factors, however, show gaps in access to knowledge, resources, and digital literacy underlying inequities in cybersecurity preparedness. For instance, gender-based differences in privacy and security behavior suggest that females ought to experience lower security control engagement than males due to discrimination during technology education and availabilities of e-resources in the past (McGill and Thompson, 2021). Such disparity explains the need for inclusive cybersecurity education and interventions that make it possible for all demographic status individuals to be able to protect themselves on the internet. Educational level and age similarly permit variation in information security behavior. While older people can present more secure security behaviors due to risk avoidance, on the contrary, they are unable to use new security technologies due to digital illiteracy. Younger users, even though they are more computer literate, also seek more risky internet conduct, such as inadequate password management and susceptibility to phishing. Further, it is not always that higher education will result in better conduct because, as some research has found, even highly educated individuals can become careless about best practice if they are not especially taught about cybersecurity. This helps to place emphasis on requiring specially targeted security awareness programs tailored to the particular needs of individual demographic groups.

Information security behavior is also influenced by cultural diversity because varying norms and values within societies influence perception of risk as well as security control compliance. Empirical evidence indicates that individuals from collectivist cultures, such as Arab nations, will have a higher level of cybersecurity control compliance intentions due to the focus on collective responsibility as opposed to individuals from individualist cultures, such as in European nations, where freedom of the individual

outweighs collective security controls (Al-Hamad et al., 2024). They also emphasize the need for more culturally relevant cybersecurity awareness messages that resonate more with the incentives and values of diverse groups. Information security equity transcends demographics to include socioeconomic status that affects access to secure digital resources, cybersecurity literacy, and technical support. Lower-income users are disadvantaged by outdated devices, limited cybersecurity education, and use of public networks that are potentially insecure, and thus are more vulnerable to cyber attacks (Haeussinger and Kranz, 2013). On the other hand, those with more economic resources can afford to invest in high-quality security software, VPNs, and expert advice, with which they can have a distinct advantage in protecting their digital assets. These disparities can be met through policy intervention providing equal access to cybersecurity resources through free or subsidized security software and large-scale cybersecurity literacy programs for marginalized communities.

To fill the gap in security behavior among various populations, the solution involves a multi-faceted approach combining education initiatives, policy recommendations, and technology solutions. Comprehensive cybersecurity training programs that account for differences in age, educational level, gender, and cultural frames need to be embraced by organizations and governments. Besides, equity-based policies such as the same access to security resources and increased cybersecurity training in public agencies will be able to stem gaps and enable all irrespective of ethnicity to engage in safe use of the internet (McGill and Thompson, 2021). Reducing demographic gaps in information security can help society reach the wider even digital society where security information and services are accessible to everyone.

Linkages between information security behavior, demographic factors, and gender differences

The relationships between information security behavior, demographic factors, and gender disparities highlight how various social and psychological factors influence cybersecurity practices. Research indicates that women tend to exhibit lower security behavior than men, typically because of differences in risk perception, confidence scores, and exposure to cybersecurity instruction (McGill and Thompson, 2021). These differences are explained by historical gender technology adoption roles, with men being more engaged in STEM areas, such as cybersecurity. The difference in adoption might therefore result in security practice diversity and thus the need to create customized cybersecurity awareness programs that will address the needs of certain gender groups (McGill and Thompson, 2021).

Self-efficacy and self-confidence in handling security threats is one of the factors why information security behavior is different between women and men. Women were less confident to handle cybersecurity threats and therefore engaged less in security behaviors, including two-factor authentication, password management, and anti-virus software (Farooq et al., 2015). On the other hand, men would be more likely to experiment with security features and actively safeguard their machines since they are more open to technical environments. By narrowing down this confidence gap through specialized cybersecurity training that supports experiential learning exercises, the gap may be narrowed and more even security practices fostered. Social and cultural influencers are also held accountable for playing a vital role in determining gender disparity in cybersecurity behavior. For instance, women will be more likely to adopt security behaviors if they are framed in the interest of the group, instead of self-interest

(Al-Hamad et al., 2024). Women can also be denied cybersecurity awareness and access to resources in predominantly male technology societies, expanding security behavior gaps. Cultural factors in this sense recognize the importance of creating inclusive security training programs in gender attitudes and cultural diversity backgrounds to ensure equality of access to information on cybersecurity.

The second primary explanation for gender disparity in security behavior is the small number of women employed in the cybersecurity sector. Because there are few female mentors and role models to influence them in the cybersecurity sector, women steer away from working in the industry, and therefore, interaction with security best practices is minimal. Besides, the masculine culture in cybersecurity settings can create unconscious stereotypes that discourage women from participating in security discussion and decision-making. Encouraging diversity in the cybersecurity field by enrolling more women can reduce gender differences in information security behavior and create a more diversified cybersecurity culture. To reverse gender imbalance in information security activity, multi-faceted intervention using education, policy-making, and workforce diversity management is necessary. Cybersecurity educational modules need to be gendered, taking learning style differences as well as differences in confidence. Gender equality measures in cybersecurity jobs need to be implemented by the organization so women are given fair opportunities to get included in the security decision space. Through facilitating a more gender-balanced approach to cybersecurity learning and career path, society can assist in minimizing gender disparity in information security practice and overall digital security resilience.

Conclusion

This paper gives an overview of the impact of demographics, psychology, and technical factors on individual information security behavior. Based on a critical review of previous literature, some surprising findings are enumerated, and they shed light on the multidimensional facets of security behavior and how these are related to internals and externals. In term of demographics aspects, education level, gender, and age all significantly affect security behavior. Increasing levels of education and age increasingly exhibit greater security awareness and obedience. Gender indicates women as security-aware and men as more likely to exhibit technically savvy security behavior. For psychological factors, Personality, cognitive functioning, and mental health disorders are factors that affect security behavior. Agreeable and conscientious personality types have a higher chance of complying with security policies, while neuroticism and anxiety are some possible risk factors.

For technical factors: Security compliance is most indicated by information security awareness (ISA), technical proficiency, and security training background. Enhanced technical proficiency correlates with active security practice, and knowledge deficiency will expose the practitioner to cyber attack. This study offers empirical support for the applicability of behavioral theories such as Protection Motivation Theory (PMT), the Theory of Planned Behavior (TPB), and the Technology Acceptance Model (TAM) in predicting security behavior. The findings indicate the need to include psychological factors (e.g., cognitive bias and mental health factors) in existing security behavior models.The study confirms the COM-B model (Capabilities, Opportunities, and Motivations for Behavior change) of security compliance, demonstrating the extent to which personality and contextual variables determine security behavior. For practical

implications, Organizations must develop specially crafted cybersecurity awareness programs based on demographic variations, thus training being age, gender, and education-specific.There must be psychologically grounded security policies, such as behavioral nudges to encourage compliance and mitigate cognitive biases.Technical training needs to be adapted, closing knowledge gaps, particularly for low digital literacy users.Multinational security policy will need to address cultural differences, with alignment between policy and social values and norms of users.

Although grounded in valuable research, the research has limitations as follows: The review synthesizes primarily findings from published research, so the results reported will be subject to publication bias. Longitudinal security behavior alterations over time are not studied in this research, possibly influencing demographic, psychological, and technical variable changes. Individual security behavior's impact of new technologies (such as artificial intelligence-based cybersecurity controls) is more deserving of investigation. Future Research Directions: (1) Application of empirical research for empirical finding-based validation of demographic, psychological, and technical factor interactions; (2) Study of how cybersecurity education influences individual behavior over the long term through longitudinal analysis; (3) Examination of the influence of artificial intelligence and automation on personal security decision-making; (4) Study of the interaction effects between demographic, psychological, and technical factors for the development of an integrated security behavior model. Determinants of individuals' security behavior may be realized by organizations, scholars, and policymakers to develop more efficient cybersecurity approaches, with increased compliance and decreased cyber risk at the individual and society levels.

Acknowledgement

The author would like to thank Rahman and Hussain for their valuable guidance and helpful suggestions throughout this study.

Conflict of interest

The author declares no conflict of interest.

REFERENCES

[1] Abdalla, M., Jarrah, M., Abu-Khadrah, A., bin Arshad, Y. (2021): Factors influencing the adoption of cyber security standards among public listed companies in Malaysia. – International Journal of Advanced Computer Science and Applications 12(11): 804-810.

[2] Alam, S.S., Ahsan, N., Kokash, H.A., Alam, S., Ahmed, S. (2025): A students' behaviors in information security: Extension of Protection Motivation Theory (PMT). – Information Security Journal: A Global Perspective 34(3): 191-213.

[3] Al-Hamad, E.A., Alshakhsi, S., Babiker, A., Erbad, A., Ali, R. (2024): The Impact of Personality Traits and Need for Cognition on Cybersecurity Behavior: A Study Across Arab and European Samples. – In International Conference on Web Information Systems Engineering, Singapore: Springer Nature Singapore 13p.

[4] Alohali, M., Clarke, N., Li, F., Furnell, S. (2018): Identifying and predicting the factors affecting end-users' risk-taking behavior. – Information & Computer Security 26(3): 306-326.

[5] Berthevas, J.F. (2021): How protection motivation and social bond factors influence information security behavior. – Systèmes D'information & Management 26(2): 77-115.
[6] Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A. (2018): Correlating human traits and cyber security behavior intentions. – Computers & Security 73: 345-358.
[7] Bu, F., Wang, N., Jiang, B., Jiang, Q. (2021): Motivating information system engineers' acceptance of Privacy by Design in China: An extended UTAUT model. – International Journal of Information Management 60: 18p.
[8] Bu, F., Wang, N., Jiang, B., Liang, H. (2020): "Privacy by Design" implementation: Information system engineers' perspective. – International Journal of Information Management 53: 16p.
[9] Candiwan, S., Sudirman, B.P., Sari, P.K. (2023): Differences in information security behavior of smartphone users in Indonesia using Pearson's Chi-square and post hoc test. – International Journal on Advanced Science, Engineering and Information Technology 13(2): 703-717.
[10] Cavoukian, A. (2012): Privacy by design: leadership, methods, and results. – In European Data Protection: Coming of Age, Dordrecht: Springer Netherlands 27p.
[11] Chongrui, L., Yan, L., Cong, W., Hongjie, W. (2021): Exploring the impact of information security climate and information security training on cybersecurity behavior: Based on protection motivation theory. – In 2021 6th International Symposium on Computer and Information Processing Technology (ISCIPT), IEEE 4p.
[12] Dontamsetti, M., Narayanan, A. (2009): Impact of the human element on information security. In Social and Human Elements of Information Security: Emerging Trends and Countermeasures, IGI Global Scientific Publishing 15p.
[13] Farooq, A., Isoaho, J., Virtanen, S., Isoaho, J. (2015): Information security awareness in educational institution: An analysis of students' individual factors. – In 2015 IEEE 1: 352-359.
[14] Flores, W.R., Ekstedt, M. (2015): Exploring the Link Between Behavioural Information Security Governance and Employee Information Security Awareness. – In HAISA 12p.
[15] Haeussinger, F.J., Kranz, J.J. (2013): Information security awareness: Its antecedents and mediating effects on security compliant behavior. – International Conference on Information Systems (ICIS 2013): Reshaping Society Through Information Systems Design 3: 2222-2237.
[16] Hassanzadeh, M., Jahangiri, N., Brewster, B. (2014): A conceptual framework for information security awareness, assessment, and training. – In Emerging Trends in ICT Security, Morgan Kaufmann 12p.
[17] He, W., Zhang, Z. (2019): Enterprise cybersecurity training and awareness programs: Recommendations for success. – Journal of Organizational Computing and Electronic Commerce 29(4): 249-257.
[18] Kießling, S., Hanka, T., Merli, D. (2021): Salt&Pepper: spice up security behavior with cognitive triggers. – In Proceedings of the 2021 European Interdisciplinary Cybersecurity Conference 6p.
[19] Kruger, H.A., Drevin, L., Flowerday, S., Steyn, T. (2011): An assessment of the role of cultural factors in information security awareness. – In 2011 Information Security for South Africa, IEEE 7p.
[20] Latih, R., Zin, A.M. (2024): Cybersecurity Behavior in the West Sumatra Universities. – JOIV: International Journal on Informatics Visualization 8(3-2): 1976-1986.
[21] Mabece, T., Futcher, L., Thomson, K.L. (2017): South African Computing Educators' Perspectives on Information Security Behaviour. – In IFIP World Conference on Information Security Education, Cham: Springer International Publishing 11p.
[22] 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.

[23] McGill, T., Thompson, N. (2021): Exploring potential gender differences in information security and privacy. – Information & Computer Security 29(5): 850-865.
[24] Park, M., Chai, S. (2020): Comparing the effects of two methods of education (online versus offline) and gender on information security behaviors. – Asia Pacific Journal of Information Systems 30(2): 308-327.
[25] 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.
[26] Pattinson, M., Jerram, C., Parsons, K., McCormac, A., Butavicius, M. (2015): Why do some people manage phishing e-mails better than others? – Information Management & Computer Security 23(4): 318-337.
[27] Pattinson, M.R., Anderson, G. (2007): How well are information risks being communicated to your computer end-users? – Information Management & Computer Security 15(5): 362-371.
[28] Stewart, G., Lacey, D. (2012): Death by a thousand facts: Criticising the technocratic approach to information security awareness. – Information Management & Computer Security 20(1): 29-38.
[29] Tanrıverdi, N., Metin, B. (2017): Evaluation of IT security perception. – In Twenty-third Americas Conference on Information Systems 3p.
[30] Uffen, J., Guhr, N., Breitner, M.H. (2012): Personality traits and information security management: An empirical study of information security executives. – Business & Information Systems Engineering 57(6): 401-413.
[31] Vedadi, A., Warkentin, M. (2018): Secure behavior over time: Perspectives from the Theory of Process Memory. – ACM SIGMIS Database: the DATABASE for Advances in Information Systems 49(SI): 39-48.