ISSN 1846-6168 (Print), ISSN 1848-5588 (Online)
https://doi.org/10.31803/tg-20240627004731

Original scientific paper
Received: 2024-06-27, Accepted: 2024-11-22

Cybersecurity in Action: Unraveling the Effects of Individual, Social, and Organizational Determinants

Somayye Nasiri, Shahram Shahabi, Aynaz Shafiesabet, Maral Talebbeidokhti*, Elmira Alvandi Behineh

Abstract: This research aimed to develop and assess a framework for exploring how factors at the organizational, social, and individual levels influence cybersecurity behavior (CB), with a particular focus on the intermediary role played by awareness of cybersecurity. Participants in this investigation included 381 employees from various public sector entities, with data being gathered via a questionnaire. The analysis was conducted through SEM, specifically employing the PLS. Outputs from this study indicate that cybersecurity awareness (CA), security self-efficacy (SSE), the perceived threat severity, and the perceived vulnerability all positively and significantly impact CBs. Additionally, the research found that initiatives focused on security training and awareness, information security culture, social media influence, family and friends influence, and information systems knowledge all significantly contribute to enhancing CA. Similarly, these elements, alongside direct experience in information security, were shown to affec SSE, with the exception of the influence exerted by family and friends, which did not show a significant impact on it. Influences from social media, family and friends, and direct experiences with information security were also found to significantly affect the perceived severity of threats and perceived of vulnerability. Thus, this study concludes that the factors analyzed are strong indicators of behavior related to cybersecurity.

Keywords: cybersecurity awareness; cybersecurity behavior; information security culture; information systems knowledge; security self-efficacy

1 INTRODUCTION

As internet technology, mobile applications, and artificial intelligence continue to evolve in size and complexity, the nature of cyberattacks is becoming increasingly destructive, leading to unprecedented security challenges for society in cyberspace [1]. Ensuring adherence to security protocols poses a difficulty for institutions across both public and private sectors. Academics and industry experts acknowledge the importance of individuals in maintaining security; however, they are often identified as the most vulnerable point in the security framework due to their frequent failure to implement optimal security measures [2, 3].

Studies examining cybersecurity, including those conducted by Han et al. [4] and Ifinedo [5], have reported that employee behavior does not always align with established security policies. Certain employees may disregard the information security policies within their organization, while others may underestimate the risks associated with information security, even when provided with security policies and written guidelines. Notably, individuals who have received sufficient information security training within their companies do not consistently display heightened levels of cybersecurity behavior (CB), as highlighted by Ng and Xu [6]. Furthermore, a survey conducted by Cybersecurity Insiders in 2018 revealed that 90% of cybersecurity professionals believe their organizations are susceptible to insider threats. This data underscores the ongoing difficulty of achieving individual security compliance. Therefore, considering the importance of CBs of employees in reducing security threats to organizations, the present study tends to propose a model to examine the effect of organizational (ST&AP, information security culture (ISC)), social (social media influence, friends and family influence), and individual (information systems knowledge (ISK) and information security experiences (ISE)) factors on CB with the mediating role of cybersecurity awareness (CA), perceived threat severity (PTS), and perceived vulnerability (PV).

CA and CB: CA is crucial within an organization. CA determines organizational readiness for any cyber-attacks and the level of employee familiarity with the subject [7, 8]. Security awareness refers to the degree to which members of an organization comprehend the significance of information security, the level of security mandated by the organization, their personal security obligations, and their corresponding actions [9]. CA has been defined as a combination of awareness and taking specific actions to protect information system of the organization [10]. According to Hansche [11], emphasizing security awareness can heighten the significance of information systems security and the potential adverse impacts of a security breach or failure. Furthermore, cultivating security awareness is crucial for promoting desired individual security compliance behaviors. Prior research acknowledges the significance of CA, highlighting its potential to influence employee behavior positively. When employees possess a heightened awareness of cybersecurity, they are better equipped to comprehend cybersecurity threats and mitigate their adverse impact on the organization [8]. Hence, fostering a culture of CA within companies is vital to enhance employees' cybersecurity practices, thereby bolstering the organization's capacity to effectively combat cybersecurity threats. Siponen [12] contended that offering security awareness plays a pivotal role in influencing employees to alter their attitudes regarding cybersecurity. In a related vein, Donalds [13] discovered that CA directly correlates with cybersecurity compliance behavior. Research conducted by Simonet and Teufel [14], Li et al. [15], Donalds and Osei-Bryson [3], and Limna et al. [16] further supports the significance of CA in influencing CB. Thus, it can be inferred that:

H_1: CA is effective on employee CB.

Security Self-Efficacy (SSE) and CB: Self-efficacy has wide applications in different situations and is an important factor in human competence construction system. The

performance of individuals with comparable skills across diverse circumstances, ranging from low to high intensity, or of a single individual in varying conditions, is contingent upon their self-confidence [17]. Self-efficacy refers to beliefs and judgments people make about their capabilities to perform specific tasks in specific situations [18]. SSE refers to judgments people make about their abilities to perform cybersecurity countermeasures and is considered the capability to counter cybersecurity threats [6]. Self-efficacy plays a significant role in influencing various behaviors associated with information security, including the intention to adhere to information systems policies [19], cybersecurity-related behaviors [3, 8, 20], and ased on the research conducted by Johnston and Warkentin [21], it is evident that user intention to utilize anti-spyware software is influenced by certain factors. Hence, it can be inferred that:

H_2: SSE is effective on employee CB.

PTS, PV, and CB: Derived from social psychology, the Protection Motivation Theory stands out as a robust explanatory framework for forecasting users' inclination towards practicing security behaviors [22, 23]. Threat appraisal is a significant component of this theory. Information about threats plays a crucial role in risk recognition. Threat appraisal relates to user assessment of the risk level stemming from negligence in information security. This threat has the potential to compromise the integrity, confidentiality, and availability of information [15; 24]. PTS and PV are two important variables in threat appraisal.

The Protection Motivation Theory has been widely applied to explore employees' perceptions of cybersecurity threats and their development of coping strategies from diverse angles [25]. Threat appraisal involves the process through which individuals evaluate the level of risk associated with a menacing cybercrime. PV denotes the degree to which employees feel at risk from a cyber-attack and perceive a deficiency in preventive measures and tools [3, 8, 26]. Research conducted [15, 8, 24, 26] also indicates the role of PTS and PV in CB. As a result, we posit that:

H_3: PTS influences employee CB.

H_4: PV is effective on employee CB.

Security Training and CA Programs: Organizations allocate a significant portion of their budgets to educational and awareness programs in the field of IT security, as a lack of awareness and expertise in this area leads to security incidents [27]. There is a growing recognition that utilizing data-driven AI systems can enhance recruitment and retention efforts to diversify the workforce, similar to how organizations invest in educational programs to mitigate risks related to IT security due to a lack of awareness and expertise [28]. Consequently, organizations need security training and cybersecurity training and awareness programs, focusing on educating employees so they act according to certain IT security principles and objectives [27, 29]. Numerous organizations disseminate security policies and provide security training and awareness initiatives, which elucidate the appropriate usage and interaction with computers and internet-connected systems. These programs encompass various topics, including password management and phishing [14]. There are two distinct approaches to implementing such security measures. While some scholars propose employing a deterrent approach through fear-based campaigns, others advocate for skill-based actions, training, and awareness [14]. Research conducted by Simonet and Teufel [14], Burns et al. [30], and Wipawayangkool [9] underscores the significance of security training and awareness programs (ST&AP) in enhancing CA and self-efficacy. As a result, it is hypothesized that:

H_5: ST&AP are effective on CA.

H6: ST&AP are effective on SSE.

Information Security and Cybersecurity Culture: Promoting an ISC within organizations is a comprehensive approach to cybersecurity [14]. ISC positively impacts employee CB and ultimately enhances organizational potential to effectively counter cyber threats [8]. Schlienger and Teufel [31] argue that ISC should change employee values to boost internal drive for safe cyber behavior. Research findings [14, 32] also highlight the role of ST&AP in enhancing CA and SSE. Therefore, it is assumed that:

H_7: ISC is effective on CA.

H_8: ISC is effective on SSE.

Social Media, Friends, and Family Influence on Cybersecurity: One of the determinants related to CBs can be found in the social environment. Social influence emphasizes the way individuals view the significance of others' viewpoints [33]. The social influence exerted by peers, family, and media affects user intentions [34]. Particularly because the effects of cybersecurity incidents may not be immediately visible, anecdotes shared by friends and family can serve as alternative illustrations, enhancing the social learning process for cybersecurity concerns [14, 32]. Over the past few years, social media platforms have risen as the primary means for sharing and seeking information regarding protective behaviors. For example, Liu [35] discovered that seeking information via social media encouraged users to adopt more protective behaviors. Leadership styles, whether in project or operational environments [35], can significantly influence the social dynamics within organizations, including behaviors rooted in social influence and organizational citizenship, ultimately impacting economic growth and governance integrity [36]. Simonton and Teufel [14] also validated the influence of social media, friends, and family in the realm of cybersecurity. From this, we can deduce the following hypotheses:

H_9: The impact of social media is significant on CA.

H_{10}: The impact of social media is significant on SSE.

H_{11}: The impact of social media is significant on PTS.

H_{12}: The impact of social media is significant on PV.

H_{13}: Friends and family is effective on CA.

H_{14}: Friends and family is effective on SSE.

H_{15}: Friends and family is effective on PTS.

H_{16}: Friends and family is effective on PV.

ISK and Cybersecurity: Technical acumen signifies an organization's capacity or proficiency in utilizing scientific and technical knowledge via a series of procedures and techniques to enhance and innovate products and operations [37, 47]. Scholarly works have emphasized the importance of skills, abilities, and distinct competencies associated with technology, along with the acquisition and utilization of technological knowledge, because of the crucial impact they have on organizational effectiveness [38, 39, 40, 48]. Knowledge is closely linked to CA. Users with a good

understanding of cybersecurity can identify negative or positive situations when using technology. Simonton and Teufel [14] also confirmed the role of ISK in cybersecurity. Therefore, it is assumed that:

H_{17}: ISK is effective on CA.

H18: ISK is effective on SSE.

ISE and Cybersecurity: The security encounters and beliefs of employees, along with the training offered by their organizations, greatly influence the perceived seriousness of information security. When employees have prior experience in handling cybersecurity incidents, they are better equipped to thwart new cyberattacks [15]. Consequently, Employees who have undergone information security incidents will possess a greater degree of practical experience in addressing cybercrimes compared to those lacking such exposure. Consequently, their hands-on experience serves as a wellspring of knowledge, enabling them to more effectively implement cybersecurity measures [41]. Li et al. [15] also affirmed the influence of information security encounters on associated cybersecurity attitudes, including PTS, vulnerability, and SSE. As a result, it is postulated that:

H_{19}: ISE are effective on PTS.

H_{20}: ISE are effective on PV.

H_{21}: ISE are effective on SSE.

In summary, as highlighted, the significance of the variables discussed in this study regarding CBs of employees has been emphasized throughout the theoretical literature. However, empirical literature shows that few research efforts have been made to present a model for examining the effect of organizational, social, and individual factors on CB with the mediating role of CA. Hence, the current research mainly aims at introducing a model that analyzes the impact of organizational, social, and individual factors on cybersecurity practices, with CA acting as a mediator. Drawing from theoretical literature and a conceptual framework originating from existing research, Fig. 1 illustrates the proposed conceptual model. In this model, ST&AP, ISC, social media influence, friends and family influence, ISK, and ISE are considered as independent variables. CA, SSE, PTS, and PV are considered as mediating variables, and employee CB is considered as dependent variable.

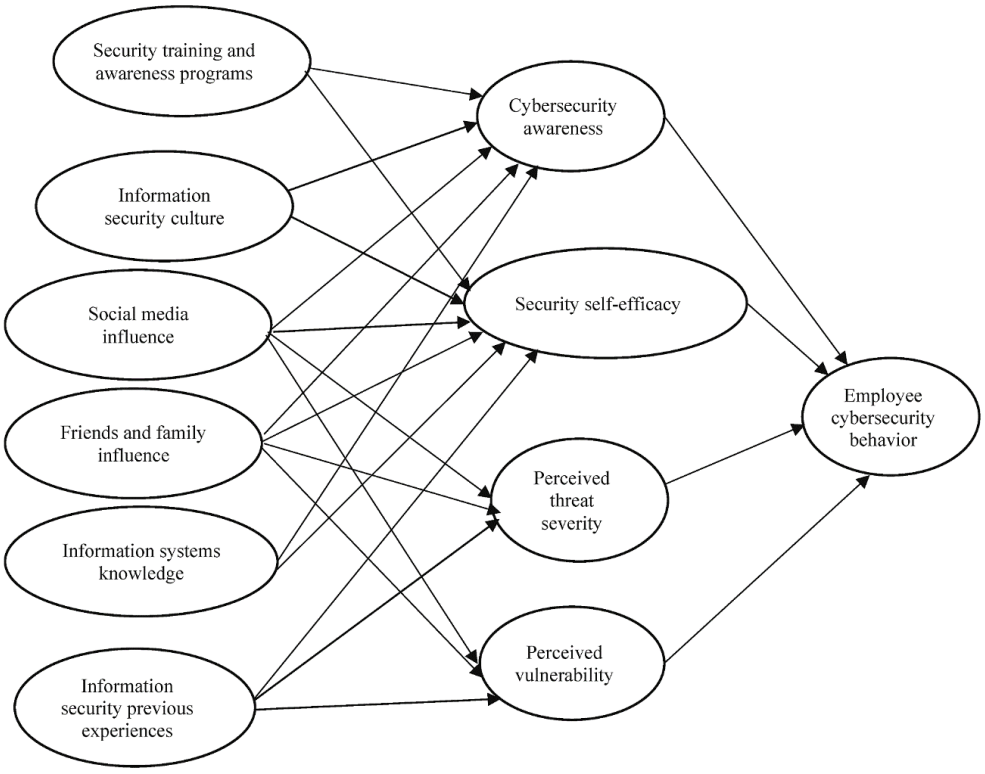

Figure 1 Conceptual model

2 RESEARCH METHODOLOGY

In the upcoming section, we will outline our research methodology.

2.1 Population and Sample

This study was conducted among Iranian public employees, among whom 450 questionnaires were distributed, with 409 returned and 28 removed due to incomplete answers, resulting in 381 questionnaires remained for analysis. Among the participants, 74% were male and 26% were female; 7% fell within the age range of 25-30 years, 41% between 31-40 years, 43% between 41-50 years, and 9% were aged 50 years or above.

2.2 Research Instruments

Questionnaires were used to measure the research constructs. The evaluation of ST&AP was conducted using the Simonet and Teufel [14] survey, which comprises two components. The evaluation of ISC was conducted utilizing

the Flores and Ekstedt [32] survey, which consists of four items. The assessment of social media influence was carried out using the Ng and Rahim [42] survey, which includes three items. The evaluation of friends and family influence was conducted using the Simonet and Teufel [14] survey, which comprises four items. To evaluate participants' knowledge of information systems, the Haeussinger & Kranz [43] questionnaire, comprising two items, was employed. The assessment of cyber security awareness utilized the Donalds and Osei-Bryson [3] survey, which includes three items. The assessment of previous experiences with information security was carried out using the Li et al. [15] survey instrument, which consists of three items measuring PTS, three items assessing PV, and three items evaluating SSE. The evaluation of CB was conducted using the Simonet and Teufel [14] survey, comprising nine items. Each item was assessed using a 5-point Likert scale.

3 RESULTS

3.1 Validity and Reliability of Instruments

To assess the validity and reliability of the research instrument, various tools were used, including Cronbach's alpha, composite reliability (CR), factor loadings, and the average variance extracted (AVE). CR utilizes factor loadings in its calculations, resulting in higher and improved values compared to those obtained from Cronbach's alpha [44]. The criterion for this index is also similar to Cronbach's alpha coefficient, which is 0.70 or higher for internal consistency of the measurement model. In confirmatory factor analysis, a factor loading of 0.60 or higher for any item signifies a clearly defined construct [45]. Tab. 1 shows that all factor loadings are above 0.6, all Cronbach's alpha and CR values are above 0.7, and all AVE values are above 0.5. According to Anbari et al. [46], an AVE value of 0.50 or higher suggests that the construct accounts for at least 50% of the variance in its associated markers.

Chin [45] proposes two criteria for assessing construct validity—each item should have a high factor loading on its own construct and a relatively low cross-loading on other constructs, with a suggested difference of at least 0.10 in factor loadings. Another criterion, the square root of the AVE should be greater than the correlations with other constructs. Based on the findings in Tab. 2, all variables exhibit the highest factor loading on their designated constructs, with a minimum difference of over 0.10 between their own factor loadings and those on other constructs, indicating satisfactory construct validity. Additionally, Tab. 3 presents results concerning correlations and the square root of the AVE.

Table 1 Results of measurement analysis

Variable	Item	Factor loading	Cronbach' alpha	CR	AVE
ST&AP	1	0.823	0.741	0.878	0.784
	2	0.944			
ISC	1	0.873	0.880	0.917	0.735
	2	0.863			
	3	0.857			
	4	0.837			
Social media influence	1	0.921	0.874	0.923	0.799
	2	0.889			
	3	0.872			
Friends and family influence	1	0.716	0.754	0.844	0.577
	2	0.715			
	3	0.828			
	4	0.773			
ISK	1	0.908	0.808	0.912	0.839
	2	0.924			
ISE	1	0.867	0.757	0.856	0.667
	2	0.856			
	3	0.718			
CA	1	0.860	0.782	0.874	0.699
	2	0.90			
	3	0.741			
SSE	1	0.891	0.858	0.913	0.779
	2	0.854			
	3	0.902			
PTS	1	0.853	0.924	0.952	0.870
	2	0.967			
	3	0.973			
PV	1	0.796	0.788	0.863	0.611
	2	0.781			
	3	0.809			
	4	0.739			
CB	1	0.820	0.929	0.941	0.638
	2	0.845			
	3	0.825			
	4	0.845			
	5	0.847			
	6	0.791			
	7	0.737			
	8	0.699			
	9	0.767			

Table 2 Cross factor loadings to assess validity of the questionnaires

	CA	CB	Family and Friends Influence	ISE	ISC	ISK	PTS	PV	ST&AP	SSE	Social Media Influence
CSA1	0.860	0.347	0.388	0.276	0.288	0.401	0.250	0.302	0.303	0.266	0.156
CSA2	0.900	0.476	0.454	0.243	0.372	0.442	0.301	0.330	0.286	0.393	0.154
CSA3	0.741	0.367	0.324	0.332	0.408	0.327	0.210	0.388	0.277	0.259	0.164
CSB1	0.362	0.820	0.468	0.380	0.547	0.448	0.521	0.492	0.441	0.402	0.414
CSB2	0.401	0.845	0.466	0.439	0.464	0.531	0.508	0.494	0.393	0.525	0.474
CSB3	0.387	0.825	0.428	0.396	0.469	0.457	0.504	0.515	0.427	0.443	0.449
CSB4	0.446	0.845	0.513	0.463	0.556	0.475	0.505	0.486	0.418	0.413	0.455
CSB5	0.446	0.847	0.533	0.431	0.575	0.500	0.577	0.558	0.414	0.502	0.375
CSB6	0.312	0.791	0.491	0.352	0.511	0.372	0.513	0.486	0.378	0.461	0.401

Table 3 Cross factor loadings to assess validity of the questionnaires (continuation)

	CA	CB	Family and Friends Influence	ISE	ISC	ISK	PTS	PV	ST&AP	SSE	Social Media Influence
CSB7	0.349	0.737	0.350	0.317	0.460	0.348	0.370	0.346	0.503	0.556	0.369
CSB8	0.353	0.699	0.324	0.342	0.430	0.315	0.381	0.350	0.437	0.498	0.379
CSB9	0.383	0.767	0.488	0.357	0.637	0.494	0.518	0.542	0.460	0.439	0.418
FFI1	0.336	0.370	0.716	0.397	0.379	0.361	0.343	0.484	0.308	0.301	0.314
FFI2	0.382	0.330	0.715	0.336	0.324	0.376	0.310	0.489	0.281	0.252	0.231
FFI3	0.316	0.526	0.828	0.475	0.543	0.494	0.531	0.540	0.439	0.373	0.464
FFI4	0.401	0.482	0.773	0.459	0.513	0.523	0.471	0.473	0.361	0.322	0.474
ISC1	0.337	0.592	0.459	0.467	0.873	0.530	0.525	0.531	0.436	0.458	0.448
ISC2	0.408	0.585	0.501	0.441	0.863	0.425	0.519	0.469	0.484	0.435	0.464
ISC3	0.343	0.540	0.500	0.465	0.857	0.482	0.540	0.539	0.464	0.375	0.509
ISC4	0.366	0.501	0.549	0.436	0.837	0.381	0.501	0.474	0.545	0.482	0.495
ISK1	0.409	0.452	0.528	0.393	0.414	0.908	0.503	0.500	0.288	0.413	0.367
ISK2	0.450	0.557	0.538	0.485	0.546	0.924	0.463	0.499	0.403	0.453	0.479
PE1	0.254	0.454	0.512	0.867	0.521	0.427	0.584	0.556	0.272	0.453	0.495
PE2	0.328	0.415	0.465	0.856	0.411	0.477	0.449	0.565	0.221	0.282	0.426
PE3	0.241	0.290	0.350	0.718	0.321	0.229	0.298	0.376	0.165	0.157	0.374
PS1	0.239	0.486	0.474	0.451	0.549	0.456	0.853	0.498	0.388	0.383	0.502
PS2	0.316	0.439	0.539	0.559	0.501	0.486	0.967	0.646	0.466	0.551	0.539
PS3	0.299	0.429	0.533	0.571	0.480	0.480	0.973	0.635	0.439	0.528	0.560
PV1	0.194	0.389	0.544	0.510	0.417	0.449	0.478	0.796	0.253	0.309	0.370
PV2	0.313	0.396	0.530	0.475	0.391	0.542	0.419	0.781	0.363	0.306	0.308
PV3	0.375	0.548	0.519	0.571	0.555	0.498	0.546	0.809	0.347	0.422	0.528
PV4	0.371	0.524	0.451	0.385	0.547	0.393	0.548	0.739	0.523	0.410	0.407
SET1	0.159	0.391	0.424	0.168	0.426	0.285	0.312	0.356	0.823	0.292	0.367
SET2	0.396	0.534	0.411	0.296	0.556	0.375	0.477	0.467	0.944	0.398	0.447
SMI1	0.102	0.457	0.423	0.531	0.490	0.398	0.454	0.492	0.428	0.291	0.921
SMI2	0.252	0.521	0.463	0.464	0.541	0.442	0.492	0.461	0.409	0.302	0.889
SMI3	0.152	0.414	0.450	0.434	0.466	0.408	0.487	0.451	0.408	0.262	0.872
SS1	0.332	0.516	0.365	0.319	0.477	0.433	0.447	0.414	0.396	0.891	0.283
SS2	0.285	0.486	0.362	0.390	0.401	0.363	0.452	0.405	0.268	0.854	0.274
SS3	0.365	0.551	0.369	0.336	0.476	0.451	0.497	0.417	0.386	0.902	0.288

Table 3 The results of construct validity

	CA	CB	Family and Friends Influence	ISE	ISC	ISK	PTS	PV	ST&AP	SSE	Social Media Influence
CA	0.836										
CB	0.480	0.799									
Family and Friends Influence	0.469	0.569	0.759								
ISE	0.334	0.486	0.553	0.817							
ISC	0.425	0.478	0.587	0.527	0.857						
ISK	0.470	0.553	0.582	0.482	0.528	0.916					
PTS	0.307	0.631	0.553	0.568	0.693	0.583	0.933				
PV	0.404	0.599	0.653	0.625	0.616	0.602	0.640	0.782			
ST&AP	0.344	0.535	0.462	0.277	0.565	0.380	0.463	0.474	0.885		
SSE	0.373	0.588	0.414	0.392	0.513	0.473	0.528	0.467	0.400	0.883	
Social Media Influence	0.188	0.520	0.497	0.534	0.558	0.465	0.572	0.524	0.464	0.319	0.894

3.2 SEM Results

Utilizing structural equation modeling (SEM), the study employed a proposed conceptual model and hypotheses to forecast the CB of public organization employees. The model was estimated using partial least squares (PLS), with t-values calculated through bootstrapping (500 subsamples). Fig. 2 visually depicts results of structural model. Tab. 4 reports the estimated path coefficients and Variance explained values.

According to the findings in Tab. 4, CA, SSE, PTS, and PV have a positive and significant impact on CB. Moreover, factors such as security training, awareness programs, ISC, social media influence, family and friends influence, and ISK demonstrate a positive and significant influence on CA.

Similarly, security training, awareness programs, ISC, social media influence, ISK, and ISE positively and significantly affect SSE. However, the influence of family and friends is not significant on SSE. Social media influence, family and friends influence, as well as ISE, have a positive and significant impact on PTS and vulnerability. The variables in the model explain 56% of the variability in CB, 33% in CA, 34% in SSE, 47% in PTS, and 54% in PV. Tab. 5 presents the indirect coefficients.

Tab. 5 indicates that CA mediates significantly the relationship between security training, awareness programs, ISC, social media influence, and family and friends influence on CB. Additionally, SSE acts as a significant and positive mediator between CA and security training, awareness programs, ISC, and social media influence in influencing CB. Moreover, PTS and vulnerability serve as significant and positive mediators between social media influence, family and friends influence, and ISE in impacting employee CB. However, the mediating role of SSE is not significant in the relationship between family and friends influence and CB. Tab. 6 presents the outcomes of hypothesis testing. The study found that the absolute Goodness of Fit (GOF) index for model is 0.571, indicating it is a well-suited fit.

4 DISCUSSION

This research aimed to introduce a model to investigate the impact of organizational, social, and individual factors on CB, incorporating the mediating role of CA through SEM. The findings indicated that the proposed model aligns well with the data collected for this study and can account for significant proportions of variance: 56% in CB, 33% in CA, 34% in cybersecurity self-efficacy, 47% in PTS, and 54% in PV.

The findings further revealed that ST&AP exert a positive and significant influence on CA and self-efficacy. Hence, these programs contribute to heightened CA and improved SSE. This outcome aligns with the research of Simonet and Teufel [14], Burns et al. [30], and Wipawayangkool [9]. It implies that when organizations offer training to enhance employees' understanding and awareness of computer and information security matters and educate them about their responsibilities in computer security, it results in increased CA and enhanced SSE. As a result, organizations should implement IT security-training programs aimed at augmenting employee knowledge and awareness of information technology security.

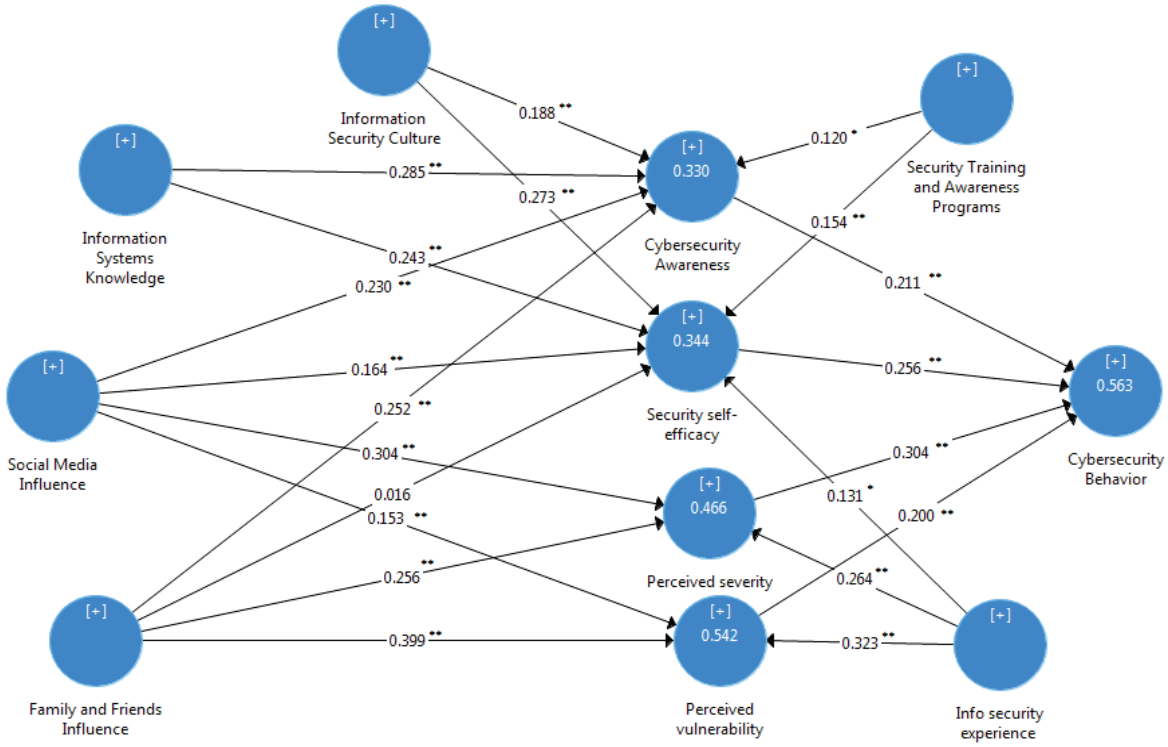

Figure 2 The tested model

Another finding of this study is the positive and significant effect of ISC on CA and SSE. Therefore, ISC leads to increased CA and SSE. This finding is consistent with Simonet and Teufel [14] and Flores and Ekstedt [32]. This finding can be attributed to the collective responsibility shared by employees within an organization to raise awareness about cybersecurity threats. When employees actively inform and caution one another about such threats, a common goal is established to protect information assets from unauthorized access and malware infection. This shared commitment leads to heightened CA and increased SSE among employees.

Furthermore, social media influences significantly CA, SSE, PTS, and PV. Therefore, social media influence leads to increased CA, SSE, PTS, and PV. This observation aligns with the work of Simonet and Teufel [14]. To clarify this result, if mass media encourages employees to practice safe cyber behaviors and reports influence employees to engage

in safe cyber behavior, employees feel pressured by mass media to practice safe cyber behavior, this will result in increased CA, SSE, PTS, and PV.

Table 4 Path coefficients and variance explained

Variable	β	t-value	p-value	Variance explained
On cybersecurity of employees via:				
CA	0.211**	4.818	0.01	0.563
SSE	0.256**	5.034	0.01	
PTS	0.304**	5.969	0.01	
PV	0.20**	4.270	0.01	
On CA via:				
ST&AP	0.12*	2.225	0.05	0.33
ISC	0.188**	2.820	0.01	
Social media influence	0.230**	3.989	0.01	
Friends and family influence	0.252**	4.034	0.01	
ISK	0.285**	4.249	0.01	
On SSE via:				
ST&AP	0.154**	3.036	0.01	0.344
ISC	0.273**	4.515	0.01	
Social media influence	0.164**	3.560	0.01	
Friends and family influence	0.016	0.223	0.01	
ISK	0.243**	5.149	0.01	
ISE	0.131*	2.382	0.01	
On PTS via:				
Social media influence	0.304**	6.056	0.01	0.466
Friends and family influence	0.256**	5.244	0.01	
ISE	0.264**	5.340	0.01	
On PV via:				
Social media influence	0.153**	3.058	0.01	0.542
Friends and family influence	0.399**	8.735	0.01	
ISE	0.323**	7.526	0.01	

*$p < 0.05$; **$p < 0.01$

Table 5 Indirect coefficients

Indirect paths	Indirect effects	t-value	p-values
Family and Friends Influence→CA→CB	0.053	3.070	0.002
ISC→CA→CB	0.040	2.268	0.024
ISK→CA→CB	0.060	3.312	0.001
ST&AP→CA→CB	0.025	1.987	0.047
Social Media Influence→CA→CB	0.049	3.101	0.002
Family and Friends Influence→PTS→CB	0.078	3.963	0.000
ISE→PTS→CB	0.080	4.279	0.000
Social Media Influence→PTS→CB	0.092	3.759	0.000
Family and Friends Influence→PV→CB	0.080	3.886	0.000
ISE→PV→CB	0.065	3.777	0.000
Social Media Influence→PV→CB	0.031	2.260	0.024
Family and Friends Influence→SSE→CB	0.004	0.214	0.831
ISE→SSE→CB	0.034	2.271	0.024
ISC→SSE→CB	0.070	3.203	0.001
ISK→SSE→CB	0.062	3.586	0.000
ST&AP→SSE→CB	0.039	2.493	0.013
Social Media Influence→SSE→CB	0.042	2.907	0.002

The study also found that the influence of friends and family positively and significantly affects CA, PTS, and PV. Therefore, their influence contributes to an increase in CA, PTS, and PV. This finding is consistent with the research by Simonet and Teufel [14]. It implies that when family members and friends encourage employees to practice safe cyber behavior and hold them accountable for doing so, it results in heightened CA, PTS, and PV. Since the consequences of cybersecurity incidents are not always observable or tangible, sharing stories about such incidents can reinforce the social learning process for cybersecurity issues and serve as alternative examples [14].

An additional outcome from the model indicated that possessing knowledge of information systems has a positive and significant impact on both CA and SSE. Therefore, ISK leads to an increase in CA and SSE of employees. This finding is consistent with Simonet and Teufel [14]. It suggests that general knowledge of employees about computers and the internet (e.g., web and email systems) can lead to an increase in their CA and SSE. In fact, employees with good knowledge of cybersecurity can identify negative or positive situations when using technology and their security behaviors can improve.

Table 6 Outcomes of hypothesis evaluation

Hypothesis	Result
H1: CA influences CB.	Confirmed
H2: SSE influences CB,	Confirmed
H3: PTS influences CB.	Confirmed
H4: PV influences CB.	Confirmed
H5: ST&AP influences CA.	Confirmed
H6: ST&AP influences SSE.	Confirmed
H7: ISC influences CA.	Confirmed
H8: ISC influences SSE.	Confirmed
H9: social media influences CA.	Confirmed
H10: social media influences SSE.	Confirmed
H11: social media influences PTS.	Confirmed
H12: social media influences PV.	Confirmed
H13: friends and family influences CA.	Confirmed
H14: friends and family influences SSE.	Rejected
H15: friends and family influence is effective on PTS.	Confirmed
H16: friends and family influence is effective on PV.	Confirmed
H17: ISK is effective on CA.	Confirmed
H18: ISK is effective on SSE.	Confirmed
H19: ISE is effective on PTS.	Confirmed
H20: ISE is effective on PV.	Confirmed

The findings also indicated that ISE have a positive and significant influence on SSE, PTS, and PV. This is consistent with the study by Li et al. [15], who also found that ISE impact PTS, PV, and SSE. Consequently, ISE contribute to an increase in SSE, PTS, and PV. This finding suggests that when employees undergo formal training on common computer security practices, their organization implements a clear information security policy, and security awareness training is provided to employees, it leads to heightened SSE, PTS, and PV.

Another significant finding of the research indicated a notable and positive correlation between CA and CB. Therefore, CA leads to an increase in CB. This finding is consistent with Simonet and Teufel [14], Li et al. [15], Donalds and Osei-Bryson [3], and Limna et al. [16]. Therefore, employee awareness of cybersecurity and its associated risks plays a determining role in their CB. Siponen [12] emphasizes that offering security awareness is crucial in motivating employees to modify their behaviors for enhanced cybersecurity measures.

The findings indicated a positive and significant correlation between SSE and CB. Therefore, SSE leads to an increase in CB. This finding is consistent with D'Arcy and Lowry [20], Donalds and Osei-Bryson [3]. This finding suggests that when employees feel assured in adjusting web

browser security settings, handling virus-infected files, and effectively removing spyware and malware from their computers, it leads to an improvement in CB.

Furthermore, the study revealed a notable and positive correlation between PTS and CB. In other words, when individuals perceive the severity of cybersecurity threats to be high, it results in an increase in their engagement in CB. This is consistent with the study by Li et al. [15] and Gerdenitsch et al. [24]. To explain this finding, if employees experience a virus infection on their computers due to opening suspicious email attachments or unauthorized access to their personal confidential information at the workplace, it becomes a serious concern for them. Additionally, the potential loss of information through hacking poses another significant problem. These factors contribute to an elevation in CB.

Another key finding from this research indicates that PV has a positive and significant impact on CB. In essence, a sense of vulnerability contributes to an increase in engaging in cybersecurity practices. This is consistent with the study by Li et al. [15] and Gerdenitsch et al. [24]. The study suggests that when employees perceive that adhering to their organization's information security policies reduces their vulnerability to security breaches, and recognize that non-compliance could make them susceptible to harmful attacks, they are more inclined to believe that their efforts safeguard organizational information against unauthorized access. Conversely, neglecting information security protocols puts organizational data and resources at risk, prompting individuals to be more proactive in practicing cybersecurity measures.

5 MANAGERIAL IMPLICATIONS

- Organizations should provide ST&AP to enhance employees' understanding and awareness of cybersecurity issues. This includes educating them on their responsibilities regarding computer security to improve their beliefs and behaviors in this area.
- Encouraging the establishment of an ISC within the organization can boost CA and SSE. Employees should be encouraged to share cybersecurity threat alerts, fostering a collective responsibility towards information security. A unified approach among employees is vital for protecting organizational assets against cyber threats.
- Offering planned ISE can empower employees to prevent new cyberattacks. Employees with prior ISE are better prepared to tackle cybercrimes compared to those without such exposure.
- Training employees in relevant cybersecurity practices and enhancing their competency in this domain can improve SSE, influencing various information security-related behaviors. Strengthening self-efficacy is crucial as it impacts different behaviors related to information security and cybersecurity.
- Accurate assessments of PTS and vulnerability are essential for shaping employee CBs. Understanding and evaluating cybersecurity risk levels accurately is critical to avoid any negligence in addressing security concerns effectively within the organization.

6 CONCLUSION

In conclusion, the variables examined in this study are strong indicators of employee CBs. CA plays a crucial mediating role, significantly impacting the influence of security training programs, ISC, social media, and personal networks on employee CB. Likewise, SSE mediates positively the impact of CA on security training, ISC, and social media on employee CB. Moreover, PTS and vulnerability also play important mediating roles, significantly affecting the influence of social media, personal networks, and ISE on employee CB. Consequently, considering these model variables is crucial for improving employee acceptance of CBs.

7 LIMITATIONS

This research focused solely on employees from public organizations in Iran, therefore generalizations may be limited. Additionally, the nature of the study is correlational, and causal inferences cannot be drawn from the relationships between model variables. The role of culture in findings of this study should not be overlooked, and further studies should explore the relationships between variables in different cultural contexts.

8 REFERENCES

[1] Darvishinia, N. (2023). AI in Education: Cracking the Code through Challenges: A Content Analysis of One of the Recent Issues of Educational Technology and Society (ET&S) Journal. *Partners Universal International Innovation Journal, 1*(4), 61-71. https://doi.org/10.5281/zenodo.8264262

[2] Samadi, H., Nazari-Shirkouhi, S., & Keramati, A. (2014). Identifying and analyzing risks and responses for risk management in information technology outsourcing projects under fuzzy environment. *International Journal of Information Technology & Decision Making, 13*(06), 1283-1323. https://doi.org/10.1142/S021962201450076X

[3] Keramati, A., Samadi, H., & Nazari-Shirkouhi, S. (2013). Managing risk in information technology outsourcing: an approach for analysing and prioritising using fuzzy analytical network process. *International Journal of Business Information Systems, 12*(2), 210-242. https://doi.org/10.1504/IJBIS.2013.052052

[4] Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, *66*, 52-65. https://doi.org/10.1016/j.cose.2016.12.016

[5] Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

[6] Ng, B. Y., & Xu, Y. (2007). Studying users' computer security behavior using the Health Belief Model. *PACIS 2007 Proceedings*, 45. https://aisel.aisnet.org/pacis2007/45

[7] Nazari-Shirkouhi, S., Miri-Nargesi, S., & Ansarinejad, A. (2017). A fuzzy decision making methodology based on fuzzy AHP and fuzzy TOPSIS with a case study for information

systems outsourcing decisions. *Journal of Intelligent & Fuzzy Systems, 32*(6), 3921-3943. https://doi.org/10.3233/JIFS-12495

[8] Ramezani, A. (2024, May). Fusion Models for Cyber Threat Defense: Integrating Clustering with Kmeans, Random Forests, and SVM against Windows Malware. In *IEEE World AI IoT Congress (AIIoT2024)*, 465-470) https://doi.org/10.1109/AIIoT61789.2024.10578947

[9] Wipawayangkool, K. (2009). Security awareness and security training: An attitudinal perspective. *SWDSI 2009*, 266-273.

[10] Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, *2019*(8), 11-14. https://doi.org/10.1016/S1361-3723(19)30085-5

[11] Hansche, S. (2001). Designing a security awareness program: Part 1. *Information Systems Security, 9*(6), 14-22. https://doi.org/10.1201/1086/43298.9.6.20010102/30985.4

[12] Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information management & computer security*, *8*(1), 31-41. https://doi.org/10.1108/09685220010371394

[13] Donalds, C. (2015). *Cybersecurity policy compliance: An empirical study of Jamaican government agencies.* Paper Presented at the SIG GlobDev Pre-ECIS Workshop.

[14] Simonet, J., & Teufel, S. (2019). The influence of organizational, social and personal factors on cybersecurity awareness and behavior of home computer users. In *ICT Systems Security and Privacy Protection: 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings 34*, 194-208. Springer International Publishing. https://doi.org/10.1007/978-3-030-22312-0_14

[15] Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

[16] Limna, P., Kraiwanit, T., Siripipattanakul, S., Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2023). The relationship between cyber security knowledge, awareness and behavioural choice protection among mobile banking users in Thailand. *International Journal of Computing Sciences Research*, *7*, 1133-1151. https://doi.org/10.25147/ijcsr.2017.001.1.123

[17] Schwarzer, R. (2014). *Self-efficacy: Thought control of action*. Taylor & Francis. https://doi.org/10.4324/9781315800820

[18] Bandura, A. (2006). Guide for constructing self-efficacy scales. *Self-efficacy beliefs of adolescents*, *5*(307-337).

[19] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548. https://doi.org/10.2307/25750690

[20] D'Arcy, J., & Lowry, P. B. (2017). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*. https://doi.org/10.1111/isj.12173

[21] Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS quarterly*, 549-566. https://doi.org/10.2307/25750691

[22] Aurigemma, S., & Mattson, T. (2018). Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. *Computers & Security*, *73*, 219-234. https://doi.org/10.1016/j.cose.2017.11.001

[23] Chehrehpak, M., Alizadeh, A., & Nazari-Shirkouhi, S. (2018). An empirical study on factors influencing technology transfer using structural equation modelling. International *Journal of Productivity and Quality Management, 23*(3), 273-288. https://doi.org/10.1504/IJPQM.2018.089801

[24] Gerdenitsch, C., Wurhofer, D., & Tscheligi, M. (2023). Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees' security behavior. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *17*(4). https://doi.org/10.5817/CP2023-4-7

[25] Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198. https://doi.org/10.1016/j.im.2012.04.002

[26] Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, *5*, 100165. https://doi.org/10.1016/j.chbr.2021.100165

[27] Kirova, D., & Baumöl, U. (2018). Factors that affect the success of security education, training, and awareness programs: A literature review. *Journal of Information Technology Theory and Application (JITTA)*, *19*(4), 4. https://aisel.aisnet.org/jitta/vol19/iss4/4

[28] Sadeghi, S., & Niu, C. (2024). Augmenting Human Decision-Making in K-12 Education: The Role of Artificial Intelligence in Assisting the Recruitment and Retention of Teachers of Color for Enhanced Diversity and Inclusivity. *Leadership and Policy in Schools*, 1-21. https://doi.org/10.1080/15700763.2024.2358303

[29] Nazari-Shirkouhi, S., Ansarinejad, A., Miri-Nargesi, S. S., Dalfard, V. M., & Rezaie, K. (2011). Information systems outsourcing decisions under fuzzy group decision making approach. *International Journal of Information Technology & Decision Making, 10*(06), 989-1022. https://doi.org/10.1142/S0219622011004683

[30] Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2015, January). Assessing the role of security education, training, and awareness on insiders' security-related behavior: An expectancy theory approach. In *48th IEEE Hawaii International Conference on System Sciences*, 3930-3940. https://doi.org/10.1109/HICSS.2015.471

[31] Schlienger, T., & Teufel, S. (2002). *Information security culture.* In: Ghonaimy, M. A., El-Hadidi, M. T., & Aslan, H. K. (eds.) *Security in the Information Society (IAICT2002), 86*, 191-201. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-35586-3_15

[32] Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & security*, *59*, 26-44. https://doi.org/10.1016/j.cose.2016.01.004

[33] Tehranian, K., Khorsand, M. S., Zarei, M., Arani, G. G., Banabari, H. G., & Sasani, F. (2024). Unveiling the Impact of Social Media Usage on Firm Performance: The Mediating Influence of Organizational Agility and Innovation Capability. *Tehnički glasnik, 18*(4), 540-548. https://doi.org/10.31803/tg-20230918233848

[34] Gao, L., & Bai, X., (2014), A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pacific Journal of Marketing and Logistics, 26*(2), 211-231. https://doi.org/10.1108/APJML-06-2013-0061

[35] Minavand, H., Minaei, V., Mokhtari, S. E., Izadian, N., & Jamshidian, A. (2013). Project Managers Vs Operations Managers: A comparison based on the style of leadership. *IOSR Journal of Business and Management (IOSR-JBM)*, *12*(5), 56-61. https://doi.org/10.9790/487X-1255661

[36] Farzad, G., & Roshdieh, N. (2024). The Interplay of Destructive Work Behaviors, Organizational Citizenship Behaviors, and Fiscal Decentralization: Implications for Economic Development in Developing Countries.

International Research Journal of Economics and Management Studies IRJEMS, *3*(8), 1-8. https://doi.org/10.56472/25835238/IRJEMS-V3I8P101

[37] Nazari-Shirkouhi, S., & Keramati, A. (2017). Modeling customer satisfaction with new product design using a flexible fuzzy regression-data envelopment analysis algorithm. *Applied Mathematical Modelling*, 50, 755-771. https://doi.org/10.1016/j.apm.2017.01.020

[38] Nazari-Shirkouhi, S., Keramati, A., & Rezaie, K. (2013). Improvement of customers' satisfaction with new product design using an adaptive neuro-fuzzy inference systems approach. *Neural Computing and Applications, 23*, 333-343. https://doi.org/10.1007/s00521-013-1431-x

[39] Nazari-Shirkouhi, S., Keramati, A., & Rezaie, K. (2015). Investigating the effects of customer relationship management and supplier relationship management on new product development. *Tehnički vjesnik, 22*(1), 191-200. https://doi.org/10.17559/TV-20140623130536

[40] Talebzadeh, H., Fattahiamin, A., Talebzadeh, M., Sanaei, F., Moghaddam, P. K., & Espahbod, S. (2024). Optimizing Supply Chains: A Grey-DEMATEL Approach to Implementing LARG Framework. *Tehnički glasnik, 19*(3), 382-389. https://doi.org/10.31803/tg-20240302201341

[41] Gholami, M. H., Asli, M. N., Nazari-Shirkouhi, S., & Noruzy, A. (2013). Investigating the influence of knowledge management practices on organizational performance: an empirical study. *Acta Polytechnica Hungarica, 10*(2), 205-216. https://doi.org/10.12700/APH.10.02.2013.2.14

[42] Ng, B. Y., & Rahim, M. (2005). A socio-behavioral study of home computer users' intention to practice security. *PACIS 2005 Proceedings*, 20. https://aisel.aisnet.org/pacis2005/20

[43] Haeussinger, F., & Kranz, J. (2013). Information security awareness: its antecedents and mediating effects on security compliant behavior. *ICIS 2013 Proceedings, 9*. https://aisel.aisnet.org/icis2013/proceedings/SecurityOfIS/9

[44] Espahbod, S., Tashakkori, A., Mohsenibeigzadeh, M., Zarei, M., Arani, G. G., Dzikuć, M., & Dzikuć, M. (2024). Blockchain-Driven Supply Chain Analytics and Sustainable Performance: Analysis Using PLS-SEM and ANFIS. *Sustainability, 16*(15), 6469. https://doi.org/10.3390/su16156469

[45] Chin, W. W. (1988). Issues and opinion on structural equation modelling. *MIS Quarterly, 22*(1), vii–xvi.

[46] Anbari, M., Talebzadeh, H., Talebzadeh, M., Fattahiamin, A., Haghighatjoo, M., & Jafari, A. M. (2024). Understanding the drivers of adoption for Blockchain-enabled intelligent transportation systems. *Tehnički glasnik, 18*(4), 598-608. https://doi.org/10.31803/tg-20240411223559

[47] Azimi Asmaroud, S. (2022). Preservice Elementary Teachers' Categorical Reasoning and Knowledge Transfer on Definition Tasks with Two Dimensional Figures. *Theses and Dissertations*. 1588. https://ir.library.illinoisstate.edu/etd/1588

[48] Latifi, K., Ebrahimi, A., Ranjbaran, M., Mirzaei, A., & Fakhri, Z. (2023). Efficient customer relationship management systems for online retailing: The investigation of the influential factors. *Journal of Management & Organization, 29*(4), 763-798. https://doi.org/10.1017/jmo.2022.65

Authors' contacts:

Somayye Nasiri
Department of Computer Engineering Zanjan Branch,
Islamic Azad University,
Daneshjoo Blvd., Lower Mountain Lands Road, Zanjan, Iran

Shahram Shahabi
Faculty of Management, North Tehran Branch,
Islamic Azad University,
Vafadar Blvd., Shahid Sadoughi St., Hakimiyeh Exit, Shahid Babaee Highway,
Tehran, Iran

Aynaz Shafiesabet
Department of Finance, Bauer Collage of Business,
University of Houston,
4250 Martin Luther King Blvd Ste 334, Houston, TX 77204, USA

Maral Talebbeidokhti
(Corresponding Author)
Department of Cybersecurity and Networks,
Tagliatela College of Engineering, University of New Haven,
300 Boston Post Rd, West Haven, CT 06516, USA
talebbeidokhtimaral@gmail.com

Elmira Alvandi Behineh
Department of Business Administration,
University of the Cumberlands,
6191 College Station Dr, Williamsburg, KY 40769, USA