ISSN:2302-8149
e-ISSN:2540-9719

Examining the Readiness of the Organization's Security Success in Improving Security Performance

[1]Nur Fatimatuz Zuhroh*, [2]Ahmad Baihaqy
[1]Accounting, Sekolah Tinggi Ilmu Ekonomi Indonesia Surabaya
[2]Management, Sekolah Tinggi Ilmu Ekonomi Indonesia Surabaya
[1,2]Jl. Menur Pumpungan No.30, Menur Pumpungan, Surabaya, Indonesia
*e-mail: nurfatimatuzz@stiesia.ac.id

(***received***: 28 November 2024, ***revised***: 20 February 2025, ***accepted***: 21 February 2025)

Abstract

Information security has become an important issue in the digital era due to increased cyber threats and data leaks. This study analyzes the influence of Organizational Culture, Risk Propensity, and Security Readiness on Organizational Security Performance, with Top Management Support as the moderation variable. This study uses a quantitative method with a survey approach and is analyzed using SPSS software for regression, mediation, and moderation tests. The results show that Organizational Culture, Risk Propensity, and Security Readiness have a significant influence on Organizational Security Performance. Security Readiness is proven to be a mediating variable that strengthens the relationship between Organizational Culture and Risk Propensity to organizational security performance. In addition, Top Management Support acts as a moderator that strengthens the relationship between independent variables and Organizational Security Performance. This research contributes by integrating Security Readiness as a mediator and Top Management Support as a moderator in the information security framework. These findings highlight the importance of a holistic approach that includes organizational culture, risk behavior, security readiness, and top management support to improve information security resilience amid the challenges of the digital age and the result can be a recommendation for the government and private sectors.

Keywords: organizational culture, risk propensity, security readiness, organization security performance

1 Introduction

Information security has emerged as a critical concern for organizations and individuals due to the escalating occurrence of cybercrimes. These crimes include unauthorized access and privacy violations within financial institutions, manufacturing sectors, educational establishments, and governmental organizations. For instance, data breaches at banks and unauthorized access to sensitive information on governmental websites have resulted in significant financial and reputational damage. Consequently, the importance of robust information security mechanisms has never been more crucial, especially as organizations face increasingly sophisticated cyber threats in the digital age. The rapid advancements in digital technology have revolutionized market trends, offering organizations opportunities to enhance product quality and operational efficiency. However, this evolution also poses considerable risks to the security of organizational assets [1]. Extensive research has been conducted to understand the multifaceted nature of information security. Notably, [2] emphasizes the dual focus on “individual and organizational factors” as crucial elements influencing information security. This perspective is reinforced by [3], which stresses the importance of a well-structured information security policy that encompasses both organizational directives and individual responsibilities.

Digital transformation not only provides growth opportunities but also challenges organizations to adapt to emerging threats. Information security management, therefore, becomes vital in safeguarding information confidentiality, integrity, and availability through a comprehensive framework of security controls [3]. Furthermore, [4] emphasizes the escalating need for organizations to fortify their defenses against increasingly sophisticated cyberattacks. Organizational culture has been identified as a significant determinant of information security performance. A strong security culture fosters an environment where information security becomes an intrinsic organizational value, leading to enhanced security performance [3]. Of the many cases related to information security, both in the external and internal environment of the organization, it poses a very crucial threat to the organization in supporting its business processes, so special attention is needed in handling information security so that the organization can minimize the risks that may arise from these information security threats. As digital threats become more sophisticated and spread, the need for organizations to strengthen their defenses against cyberattacks has never been greater [4].

Organizational culture has been identified as a significant determinant of information security performance. A strong security culture fosters an environment where information security becomes an intrinsic organizational value, leading to enhanced security performance [3]. Additionally, risk propensity, which reflects an individual’s tendency towards risk-taking or risk aversion, significantly influences security behaviors [5][6]. Despite the critical roles of security culture and risk propensity, there is a notable scarcity of studies exploring the combined effects of these factors on organizational security performance, thus presenting a clear research gap. Despite extensive research on information security management, organizations continue to face substantial threats, both internally and externally, which jeopardize business continuity. As digital threats become more advanced and pervasive, organizations must enhance their defensive strategies to minimize the risks associated with these security threats [4]. Information security management aims to protect organizations from potential losses by safeguarding information confidentiality, integrity, and availability [3].

Change management also plays an active role in the sustainability of the organization. However, for organizations in the future, change is not only limited to adaptation because innovative thinking is also one of the factors in organizational sustainability [5]. However, the success of information security depends not only on technological solutions but also on organizational readiness and human behaviors. Organizational culture significantly influences security performance by shaping employees' security attitudes and behaviors [3]. Simultaneously, individual risk propensity affects decision-making processes in security contexts [6][7]. Despite recognizing the importance of these factors, previous research has inadequately explored their integrated impact on security readiness and performance, especially within the context of digital transformation.

This study aims to investigate the influence of organizational security culture and individual risk propensity on organizational security performance, mediated by security readiness. Additionally, it examines the moderating role of top management support in strengthening the relationship between security culture, risk propensity, security readiness, and security performance. This approach provides a holistic understanding of how organizational and individual factors interact to enhance information security performance [6]. The tendency to take risks is common to any individual's orientation towards risk-taking or risk aversion [7]. The research [8] explains that there are still very few studies that discuss the relationship between security culture issues and risk trends in information security, so in this case, there is a gap in this study, so it is necessary to conduct an analysis related to the influence of security culture issues based on organizational factors and risk trends on individual factors in information security. Top management support is one of the success factors in information security [9].

A critical research gap exists in the integrated analysis of security culture and risk propensity within the context of organizational security performance. Although prior studies have highlighted the significance of security culture [3] and risk propensity [6][7], limited research explores their combined influence on security readiness and organizational security performance. Furthermore, the moderating effect of top management support on these relationships remains underexplored. This gap underscores the need for a comprehensive investigation to understand the interplay of organizational and individual factors in enhancing information security performance. This study introduces a novel framework that examines the combined effects of security culture and risk propensity on security readiness and organizational security performance. It uniquely explores the moderating role of top management support, providing a more nuanced understanding of how leadership influences information security outcomes. Additionally, by focusing on the digital transformation context, this research offers fresh insights into the evolving challenges and opportunities in organizational information security management.

In the explanation above, it is concluded that the formulation of the problem in this study [10] is whether the security culture and risk tendency influence the security performance of the organization through security readiness. [11] how does the influence of security readiness on the security performance of the organization? Does the support of top management moderate the impact of security culture and risk tendencies on security readiness? [12] does the support of top management moderate the influence of security readiness on security performance organization?

This research makes several significant contributions to the field of information security management by advancing both theoretical and practical understanding of the factors influencing organizational security performance. Firstly, it provides a comprehensive framework that integrates organizational culture, individual risk propensity, and top management support to examine their combined impact on security readiness and organizational security performance. By doing so, this study not only highlights the importance of security culture and risk propensity as individual drivers but also explores how their interaction influences security outcomes, offering a more nuanced perspective on information security performance drivers. This integrated approach addresses the fragmented understanding present in existing literature, thereby bridging a crucial research gap and contributing to the development of a more holistic security management model.

Additionally, this research underscores the critical importance of leadership commitment by examining the moderating role of top management support in influencing the relationship between security culture, risk propensity, security readiness, and organizational security performance. The results demonstrate that top management support not only strengthens the organization's security culture but also enhances security readiness by providing strategic direction, resource allocation, and motivational reinforcement. This finding reinforces the view that effective information security management is not solely dependent on technological controls but also relies on strong leadership and organizational commitment.

The research method carried out in this study uses a quantitative method using data analysis techniques using SEM-PLS. The limitation of the problem in this study is that data collection is only carried out in certain organizations, such as organizations engaged in education, manufacturing, and services. The research results are expected to provide contributions and recommendations of the latest literature that connect organizational and individual factors in looking at the readiness and performance of organizational security in Indonesia and how the role of top management can influence the success of information security.

2 Literature Review

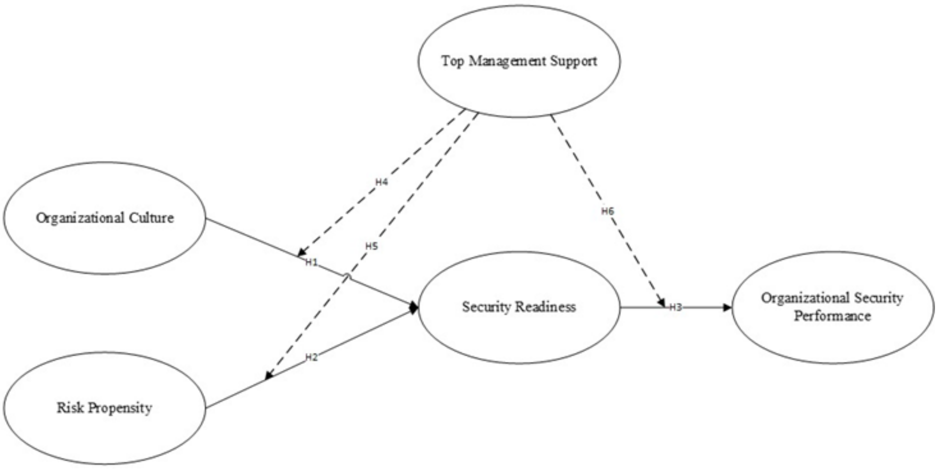


Figure 1. Hypothesis model

Source: Researcher

Figure 1 explains the conceptual framework of the model to be studied so that it will produce an in-depth analysis of the available hypothesis designs**.** The hypothesis formulation will be explained below based on a review of previous research.

2.1 Organizational Culture Towards Organizational Security Performance

Organizational culture significantly influences an organization's security performance, as supported by various previous studies. A strong organizational culture, characterized by leadership support and effective communication, positively contributes to security practices and improves the overall security performance of the organization [10], [11]. For example, a strong security culture can strengthen an organization's resilience to cyber threats, such as ransomware attacks, through the implementation of better security policies and employee behavior that aligns with organizational goals[10], [11], [13]. Additionally, research shows that organizational culture directly influences performance outcomes, including security behavior and compliance with information security policies. The role of employee behavior is a key element of organizational culture and information security. A positive organizational culture can encourage employee behavior that supports security practices, thereby strengthening the organization's security posture. [11], [12], [14]. This is in line with findings [15], [16], [17] that emphasize the importance of building a safety culture that can positively influence employee actions. In this context, organizations that have a strong security culture tend to show better compliance with security policies and risk management. Support from top management is an important predictor factor in creating an effective security culture. Organizations that have strong leadership support can build a better security culture, which in turn improves the organization's security performance. [18]. This support not only influences the implementation of security policies but also builds trust among employees to comply with existing policies and procedures. Empirical research also shows that the relationship between organizational culture and security performance is mediated by employee attitudes and behaviors, further underscoring the importance of organizational culture in improving security performance. There are several reasons why organizational culture may not always have a significant impact on security performance. For example, inefficient training programs and a lack of awareness and compliance among certain employees can be a hindrance. In addition, the overly flexible nature of organizational culture, such as orientation to innovation without adequate control, can reduce the effectiveness of the implementation of information security management principles [13].

H1: Organizational culture has a direct and significant influence on an organization's security performance.

2.2 Risk Propensity to Organizational Security Performance

Risk propensity has become one of the factors that attract attention in research related to organizational security performance. Risk propensity indicates the extent to which an individual or organization is willing to take risks in a variety of situations, including in the context of information security. Previous research has shown that risk trends can have a significant impact on pro-social behaviors, such as pro-social rule-breaking behaviors and organizational citizenship behaviors. Both of these behaviors, influenced by the courage to take risks, can support the implementation of more effective information security policies and procedures. In addition, individuals with high-risk propensity tend to have a better awareness of technological threats, which ultimately influences their behavior to avoid such risks and improve the security posture of the organization [19]. Findings [20], and [21] significantly suggest that risk trends can indirectly affect security performance through increased engagement in security training and knowledge sharing among employees. Security training and awareness-raising programs have been shown to improve overall information security performance. [19], [21], [22]. In this context, risk tendencies motivate employees to be more actively involved in the effort, which in turn strengthens the organization's security culture and the effectiveness of risk management. Some findings suggest an insignificant influence of risk bias on the security performance of organizations directly [22], [23]. This relationship is often mediated by other factors, such as security training programs, employee awareness levels, and compliance with security policies. In addition, managerial perceptions of security risks, which are influenced by risk tendencies, are not always in line with the actual security conditions of the organization. This discrepancy can create gaps in information security management, thereby reducing the effectiveness of risk tendencies in directly improving security performance.

H2: Risk Propensity Affects Organizational Security Performance.

2.3 Security Readiness for Organizational Security Performance

Security readiness plays a crucial role in improving an organization's security performance, as shown by various studies. Findings [24], and [25] significantly show that good security readiness significantly improves an organization's security performance, which in turn has a positive impact on both financial and non-financial performance. A study conducted in Bahrain, for example, found that cybersecurity readiness has a direct impact on improving organizational security performance, including effectiveness in risk management and strengthening information security governance [1], [24], [26]. These findings reinforce the argument that optimal security readiness can provide real benefits to organizations, both in the form of information asset protection and overall increased competitiveness. Key factors that support security readiness, such as security training, knowledge sharing, security education, and security visibility, are also identified as critical elements in improving information security performance. In the context of manufacturing companies in the UK, for example, continuous training and knowledge sharing among employees have been shown to significantly improve the security posture of the organization. Top management support also plays a crucial role, where organizations with supportive leadership tend to have better security readiness, which then translates into improved security performance. Some findings suggest that the influence of security readiness on an organization's security performance is not always significant [1], [17], [27], [28]. For example, some studies have not found a clear relationship between strategic decision-making and the successful implementation of information security strategies. In addition, the lack of comprehensive research on the factors that affect security readiness holistically is an obstacle to understanding its impact thoroughly. Other factors such as stress felt by employees due to the complexity of security requirements can also lead to non-compliance, which ultimately reduces the effectiveness of security readiness in improving the security performance of the organization.

H3: Security Readiness Affects Organizational Security Performance.

2.4 Security Readiness as Mediation

Security readiness has an important role as a mediating variable in research related to information security and organizational effectiveness. As a mediating variable, security readiness bridges the influence of independent variables on dependent variables, thus providing a deeper understanding of the relationship between the two variables[6], [29], [30]. In this context, security readiness can mediate the relationship between factors such as strategic vigilance and organizational effectiveness, amplifying the impact of strategic vigilance on the overall performance of the organization [9], [31], [32]. Previous research has shown that security readiness affects employee security behavior, where information security awareness acts as an important component in shaping compliance with information security policies [33], [34]. This awareness, mediated by security readiness, increases employees' willingness to comply with security policies and procedures, thereby strengthening the security culture within the organization. In addition, supportive psychological empowerment structures, such as safety training and education, have also been shown to mediate the relationship between structural empowerment and employees' intentions to comply with security policies. This emphasizes the importance of security readiness as a key factor in creating a secure organizational environment [1], [35], [36]

2.5 Top Management Support as a Moderation

Top management support plays an important role in various organizational processes and serves as a significant moderating factor in various contexts. In information systems, top management support significantly influences the performance of information systems projects by moderating the relationship between managerial control and project performance. Previous research has shown that top management support strengthens the effectiveness of outcome control and clan control, which directly impacts the success of the project. In addition, the role of certain executives in providing managerial support has proven to be a key factor in the successful implementation of information systems. In the context of managing the management accounting system in SMEs, top management support improves the utilization of the system by improving user satisfaction and providing adequate training. These factors contribute to a more effective and efficient decision-making process. In addition, top management support also has a positive impact on knowledge sharing and employee performance, by acting as a mediator that connects the two aspects. This emphasizes the importance of the role of top management in creating a collaborative work environment and supporting the development of employee knowledge. In the public sector, the various dimensions of top management support have been shown to have a significant positive influence on project performance. Research shows that projects managed with the full support of top management have a higher success rate compared to projects that receive less attention from top management. In technology adoption, such as cloud computing, top management support serves as a mediator that strengthens the relationship between innovation characteristics, technological context, organization, and environment and the rate of technology adoption among SMEs. However, challenges in the implementation of top management support often arise. One of the main obstacles is the difficulty of obtaining full support from top management due to the many competing priorities in the organization. Low levels of support are often caused by a lack of reliable knowledge of the specific behaviors underlying top management support. Nonetheless, research also shows that top management leadership styles and the types of behaviors applied contribute significantly to the success of organizational strategies, particularly in information systems strategic projects.

H4- H6: Top Management Support Moderating Organizational Culture, Risk Propensity, and Security Readiness for Organizational Culture.

3 Research Method

This research was conducted on organizations engaged in education, manufacturing, and services to see how the results of the analysis related to the success of their information security. The research method used uses a quantitative research method that uses the darmed linear regression test as a data analysis technique using SPSS analysis tools.

3.1 Sample and Data

Data collection was carried out using a questionnaire to examine the results of the hypothesis model. The sample used in this study is 100 respondents with the criteria that will be explained in Table 1.

Table 1. Characteristic respondents

	Gender	Age	Education	Position	Working Experience
Characteristic	Male Female	20-30 31-40 41-50 More than 50	Senior High School Diploma Graduate Post Graduate PhD	Operational Management Middle Management Top Management	Less than 1 year 1-5 years 6-10 years More than 10 years

3.2 Measures

The measurements carried out in the study used a survey technique with a questionnaire as a data collection tool. The measurement scale was carried out using a Likert scale with categories (STS=Strongly Disagree), (TS= Disagree), (S= Agree), (CS= Somewhat Agree), and (SS=Strongly Agree). The explanation of each variable in this study will be explained in Table 2. The variables in this study consist of independent variables, namely organizational culture and risk tendencies, and dependent variables, namely organizational security performance. Intervening and moderation variables were also carried out in this study. The intervening variable is security readiness and the moderation variable is top management support serves to see how security readiness is an intervening variable and top management support is a moderation variable.

Table 2. Definitions of variables

Variable	Definitions	Source
Organizational Culture	The shared values and beliefs in an organization regarding information security issues.	[1][37][5][38]

Top Management Support	The commitment and support provided by senior executives in the organization to maintain and enhance information security issues.	[1], [20]
Risk Propensity	Risk-taking tendency or willingness to take risks, is defined as an individual's current tendency towards taking or avoiding risks.	[39][6], [40]
Security Readiness	The organization's level of awareness, preparedness, and commitment to preventing and combating information security issues	[1]
Organizational Security Performance	The security benefits anticipated by organizations due to readiness to combat cyber-attacks on information security issues	[1]

After defining what variables are used in this study, the next step is to define the measurement indicators on each variable and then make a questionnaire for each respondent. The following are the variable indicators used in this study described in Table 3.

Table 3. Indicators of variables

Variable	Indicators	Source
Organizational Culture	a. Our organization emphasizes security knowledge sharing across different organizational units.	[1][37]
	b. Our organization emphasizes sharing information security issues incidents.	
	c. Our organization emphasizes sharing information security issues and failures.	
Top Management Support	a. Top management considers that information security issues play a strategically important role.	[1], [20]
	b. Top management demonstrates a commitment to information security issues by developing policies/guidelines.	
	c. Top management assumes responsibility for information security issues performance.	
	d. Top management gets personally involved in matters related to information security issues within the organization.	
	e. Top management sponsors information security issues initiatives.	
	f. Top management supports information security issues improvement processes.	
	g. Top management articulates a vision for improving the organization's information security issues in the future.	
Risk Propensity	a. Taking risks is an important part of my life	[39]
	b. I commonly make risky decisions	
	c. I am a believer in taking chances	
Security Readiness	a. Our organization is aware of and committed to using advanced methods for vulnerability assessment.	[1]
	b. Our organization is committed to controlling computer ports that could be used for attacks.	
	c. Our organization is committed to ensuring that system vulnerabilities are within accepted risks.	
Organizational Security Performance	a. The number of data breaches in our organization is decreasing over time.	[1]
	b. The internal processes of our organization are becoming more secure.	

Variable	Indicators	Source
	c. Our organization has a reliable system with adequate capabilities and capacities for information processing.	

4 Results and Analysis

The following section presents the results of data analysis collected from 150 respondents spread across 10 companies in East Java in the service sector and the manufacturing sector that have implemented system security performance in their organizations. The first sub-section explains the results of the validity test and the reality test. Second, explain the results of the multiple linear regression analysis test between independent to dependent variables. Third, explain the results of the mediation analysis test. Fourth, explain the results of the moderator analysis test.

4.1 Validity and Reliability

In this sub-chapter, a validity and reliability test is carried out to ensure that the research instruments used are able to measure the variables in question consistently and accurately. Validity measures the extent to which indicators reflect the variables they represent, while reliability evaluates the internal consistency of each variable in the research instrument.

Table 4. Variable validity test

Variables	Indicator	Sig.	Result
Organizational Culture	OC1	,000	Valid
	OC2	,000	Valid
	OC3	,000	Valid
Risk Propensity	RP1	,000	Valid
	RP2	,000	Valid
	RP3	,000	Valid
Security Readiness	SR1	,000	Valid
	SR2	,000	Valid
	SR3	,000	Valid
Organizational Security Performance	OSP1	,000	Valid
	OSP2	,000	Valid
	OSP3	,000	Valid
Top Management Support	TMS1	,000	Valid
	TMS2	,000	Valid
	TMS3	,000	Valid
	TMS4	,000	Valid
	TMS5	,000	Valid
	TMS6	,000	Valid
	TMS7	,000	Valid
		,000	

Based on the results from Table 4 of the validity test on each variable in each indicator, it can be determined that the significance value of P-Value <0.05, where all indicators in each variable can be said to be valid and significant.

Table 5. Variable reliability test

Variable	Cronbach's Alpha
Organizational Culture	,847
Risk Propensity	,809
Security Readiness	,805
Organizational Security Performance	,805
Top Management Support	,715

The results in Table 5 of the reliability test showed that all variables had a Cronbach's Alpha value above 0.7, which indicates good consistency. Organizational Culture has a reliability value of 0.847, Risk Propensity of 0.809, Security Readiness of 0.805, Organizational Security Performance of 0.805, and Top Management Support of 0.715, all of which are in the reliable category to support further analysis.

4.2 Multiple Linear Regression Test

This sub-chapter discusses the results of multiple linear regression analyses used to test the influence of independent variables on dependent variables simultaneously. This analysis aims to understand the extent to which independent variables, such as Organizational Culture, Risk Propensity, and Security Readiness, affect Organizational Security Performance. With this approach, research can identify the direct relationship between these variables as well as the significant contribution of each variable to the security performance of the organization.

Table 6. Multiple linear regression test organizational security performance

Type	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
	B	Std. Error	Beta			Tolerance	VIF
(Constant)	13,097	1,894		6,915	,000		
Organizational Culture	,192	,065	,231	2,954	,004	,699	1,431
Risk Propensity	,246	,078	,251	3,146	,002	,672	1,489
Security Readiness	,301	,094	,266	3,217	,002	,628	1,592

The results from Table 6 of the regression analysis show that the variables Organizational Culture, Risk Propensity, and Security Readiness significantly affect Organizational Security Performance. Organizational Culture has a regression coefficient value of 0.192 (β = 0.231, p = 0.004), which shows that organizational culture has a positive and significant influence on organizational security performance. Risk Propensity also has a positive influence with a regression coefficient value of 0.246 (β = 0.251, p = 0.002), which indicates that employee risk tendency also contributes significantly to improving organizational security performance. In addition, Security Readiness had the greatest positive influence with a regression coefficient of 0.301 (β = 0.266, p = 0.002), indicating that security readiness is a very important factor in supporting organizational security performance. All independent variables have a Tolerance value above 0.1 and a VIF below 10, indicating that there is no multicollinearity problem in this model. This confirms that the hypothesis proposed is accepted and each independent variable makes a significant contribution to the security performance of the organization.

Table 7. Multiple linear regression test security readiness

Type	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
	B	Std. Error	Beta			Tolerance	VIF
(Constant)	18.298	.714		25.67	.000		
Organizational Culture	.243	.054	.332	4.534	.000	.797	1.255
Risk Propensity	.331	.063	.383	5.228	.000	.797	1.255
(Constant)	18.298	.714		25.67	.000		

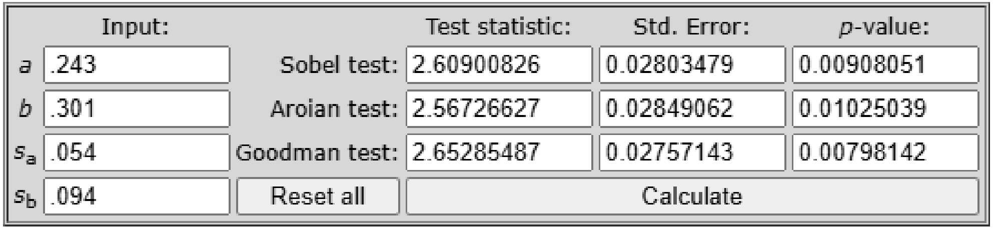
The results from Table 7 of the regression analysis show that the variables of Organizational Culture and Risk Propensity significantly affect Security Readiness. Organizational Culture has a regression coefficient of 0.243 (β = 0.332, p = 0.000), which shows that organizational culture has a positive and significant influence on security readiness. In addition, Risk Propensity showed a greater positive influence with a regression coefficient of 0.331 (β = 0.383, p = 0.000), indicating that risk propensity also contributed significantly to the improvement of security readiness. The Tolerance value of 0.797 and VIF of 1.255 for both independent variables indicates the absence of multicollinearity problems in

ISSN:2302-8149
e-ISSN:2540-9719

this model. Thus, these results support the hypothesis that organizational culture and risk propensity have a significant influence on security readiness.

4.3 Mediating Variable Test

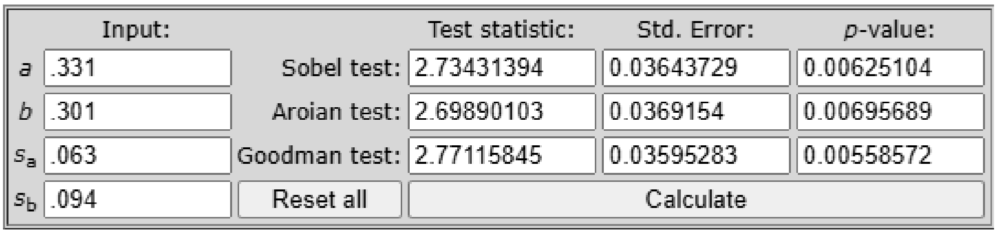
This sub-chapter explains the results of the mediator variable test to determine the role of Security Readiness as a mediating variable in the relationship between independent variables, such as Organizational Culture and Risk Propensity, and the dependent variable, namely Organizational Security Performance. This analysis aims to identify whether the influence of independent variables on dependent variables is amplified through the existence of mediating variables, as well as to understand the underlying mechanisms of the relationship between these variables.



Input:			Test statistic:	Std. Error:	*p*-value:
a	.243	Sobel test:	2.60900826	0.02803479	0.00908051
b	.301	Aroian test:	2.56726627	0.02849062	0.01025039
s_a	.054	Goodman test:	2.65285487	0.02757143	0.00798142
s_b	.094	Reset all	Calculate		

Figure 1. Test the influence of organizational culture on organizational security performance through security readiness. source: quantity

The results of the Sobel Test in Figure 2 show that the indirect influence of Organizational Culture on Organizational Security Performance through Security Readiness is significant. The Sobel statistical test value of 2.609 with a p-value of 0.009 (< 0.05) indicates that the influence of Security Readiness mediation in the relationship between Organizational Culture and Organizational Security Performance is statistically significant. This shows that Organizational Culture not only has a direct influence on Organizational Security Performance but also provides an indirect influence that is strengthened by Security Readiness as a mediator. Thus, the hypothesis that Security Readiness mediates the relationship between Organizational Culture and Organizational Security Performance is acceptable.



Input:			Test statistic:	Std. Error:	*p*-value:
a	.331	Sobel test:	2.73431394	0.03643729	0.00625104
b	.301	Aroian test:	2.69890103	0.0369154	0.00695689
s_a	.063	Goodman test:	2.77115845	0.03595283	0.00558572
s_b	.094	Reset all	Calculate		

Figure 2. Test the influence of risk propensity on organizational security performance through security readiness. source: quantspy

The results of the Sobel Test shown in Figure 3 show that the indirect influence of Risk Propensity on Organizational Security Performance through Security Readiness is significant. The Sobel statistical test value of 2.734 with a p-value of 0.006 (< 0.05) shows that the effect of Security Readiness mediation in the relationship between Risk Propensity and Organizational Security Performance is statistically significant. This indicates that Risk Propensity not only has a direct influence on Organizational Security Performance but also has an indirect influence that is strengthened by Security Readiness as a mediator. Thus, the hypothesis that Security Readiness mediates the relationship between Risk Propensity and Organizational Security Performance is acceptable.

4.4. Moderating Variable Test

Table 8. Moderate variable test

Type	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
	B	Std. Error	Beta			Tolerance	VIF
(Constant)	13.612	1.178		11.54	.000		
Moderation of Top Management Support	.006	.002	.265	3.341	.001	.665	1.503

with Organizational Culture							
Moderation of Top Management Support with Risk Propensity	.008	.002	.296	3.685	.000	.650	1.538
Moderation of Top Management Support with Security Readiness	.009	.002	.268	4.009	.000	.937	1.067

The results of regression analysis show in Table 8 that Top Management Support plays a significant role as a moderator in the relationship between Organizational Culture, Risk Propensity, and Security Readiness to Organizational Security Performance. The interaction between Top Management Support and Organizational Culture has a regression coefficient of 0.006 ($\beta = 0.265$, $p = 0.001$), which shows that top management support significantly strengthens the influence of organizational culture on organizational security performance. In addition, the interaction between Top Management Support and Risk Propensity resulted in a regression coefficient of 0.008 ($\beta = 0.296$, $p = 0.000$), which shows that top management support also strengthens the influence of risk propensity on the security performance of the organization. The same is true for the interaction between Top Management Support and Security Readiness, which has a regression coefficient of 0.009 ($\beta = 0.268$, $p = 0.000$), indicating that top management support strengthens the relationship between security readiness and security performance of the organization. A high tolerance value (≥ 0.650) and a low VIF (< 10) indicate the absence of multicollinearity problems in the model, so the analysis results are reliable. Thus, it can be concluded that Top Management Support not only provides direct support but also significantly strengthens the relationship between independent variables and organizational security performance, making it a key element in improving the effectiveness of information security management.

4.5 Discussion

This study makes significant contributions to the field of information security management by advancing both theoretical and practical understanding of how Organizational Culture, Risk Propensity, Security Readiness, and Top Management Support influence organizational security performance. Organizational culture plays a pivotal role in shaping employee behaviors toward information security policies. According to Schein's Organizational Culture Theory, the shared values, beliefs, and norms within an organization profoundly influence employees' security compliance behaviors. This study aligns with previous research that demonstrates a positive security culture enhances employee adherence to security policies, ultimately leading to improved organizational security performance [3], [4]. However, unlike prior studies that examined security culture and security readiness in isolation, this research provides new insights into the dynamic interplay between these constructs. Specifically, it reveals that a proactive security culture not only fosters compliance but also significantly enhances an organization’s capacity to anticipate and mitigate security threats through improved security readiness [1]. This nuanced understanding bridges the gap identified in previous research, which called for integrated frameworks linking cultural factors with security preparedness [2], [4]. Therefore, this study contributes to a more comprehensive model of information security management by demonstrating that security culture influences security performance indirectly through security readiness, a relationship that has been underexplored in the existing literature [3].

This study reveals that Security Readiness plays a significant role as a mediating variable in bridging the influence of organizational culture and risk tendencies on organizational security performance. These findings not only expand the information security literature but also provide practical insights for organizations to integrate these elements into more effective security policies and strategies. A holistic approach that includes organizational culture, security readiness, risk propensity, and top management support is relevant to face the increasingly complex challenges of information security in the digital age. In addition to organizational culture, Risk Propensity is identified as a crucial factor influencing security behaviors. Rooted in Organizational Behaviour Theory, risk propensity refers to an individual's tendency towards risk-seeking or risk-averse behaviors, which in turn shape strategic decision-making processes. This study supports the findings of previous research, which argued that risk propensity significantly affects organizational success, particularly in uncertain and dynamic environments [6]. In the context of information security, this research reveals that individuals with a balanced risk propensity demonstrate greater adaptability and innovativeness in identifying and responding to security threats. However, unlike previous studies that viewed risk propensity as a static trait, this research introduces a novel perspective by conceptualizing it as a dynamic and contextual variable influenced by organizational culture and leadership support [7]. This approach challenges the traditional understanding presented in earlier studies and demonstrates that risk propensity interacts with security culture and top management support, thereby influencing security readiness through a continuous feedback loop. This finding presents a new theoretical proposition by positioning risk propensity as a contextual and adaptive factor in information security management, thereby contributing to a more flexible and situationally responsive security framework.

Security Readiness is another key component explored in this study. Defined within the framework of Organizational Readiness Theory, security readiness encompasses an organization's ability to recognize security risks, foster employee awareness, and proactively implement mitigation strategies. This research confirms that security readiness is a strategic mediator that translates organizational culture and individual risk orientations into improved security performance. This aligns with findings that emphasize the importance of security readiness and ineffective policy implementation [1]. However, unlike previous studies that treated security readiness as an outcome variable, this study demonstrates its mediating role, thereby offering a more sophisticated understanding of its strategic function within the security management process. By establishing security readiness as a bridge between organizational culture, risk propensity, and security performance, this study addresses the theoretical gap noted in prior research, which called for more comprehensive models exploring mediating effects in security behaviors frameworks [5], [8].

Top Management Support is also a critical factor examined in this study. Grounded in Contingency Theory, top management support emphasizes the strategic importance of leadership in influencing organizational effectiveness. Prior research demonstrated that strategic leadership significantly impacts security policy adoption [9]. This study reinforces this perspective by empirically validating the moderating role of top management support in amplifying the influence of organizational culture and risk propensity on security readiness and performance. Notably, this research diverges from traditional approaches by examining top management support as a moderator rather than a direct determinant of security performance. This nuanced perspective reveals that top management support enhances the effectiveness of security culture and risk propensity by providing strategic direction, resource allocation, and motivational reinforcement. These findings challenge earlier models that emphasized direct leadership influence [9]. By highlighting its moderating role, this study offers a strategic perspective on leadership's contribution to building organizational security resilience.

This research makes distinct contributions by offering a more integrated and comprehensive framework for understanding information security performance drivers. Unlike previous studies that analyzed organizational culture, risk propensity, and top management support independently, this research integrates these factors to provide a holistic perspective on security performance. This approach not only bridges theoretical gaps but also advances the academic discourse by introducing and empirically validating novel mediating and moderating relationships, particularly the role of security readiness as a mediator and top management support as a moderator [1], [9]. Furthermore, this study challenges static models of risk propensity by conceptualizing it as a contextual and dynamic variable influenced by cultural and leadership factors. This innovative approach contributes to a more adaptive and responsive security behaviors framework.

The findings of this study also have significant practical implications. By demonstrating the importance of balancing technological solutions with human behavioral factors, this research provides actionable insights for organizational leaders and policymakers to enhance security readiness and performance. Specifically, it underscores the necessity of fostering a security-conscious culture, understanding employees' risk orientations, and leveraging strategic leadership support. This balanced approach offers a more sustainable security management strategy, particularly in the context of digital transformation, where human factors are critical to addressing emerging security challenges [1].

5 Conclusion

This study makes significant theoretical and practical contributions to the field of information security management by offering a comprehensive model that integrates Security Readiness as a mediator and Top Management Support as a moderator. This approach provides a novel perspective on how the dynamic interplay between Organizational Culture, Risk Propensity, and Strategic Leadership Support influences organizational security performance. The findings underscore the importance of cultivating a proactive security culture, understanding individual risk orientations, and leveraging top management support to enhance security readiness and overall security performance. By empirically validating the mediating role of security readiness and the moderating effect of top management support, this study advances the current understanding of information security behavior, providing a more nuanced and holistic analytical framework for assessing security performance drivers.

One of the key contributions of this research lies in bridging the gap in the existing literature by simultaneously examining mediation and moderation mechanisms within a unified model. Unlike prior studies that explored these constructs in isolation, this study presents an integrated framework that elucidates the complex interdependencies between organizational and individual factors influencing security performance. This innovative approach not only enhances theoretical understanding but also offers strategic insights for practitioners to develop adaptive and sustainable information security policies. Specifically, the findings suggest that organizations can significantly improve their security posture by fostering a security-conscious culture, strategically managing individual risk tendencies, and ensuring active top management support. This balanced approach aligns with the evolving challenges of the digital era, where human behavioral factors play a critical role in managing information security risks.

Despite its valuable contributions, this study has several limitations that must be acknowledged. First, the research data was collected from specific sectors, limiting the generalizability of the findings across different industries and geographic locations. Future research should extend the scope to diverse organizational contexts and cultural settings to enhance external validity. Second, the study employed a quantitative approach using SEM-PLS to analyze the relationships between variables. Although effective in testing hypothesized relationships, this approach lacks qualitative insights into the underlying motivations and behavioral dynamics influencing security practices. To address this limitation, future studies could adopt qualitative methods, such as case studies, interviews, or focus groups, to explore the psychological and cultural nuances of information security behavior. Additionally, employing a longitudinal research design could provide a more dynamic understanding of how organizational culture, risk propensity, and top management support evolve and influence security readiness and performance.

The novelty of this study lies in its integrated examination of security readiness as a strategic mediator and top management support as a strategic moderator, highlighting their synergistic effects on information security performance. This research contributes to the theoretical advancement of information security management by demonstrating that security readiness not only directly enhances security performance but also mediates the influence of organizational culture and risk propensity. Furthermore, it shows that top management support strengthens the impact of security culture and risk propensity on security readiness, underscoring the strategic role of leadership commitment in fostering a robust security culture. These findings offer a new lens through which to view the interactions between organizational, individual, and strategic factors, thereby providing a more comprehensive understanding of the mechanisms driving information security effectiveness.

In conclusion, this study not only contributes to the academic literature by addressing theoretical gaps but also offers practical recommendations for organizations aiming to improve their security performance. By integrating organizational culture, risk propensity, security readiness, and top management support into a unified model, this research provides strategic insights for developing adaptive, sustainable, and holistic information security policies. The findings emphasize the need for a balanced approach that combines technological solutions with human behavioral factors, thereby enhancing organizational resilience against increasingly sophisticated digital threats. As digital transformation continues to reshape the security landscape, this study serves as a strategic guide for practitioners, policymakers, and academics to navigate the complexities of information security management effectively. Future research should build on these insights by exploring cross-cultural contexts, longitudinal effects, and qualitative dimensions to provide a richer, more dynamic understanding of information security behavior.

Reference

[1] S. Hasan, M. Ali, S. Kurnia, and R. Thurasamy, "*Evaluating the Cyber Security Readiness of Organizations and its Influence on Performance*," *Journal of Information Security and Applications*, vol. 58, May 2021, doi: 10.1016/j.jisa.2020.102726.

[2] A. Tsohou, M. Karyda, and S. Kokolakis, "*Analyzing the Role of Cognitive and Cultural Biases in the Internalization of Information Security Policies*: *Recommendations for Information Security Awareness Programs*," *Comput Secur*, vol. 52, pp. 128–141, Jul. 2015, doi: 10.1016/j.cose.2015.04.006.

[3] P. K. Sari *et al.*, "*Information Security Cultural Differences among Health Care Facilities in Indonesia*," *Heliyon*, vol. 7, no. 6, Jun. 2021, doi: 10.1016/j.heliyon.2021.e07248.

[4] A. Zanke, T. Weber, P. Dornheim, and M. Engel, "*Assessing Information Security Culture: A Mixed-Methods Approach to Navigating Challenges in International Corporate IT Departments*," *Comput Secur*, vol. 144, Sep. 2024, doi: 10.1016/j.cose.2024.103938.

[5] A. H. Olafsen, E. R. Nilsen, S. Smedsrud, and D. Kamaric, "*Sustainable Development Through Commitment to Organizational Change: The Implications of Organizational Culture and Individual Readiness for Change,*" *Journal of Workplace Learning*, vol. 33, no. 3, pp. 180–196, 2020, doi: 10.1108/JWL-05-2020-0093.

[6] K. U. Islam, S. A. Bhat, U. M. Lone, M. A. Darzi, and I. A. Malik, "*Financial Risk Propensity and Investment Decisions: an Empirical Analysis using Behavioral Biases*," *IIMB Management Review*, Jun. 2024, doi: 10.1016/j.iimb.2024.06.004.

[7] S. Combrink and C. Lew, "*Potential Underdog Bias, Overconfidence and Risk Propensity in Investor Decision-making Behavior*," *Journal of Behavioral Finance*, vol. 21, no. 4, pp. 337–351, Oct. 2020, doi: 10.1080/15427560.2019.1692843.

[8] M. H. Shah, H. R. Peikari, and N. M. Yasin, "*The Determinants of Individuals' Perceived E-Security: Evidence from Malaysia*," *Int J Inf Manage*, vol. 34, no. 1, pp. 48–57, 2014, doi: 10.1016/j.ijinfomgt.2013.10.001.

[9] M. Zhang *et al.*, "*Top of the Tide: Nexus between Organization Agility, Digital Capability and Top Management Support in SME Digital Transformation*," *Heliyon*, vol. 10, no. 10, May 2024, doi: 10.1016/j.heliyon.2024.e31579.

[10] C. Alexander and B. Soewito, "*Convolutional Neural Network to Modify the Restoration of a CCTV E-Ticket Image*," *International Journal of Engineering Trends and Technology*, vol. 72, no. 4, pp. 366–377, Apr. 2024, doi: 10.14445/22315381/IJETT-V72I4P136.

[11] V. Kumar, S. Ahmareen, M. Kumar, Y. N. Prajapati, B. Pant, and S. Bohra, *Enhancing OTP Generation Efficiency through Cryptographic Techniques*. in 2023 3rd International *Conference on Advance Computing and Innovative Technologies in Engineering* (ICACITE). *Institute of Electrical and Electronics Engineers Inc.*, 2023. doi: 10.1109/ICACITE57410.2023.10182488.

[12] A. Aljoghaiman and V. P. K. Sundaram, "*Mitigating Ransomware Risks in Manufacturing and the Supply Chain: A Comprehensive Security Framework*," *International Journal of Cyber Criminology*, vol. 17, no. 2, pp. 231–249, Nov. 2023, Accessed: Nov. 25, 2024. [Online]. Available: https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/214

[13] S. E. Chang and C. S. Lin, "*Exploring Organizational Culture for Information Security Management,*" *Industrial Management and Data Systems*, vol. 107, no. 3, pp. 438–458, 2007, doi: 10.1108/02635570710734316.

[14] T. O. Nævestad, J. H. Honerud, and S. F. Meyer, "*Information Security Behaviour in an Organisation Providing Critical Infrastructure*: *A Pre-post Study of Efforts to Improve Information Security Culture*," *SpringerBriefs in Applied Sciences and Technology*, vol. Part F1246, pp. 103–117, 2023, doi: 10.1007/978-3-031-32633-2_10.

ISSN:2302-8149
e-ISSN:2540-9719

[15] Š. Orehek and G. Petrič, "*A Systematic Review of Scales for Measuring Information Security Culture*," *Information and Computer Security*, vol. 29, no. 1, pp. 133–158, 2020, doi: 10.1108/ICS-12-2019-0140/FULL/PDF.

[16] A. da Veiga, L. V. Astakhova, A. Botha, and M. Herselman, "*Defining Organizational Information Security Culture—Perspectives from Academia and Industry*," *Comput Secur*, vol. 92, p. 101713, May 2020, doi: 10.1016/J.COSE.2020.101713.

[17] J. S. Lim, S. Chang, A. Ahmad, and S. Maynard, "*Towards an Organizational Culture Framework for Information Security Practices*," *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions*, pp. 296–315, 2012, doi: 10.4018/978-1-4666-0197-0.CH017.

[18] M. Choi, "*Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing*," *Sustainability 2016, Vol. 8, Page 638*, vol. 8, no. 7, p. 638, Jul. 2016, doi: 10.3390/SU8070638.

[19] L. Alzahrani and K. P. Seth, "*The Impact of Organizational Practices on the Information Security Management Performance*," *Information 2021, Vol. 12, Page 398*, vol. 12, no. 10, p. 398, Sep. 2021, doi: 10.3390/INFO12100398.

[20] X. Zhang and C. H. Huang, "*Investor Characteristics, Intention Toward Socially Responsible Investment (SRI), and SRI behavior in Chinese Stock Market: The Moderating Role of Risk Propensity*," *Heliyon*, vol. 10, no. 14, Jul. 2024, doi: 10.1016/j.heliyon.2024.e34230.

[21] W. Yaokumah, "*Evaluating the Effectiveness of Information Security Governance Practices in Developing Nations: A Case of Ghana*," *Standards and Standardization: Concepts, Methodologies, Tools, and Applications*, pp. 1317–1333, Feb. 2015, doi: 10.4018/978-1-4666-8111-8.CH062.

[22] J. H. Hall, S. Sarkani, and T. A. Mazzuchi, "*Impacts of Organizational Capabilities in Information Security*," *Information Management &amp; Computer Security*, vol. 19, no. 3, pp. 155–176, 2011, Accessed: Nov. 25, 2024. [Online]. Available: https://www.academia.edu/66246228/Impacts_of_Organizational_Capabilities_In_Information_Security

[23] H. Zafar, M. S. Ko, and J. G. Clark, "*Security Risk Management in Healthcare: A Case Study," Communications of the Association for Information Systems*, vol. 34, no. 1, pp. 737–750, 2014, doi: 10.17705/1CAIS.03437.

[24] A. Al-Sharhan, A. Alsaber, Y. Al Khasham, A. Al Kandari, R. Nafea, and P. Setiya, "*The Influence of Governmental Support on Cyber-Security Adoption and Performance: The Mediation of Cyber Security and Technological Readiness*," *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/IJBDCN.341264*, vol. 19, no. 1, pp. 1–16, Jan. 1AD, doi: 10.4018/IJBDCN.341264.

[25] F. M. Kaaffah, Darwan, B. Subaeki, A. B. A. Rahman, K. Manaf, and H. A. Sukardi, "*The Information Security Readiness in Indonesian Government Institution: A Systematic Literature Review*," *International Conference on Telecommunication Systems, Services, and Applications*, 2023, doi: 10.1109/TSSA59948.2023.10366969.

[26] S. Aziz and M. J. Zickar, "*A Cluster Analysis Investigation of Workaholism as a Syndrome*," *J Occup Health Psychol*, vol. 11, no. 1, pp. 52–62, Jan. 2006, doi: 10.1037/1076-8998.11.1.52.

[27] M. Frank and V. Kohn, "*How to Mitigate Security-Related Stress: The Role of Psychological Capital*," *Proceedings of the Annual Hawaii International Conference on System Sciences*, vol. 2020-January, pp. 4538–4547, Jan. 2021, doi: 10.24251/HICSS.2021.550.

[28] S. Kraemer, P. Carayon, and J. Clem, "*Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities*," *Comput Secur*, vol. 28, no. 7, pp. 509–520, Oct. 2009, doi: 10.1016/J.COSE.2009.04.006.

[29] O. Viberg *et al.*, "*Cultural Differences in Students' Privacy Concerns in Learning Analytics Across Germany, South Korea, Spain, Sweden, and the United States*," *Computers in Human Behavior Reports*, vol. 14, p. 100416, May 2024, doi: 10.1016/J.CHBR.2024.100416.

[30] S. Mikuletič, S. Vrhovec, B. Skela-Savič, and B. Žvanut, "*Security and Privacy-Oriented Information Security Culture (ISC): Explaining Unauthorized Access to Healthcare Data by Nursing Employees*," *Comput Secur*, vol. 136, Jan. 2024, doi: 10.1016/j.cose.2023.103489.

[31] X. Zhang and C. H. Huang, "*Investor Characteristics, Intention Toward Socially Responsible Investment (SRI), and Sri Behavior in Chinese Stock Market: The Moderating Role of Risk Propensity*," *Heliyon*, vol. 10, no. 14, p. e34230, Jul. 2024, doi: 10.1016/J.HELIYON.2024.E34230.

[32] A. Zanke, T. Weber, P. Dornheim, and M. Engel, "*Assessing Information Security Culture: A Mixed-Methods Approach To Navigating Challenges In International Corporate It Departments*," *Comput Secur*, vol. 144, p. 103938, Sep. 2024, doi: 10.1016/J.COSE.2024.103938.

[33] S. Sharma and E. Aparicio, "*Organizational and Team Culture as Antecedents of Protection Motivation among It Employees*," *Comput Secur*, vol. 120, p. 102774, Sep. 2022, doi: 10.1016/J.COSE.2022.102774.

[34] M. Thangavelu, V. Krishnaswamy, and M. Sharma, "*Impact of Comprehensive Information Security Awareness and Cognitive Characteristics on Security Incident Management – an Empirical Study*," *Comput Secur*, vol. 109, p. 102401, Oct. 2021, doi: 10.1016/J.COSE.2021.102401.

[35] A. Wiley, A. McCormac, and D. Calic, "*More than the Individual: Examining the Relationship between Culture and Information Security Awareness*," *Comput Secur*, vol. 88, p. 101640, Jan. 2020, doi: 10.1016/J.COSE.2019.101640.

[36] M. Sas, G. Reniers, K. Ponnet, and W. Hardyns, "*The Impact of Training Sessions on Physical Security Awareness: Measuring Employees' Knowledge, Attitude and Self-Reported Behavior*," *Saf Sci*, vol. 144, Dec. 2021, doi: 10.1016/j.ssci.2021.105447.

[37] A. B. Ruighaver, S. B. Maynard, and S. Chang, "*Organisational Security Culture: Extending the End-User Perspective*," *Comput Secur*, vol. 26, no. 1, pp. 56–62, Feb. 2007, doi: 10.1016/j.cose.2006.10.008.

[38] K. M. Parsons, E. Young, M. A. Butavicius, A. McCormac, M. R. Pattinson, and C. Jerram, "*The Influence of Organizational Information Security Culture on Information Security Decision Making*," *J Cogn Eng Decis Mak*, vol. 9, no. 2, pp. 117–129, Jun. 2015, doi: 10.1177/1555343415575152.

[39] R. Baber, P. Baber, and S. Narula, "*Examining the Moderating Role of Online Celebrity Trustworthiness and Risk Propensity in Utaut2 Framework: A Mixed-Method Approach*," *International Journal of Information Management Data Insights*, vol. 4, no. 2, Nov. 2024, doi: 10.1016/j.jjimei.2024.100239.

[40] C. M. Wang, B. B. Xu, S. J. Zhang, and Y. Q. Chen, "*Influence of Personality and Risk Propensity on Risk Perception of Chinese Construction Project Managers*," *International Journal of Project Management*, vol. 34, no. 7, pp. 1294–1304, Oct. 2016, doi: 10.1016/j.ijproman.2016.07.004.