Management Strategies and Engineering Sciences 2026; 8(3):1-13



Evaluation of Cybersecurity Strategies for Improving Information Technology Services: Design and Quantitative Testing of an Integrated Model

Amin Moghimi[1], Ahmad Reza Kasraee[1*], Sina Abuei Mehrizi[2], Hedeyeh Divsalar[2]

[1] Department of Industrial Management, CT.C., Islamic Azad University, Tehran, Iran
[2] Department of Business Management, TeMS.C., Islamic Azad University, Tehran, Iran

*** Corresponding author email address**: ah.kasraee1349@iau.ac.ir

Received: 2026-01-08 **Revised:** 2026-05-07 **Accepted:** 2026-05-14 **Published:** 2026-05-30

Abstract

The present study aimed to evaluate cybersecurity strategies for improving information technology services through the design and quantitative testing of an integrated model. Given organizations' increasing dependence on information technology services and the growing complexity of cyber threats in cloud environments, there is a clear need for a comprehensive model that simultaneously incorporates strategic and organizational dimensions as well as technical and environmental dimensions. In terms of purpose, this study is applied-developmental, and in terms of methodology, it adopts a mixed (quantitative) approach. In the quantitative phase, data were collected through a questionnaire administered to organizations providing information technology services and were analyzed using partial least squares structural equation modeling (PLS-SEM). The results indicated that strategic readiness has positive and significant effects on organizational enablement, environmental complexity, and integrated cybersecurity capability. Organizational enablement and environmental complexity also influence integrated cybersecurity capability and cybersecurity governance excellence. Furthermore, integrated cybersecurity capability has a significant effect on cybersecurity governance excellence, while cybersecurity governance excellence was ultimately identified as the most influential factor affecting digital resilience performance. Cybersecurity strategies are effective when they are designed and implemented within an integrated, multilayered model encompassing governance, risk management, and socio-technical dimensions. Cybersecurity governance constitutes the final linkage connecting security capabilities to digital resilience performance; without effective governance, investment in technology alone cannot ensure sustainable resilience. The findings are consistent with the existing theoretical literature on information security governance, risk management, and socio-technical systems, and the proposed model can be employed as a context-specific framework for assessing cybersecurity maturity in organizations providing information technology services.

Keywords: *Cybersecurity, cybersecurity strategy, information technology services, cybersecurity governance, digital resilience, integrated model, structural equation modeling.*

How to cite this article:
Moghimi, A., Kasraee, A. R., Mehrizi, S. A., & Divsalar, H. (2026). Evaluation of Cybersecurity Strategies for Improving Information Technology Services: Design and Quantitative Testing of an Integrated Model. Management Strategies and Engineering Sciences, 8(3), 1-13.

1. Introduction

The rapid expansion of digital technologies has fundamentally transformed the way organizations design, deliver, monitor, and improve information technology services. Cloud computing, mobile platforms, interconnected enterprise systems, artificial intelligence, the Internet of Things, and data-intensive applications have increased both the strategic value of information technology and the organizational dependence on digital infrastructures. This growing dependence has simultaneously expanded the attack surface available to malicious actors and has made cybersecurity an essential determinant of service continuity, organizational reliability, stakeholder trust, and long-term operational resilience. Cybersecurity can therefore no longer be viewed merely as a technical function confined to

© 2026 The author(s). Published By: The Research Department of Economics and Management of Tomorrow's Innovators. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

firewalls, intrusion detection systems, access controls, or antivirus technologies. Rather, it has evolved into a multidimensional organizational capability that requires strategic alignment, managerial commitment, governance mechanisms, risk-based decision making, organizational learning, and coordination between technological and human resources [1]. In this context, organizations that provide information technology services face particular pressure because disruptions, cyber incidents, data breaches, and service failures may directly affect not only their internal operations but also the activities of customers, partners, public institutions, and other dependent stakeholders.

The growing strategic importance of cybersecurity is closely associated with the broader process of digital transformation. Digital transformation creates new opportunities for efficiency, service innovation, automation, and data-driven decision making, but it also introduces interconnected risks related to confidentiality, integrity, availability, privacy, system dependency, and third-party exposure. As organizations migrate critical processes to digital and cloud-based infrastructures, traditional security models based on isolated technological controls become increasingly insufficient. Contemporary cyber threats are adaptive, distributed, and often embedded in complex organizational and technological ecosystems, which makes risk identification and mitigation more difficult. The expansion of digital platforms also increases the number of interfaces through which attackers may gain access to organizational assets, while dependency on external vendors, software providers, cloud platforms, and supply-chain partners introduces risks that cannot be managed solely through internal controls. Accordingly, cybersecurity has become one of the central challenges associated with digital transformation, requiring organizations to develop integrated strategies that connect technological protection with governance, organizational readiness, and risk management [2].

One of the fundamental challenges in cybersecurity management is the distinction and relationship between information security and cybersecurity. Information security has traditionally focused on protecting information assets against threats affecting confidentiality, integrity, and availability, whereas cybersecurity encompasses a broader environment that includes digital infrastructures, cyberspace interactions, interconnected technologies, users, networks, and external threat actors. Although the two concepts substantially overlap, cybersecurity is broader in scope and increasingly involves organizational resilience, governance, external dependencies, and the ability to anticipate, withstand, recover from, and adapt to disruptive cyber events [1]. This broader perspective is especially relevant to organizations providing information technology services because their security effectiveness cannot be evaluated solely on the basis of preventing unauthorized access. It must also be assessed in terms of continuity of service delivery, recovery from incidents, preservation of stakeholder confidence, adaptability to emerging threats, and maintenance of competitive and operational capabilities under adverse conditions.

Cybersecurity governance represents a critical mechanism through which strategic objectives are translated into coordinated security practices. Governance establishes accountability, decision rights, priorities, monitoring mechanisms, and control structures that guide organizational security activities. Early conceptualizations of information security governance emphasized the importance of structured management cycles linking direction, control, implementation, monitoring, and corrective action. The direct-control cycle proposed in the literature highlights that security must be guided by formal governance structures rather than treated as a fragmented operational responsibility [3]. This principle remains highly relevant in contemporary cybersecurity environments because investment in technological safeguards cannot by itself guarantee effective risk reduction. Without clear governance, responsibility may be dispersed, security priorities may conflict with operational objectives, resources may be allocated inefficiently, and risk responses may be inconsistent across organizational units. Therefore, governance excellence may serve as the institutional mechanism through which strategic readiness and cybersecurity capabilities are transformed into resilient organizational performance.

At the same time, effective cybersecurity depends heavily on organizational preparedness. Cybersecurity preparedness refers to the extent to which an organization possesses the strategic awareness, technological infrastructure, managerial support, policies, competencies, and resources required to anticipate and respond to cyber threats. Evidence from organizations, particularly small and medium-sized enterprises, demonstrates that cybersecurity preparedness is often constrained by limited resources, insufficient expertise, weak policies, low employee awareness, and inadequate strategic prioritization [4]. These challenges are not exclusive to smaller organizations; they reflect broader organizational vulnerabilities that may occur whenever cybersecurity is treated as an operational afterthought rather

than as a strategic capability. Strategic readiness therefore involves more than the existence of security technologies. It includes management commitment, regulatory awareness, infrastructure readiness, organizational security maturity, and the capacity to integrate cybersecurity considerations into strategic planning and service management.

The importance of strategic readiness becomes even more evident in environments characterized by high technological and environmental complexity. Organizations are increasingly exposed to dynamic threat landscapes involving ransomware, phishing, social engineering, distributed denial-of-service attacks, supply-chain compromise, credential theft, cloud misconfiguration, and exploitation of emerging technologies. In addition to the increasing sophistication of threats, organizations must respond to rapid technological change, regulatory requirements, ecosystem dependencies, and uncertainty regarding future vulnerabilities. Cybersecurity decisions consequently involve multiple competing priorities and incomplete information. Studies in highly sensitive sectors such as banking and finance have shown that cybersecurity risk management requires systematic prioritization of risks and strategic responses rather than isolated control measures [5]. The use of strategic decision-making models to prioritize cybersecurity interventions reflects the increasing need for organizations to evaluate threats according to their organizational context, operational consequences, likelihood, and strategic significance.

Cybersecurity strategy is also strongly related to organizational information and data protection. Organizations increasingly generate, store, process, and exchange large volumes of sensitive operational, financial, managerial, and personal information through emerging information and communication technologies. The adoption of such technologies creates significant opportunities for improving administrative efficiency and service delivery, but it also creates vulnerabilities related to data protection, access control, privacy, system integration, and unauthorized disclosure. Organizational studies have therefore emphasized that information protection and cybersecurity must evolve alongside emerging ICT infrastructures and should be embedded in broader management systems [6]. This requirement is particularly important in public and service-oriented organizations because the consequences of inadequate cybersecurity may include operational disruption, legal liability, reputational damage, loss of citizen or customer trust, and diminished institutional legitimacy. As a result, cybersecurity strategies must be aligned with information governance and organizational objectives rather than implemented as isolated technical programs.

A further challenge concerns the design of effective information security management strategies for countering cyberattacks. Cyberattacks increasingly target organizational networks through multiple vectors and may combine technological exploitation with human manipulation. Effective defense therefore requires a layered approach involving preventive, detective, responsive, and recovery capabilities. Security strategies should incorporate network protection, monitoring, incident response, access management, risk analysis, employee awareness, and continuous improvement. The development of information security management strategies emphasizes the importance of combining technical controls with managerial and organizational practices when responding to cyberattacks [7]. Such an approach is particularly relevant to information technology service organizations, where service quality and cybersecurity performance are closely interconnected. A technically secure system that cannot maintain service availability may still fail organizational objectives, just as a highly available service with inadequate protection may expose the organization and its customers to unacceptable risk.

The organizational dimension of cybersecurity can be better understood through a socio-technical perspective. Socio-technical systems theory argues that organizational performance emerges from the interaction of technical and social subsystems rather than from technology alone. Information systems are embedded within organizational structures, work processes, human behaviors, policies, communication patterns, and institutional environments. Consequently, security failures may arise not only from technical vulnerabilities but also from poor coordination, inadequate training, unclear responsibilities, inappropriate incentives, weak organizational culture, or misalignment between systems and users. Socio-technical systems thinking therefore encourages the joint optimization of technological and organizational elements [8]. Applied to cybersecurity, this perspective suggests that resilience requires a combination of secure technologies, competent personnel, effective governance, coordinated processes, and adaptive organizational structures. It also implies that cybersecurity capability should be conceptualized as an integrated organizational competence rather than as a collection of independent technical controls.

The socio-technical character of cybersecurity becomes especially visible in the design and delivery of digital services. Security measures that are technologically sophisticated may fail if they do not account for the needs, limitations, behaviors, and vulnerabilities of users. Research on digital service delivery has shown that cybersecurity concerns can disproportionately affect vulnerable users when service design does not sufficiently consider usability, access, inclusion, and user-centered security requirements [9]. This finding has broader implications for information technology services because cybersecurity controls must support, rather than unnecessarily obstruct, service accessibility and user experience. Organizations therefore face the challenge of balancing security with usability, continuity, inclusiveness, and operational efficiency. An integrated cybersecurity model should consequently account for both protective effectiveness and the ability of security arrangements to support sustainable service delivery.

Another important dimension is cybersecurity risk communication and disclosure. Cybersecurity strategy does not affect only internal control processes; it also shapes stakeholder perceptions of organizational competence, transparency, and risk. Research examining cybersecurity risk management strategy disclosure has demonstrated that the way organizations communicate their cybersecurity strategies can influence investor judgments and decisions [10]. This evidence indicates that cybersecurity governance has external as well as internal consequences. Stakeholders increasingly expect organizations to demonstrate that cyber risks are identified, governed, monitored, and addressed systematically. Weak cybersecurity governance may therefore undermine trust even when no major incident has occurred, while clear and credible risk-management strategies can signal organizational preparedness and managerial competence. For information technology service providers, whose business models depend substantially on reliability and trust, these effects are particularly important.

Cybersecurity performance should therefore be evaluated not merely in terms of incident prevention but also in terms of resilience. Digital resilience refers to the ability of an organization to sustain critical digital functions, absorb disruptions, recover rapidly, and adapt its capabilities in response to changing threats. This perspective recognizes that complete prevention of cyber incidents is unrealistic in complex digital environments. The strategic objective must consequently shift from attempting to eliminate all risk toward developing the capability to anticipate, withstand, respond to, recover from, and learn from disruptions. Such resilience depends on organizational readiness, environmental awareness, integrated cybersecurity capabilities, and governance mechanisms that coordinate decision making before, during, and after security incidents. Cybersecurity governance excellence can thus be viewed as a central mechanism connecting organizational capabilities to resilience outcomes.

Despite the increasing recognition of these dimensions, cybersecurity research and practice often remain fragmented. Some approaches emphasize technological controls, whereas others focus on governance, risk management, compliance, employee behavior, or organizational preparedness. This fragmentation can make it difficult for managers to understand how different cybersecurity capabilities interact and how they jointly influence information technology service performance. In practice, an organization may demonstrate high technical maturity but weak governance, strong policies but limited implementation capacity, or effective risk identification without sufficient organizational enablement. An integrated model is therefore necessary to explain how strategic readiness, organizational enablement, environmental complexity, integrated cybersecurity capability, and governance excellence interact to produce resilient outcomes.

Strategic readiness may function as an upstream organizational capability that shapes the extent to which cybersecurity resources and responsibilities can be mobilized. Organizations with greater security maturity, stronger technological infrastructure, committed senior management, and higher regulatory compliance are likely to be better positioned to develop organizational enablement and integrated security capabilities. Evidence on cybersecurity preparedness suggests that managerial support, resources, formal policies, and organizational awareness significantly influence the ability to respond to cyber threats [4]. Similarly, the increasing importance of organizational data protection in technologically advanced environments reinforces the need for strategic alignment between cybersecurity initiatives and organizational structures [6]. Accordingly, strategic readiness should be regarded as a foundation for the development of more advanced cybersecurity capabilities.

Organizational enablement represents another critical dimension because cybersecurity strategies must be operationalized through people, culture, competencies, and processes. An organization may possess security policies and technologies but still remain vulnerable if employees

lack awareness, security responsibilities are unclear, processes are poorly integrated, or security capabilities are disconnected from operational units. The socio-technical perspective emphasizes that organizational and technical factors must be jointly designed and coordinated [8]. In cybersecurity practice, this means developing an information security culture, strengthening technological competencies, improving human resource security management, and integrating security requirements into organizational processes. These mechanisms provide the organizational foundation through which strategic intentions can be converted into practical cybersecurity performance.

Environmental complexity further influences cybersecurity capability because organizations operate within ecosystems characterized by evolving technologies, interorganizational dependencies, emerging threats, and regulatory uncertainty. The importance of systematic cybersecurity risk assessment and prioritization in complex industries illustrates that threat management requires strategic adaptation rather than static controls [5]. Digital transformation intensifies this complexity by increasing connectivity, dependence on external systems, and exposure to emerging vulnerabilities [2]. Consequently, organizations must develop capabilities that allow them to continuously identify, interpret, and respond to changes in the cyber environment.

Integrated cybersecurity capability can be understood as the organization's ability to align cybersecurity with business priorities, coordinate security activities, manage cyber risk in an integrated manner, and develop cyber resilience. Such integration is necessary because fragmented security practices may create gaps between strategic policy and operational implementation. Effective cybersecurity strategies require both technical protection and coordinated management mechanisms [7]. Moreover, cybersecurity should be distinguished from narrower conceptions of information security precisely because it involves broader organizational, technological, and environmental interactions [1]. Integrated capability therefore provides a bridge between strategic preparedness and governance excellence.

Cybersecurity governance excellence, in turn, may represent the institutional mechanism through which organizational capabilities are converted into sustained resilience performance. Governance establishes accountability, supervises security operations, guides human capital development, coordinates stakeholders, and ensures that cybersecurity priorities remain aligned with organizational objectives. The governance perspective emphasizes that effective information security requires systematic direction and control rather than ad hoc technical interventions [3]. Furthermore, because cybersecurity practices increasingly affect stakeholder judgments and perceptions of organizational credibility, governance quality may also contribute to trust and legitimacy [10]. In digital service environments, such governance must additionally consider the needs and vulnerabilities of diverse users so that security mechanisms do not unintentionally reduce accessibility or service quality [9].

Taken together, the existing literature suggests that cybersecurity effectiveness emerges from a multilayered system of strategic, organizational, technical, environmental, and governance factors. However, these elements are frequently investigated separately, and there remains a need for models that explain how they interact in organizations providing information technology services. An integrated approach can contribute to both theory and practice by clarifying the pathways through which strategic readiness influences organizational enablement and security capability, how environmental complexity shapes cybersecurity responses, and how governance excellence translates these capabilities into digital resilience. Such a framework can also provide managers with a structured basis for evaluating cybersecurity maturity, identifying capability gaps, prioritizing investments, and improving the continuity and reliability of information technology services.

Accordingly, the aim of this study is to design and quantitatively test an integrated model for evaluating cybersecurity strategies aimed at improving information technology services through the relationships among strategic readiness, organizational enablement, environmental complexity, integrated cybersecurity capability, cybersecurity governance excellence, and digital resilience performance.

2. Methodology

The present study is applied in terms of purpose and quantitative and survey-based in terms of methodology. Since it objectively describes and analyzes the existing situation and solicits the views of officials, managers, policymakers, cybersecurity managers, and information technology managers, it is classified as a descriptive and non-experimental study. The statistical population in the quantitative phase consisted of cybersecurity and information technology managers involved in cybersecurity

strategy processes within information technology services. Given the assumption of an unlimited population, the sample size was determined using Cochran's formula at a 95% confidence level, with $\alpha = 0.05$ and a standard deviation of 0.677, resulting in a required sample of 384 participants. Stratified random sampling was employed. The data collection instrument was a researcher-developed questionnaire based on the components extracted from the research literature and organized into three sections corresponding to the variables related to cybersecurity strategies and information technology services. The items were measured using a five-point Likert scale. The content validity of the questionnaire was confirmed through expert judgment; construct validity was assessed using confirmatory factor analysis and the average variance extracted (AVE) criterion; discriminant validity was evaluated using the Fornell–Larcker criterion and the heterotrait–monotrait ratio (HTMT); and reliability was confirmed using Cronbach's alpha and composite reliability. Data were analyzed using structural equation modeling based on the partial least squares approach (PLS-SEM). Structural equation modeling is a powerful multivariate analytical technique belonging to the family of multivariate regression methods that enables researchers to test a set of regression equations simultaneously (Hooman, 2016). In the present study, structural equation modeling was applied in two stages: first, to assess the fit of the measurement models, and second, to evaluate the proposed model and determine the significance of relationships among the variables using path analysis. Structural equation modeling quantitatively tests the theoretical model hypothesized by the researcher and represents the relationships among observed variables. Its purpose is to determine whether the theoretical model is supported by the sample data. Data analysis was conducted at both descriptive and inferential levels. Descriptive statistics included mean, standard deviation, and frequency, whereas inferential statistics included factor loadings, AVE, composite reliability (CR), Cronbach's alpha (α), path coefficients, t-values, R^2, Q^2, and goodness-of-fit (GoF) indices. Importance–Performance Map Analysis (IPMA) was also employed to prioritize the components. In inferential analysis, the researcher deals with the process of sampling and selecting a smaller group, referred to as the sample, from a larger group, referred to as the statistical population. Data and information obtained from the sample are then used to estimate and predict the characteristics of the population under study. Accordingly, the purpose of inferential analysis is to generalize the findings derived from the selected sample to the target population.

3. Findings and Results

In the quantitative phase, considering maximum variance and a 5% error level, more than 400 questionnaires were distributed electronically in order to increase the questionnaire return rate and facilitate implementation of the study. Of these, 384 respondents completed the questionnaire, and these responses formed the basis for the analyses and hypothesis testing. In this study, the selected variables were examined based on a conceptual model. Data normality was evaluated using skewness and kurtosis indices. The sample consisted of 384 respondents. Construct validity and reliability were assessed through the measurement model, while the hypotheses were tested and model fit was evaluated using structural equation modeling with SPSS version 24 and SmartPLS version 2. The application of structural equation modeling for latent variables provided a more appropriate representation of the conceptual relationships. As stated by Mittal et al., the partial least squares approach assumes that individual variables covary with other variables in the model and that the resulting model-fit indices are examined within the measurement-model assessment. Moreover, this method calculates bootstrapped standard errors and generates approximate t-values for testing the significance of structural paths. Therefore, as shown in Table 1, all variables were found to be at satisfactory levels.

Table 1. Descriptive Indices for the Dimensions of the Research Variables

Main Factor	Mean	Standard Deviation	Skewness	Kurtosis
Causal Conditions	3.454	0.736	0.498	1.335
Contextual Conditions	3.113	0.554	-0.500	0.580
Intervening Conditions	3.355	0.600	-0.263	0.378
Strategies	3.765	0.398	-0.476	0.608
Consequences	3.400	0.457	-0.740	0.699

Cronbach's alpha and composite reliability were used to assess questionnaire reliability. The reliability results for each individual variable indicated that all values exceeded 0.70, demonstrating satisfactory reliability. Convergent and discriminant validity were used to assess construct validity. Table 2 presents the results pertaining to convergent validity. The convergent validity values obtained for the latent variables in the model exceeded 0.50; therefore, the convergent validity of the measurement models was considered satisfactory.

Table 2. Results of the Assessment of Construct Reliability and Validity

Variable	Cronbach's Alpha	AVE	CR	Rho
Causal Conditions	0.788	0.530	0.800	0.849
Contextual Conditions	0.809	0.587	0.714	0.855
Intervening Conditions	0.711	0.530	0.755	0.760
Strategies	0.857	0.601	0.760	0.780
Consequences	0.744	0.590	0.793	0.798

The goodness-of-fit (GoF) index for the model was 0.622, indicating an acceptable overall model fit.

The second category of findings concerned examination of the structural model. Following confirmation of validity and reliability, the structural model of the study was evaluated. This model makes it possible to examine the hypothesized relationships proposed in the study. Figure 1 presents the results obtained from the SmartPLS 2 software output. According to this model, the factor loadings were significant at the 95% confidence level, and all t-statistic values fell outside the range of -1.96 to +1.96.

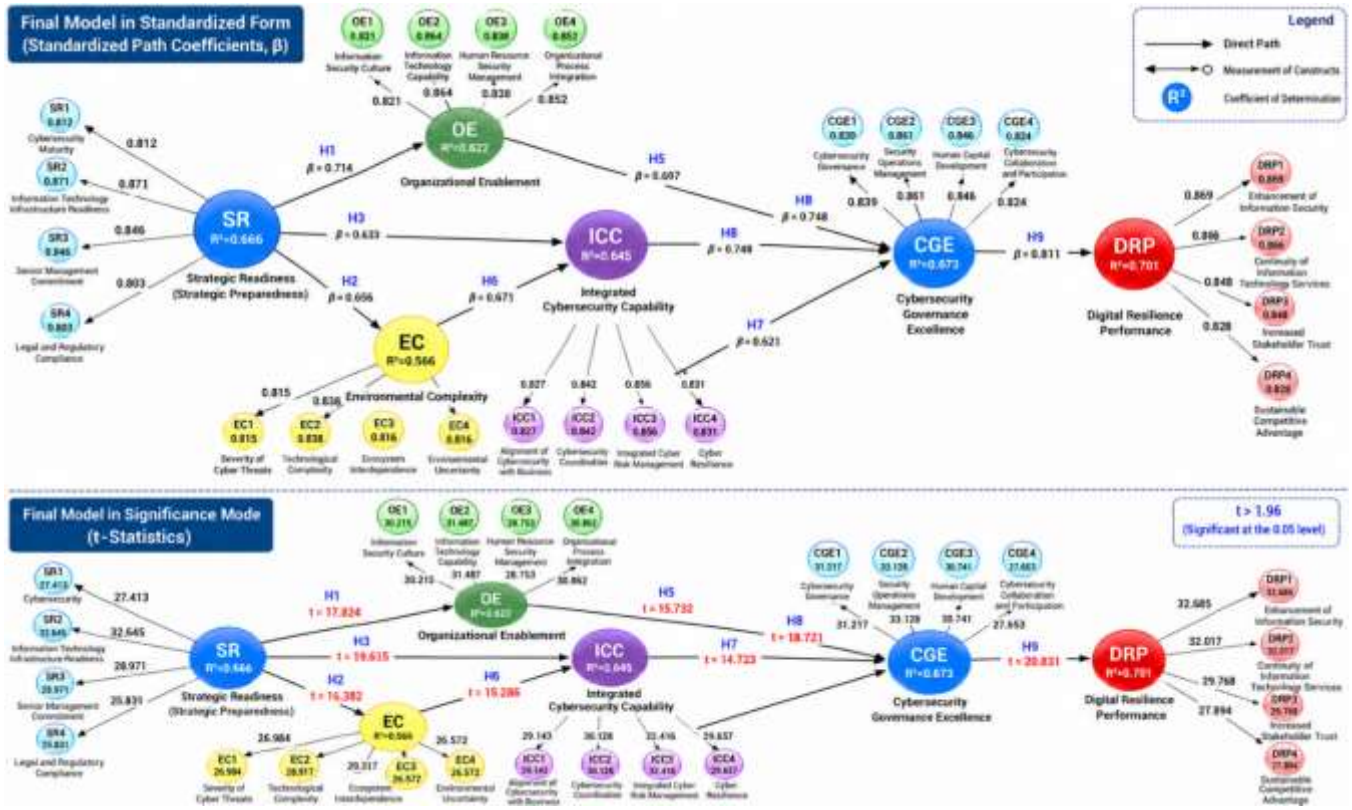


Figure 1. Final Structural Model of the Study

In the quantitative phase, the research model was analyzed using SmartPLS. Data analysis was performed using the partial least squares technique and SmartPLS software. This approach was selected because of its lower dependence on sample size, lack of a strict normality requirement, and emphasis on maximizing explained variance, which make it particularly suitable for practical applications compared with covariance-based software packages such as LISREL and AMOS. In this technique, the strength of the relationship between a factor, or latent

variable, and an observed variable is represented by the factor loading. In the standardized measurement model, indicators with weak factor loadings may be removed from the model. According to Hair et al. (2013), items with low factor loadings should also be considered for removal, while desirable factor loading values are relatively high and close to 1. After identifying correlations among the variables, significance testing was performed through bootstrapping, which produces t-statistics. At a 5% significance level, sufficiently large t-statistic values indicate that the observed relationships are statistically significant. Relationships among the variables were examined through two components: the outer model, which corresponds to the measurement model and confirmatory factor analysis, and the inner model, which corresponds to the structural model and path analysis. In the overall research model, standardized factor loadings and bootstrapped t-statistics were calculated to assess the significance of the relationships. The results indicated that all tested relationships were significant at the 5% error level; therefore, all research hypotheses were supported. Specifically, causal conditions had a direct and significant effect on the core category; contextual conditions had a direct and significant effect on strategies; intervening conditions had a direct and significant effect on strategies; the core category had a direct and significant effect on strategies; and strategies had a direct and significant effect on consequences. The largest path coefficients were associated with the relationships between the "core category and strategies" and between "causal conditions and the core category," whereas the smallest path coefficient was observed for the relationship between "contextual conditions and strategies." In contrast, the highest t-statistics were associated with the relationships between "contextual conditions and strategies" and between "strategies and consequences," indicating a high degree of precision in the estimation of these relationships. Overall, these findings demonstrate that the conceptual model of the study is statistically supported by the data and that the proposed structure of relationships among the variables is confirmed.

4. Discussion and Conclusion

The present study developed and quantitatively tested an integrated model for evaluating cybersecurity strategies aimed at improving information technology services. The findings showed that the proposed structural relationships were statistically significant and that the conceptual model was supported by the empirical data. Specifically, strategic readiness had significant positive effects on organizational enablement, environmental complexity, and integrated cybersecurity capability. Environmental complexity significantly affected integrated cybersecurity capability and cybersecurity governance excellence, while organizational enablement also had a significant positive effect on cybersecurity governance excellence. Integrated cybersecurity capability exerted a significant effect on cybersecurity governance excellence, and cybersecurity governance excellence, in turn, had the strongest direct effect on digital resilience performance. These findings indicate that cybersecurity effectiveness is not produced by a single technological or managerial factor; rather, it emerges through a multilayered configuration in which strategic preparedness, organizational capacity, environmental awareness, integrated security capability, and governance mechanisms jointly contribute to the resilience of digital services.

The significant positive effect of strategic readiness on organizational enablement indicates that organizations with stronger cybersecurity maturity, better information technology infrastructure, greater senior management commitment, and stronger legal and regulatory compliance are more capable of developing the internal conditions required for effective cybersecurity implementation. Strategic readiness therefore appears to function as an upstream capability that creates the organizational foundation for security culture, technological capability, human resource security management, and process integration. This finding is consistent with the argument that cybersecurity preparedness depends not only on technical controls but also on organizational awareness, formal policies, managerial support, and the allocation of adequate resources [4]. Organizations that treat cybersecurity as a strategic responsibility are more likely to institutionalize security-related roles and practices across departments rather than confining them to technical units. This result is also consistent with the broader view that information and data protection must be embedded within organizational structures and management systems, particularly as emerging information and communication technologies increase the scope and complexity of security responsibilities [6].

The effect of strategic readiness on integrated cybersecurity capability further demonstrates that security maturity and preparedness are necessary antecedents of coordinated cybersecurity performance. An organization

cannot effectively align cybersecurity with business objectives, integrate cyber risk management, coordinate security functions, or develop resilience if it lacks basic strategic preparedness. This finding supports the argument that contemporary cybersecurity strategies should integrate technical, managerial, and organizational dimensions rather than relying on isolated protective measures [7]. The result also aligns with the conceptual distinction between information security and cybersecurity, according to which cybersecurity extends beyond information protection and includes broader relationships among digital systems, organizations, users, infrastructures, and external environments [1]. In this sense, strategic readiness enables organizations to move from fragmented security activities toward a more integrated cybersecurity capability that is connected to organizational strategy and service delivery.

The significant relationship between strategic readiness and environmental complexity may initially appear conceptually different from traditional causal pathways because environmental complexity is often viewed as an external condition. However, the result can be interpreted as evidence that strategically prepared organizations are better able to recognize, assess, and respond to the complexity of their cyber environment. Greater readiness may enhance organizational sensitivity to evolving cyber threats, technological complexity, ecosystem interdependence, and environmental uncertainty. Organizations with mature security programs are generally more capable of detecting external dependencies and evaluating changing risk conditions. This interpretation is consistent with research emphasizing the importance of structured cybersecurity risk assessment and strategic prioritization under conditions of uncertainty and complexity [5]. It is also consistent with the argument that digital transformation expands interconnectivity and increases exposure to new cybersecurity risks, requiring organizations to continuously reassess their threat landscape [2]. Therefore, strategic readiness may strengthen the organization's capacity to understand environmental complexity rather than simply being influenced by it.

The significant effect of environmental complexity on integrated cybersecurity capability demonstrates that cybersecurity capability must evolve in response to external pressures and technological change. As cyber threats become more sophisticated and organizations become increasingly dependent on complex digital ecosystems, cybersecurity capabilities must become more coordinated, adaptive, and risk-oriented. The finding suggests that high levels of threat intensity, technological complexity, ecosystem dependence, and uncertainty stimulate the development of capabilities such as cyber risk integration, cybersecurity-business alignment, cross-functional coordination, and cyber resilience. This result is consistent with the evidence from risk-sensitive industries showing that cybersecurity strategies must be prioritized according to changing risk conditions and the strategic importance of different threats [5]. It is also aligned with research on digital transformation, which emphasizes that the adoption of new digital infrastructures and technologies creates new risk interdependencies and increases the need for dynamic cybersecurity responses [2].

The positive relationship between organizational enablement and cybersecurity governance excellence also provides an important insight into the mechanism through which organizational resources are translated into governance quality. Organizational enablement encompasses the information security culture, technological capabilities, human resource security management, and integration of organizational processes. These elements support governance because governance cannot function effectively without organizational structures capable of implementing decisions, monitoring compliance, coordinating stakeholders, and integrating cybersecurity into operational processes. The finding is compatible with the socio-technical perspective, which maintains that successful information systems and security outcomes result from the interaction of technological and social subsystems rather than from technical design alone [8]. A governance framework may be formally well designed, but if employees lack competence, security culture is weak, or processes are poorly integrated, governance mechanisms are unlikely to achieve their intended objectives.

This result is also consistent with research emphasizing the organizational management of information security. Cybersecurity governance requires that policies, responsibilities, technologies, and human behaviors be aligned with organizational objectives. The direct-control logic of information security governance emphasizes the role of direction, implementation, control, monitoring, and corrective action in achieving effective security management [3]. Organizational enablement provides the capabilities necessary for this governance cycle to operate effectively. For example, an information security culture strengthens compliance with security policies, human resource security reduces behavior-related vulnerabilities, technological capability improves implementation capacity,

and process integration ensures that cybersecurity requirements are embedded in routine organizational activities. Thus, the present findings suggest that governance excellence should be understood not merely as a formal policy architecture but as an organizationally enabled capability.

The significant effect of environmental complexity on cybersecurity governance excellence further indicates that governance structures must adapt to the complexity of the external cyber environment. When organizations face more severe threats, greater technological heterogeneity, stronger ecosystem dependencies, and higher uncertainty, governance becomes increasingly important for coordinating risk responses and assigning responsibilities. This finding supports the view that modern cyber risk cannot be effectively managed through static policies or isolated technical interventions. Instead, governance mechanisms need to continuously incorporate information about changing threats, dependencies, regulatory expectations, and stakeholder concerns. The growing complexity associated with digital transformation reinforces this need because digitally connected environments expose organizations to risks that may originate beyond their direct organizational boundaries [2]. Similarly, studies of cybersecurity prioritization demonstrate that effective governance requires systematic evaluation of alternative security strategies when decision makers face multidimensional and uncertain risk conditions [5].

One of the most important findings was the significant positive effect of integrated cybersecurity capability on cybersecurity governance excellence. This relationship suggests that governance quality is strengthened when cybersecurity is aligned with business objectives, cyber activities are coordinated, risk management is integrated, and resilience is treated as an organizational capability. Integrated cybersecurity capability therefore appears to serve as a practical foundation for effective governance. This result is consistent with the argument that cybersecurity is broader than traditional information security because it involves the protection and resilience of interconnected digital environments and organizational ecosystems [1]. It also supports the view that information security strategies should combine technical controls with managerial processes, risk assessment, monitoring, and organizational coordination [7]. Governance excellence may thus be interpreted as the institutional expression of integrated cybersecurity capability.

The strong effect of cybersecurity governance excellence on digital resilience performance was particularly notable. Among the structural relationships, this path demonstrated the highest standardized coefficient, indicating that governance excellence plays a central role in translating cybersecurity capabilities into tangible resilience outcomes. This finding suggests that digital resilience is not achieved solely through the acquisition of advanced security technologies or the implementation of specific controls. Instead, organizations require governance systems capable of coordinating cybersecurity functions, managing accountability, developing human capital, supporting collaboration, and ensuring that security priorities are continuously aligned with organizational objectives. This result strongly supports the governance perspective advanced in the information security literature, which emphasizes that security outcomes depend on structured direction and control rather than on isolated technological actions [3].

The relationship between governance excellence and digital resilience can also be explained in terms of trust and stakeholder confidence. Digital resilience performance in the present model included improvement in information security, continuity of information technology services, increased stakeholder trust, and sustainable competitive advantage. Effective cybersecurity governance contributes to all of these outcomes by reducing ambiguity regarding responsibilities, strengthening security oversight, improving incident coordination, and promoting transparent risk management. Research has shown that the disclosure and communication of cybersecurity risk management strategies can significantly influence stakeholder judgments and decisions [10]. Although that study focused specifically on investors, its broader implication is that stakeholders evaluate organizations partly on the basis of their perceived ability to manage cybersecurity risks. Therefore, governance excellence may support digital resilience not only through technical and operational effectiveness but also through enhanced organizational credibility.

The relationship between governance and resilience is further reinforced when the needs of service users are considered. Information technology services increasingly operate in environments where cybersecurity measures affect not only technical systems but also the accessibility and usability of digital services. Studies of digital delivery systems have shown that security mechanisms can create difficulties for vulnerable users when cybersecurity concerns are not incorporated into service design in a user-

sensitive manner [9]. This finding complements the present results by suggesting that governance excellence should incorporate user-centered and service-oriented considerations. Effective cybersecurity governance must therefore balance protection, continuity, usability, inclusion, and operational performance. This balance is especially important for organizations providing information technology services because excessive security restrictions may reduce service effectiveness, while inadequate controls may undermine trust and resilience.

The findings as a whole strongly support a socio-technical interpretation of cybersecurity. The model indicates that resilience emerges from interdependent strategic, organizational, environmental, technical, and governance dimensions rather than from a purely technological security architecture. This is consistent with socio-technical systems theory, which emphasizes that organizational systems perform effectively when technical and social components are designed and managed in an integrated manner [8]. From this perspective, cybersecurity technology is only one component of a larger system involving management, human resources, organizational culture, policies, processes, external dependencies, and stakeholder relationships. The significant paths in the model demonstrate that these dimensions influence one another and collectively shape digital resilience.

The findings also reinforce the importance of cybersecurity preparedness as an organizational capability. Evidence from small and medium-sized businesses indicates that limitations in expertise, awareness, resources, and formal planning can significantly weaken cybersecurity preparedness [4]. The present study extends this insight by demonstrating that strategic readiness is associated with broader organizational and cybersecurity capabilities and ultimately contributes indirectly to resilience through governance mechanisms. Similarly, the importance of information and data protection in organizations adopting emerging ICT suggests that cybersecurity must be incorporated into organizational planning rather than treated as a separate technical issue [6]. Taken together, these findings indicate that organizations seeking to improve information technology services should focus on building an integrated cybersecurity architecture that begins with strategic readiness and culminates in governance-enabled resilience.

Another relevant implication concerns the need to move beyond a prevention-only cybersecurity logic. In highly interconnected digital environments, complete prevention of cyber incidents is neither realistic nor economically efficient. The stronger emphasis should be placed on resilience, meaning the ability to anticipate, withstand, recover from, and adapt to disruption. The present model supports this perspective because digital resilience performance is positioned as the final outcome of governance excellence rather than as a direct consequence of individual security controls. This finding is consistent with the increasing complexity of cyber risk management in sectors where organizations must evaluate multiple strategies under uncertain conditions [5]. It also corresponds with the broader recognition that cybersecurity strategy must evolve with digital transformation and changing patterns of technological dependence [2].

Overall, the results suggest a sequential and interconnected process through which cybersecurity strategies contribute to improved information technology services. Strategic readiness establishes the foundation for organizational enablement and integrated capability; environmental complexity creates pressure for more adaptive security responses; organizational enablement and integrated cybersecurity capability strengthen governance excellence; and governance excellence translates these capabilities into digital resilience performance. This configuration is theoretically consistent with information security governance, socio-technical systems theory, organizational preparedness research, and contemporary cybersecurity risk management. The findings therefore contribute to the literature by demonstrating that digital resilience is best understood as the outcome of an integrated cybersecurity system rather than as the result of isolated investments in technology, compliance, or risk controls.

Despite the contribution of the study, several limitations should be acknowledged. First, the research relied on a cross-sectional survey design, and the relationships identified among strategic readiness, organizational enablement, environmental complexity, integrated cybersecurity capability, governance excellence, and digital resilience therefore represent associations observed at one point in time rather than longitudinal causal processes. Second, the use of self-reported questionnaire data may have introduced common method bias, social desirability bias, and differences in respondents' interpretations of cybersecurity concepts. Third, the sample was limited to managers and professionals involved in cybersecurity and information technology functions, meaning that the perspectives of end users, operational employees, external service providers, customers, and regulators were not

directly captured. Fourth, the model evaluates cybersecurity at an aggregate organizational level and may not fully represent differences among industries, organization sizes, technological architectures, or regulatory environments. Finally, although the model demonstrates satisfactory explanatory power, cybersecurity performance is inherently dynamic and may also be influenced by variables that were not included in the present framework, such as incident response maturity, supply-chain exposure, cybersecurity investment intensity, organizational learning, and threat intelligence capability.

Future studies should test the proposed model using longitudinal designs in order to examine how cybersecurity capabilities and resilience evolve over time and whether changes in strategic readiness or governance produce subsequent changes in digital resilience performance. Researchers may also replicate the model across different sectors, such as banking, healthcare, government, telecommunications, transportation, and cloud-service industries, to assess the generalizability of the structural relationships. Multi-group analysis could be employed to compare organizations according to size, ownership, cybersecurity maturity, regulatory intensity, or level of digital transformation. Future research may also extend the model by incorporating additional variables such as cybersecurity investment, threat intelligence, organizational learning, supply-chain cyber risk, incident response capability, employee cybersecurity behavior, zero-trust maturity, and artificial intelligence-supported security management. Combining survey data with objective indicators such as number of security incidents, recovery time, service downtime, penetration-test results, and audit scores would provide stronger evidence regarding actual resilience outcomes. Qualitative studies could additionally explore how managers interpret governance excellence and how organizational politics, interdepartmental coordination, and leadership practices influence the implementation of integrated cybersecurity strategies.

Organizations providing information technology services should treat cybersecurity as an enterprise-level capability rather than as an isolated technical responsibility. Senior management should establish cybersecurity as a strategic priority, allocate adequate resources, clarify accountability, and ensure that security objectives are integrated into organizational planning and service management. Managers should strengthen information security culture, improve employee competence, embed security responsibilities into human resource processes, and integrate cybersecurity requirements into routine operational procedures. Continuous assessment of environmental complexity should be institutionalized so that emerging threats, technological changes, ecosystem dependencies, and regulatory developments are incorporated into risk decisions. Organizations should also develop an integrated cybersecurity capability by aligning security with business objectives, coordinating security functions across departments, integrating cyber risk management, and building explicit resilience capabilities. Most importantly, cybersecurity governance should be strengthened through clearly defined decision rights, effective oversight, human capital development, cross-functional collaboration, performance monitoring, and continuous improvement mechanisms. Such measures can help organizations convert cybersecurity investments into stronger service continuity, higher stakeholder trust, improved information security, and more sustainable digital resilience.

Authors' Contributions

Authors equally contributed to this article.

Acknowledgments

Authors thank all participants who participate in this study.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

References

[1] R. Von Solms and S. H. Von Solms, "Cybersecurity and Information Security - What Goes Where?," *Information & Computer Security*, vol. 26, no. 1, pp. 2-9, 2018, doi: 10.1108/ICS-04-2017-0025.

[2] N. Türegün, "Digital Transformation and Cybersecurity Risks," *International Journal of Accounting Information Systems*, 2024, doi: 10.1016/j.accinf.2025.100749.

[3] R. Von Solms and S. H. Von Solms, "Information Security Governance: A Model Based on the Direct-Control Cycle,"

Computers & Security, vol. 25, no. 6, pp. 408-412, 2006, doi: 10.1016/j.cose.2006.07.005.

[4] A. Chidukwani, S. Zander, and P. Koutsakis, "Cybersecurity Preparedness of Small-to-Medium Businesses: A Western Australia Study with Broader Implications," *Computers & Security*, vol. 145, p. 104026, 2024, doi: 10.1016/j.cose.2024.104026.

[5] P. H. Nguyen, T. V. Pham, L. A. T. Nguyen, H. A. T. Pham, T. H. T. Nguyen, and T. G. Vu, "Assessing Cybersecurity Risks and Prioritizing Top Strategies in Vietnam's Finance and Banking System Using Strategic Decision-Making Models-Based Neutrosophic Sets and Z Number," *Heliyon*, vol. 10, no. 19, p. e37893, 2024, doi: 10.1016/j.heliyon.2024.e37893.

[6] M. Omrani, "An Analysis of Organizational Information and Data Protection and Cybersecurity Using Emerging Information and Communication Technologies (ICT) in Municipalities," (in Persian), *Quarterly Journal of New Research in Management and Accounting*, vol. 6, no. 12, 2025.

[7] M. Hossein Gholipour, "Information Security Management Strategies for Countering Cyberattacks in Computer Networks," presented at the 24th National Conference on Applied Research in Electrical, Computer, and Biomedical Engineering Sciences, 2025.

[8] G. Baxter and I. Sommerville, "Socio-Technical Systems: From Design Methods to Systems Engineering," *Interacting with Computers*, vol. 23, no. 1, pp. 4-17, 2011, doi: 10.1016/j.intcom.2010.07.003.

[9] A. Capaccioli, L. Urciuoli, F. Di Ciommo, G. Rondinella, S. Giorgi, and R. Hueting, "Including the Excluded: How Can Design of Digital Delivery Service Address Cybersecurity Concerns of Vulnerable Users?," *Transportation Research Procedia*, vol. 72, pp. 2604-2611, 2023, doi: 10.1016/j.trpro.2023.11.791.

[10] J. Huang and U. Murthy, "The Impact of Cybersecurity Risk Management Strategy Disclosure on Investors' Judgments and Decisions," *International Journal of Accounting Information Systems*, vol. 54, p. 100696, 2024, doi: 10.1016/j.accinf.2024.100696.