KMAN PUBLISHING INSTITUTE

**Article history:**
**Received 01 November 2025**
**Revised 11February 2026**
**Accepted 11 May 2026**
**Initial Publish 28 May 2026**
**Published online 01 March 2027**

**Journal of Resource Management and Decision Engineering**

**Volume 5, Issue 2, pp 1-13**


# Designing a Cybersecurity Strategies Model in Information Technology Services

Amin. Moghimi[1], Ahmad Reza. Kasraei[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

A r t i c l e  I n f o

**Article type:**
*Original Research*

**How to cite this article :**
Moghimi, A., Kasraei, A. R., Abuei Mehrizi, S., & Divsalar, H. (2027). Designing a Cybersecurity Strategies Model in Information Technology Services. *Journal of Resource Management and Decision Engineering*, *5*(2), 1-13.
https://doi.org/10.61838/kman.jrmde.314



A B S T R A C T

This study was conducted with the aim of designing a cybersecurity strategies model in information technology services. The statistical population consisted of academic experts and specialists in the fields of cybersecurity and information technology. Sampling was performed using purposive and snowball methods, and data were collected through 15 in-depth semi-structured interviews. Data analysis was conducted through the stages of open, axial, and selective coding. To ensure the credibility of the findings, strategies such as coding by two researchers, peer review, member checking, and calculation of Cohen's kappa coefficient (86.9%) were employed. The findings led to the identification of a set of causal, contextual, and intervening conditions that, through their interaction, explain the formation of the core category of "Integrated Cybersecurity Strategy in Information Technology Services." Furthermore, the strategies were identified at three levels: governance and policymaking, technical and operational, and human and interactive. The implementation of these strategies results in outcomes such as enhanced security levels, continuity and sustainability of information technology services, increased stakeholder trust, improved organizational maturity, and the creation of competitive advantage. Overall, the present study, by presenting a grounded, integrated, and context-oriented model, addresses the existing theoretical gap in the cybersecurity literature and can serve as a practical framework for managers, policymakers, and researchers in the field of information technology services.

***Keywords:*** *Cybersecurity, Information Technology Services, Cybersecurity Strategy, Grounded Theory, Paradigmatic Model*

## 1. Introduction

The rapid expansion of digital technologies, cloud computing, artificial intelligence, the Internet of Things (IoT), and interconnected service ecosystems has transformed information technology services into one of the most critical infrastructures of modern organizations. Organizations increasingly rely on digital platforms and information systems to deliver services, manage operations, maintain customer relationships, and support strategic decision-making. However, this technological transformation has simultaneously intensified cybersecurity threats and vulnerabilities, exposing organizations to increasingly sophisticated cyberattacks, data breaches, operational disruptions, and reputational damages (Rampasek et al., 2024; Turegun, 2024). As digital transformation accelerates across public and private sectors, cybersecurity has evolved from a purely technical concern into a strategic organizational issue that directly affects organizational resilience, service continuity, competitive advantage, and stakeholder trust (Huang & Murthy, 2024; Omrani, 2025). In this context, the development of integrated cybersecurity strategies has become essential for ensuring the sustainability and effectiveness of information technology services.

The increasing complexity of digital infrastructures and the interconnected nature of information technology ecosystems have significantly expanded the attack surface available to cybercriminals. Modern organizations operate within environments characterized by cloud-based architectures, distributed systems, mobile platforms, IoT devices, and externally integrated services, all of which introduce new cybersecurity risks and governance challenges (Abdelwahed et al., 2025; Ali et al., 2025). Cyber threats are no longer limited to isolated malware attacks or unauthorized access attempts; instead, organizations now face advanced persistent threats, ransomware campaigns, phishing attacks, supply chain attacks, and sophisticated forms of social engineering capable of disrupting entire service ecosystems (Dominguez-Jimenez et al., 2024; Nguyen et al., 2024). Furthermore, the integration of artificial intelligence into digital services has created both new opportunities and new security concerns, as AI-enabled systems may themselves become targets of manipulation, exploitation, or adversarial attacks (Ali et al., 2025). Consequently, organizations must adopt cybersecurity strategies that extend beyond reactive defense mechanisms and encompass proactive governance, resilience, risk management, and adaptive organizational capabilities.

Recent studies have emphasized that cybersecurity preparedness requires multidimensional and integrated approaches rather than fragmented technical interventions. Chidukwani et al. highlighted that many organizations, particularly small and medium-sized enterprises, remain insufficiently prepared to address the evolving landscape of cyber threats due to limited strategic planning, inadequate awareness, and insufficient cybersecurity governance structures (Chidukwani et al., 2024). Similarly, Ahmed et al. argued that Industry 5.0 environments have intensified the need for decision-support models capable of prioritizing cybersecurity challenges and aligning cybersecurity initiatives with organizational objectives (Ahmed et al., 2024). These findings indicate that cybersecurity management can no longer be treated as an isolated operational function but must instead be integrated into organizational strategy, policy formulation, and managerial decision-making processes. Effective cybersecurity strategies therefore require coordination among technical, managerial, legal, and human dimensions to ensure comprehensive protection of digital assets and information technology services.

Another important issue in contemporary cybersecurity literature concerns the growing significance of cybersecurity governance and strategic legislation. Cappelletti and Papakonstantinou demonstrated that cybersecurity challenges increasingly transcend organizational boundaries and require coordinated governance frameworks, particularly in highly sensitive and technologically advanced sectors (Cappelletti & Papakonstantinou, 2025). In parallel, Omrani emphasized the importance of organizational information protection strategies and the role of modern ICT technologies in strengthening cybersecurity management within complex organizational environments (Omrani, 2025). These studies collectively suggest that cybersecurity effectiveness depends not only on technological infrastructure but also on governance structures, regulatory compliance, institutional commitment, and strategic alignment with organizational missions. Consequently, organizations that fail to establish integrated governance frameworks often encounter fragmented security practices, weak incident response capabilities, and inconsistent security policies.

The literature also demonstrates that cybersecurity risk management has become a critical component of strategic organizational planning. Huang and Murthy found that

cybersecurity risk management disclosures significantly influence investors' judgments and organizational credibility, highlighting the broader economic and strategic implications of cybersecurity governance (Huang & Murthy, 2024). Similarly, Nguyen et al. emphasized the necessity of systematic cybersecurity risk assessment and prioritization models within financial and banking systems, particularly in environments characterized by high digital dependency and elevated operational risks (Nguyen et al., 2024). The integration of cybersecurity risk management into organizational strategy enables institutions to identify vulnerabilities, prioritize threats, allocate resources effectively, and improve resilience against emerging cyber threats. However, many organizations continue to rely on fragmented or reactive security measures that fail to address the dynamic and interconnected nature of contemporary cybersecurity risks.

The role of human factors and organizational culture in cybersecurity effectiveness has also attracted considerable scholarly attention. Studies indicate that technical controls alone cannot ensure cybersecurity resilience in the absence of employee awareness, security-oriented organizational culture, and continuous capability development (Hosseingholipour, 2025). Human error, weak security awareness, noncompliance with security protocols, and inadequate training remain among the leading causes of cybersecurity incidents across organizations. Capaccioli et al. further emphasized that cybersecurity strategies must consider the needs and vulnerabilities of diverse users within digital service systems, particularly vulnerable or digitally marginalized populations (Capaccioli et al., 2023). Therefore, successful cybersecurity strategies require a balanced integration of technical safeguards, organizational learning, behavioral awareness, and human-centered design principles. Organizations must cultivate security cultures in which cybersecurity becomes embedded within daily operational practices, managerial priorities, and employee responsibilities.

At the same time, technological evolution continues to reshape cybersecurity requirements and strategic priorities. Rampasek et al. highlighted the increasing role of standardization, certification, and regulatory frameworks in enhancing the cybersecurity of AI-enabled digital products and services (Rampasek et al., 2024). Similarly, Abdelwahed et al. emphasized that IoT-based service environments require multi-layered cybersecurity architectures capable of managing heterogeneous communication protocols, distributed infrastructures, and interconnected systems (Abdelwahed et al., 2025). These developments indicate that cybersecurity strategies must remain adaptive and resilient in response to continuously evolving technological ecosystems. Traditional security approaches based solely on perimeter defense are no longer sufficient in environments characterized by distributed cloud services, mobile workforces, API-based integrations, and real-time data exchanges. As a result, organizations increasingly require integrated cybersecurity models capable of supporting resilience, service continuity, and sustainable digital transformation.

In addition, cybersecurity strategies are becoming increasingly important in relation to digital service continuity and organizational resilience. The disruption of information technology services caused by cyber incidents may result in severe operational, financial, and reputational consequences for organizations. Dominguez-Jimenez et al. emphasized the importance of early detection systems and advanced cybersecurity monitoring services for improving organizational responsiveness to cyber incidents (Dominguez-Jimenez et al., 2024). Moghaddasi similarly argued that cyber deterrence strategies play a critical role in reducing vulnerabilities and enhancing national and organizational cybersecurity capabilities within information and communication technology environments (Moghaddasi, 2022). Consequently, organizations must adopt comprehensive cybersecurity strategies that not only focus on prevention but also prioritize resilience, rapid recovery, incident response, and continuity planning. The capacity to maintain operational continuity during cyber crises has become a defining characteristic of digitally resilient organizations.

Despite the growing body of cybersecurity research, several theoretical and practical gaps remain within the literature concerning integrated cybersecurity strategies in information technology services. Much of the existing literature has focused on technical mechanisms, regulatory frameworks, or specific cybersecurity domains independently, while limited attention has been given to the development of comprehensive, context-oriented models that simultaneously integrate causal conditions, contextual factors, intervening variables, strategic actions, and organizational outcomes. Furthermore, previous studies have often examined cybersecurity from quantitative or technical perspectives without adequately exploring the underlying organizational processes, interactions, and strategic dynamics that shape cybersecurity practices in information technology service environments (Ahmed et al.,

2024; Chidukwani et al., 2024). Given the complexity and multidimensional nature of cybersecurity challenges, qualitative and grounded approaches are necessary to achieve a deeper understanding of how organizations conceptualize, implement, and operationalize cybersecurity strategies.

Moreover, the rapid evolution of cyber threats, regulatory requirements, technological infrastructures, and digital service ecosystems has created a pressing need for adaptive and integrated cybersecurity strategy models capable of addressing diverse organizational realities. Existing frameworks frequently lack sufficient attention to contextual and organizational variables such as governance structures, managerial commitment, organizational culture, resource allocation, ecosystem dependencies, and interorganizational collaboration. The absence of integrated models may lead organizations to adopt fragmented cybersecurity initiatives that fail to achieve sustainable resilience or strategic alignment. Consequently, there is a need for research capable of identifying the interconnected dimensions of cybersecurity strategies within information technology services and explaining the relationships among organizational conditions, strategic actions, and cybersecurity outcomes.

Accordingly, the present study seeks to design a grounded and integrated model of cybersecurity strategies in information technology services by identifying the causal, contextual, and intervening conditions influencing cybersecurity governance and by explaining the strategic actions and outcomes associated with cybersecurity implementation in organizational environments.

## 2. Methods and Materials

The present study is considered a qualitative research investigation. Given the existing theoretical gap, the systematic approach of Strauss and Corbin (1998) to grounded theory was employed as the primary qualitative research approach for designing a cybersecurity strategies model in information technology services. This approach seeks to provide a framework for the in-depth understanding and interpretation of cybersecurity strategies in information technology services. Grounded theory is a type of qualitative research methodology that inductively applies a series of systematic procedures to develop a theory regarding the phenomenon under investigation.

The statistical population consisted of academic experts and specialists in cybersecurity and information technology. The sample size included 15 participants selected through purposive and snowball sampling methods. Interviewees were asked to introduce other experts with relevant expertise in the field, which reflects the application of snowball sampling in qualitative research. The concept of purposive sampling in qualitative studies implies that the researcher intentionally selects participants who can significantly contribute to understanding the research problem and the central phenomenon under investigation. To collect the data, in-depth semi-structured interviews were conducted. Prior to the interviews, a summary of the research design, definitions of key concepts used in the study, as well as the main objectives and research questions, were sent to the interviewees via email, Telegram, or through the researcher's in-person visits in order to facilitate preliminary preparation for the interviews. At the beginning of each interview session, a brief explanation regarding the completed procedures and the research process was also provided.

Furthermore, according to Creswell and Creswell, qualitative researchers should employ validation strategies in their studies. The validation of the present research was conducted through dual coding, peer review, and member checking. Coding was independently performed by two individuals (the researcher and a collaborator), and the extracted codes were subsequently compared. Cohen's kappa coefficient was calculated at 86.9%, with a significance level of 0.001, indicating an almost complete agreement between the two coders. In addition to the researcher, the categories and the proposed model were reviewed by the academic supervisors, advisors, and three researchers specializing in startup innovation, and their comments were utilized to enrich and improve the model. For member checking, the results of the coding, analysis, categorization, and modeling processes were shared with three interviewees who possessed relevant academic backgrounds, and the findings were revised and refined based on their feedback.

## 3. Findings and Results

The data collection instrument consisted of interviews with specialists. The participants included managers, senior consultants, representatives, university professors, and senior managers in the fields of cybersecurity and information technology. Using the interview protocol, interviews were conducted with a sample of expert managers from various fields, and the required data for the study were

extracted from these interviews. Data analysis was carried out based on the grounded theory approach through coding and categorization procedures. In the initial phase of the study, understanding of the subject was achieved through open interviews with university professors and managers from different cybersecurity and information technology sectors. Moreover, observing the behavior of experts contributed to deepening the researcher's understanding. Subsequently, based on the coding and categorization processes, the conceptual model of the research was developed.

In addition, after each interview, the researcher extracted and coded the interview texts. Three stages of coding, namely open coding, axial coding, and selective coding, were performed on the data. Initially, the data were read line by line, and open codes, representing the participants' own words, were extracted.

The resulting codes were compared with previous codes, and conceptually similar codes were grouped into the same category, gradually leading to the formation of categories. The categories were then compared with one another and, where necessary, merged or divided into additional categories. In some cases, codes were transferred from one category to another until the axial category was ultimately identified. The basis of relational analysis in axial coding is the elaboration and expansion of one category, as demonstrated in the present study through the axial category entitled "The Role of the Cybersecurity Strategies Model in Information Technology Services," which emerged from causal conditions and influenced both the process and strategies, ultimately leading to the final outcomes. Selective coding subsequently clarified the relationships among the categories.

Following the scientific interviews conducted with academic and executive experts, the cybersecurity strategies model in information technology services emerged based on the grounded theory methodology. However, in order to document the methodology as well as the validity and reliability of the study, a brief overview of this process is presented below.

The next stage of analysis in grounded theory is axial coding. The objective of this stage is to establish relationships among the categories generated during the open coding stage. This process is conducted according to a paradigmatic model and assists the theorist in facilitating the theorization process. The essence of relational analysis in axial coding lies in the expansion and development of one category. However, conducting axial coding through this process is complex and requires four analytical operations to be performed simultaneously and distinctly.

In this model, causal conditions refer to events that create situations and issues related to a phenomenon and explain why and how individuals and groups respond through particular methods (Strauss & Corbin, 2008). Causal conditions include categories that directly influence the cybersecurity strategies model in information technology services, or factors that contribute to the creation and development of the phenomenon. In the present study, causal conditions constituted the cybersecurity strategies model in information technology services. The categories related to causal conditions are presented in Table 1.

**Table 1**

*Causal Categories (Main and Subcategories)*

| Row | Main Category | Subcategory | Codes Extracted from Interviews |
|---|---|---|---|
| 1 | Technological Conditions | Complexity of IT Infrastructure | Heterogeneity of systems and platforms; difficulty integrating legacy and modern systems; dependence on cloud services and SaaS; expansion of APIs and access points; use of emerging technologies such as artificial intelligence and the Internet of Things; increased attack surface |
| | | Cybersecurity Technical Maturity | Lack of integrated security architecture; limited use of SOC and SIEM; reactive security measures; weaknesses in vulnerability management; absence of regular penetration testing; lack of a zero-trust approach |
| 2 | Organizational Conditions | Governance and Management | Absence of a formal cybersecurity strategy; lack of senior management support; unclear roles and responsibilities; absence of a defined CISO role; fragmented decision-making in security matters; low prioritization of security in strategic planning |
| | | Resources and Investment | Limited cybersecurity budget; cost-oriented perspective toward security; shortage of specialized human resources; dependence on external contractors; absence of long-term investment planning; unbalanced resource allocation |
| 3 | Human Conditions | Security Awareness and Culture | Low employee awareness; neglect of continuous training; recurring human errors; disregard for security policies; weak incident-reporting culture; resistance to security controls |
| | | Specialized Skills and Competencies | Shortage of cybersecurity specialists; skill gaps within IT teams; unfamiliarity with emerging threats; weaknesses in security incident analysis; absence of professional development pathways; high turnover of specialized personnel |

| | | | |
|---|---|---|---|
| 4 | Environmental and Threat Conditions | Dynamics of Cyber Threats | Increase in targeted attacks; increasing complexity of malware; growth of ransomware attacks in IT services; supply chain threats; social engineering-based attacks; unfamiliarity with emerging attack patterns |
| | | Ecosystem Dependency | Dependence on technology suppliers; data sharing with business partners; security risks arising from outsourcing; lack of uniform security controls across the value chain; transfer of risks from partner organizations; weak third-party oversight |
| 5 | Legal and Governance Conditions | Regulatory Requirements | Obligation to comply with data protection regulations; pressure from regulatory bodies; ambiguity in cybersecurity legal requirements; differences between domestic and international regulations; risks of penalties and legal liabilities; mandatory reporting of security incidents |
| | | Frameworks and Standards | Necessity of compliance with ISO/IEC 27001; use of the NIST framework; lack of localization of security standards; symbolic implementation of frameworks; incomplete alignment of standards with IT services; excessive focus on documentation |

Contextual conditions represent a specific set of characteristics related to the phenomenon and generally refer to the location and circumstances of relevant events and occurrences. Contextual characteristics include factors without which the realization of the cybersecurity strategies model in information technology services would not be possible, and they provide the conditions under which strategies for managing, controlling, and responding to the phenomenon are implemented. These conditions consist of a set of contextual concepts, categories, and variables (Mohammadi, 2021). In Table 2, the main contextual factors of the cybersecurity strategies model in information technology services are presented.

**Table 2**

*Contextual Categories (Main and Subcategories)*

| Row | Main Category | Subcategory | Sample Codes Extracted from Interviews |
|---|---|---|---|
| 1 | Organizational Policies and Strategies | Management Commitment to Cybersecurity | Senior management emphasis on protocol compliance; allocation of security budget; direct managerial supervision; establishment of security KPIs; regular incident review meetings; issuance of formal guidelines |
| 2 | | Compliance with Standards and Regulations | Implementation of ISO 27001; monitoring privacy regulations; documentation of procedures; periodic audits; compliance with GDPR; updating internal regulations |
| 3 | Human Resources and Organizational Culture | Information Security Culture | Collective belief in the importance of security; individual accountability; team participation; support for whistleblowers; encouragement of responsible digital behavior; constructive criticism of weaknesses |
| 4 | Technology and Technical Infrastructure | Access Management and Authentication | Multi-factor authentication; role-based access control; account reviews; suspicious login detection; password encryption; removal of inactive accounts |
| 5 | | Network and Systems Protection | Multi-layer firewalls; IDS implementation; traffic monitoring; patch updates; environment segmentation; communication encryption |
| 6 | Risk Management and Security Monitoring | Threat and Vulnerability Assessment | Regular scanning; monthly risk reports; analysis of previous incidents; threat prioritization; risk management tools; documentation of findings |
| 7 | | Incident Response and Recovery | Incident response planning; rapid response teams; attack simulations; backup recovery; post-incident assessment; stakeholder notification |
| 8 | External Interactions and Technology Partners | Collaboration with Regulatory and Security Institutions | Information exchange with CERT; industry meetings; official alerts; cooperation with secure cloud providers; educational memoranda of understanding; collaborative investigations |
| 9 | | Supplier Security Assessment | Background checks; confidentiality commitments; outsourcing risk assessment; auditing external equipment; third-party access control; supplier selection guidelines |

Intervening conditions include broader circumstances such as time, environment, and culture that function as facilitators or constraints for strategies. These conditions either facilitate or restrict actions/interactions within a specific context. Each of these conditions forms a spectrum in which their influence may range from highly distant to highly proximate (Mohammadi, 2021). Table 3 presents the intervening conditions based on the factors of cybersecurity strategies in information technology services.

**Table 3**

*Intervening Categories (Main and Subcategories)*

| Main Category | Subcategory | Sample Concepts Extracted from Interviews |
|---|---|---|
| Environmental and Technological Factors | 1. Dynamics of the Information Technology Environment | Rapid technological changes; continuous system updates; shortened software life cycles; emergence of new technologies; instability of digital platforms; continuous changes in security requirements |
| | 2. Technical Complexity of Infrastructure | Complex network architectures; diversity of systems and platforms; difficulty integrating systems; interdependence of IT components; increase in vulnerable points; difficult management of distributed infrastructures |
| | 3. Intensity and Diversity of Cyber Threats | Increase in phishing attacks; advanced malware; ransomware attacks; insider threats; advanced persistent threats (APT); exploitation of security weaknesses |
| | 4. Dependence on External Technologies and Services | Use of cloud services; outsourcing IT services; dependence on software vendors; third-party security risks; limited control over external infrastructure; data sharing with partners |
| | 5. Environmental Uncertainty and Risk | Unpredictability of threats; sudden changes in technology regulations; innovation-related risks; ambiguity regarding security consequences; decision-making under uncertainty; increased operational risk |

The phenomenon under investigation must possess centrality, meaning that all other major categories can be related to it and that it repeatedly appears throughout the data. In other words, in all or nearly all cases, there are indications referring to that concept. The core phenomenon refers to the idea or phenomenon that forms the basis and central axis of the process to which all other major categories are connected. In this study, Table 4 presents the core categories of the cybersecurity strategy factors in information technology services.

**Table 4**

*Core Categories (Main and Subcategories)*

| Main Category | Subcategory | Sample Concepts Extracted from Interviews |
|---|---|---|
| Integrated Cybersecurity Strategy in Information Technology Services | 1. Alignment of Cybersecurity with Business Strategies | Alignment of security objectives with organizational goals; security support for IT service continuity; role of security in competitive advantage; security-oriented decision-making at the macro level; integration of security into strategic planning; value-oriented perspective toward security |
| | 2. Comprehensive Cyber Risk Management | Systematic identification of cyber risks; analysis of risk impacts on IT services; prioritization of threats; informed risk acceptance; implementation of risk management frameworks; continuous risk monitoring |
| | 3. Cybersecurity Governance and Policymaking | Development of formal cybersecurity policies; definition of roles and responsibilities; security governance structure; macro-level supervision and control; managerial accountability; policy compliance with laws and regulations |
| | 4. Resilience and Continuity of Information Technology Services | Maintaining the availability of critical services; preparedness against cyberattacks; rapid post-incident recovery; resilient architecture design; reduction of service downtime; continuity of digital business operations |
| | 5. Development of Technical and Human Cybersecurity Capabilities | Enhancement of specialized security team skills; utilization of modern security technologies; organizational learning in cybersecurity; integration of human and technical factors; investment in intelligent security tools; strengthening threat response capabilities |

Strategies are essentially plans and actions that emerge from the core category of the model and lead to outcomes. Strategies represent a set of measures adopted for managing, controlling, or responding to the phenomenon under investigation (Strauss & Corbin, 2008). Table 5 presents the strategies based on the core categories of cybersecurity strategy factors in information technology services.

**Table 5**

*Strategies Category (Action/Interaction, Main and Subcategories)*

| Row | Main Category | Subcategory | Sample Concepts Extracted from Interviews |
|---|---|---|---|
| 1 | Cybersecurity Governance and Policymaking Strategies | 1. Institutionalization of Cybersecurity Governance | Establishment of formal cybersecurity structures; definition of the CISO role; assignment of clear responsibilities; development of a cybersecurity charter; continuous managerial oversight; accountability at the macro level |
| | | 2. Integration of Security with Organizational Strategies | Inclusion of security in strategic decisions; alignment of security with business objectives; participation of the security unit in strategic planning; security as an organizational value; support from senior management; long-term perspective toward security |
| 2 | Technical and Operational Cybersecurity Strategies | 1. Strengthening Technical Infrastructure and Cyber Defense | Deployment of advanced security systems; use of SIEM and SOC; implementation of multilayer defense; encryption of communications; intelligent threat monitoring; automation of security processes |
| | | 2. Enhancing Resilience and Continuity of IT Services | Design of resilient architectures; regular backup procedures; business continuity planning; reduction of recovery time objectives (RTO); crisis scenario testing; preparedness for cyberattacks |
| 3 | Human, Knowledge-Based, and Interactive Cybersecurity Strategies | 1. Development of Human Cybersecurity Competencies | Specialized employee training; empowerment of security teams; enhancement of user security awareness; continuous learning; recruitment of specialized personnel; evaluation of security competencies |
| | | 2. Interaction and Collaboration within the Cybersecurity Ecosystem | Collaboration with security institutions; exchange of threat intelligence; supplier security management; participation in specialized networks; coordination with cloud service providers; interorganizational synergy |

Outcomes refer to the outputs or results of actions and interactions (Mohammadi, 2021). The final section of the cybersecurity strategies model in information technology services relates to outcomes. Based on open coding, the concepts associated with the model outcomes were extracted. Subsequently, through continuous movement between themes and concepts, the main categories were identified and labeled. Table 6 addresses the categories and concepts related to the outcomes.

**Table 6**

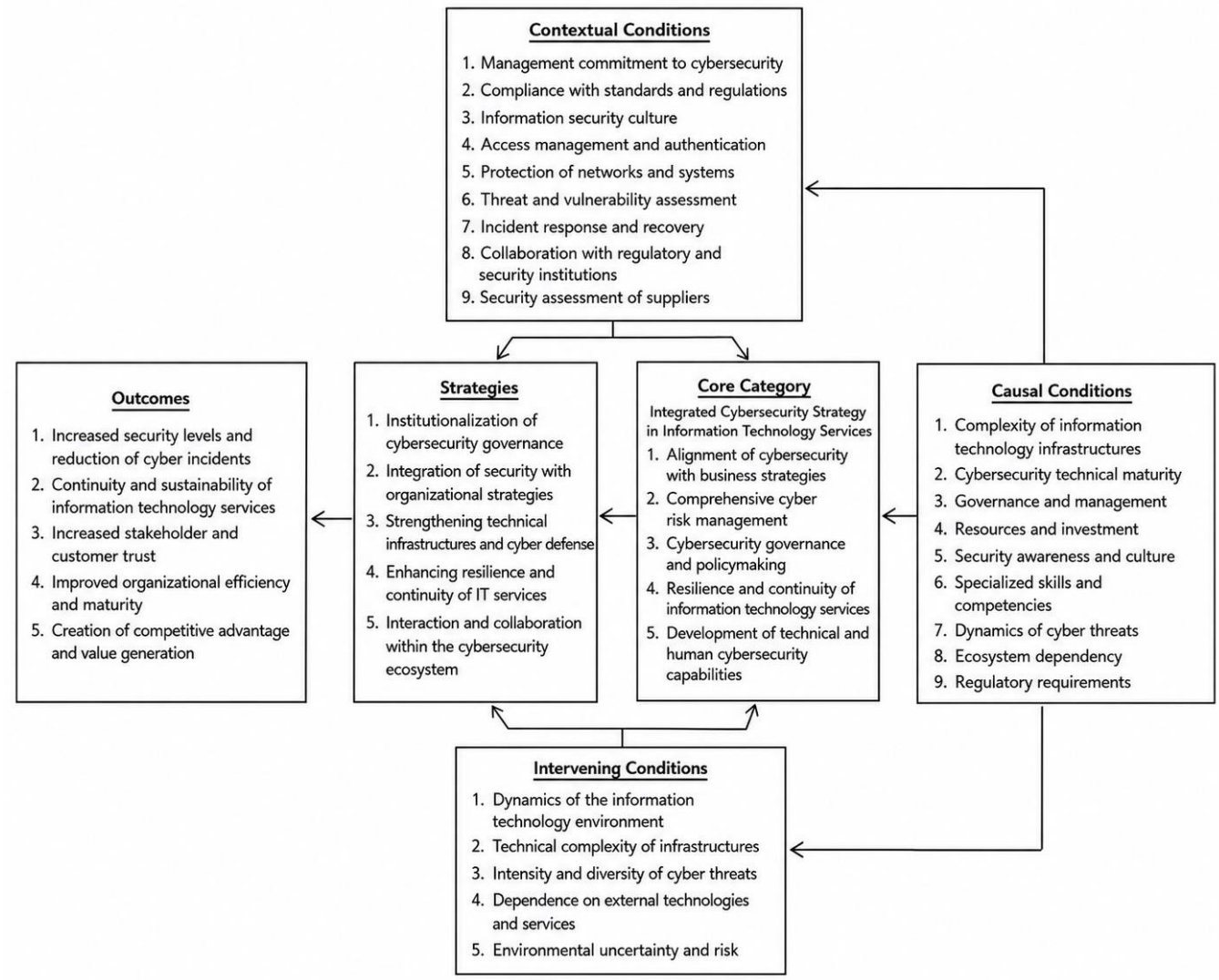
*Outcomes Category (Main and Subcategories)*

| Main Category | Subcategory | Sample Concepts Extracted from Interviews |
|---|---|---|
| Enhancing the Performance and Sustainability of Information Technology Services through Cybersecurity | 1. Increasing Security Levels and Reducing Cyber Incidents | Reduction in successful attacks; rapid threat detection; decreased system vulnerability; effective access control; reduction in security-related damages; improvement of cybersecurity status |
| | 2. Continuity and Sustainability of Information Technology Services | Increased service availability; reduction in system outages; maintenance of service delivery during crises; reduced downtime; assurance of digital service continuity; increased reliability of IT services |
| | 3. Increasing Stakeholder and Customer Trust | Increased customer trust in services; improvement of organizational image; user confidence in data protection; strengthening organizational credibility; stakeholder satisfaction; increased customer loyalty |
| | 4. Improvement of Organizational Efficiency and Maturity | Standardization of security processes; enhancement of cybersecurity maturity; more informed managerial decision-making; improved coordination among units; organizational learning; advancement of risk management levels |
| | 5. Creation of Competitive Advantage and Value Generation | Differentiation of secure services in the market; increased competitive advantage; support of digital innovation through security; reduction of incident-related costs; increased value of IT services; strengthening the strategic position of the organization |

The paradigmatic model of this study was designed based on the Strauss and Corbin paradigmatic framework. Considering these factors and conditions, the cybersecurity strategies model and process in information technology services were developed. Explaining the factors contributing to the formation of this phenomenon constituted the primary concern of the present study. The paradigmatic model of the research is illustrated in Figure 1.

**Figure 1**

*Paradigmatic Model*




## 4. Discussion and Conclusion

The present study aimed to design a grounded model of cybersecurity strategies in information technology services. The findings demonstrated that cybersecurity strategy formation in information technology services is a multidimensional and context-dependent process influenced by causal, contextual, and intervening conditions. The results identified technological, organizational, human, environmental, and regulatory conditions as the primary causal drivers shaping cybersecurity strategies in information technology services. In addition, the study revealed that contextual factors such as organizational commitment, security culture, technical infrastructure, and risk management mechanisms significantly affect the implementation and effectiveness of cybersecurity strategies. The findings further indicated that the core phenomenon emerging from the data was the development of an integrated cybersecurity strategy in information technology services, which encompasses strategic alignment, cyber risk management, governance, resilience, and capability development. The identified strategies included governance-oriented, technical-operational, and human-interactive approaches, which collectively contributed to outcomes such as enhanced security levels, continuity of IT services, increased stakeholder trust, improved organizational maturity, and competitive advantage creation.

One of the important findings of the study was the significant role of technological complexity and digital infrastructure evolution in shaping cybersecurity strategies. The participants emphasized that increasing dependence on

cloud services, distributed infrastructures, APIs, IoT systems, and AI-based technologies has considerably expanded the cybersecurity attack surface and intensified organizational vulnerabilities. This finding is consistent with the studies of Abdelwahed et al., who highlighted that interconnected IoT ecosystems and heterogeneous digital architectures require multilayered cybersecurity strategies capable of managing diverse communication protocols and distributed infrastructures (Abdelwahed et al., 2025). Similarly, Rampasek et al. emphasized that AI-enabled digital products and services have introduced new cybersecurity risks that necessitate adaptive governance mechanisms, certification frameworks, and dynamic security architectures (Rampasek et al., 2024). The present findings therefore reinforce the argument that cybersecurity in modern information technology services can no longer rely on traditional perimeter-based security models, but instead requires integrated and resilient approaches capable of responding to rapidly evolving technological ecosystems.

Another major finding of the study concerned the central role of governance and strategic management in cybersecurity effectiveness. The results indicated that organizations lacking formal cybersecurity governance structures, strategic security planning, and senior management commitment often experience fragmented security practices, weak coordination, and ineffective risk responses. Participants repeatedly emphasized the importance of defining clear security responsibilities, institutionalizing cybersecurity governance, and integrating cybersecurity into strategic organizational decision-making. This finding aligns with the research of Omrani, who demonstrated that cybersecurity management within organizations requires structured governance mechanisms, coordinated managerial oversight, and strategic ICT-based information protection systems (Omrani, 2025). Furthermore, Cappelletti and Papakonstantinou argued that cybersecurity governance increasingly depends on coordinated legislative and institutional frameworks capable of addressing complex digital security challenges (Cappelletti & Papakonstantinou, 2025). The findings of the present study suggest that cybersecurity governance functions as a strategic organizational capability rather than merely a technical control mechanism, and organizations that institutionalize governance structures are more capable of achieving resilience and sustainable cybersecurity performance.

The findings also demonstrated that cybersecurity risk management constitutes one of the central dimensions of integrated cybersecurity strategies. The participants highlighted the importance of continuous risk assessment, threat prioritization, vulnerability management, and proactive monitoring in maintaining cybersecurity resilience. The study identified that effective cybersecurity strategies depend on systematic risk management frameworks capable of identifying, evaluating, and mitigating evolving cyber threats. These findings are strongly supported by Nguyen et al., who emphasized the significance of strategic decision-making models for prioritizing cybersecurity risks within complex financial and banking systems (Nguyen et al., 2024). Similarly, Huang and Murthy found that organizations that disclose structured cybersecurity risk management strategies positively influence investor confidence and organizational credibility (Huang & Murthy, 2024). The convergence between these studies and the present findings indicates that cybersecurity risk management is not only a technical necessity but also a strategic organizational process that directly affects organizational trust, sustainability, and long-term performance.

Human and cultural factors also emerged as critical dimensions within the proposed cybersecurity strategy model. The findings revealed that employee awareness, organizational security culture, continuous training, and specialized cybersecurity competencies significantly influence the success or failure of cybersecurity initiatives. Participants emphasized that recurring human errors, insufficient awareness, and resistance to security policies frequently weaken cybersecurity systems despite the presence of technical safeguards. This finding is consistent with the study of Hosseingholipour, which emphasized that cybersecurity management strategies require continuous organizational learning, employee training, and security awareness development to effectively counter cyberattacks (Hosseingholipour, 2025). Likewise, Capaccioli et al. highlighted that cybersecurity-oriented service design should address human vulnerabilities and support responsible digital behavior among users (Capaccioli et al., 2023). The present findings therefore support the perspective that cybersecurity resilience depends heavily on organizational culture and human capability development in addition to technological investments.

The study additionally identified the importance of external interactions and ecosystem collaboration in cybersecurity management. Participants emphasized that organizations increasingly depend on external technology providers, cloud services, software vendors, and

interconnected partners, all of which introduce new forms of ecosystem risk and third-party vulnerabilities. As a result, collaboration with regulatory institutions, information-sharing networks, security agencies, and technology partners emerged as a key strategic dimension within the proposed model. These findings correspond with the research of Chidukwani et al., who found that organizations with stronger collaborative and preparedness mechanisms demonstrate higher levels of cybersecurity resilience and adaptive capability (Chidukwani et al., 2024). Similarly, Ahmed et al. argued that Industry 5.0 cybersecurity challenges require collaborative decision-support frameworks that integrate technical, organizational, and interorganizational dimensions (Ahmed et al., 2024). The results of the present study therefore indicate that cybersecurity strategies must extend beyond organizational boundaries and address the broader digital ecosystem within which information technology services operate.

Another significant finding was the identification of resilience and continuity as central outcomes of cybersecurity strategy implementation. The findings demonstrated that integrated cybersecurity strategies improve service availability, reduce downtime, strengthen incident response capability, and support business continuity during cyber crises. Participants emphasized that organizations capable of rapidly recovering from cyber incidents are better positioned to maintain stakeholder trust and sustain operational stability. This finding is consistent with Dominguez-Jimenez et al., who highlighted the importance of advanced cybersecurity event detection and monitoring systems in improving organizational responsiveness and operational continuity (Dominguez-Jimenez et al., 2024). Furthermore, Moghaddasi argued that cyber deterrence and preparedness strategies play essential roles in strengthening resilience and reducing cybersecurity vulnerabilities within information and communication technology environments (Moghaddasi, 2022). These findings collectively indicate that cybersecurity resilience is increasingly becoming a strategic determinant of organizational sustainability and digital service continuity.

The findings further revealed that integrated cybersecurity strategies contribute significantly to organizational maturity, strategic value creation, and competitive advantage. Participants reported that organizations implementing structured cybersecurity governance and proactive security mechanisms experience improved coordination, more informed managerial decision-making, greater stakeholder confidence, and stronger market positioning. This result aligns with the findings of Huang and Murthy, who demonstrated that cybersecurity risk management strategies influence stakeholder perceptions and organizational legitimacy (Huang & Murthy, 2024). Similarly, Turegun emphasized that digital transformation processes expose organizations to significant cybersecurity risks that can only be effectively managed through integrated and strategically aligned security approaches (Turegun, 2024). The present study therefore suggests that cybersecurity has evolved into a strategic organizational asset capable of supporting innovation, competitiveness, and sustainable digital transformation.

The proposed grounded model contributes to the cybersecurity literature by integrating causal conditions, contextual factors, intervening variables, strategic actions, and organizational outcomes into a unified explanatory framework. Unlike many previous studies that primarily focused on technical or regulatory aspects independently, the present research provides a multidimensional understanding of cybersecurity strategy formation within information technology services. The model highlights the interconnectedness of governance structures, technological infrastructures, organizational culture, ecosystem interactions, and risk management processes in shaping cybersecurity effectiveness. In doing so, the study extends existing cybersecurity research by demonstrating that cybersecurity strategy should be conceptualized as an integrated organizational phenomenon influenced by dynamic technological, managerial, and environmental conditions.

One of the theoretical implications of the findings is the recognition that cybersecurity strategies in information technology services cannot be universally standardized without considering contextual organizational conditions. The grounded theory approach revealed that cybersecurity effectiveness depends on the interaction among organizational resources, technological maturity, leadership commitment, environmental uncertainty, and ecosystem dependencies. Consequently, organizations require adaptive and context-sensitive cybersecurity strategies capable of evolving alongside digital transformation processes and emerging cyber threats. The findings also reinforce the argument that cybersecurity governance must be embedded within organizational strategic planning rather than isolated within technical departments. This integrated perspective contributes to the growing body of research emphasizing the strategic, organizational, and socio-technical nature of cybersecurity management.

The study was subject to several limitations. First, the research adopted a qualitative grounded theory approach and relied on interviews with a relatively limited number of experts, which may restrict the generalizability of the findings to all organizational contexts. Second, the study focused primarily on experts within cybersecurity and information technology environments, and therefore the perspectives of end-users, operational staff, and nontechnical stakeholders were not extensively examined. Third, the rapidly evolving nature of cybersecurity technologies and threats means that some identified concepts and relationships may change over time as digital ecosystems continue to evolve. Finally, organizational confidentiality and sensitivity surrounding cybersecurity issues may have limited the depth of disclosure provided by some participants during interviews.

Future research could further examine the proposed model through quantitative or mixed-method approaches in order to validate the identified relationships and categories across larger organizational populations. Comparative studies across industries, countries, and organizational sizes may also provide deeper insights into contextual differences influencing cybersecurity strategy implementation. Future studies may additionally explore the role of emerging technologies such as artificial intelligence, blockchain, quantum computing, and autonomous systems in reshaping cybersecurity governance and resilience strategies. Investigating the behavioral and psychological dimensions of cybersecurity culture and decision-making may also contribute to a more comprehensive understanding of organizational cybersecurity dynamics.

From a practical perspective, organizations should prioritize the integration of cybersecurity into strategic planning and organizational governance structures rather than treating security solely as a technical function. Managers should invest in continuous cybersecurity training, organizational awareness programs, and the development of specialized human capabilities to reduce human-related vulnerabilities. Organizations should also strengthen collaboration with regulatory institutions, technology partners, and cybersecurity ecosystems in order to improve information sharing and coordinated threat response. Furthermore, implementing proactive risk management frameworks, resilient technical infrastructures, and incident recovery mechanisms can significantly enhance service continuity, stakeholder trust, and long-term organizational sustainability in increasingly complex digital environments.

## Authors' Contributions

Authors contributed equally to this article.

## Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

## Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

## Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

## Declaration of Interest

The authors report no conflict of interest.

## Funding

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

## Ethics Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were considered.

## References

Abdelwahed, S. H., Hefny, I. M., Hegazy, M., Said, L. A., & Soltan, A. (2025). Survey of IoT Multi-Protocol Gateways: Architectures, Protocols, and Cybersecurity. *Internet of Things*, *33*, 101703. https://doi.org/10.1016/j.iot.2025.101703

Ahmed, I., Hossain, N. U., Fazio, S. A., Lezzi, M., & Islam, M. S. (2024). A Decision Support Model for Assessing and Prioritization of Industry 5.0 Cybersecurity Challenges. *Sustainable Manufacturing and Service Economics*, *3*, 100018. https://doi.org/10.1016/j.smse.2024.100018

Ali, S., Wang, J., Leung, V. C. M., Bashir, F., Bhatti, U. A., Wadho, S. A., & Humayun, M. (2025). CLDM-MMNNs: Cross-Layer Defense Mechanisms Through Multi-Modal Neural Networks Fusion for End-to-End Cybersecurity—Issues, Challenges, and Future Directions. *Information Fusion*, *122*, 103222. https://doi.org/10.1016/j.inffus.2025.103222

Capaccioli, A., Urciuoli, L., Di Ciommo, F., Rondinella, G., Giorgi, S., & Hueting, R. (2023). Including the Excluded: How Can Design of Digital Delivery Service Address Cybersecurity Concerns of Vulnerable Users? *Transportation Research Procedia*, *72*, 2604-2611. https://doi.org/10.1016/j.trpro.2023.11.791

Cappelletti, F., & Papakonstantinou, V. (2025). A Question of Strategic Legislation: Can the EU Deal with Cybersecurity Issues in Space? *Telecommunications Policy*, *49*(5), 102954. https://doi.org/10.1016/j.telpol.2025.102954

Chidukwani, A., Zander, S., & Koutsakis, P. (2024). Cybersecurity Preparedness of Small-to-Medium Businesses: A Western Australia Study with Broader Implications. *Computers & Security*, *145*, 104026. https://doi.org/10.1016/j.cose.2024.104026

Dominguez-Jimenez, J. J., Gomez Sanchez, R., Medina-Bulo, I., Boubeta-Puig, J., Rodriguez-Garcia, M., Munoz-Ortega, A., Balderas-Diaz, S., Guerrero-Contreras, G., Silva-Ramirez, E. L., Rosa-Bilbao, J., Luna-Ramos, P., Carretero Henares, J. J., Molina Cabrera, A. J., Fuentes Landi, G., & Torres Gomez, P. (2024). SEADETEC: Advanced Service for Early Detection of Cybersecurity Events. *Heliyon*, *10*(19), e37893. https://doi.org/10.1016/j.heliyon.2024.e37893

Hosseingholipour, M. (2025). Information Security Management Strategies to Counter Cyberattacks in Computer Networks. Twenty-Fourth National Conference on Applied Research in Electrical, Computer, and Biomedical Engineering Sciences,

Huang, J., & Murthy, U. (2024). The Impact of Cybersecurity Risk Management Strategy Disclosure on Investors' Judgments and Decisions. *International Journal of Accounting Information Systems*, *54*, 100696. https://doi.org/10.1016/j.accinf.2024.100696

Moghaddasi, A. (2022). Cyber Deterrence Strategies in the Context of Information and Communication Technology. Fifth National Conference on Modern Technologies in Electrical, Computer, and Mechanical Engineering of Iran,

Nguyen, P. H., Pham, T. V., Nguyen, L. A. T., Pham, H. A. T., Nguyen, T. H. T., & Vu, T. G. (2024). 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*, *10*(19), e37893. https://doi.org/10.1016/j.heliyon.2024.e37893

Omrani, M. (2025). Analysis and Review of Organizational Information and Data Protection and Cybersecurity Using Modern Information and Communication Technologies (ICT) in Municipalities. *Quarterly Journal of New Research in Management and Accounting*, *6*(12).

Rampasek, M., Mesarcik, M., & Andrasko, J. (2024). Evolving Cybersecurity of AI-Featured Digital Products and Services: Rise of Standardisation and Certification? *Computer Law & Security Review*, *56*, 106093. https://doi.org/10.1016/j.clsr.2024.106093

Turegun, N. (2024). Digital Transformation and Cybersecurity Risks. *International Journal of Accounting Information Systems*.