

# Building Cyber Resilient IT Service Organizations Through Digital Leadership and Employee Cybersecurity Capability

Rasyid Tarmizi<sup>1\*</sup> , Andriyansah<sup>2</sup> , Mohd Faiz Hilmi<sup>3</sup> , Yuce Sariningsih<sup>4</sup> , Richard Evans<sup>5</sup> 

<sup>1</sup>Faculty of Economics and Business, Universitas Raharja, Indonesia

<sup>2</sup>Faculty of Economics and Business, Universitas Terbuka, Indonesia

<sup>3</sup>School of Distance Education, Universiti Sains Malaysia, Malaysia

<sup>4</sup>Department of Social Work, Universitas Pasundan, Indonesia

<sup>5</sup>ADI Research Center, United States

<sup>1</sup>rasyid@raharja.info, <sup>2</sup>andri@ecampus.ut.ac.id, <sup>3</sup>faiz@usm.my, <sup>4</sup>yucesp@unpas.ac.id, <sup>5</sup>vans.richard@adi-journal.org

\*Corresponding Author

## Article Info

### Article history:

Submission April 13, 2026

Revised September 18, 2026

Accepted October 13, 2026

Published October 20, 2026

### Keywords:

Digital Leadership

Cybersecurity Capability

Cyber Resilience

IT Service Management

Digital Transformation



## ABSTRACT

**The rapid advancement** of digital transformation has significantly enhanced organizational efficiency while simultaneously increasing exposure to sophisticated cyber threats that may compromise business continuity, stakeholder trust, and long-term organizational sustainability. These challenges require IT service organizations to strengthen cyber resilience by integrating effective digital leadership with employee cybersecurity capability, thereby fostering a secure, innovative, and sustainable digital ecosystem. **This study aims** to examine the influence of digital leadership on employee cybersecurity capability and its subsequent impact on organizational cyber resilience. **A quantitative research** approach was employed using a survey of employees working in IT service organizations, and the proposed research model was analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). The **findings** indicate that digital leadership positively and significantly enhances employee cybersecurity capability, which in turn plays a crucial role in strengthening organizational cyber resilience. Furthermore, employee cybersecurity capability acts as a significant mediating mechanism between digital leadership and cyber resilience, enabling organizations to anticipate, detect, respond to, and recover more effectively from evolving cyber threats. These **findings** demonstrate that adaptive digital leadership combined with continuous investment in employees' cybersecurity competencies constitutes a critical organizational capability for maintaining resilient digital operations and sustaining long-term organizational performance. **This study contributes** to the growing literature on digital leadership and cyber resilience while providing strategic insights for IT service organizations seeking to establish a sustainable cybersecurity culture that supports resilient digital infrastructure and inclusive technological innovation.

*This is an open access article under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.*



DOI: <https://doi.org/10.34306/ijcitsm.v6i2.278>

This is an open-access article under the CC-BY license (<https://creativecommons.org/licenses/by/4.0/>)

©Authors retain all copyrights

## 1. INTRODUCTION

The rapid advancement of digital transformation has reshaped organizational processes through technologies such as cloud computing, artificial intelligence (AI), big data analytics, and the Internet of Things

(IoT). For IT service organizations, these technologies support operational efficiency, service innovation, and competitive advantage, but they also increase exposure to sophisticated cyber threats. Cybersecurity therefore represents not only a technical concern but also a strategic organizational priority affecting business continuity, stakeholder trust, and organizational sustainability [1].

Cyberattacks such as ransomware, phishing, advanced persistent threats, insider threats, and supply chain attacks can disrupt operations, compromise sensitive information, and damage organizational reputation [2]. Consequently, organizations require not only preventive cybersecurity measures but also the capability to maintain critical operations, respond effectively to incidents, recover from disruptions, and adapt to evolving threats. This capability is reflected in Organizational Cyber Resilience.

Building cyber resilience requires more than technological safeguards. Effective governance, cybersecurity-oriented leadership, and capable employees are also essential. Digital Leadership can establish strategic cybersecurity priorities, allocate resources, promote security-oriented culture, and support continuous organizational learning [3]. At the employee level, Employee Cybersecurity Capability encompasses cybersecurity knowledge, technical competence, security awareness, policy compliance, and the ability to recognize and respond to cyber threats.

Although research on digital leadership, cybersecurity, and organizational resilience has expanded, their interrelationship remains insufficiently understood. Existing studies frequently examine digital leadership in relation to digital transformation and organizational performance, while cybersecurity and resilience studies tend to emphasize technological, governance, and risk management mechanisms [4]. The role of Employee Cybersecurity Capability as a mechanism linking Digital Leadership to Organizational Cyber Resilience therefore remains underexplored, particularly in IT service organizations. To address this gap, this study proposes an integrated model linking Digital Leadership, Employee Cybersecurity Capability, and Organizational Cyber Resilience. The study examines the direct influence of Digital Leadership on Employee Cybersecurity Capability and Organizational Cyber Resilience, the effect of Employee Cybersecurity Capability on Organizational Cyber Resilience, and the mediating role of Employee Cybersecurity Capability.

To further distinguish the proposed model from previous cybersecurity and organizational resilience studies, this study positions Employee Cybersecurity Capability as a mediating mechanism between Digital Leadership and Organizational Cyber Resilience. Previous studies have commonly examined cybersecurity awareness or employee security behavior as individual-level outcomes, while leadership studies have primarily focused on digital transformation, organizational performance, or technology adoption [5]. Other cyber resilience studies have emphasized technological preparedness, governance, and organizational response capabilities. In contrast, the proposed model explains how leadership-driven organizational conditions are translated into employees' cybersecurity knowledge, competence, awareness, compliance, and threat response capability, which subsequently contributes to organizational cyber resilience [6]. Therefore, the unique contribution of this study lies in empirically examining Employee Cybersecurity Capability as a mediating mechanism that connects Digital Leadership with Organizational Cyber Resilience within IT service organizations.

The organizational focus of this study also relates to the Sustainable Development Goals (SDGs), particularly SDG 9 and SDG 16. Strengthening Organizational Cyber Resilience can support the continuity and reliability of digital infrastructure and IT services, while Digital Leadership and Employee Cybersecurity Capability contribute to secure conditions for technological innovation and sustainable digital operations, aligning with SDG 9 [7]. At the same time, cybersecurity-oriented leadership, employee compliance, and organizational preparedness strengthen responsible digital governance and trustworthy organizational operations, which are relevant to SDG 16. These linkages highlight the broader contribution of the proposed framework to secure, resilient, and trustworthy digital service environments.

## 2. LITERATURE REVIEW

This section provides the conceptual and theoretical foundation for the relationships among Digital Leadership, Employee Cybersecurity Capability, and Organizational Cyber Resilience. The review goes beyond defining the key constructs by explaining their roles within IT service organizations and the mechanisms through which leadership and employee capability contribute to cyber resilience [8]. Particular attention is given to the organizational relationship between leadership practices, employee capability development, and the capacity to maintain secure and resilient digital operations.

### 2.1. Digital Leadership

Digital Leadership refers to leaders' ability to leverage digital technologies to guide organizational transformation, stimulate innovation, and strengthen organizational adaptability in dynamic business environments. Unlike traditional leadership, digital leadership integrates technological initiatives with strategic decision-making, organizational culture, and employee development to support sustainable organizational performance [9]. Digital leaders therefore act not only as decision makers but also as change agents who establish digital direction, encourage continuous learning, foster collaboration, and support the implementation of digital transformation initiatives.

In cybersecurity contexts, Digital Leadership plays a strategic role in establishing security priorities, allocating organizational resources, promoting a cybersecurity-oriented culture, and supporting employee capability development [10]. These leadership practices create organizational conditions in which cybersecurity becomes part of strategic and operational decision-making rather than a separate technical responsibility. Within IT service organizations, such conditions are particularly important because continuous digital operations require organizations to remain adaptable while maintaining secure and reliable services. Accordingly, Digital Leadership provides the strategic and organizational foundation for developing employee cybersecurity capability and strengthening organizational cyber resilience.

### 2.2. Employee Cybersecurity Capability

Employee Cybersecurity Capability represents employees' ability to understand, apply, and maintain secure practices while performing their work [11]. It encompasses cybersecurity knowledge, technical competence, security awareness, compliance with organizational security policies, and the ability to identify, prevent, and respond to cyber threats [12]. These capabilities are important because employees interact directly with organizational information systems and digital services, making their knowledge and behavior an essential part of organizational cybersecurity.

Employee Cybersecurity Capability should therefore be understood not only as an individual competency but also as an organizational capability that supports secure and sustainable digital operations [13]. Employees with adequate cybersecurity capability can translate organizational security policies and leadership direction into daily practices, including threat recognition, policy compliance, incident reporting, and appropriate response activities [14]. Strengthening these capabilities can reduce human-related vulnerabilities while enabling employees to contribute more effectively to cybersecurity preparedness, response, and recovery. In this context, employee capability provides an important human component for sustaining organizational cyber resilience.

### 2.3. Organizational Cyber Resilience

Organizational Cyber Resilience refers to an organization's ability to anticipate, withstand, respond to, recover from, and adapt to cybersecurity disruptions while maintaining critical operations [15]. Unlike cybersecurity approaches that primarily emphasize protection and prevention, cyber resilience focuses on the organization's ability to maintain operational continuity, respond effectively to incidents, recover from disruption, and adapt to an evolving threat landscape [16]. This distinction makes cyber resilience particularly relevant to IT service organizations whose operations depend heavily on continuous digital service availability.

Organizational Cyber Resilience is not determined solely by technological safeguards. It requires the integration of technological infrastructure, cybersecurity governance, organizational preparedness, and competent human resources. Employees contribute to this resilience through their ability to recognize threats, follow security procedures, report incidents, and participate in response and recovery activities [17]. Effective organizational cyber resilience therefore reflects a broader organizational capability that combines technology, governance, and human competencies to sustain critical digital services during and after cybersecurity disruptions.

### 2.4. Theoretical Integration and Conceptual Relationships

The proposed relationships can be understood from an organizational capability perspective [18]. Digital Leadership establishes strategic priorities, governance conditions, resource support, and learning opportunities that facilitate the development of Employee Cybersecurity Capability [19]. Through these organizational conditions, employees can develop the knowledge, awareness, technical competence, and compliance necessary to perform secure digital practices [20]. Employee Cybersecurity Capability consequently represents the operational mechanism through which leadership support can be translated into cybersecurity practices at

---

the employee level. The relationship between Employee Cybersecurity Capability and Organizational Cyber Resilience follows from employees' direct involvement in cybersecurity activities. Employees with sufficient capability can recognize emerging threats, apply preventive practices, comply with security policies, report incidents, and support response and recovery activities [21]. These contributions strengthen the organization's ability to maintain critical operations and recover from cybersecurity disruptions. Thus, employee capability complements technological and governance mechanisms in supporting organizational cyber resilience.

The model therefore proposes both a direct pathway from Digital Leadership to Organizational Cyber Resilience and an indirect pathway through Employee Cybersecurity Capability [22]. The direct pathway reflects leadership's role in establishing cybersecurity priorities, allocating resources, supporting governance, and creating organizational preparedness. The indirect pathway reflects how leadership practices are translated into employee cybersecurity capabilities and subsequently into resilient cybersecurity practices. This mechanism provides the theoretical basis for positioning Employee Cybersecurity Capability as a mediator between Digital Leadership and Organizational Cyber Resilience.

Accordingly, the proposed framework views leadership and employee capability as complementary organizational resources rather than independent determinants. Digital Leadership creates the strategic and organizational conditions for capability development, while Employee Cybersecurity Capability enables those conditions to be implemented through employees' daily cybersecurity practices. This integrated relationship provides the conceptual basis for examining how leadership, human capability, and organizational resilience are connected within IT service organizations.

### 3. RESEARCH METHODOLOGY

This study was designed to examine the relationships among Digital Leadership, Employee Cybersecurity Capability, and Organizational Cyber Resilience within IT service organizations [23]. Building upon the conceptual framework developed in the literature review, the research investigates how digital leadership contributes to organizational cyber resilience both directly and indirectly through the enhancement of employees' cybersecurity capability. To empirically validate the proposed relationships, a quantitative survey approach was employed and analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM).

#### 3.1. Research Design

This study adopted a quantitative explanatory research design to examine the causal relationships among the proposed latent constructs. The explanatory approach was selected because it enables empirical testing of both direct and indirect relationships represented in the conceptual model while providing predictive insights into organizational cyber resilience [15]. The proposed research model consists of three principal constructs: Digital Leadership (DL) as the exogenous construct, Employee Cybersecurity Capability (ECC) as the mediating construct, and Organizational Cyber Resilience (OCR) as the endogenous construct. The model explains how leadership-driven initiatives foster employees' cybersecurity capability, which subsequently strengthens organizational resilience against evolving cyber threats [24].

#### 3.2. Population, Sample, and Data Collection

The target population comprised employees working in IT service organizations in Indonesia, including software development companies, cloud service providers, IT consulting firms, managed IT service providers, and cybersecurity-related organizations. Purposive sampling was employed because the study required respondents with relevant professional experience in digital operations and organizational cybersecurity practices [25]. Respondents were required to work in an IT service organization, have at least one year of professional experience, regularly use organizational digital systems in their work, and have sufficient familiarity with organizational cybersecurity policies and practices. These criteria ensured that respondents possessed adequate organizational and cybersecurity-related experience to provide informed assessments of Digital Leadership, Employee Cybersecurity Capability, and Organizational Cyber Resilience.

Primary data were collected through an online questionnaire distributed to respondents who met the predefined eligibility criteria. Participation was voluntary, and respondents were informed about the research purpose and the confidentiality of their responses. The collected responses were screened to exclude incomplete questionnaires, duplicate submissions, and responses with inconsistent patterns. After the screening process, 245 valid responses were retained for subsequent analysis.

### 3.3. Research Instrument

The research instrument was developed based on the conceptual definitions and dimensions of the three constructs examined in this study and was contextualized to the IT service environment [26]. The measurement items were formulated to represent the substantive dimensions of each construct [27]. Digital Leadership was operationalized through indicators reflecting leaders' ability to drive digital transformation, integrate digital strategies, cultivate a cybersecurity-oriented culture, encourage innovation, and support technology-based decision-making. Employee Cybersecurity Capability was operationalized through indicators covering cybersecurity knowledge, security awareness, policy compliance, technical competence, and secure digital behavior [6]. Organizational Cyber Resilience was operationalized through indicators reflecting the organizations' capability to anticipate, withstand, respond to, recover from, and adapt to cybersecurity threats and disruptions.

All constructs were measured using a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). The measurement items were reviewed to ensure that their wording was clear and relevant to the IT service organizational context [28]. The instrument was subsequently prepared for the main survey after the measurement items had been assessed for their relevance to the conceptual definitions of the respective constructs.

### 3.4. Data Analysis

The collected data were analyzed using SmartPLS 4 through the Partial Least Squares Structural Equation Modeling (PLS-SEM) approach [29]. PLS-SEM was selected because the proposed model involves multiple latent constructs and examines both direct and indirect relationships, with Employee Cybersecurity Capability positioned as a mediating construct [7]. The approach is particularly appropriate for the prediction oriented objective of this study, which examines how Digital Leadership contributes to Employee Cybersecurity Capability and how both constructs contribute to Organizational Cyber Resilience [30]. PLS-SEM also enables the simultaneous evaluation of the reflective measurement model and the structural relationships among the proposed constructs.

Model evaluation was conducted in two stages. The first stage assessed the measurement model (outer model) by examining indicator loadings, Cronbach's alpha, Composite Reliability (CR), Average Variance Extracted (AVE), discriminant validity using the Fornell–Larcker Criterion and the Heterotrait–Monotrait Ratio (HTMT), and multicollinearity using the Variance Inflation Factor (VIF). The second stage evaluated the structural model (inner model) through the coefficient of determination ( $R^2$ ), effect size ( $f^2$ ), predictive relevance ( $Q^2$ ), and the Standardized Root Mean Square Residual (SRMR) to assess the model's explanatory and predictive performance [31].

### 3.5. Hypothesis Testing

Hypothesis testing was performed using the bootstrapping procedure with 5,000 resamples at a 5% significance level. The significance of the proposed relationships was evaluated using the path coefficient ( $\beta$ ), t-statistics, p-values, and confidence intervals [32]. The analysis examined the direct effects of Digital Leadership on Employee Cybersecurity Capability, Digital Leadership on Organizational Cyber Resilience, and Employee Cybersecurity Capability on Organizational Cyber Resilience, as well as the indirect effect assessing the mediating role of Employee Cybersecurity Capability in translating digital leadership practices into enhanced organizational cyber resilience [33]. The findings provide empirical evidence for validating the proposed conceptual model and addressing the research objectives.

## 4. RESULTS AND DISCUSSION

This section presents the empirical findings resulting from the data analysis conducted via Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS 4. The evaluation is structured into two main phases: the assessment of the measurement model (outer model) to ensure data reliability and validity, followed by the assessment of the structural model (inner model) to evaluate the hypothesized relationships [34]. Subsequently, a comprehensive discussion is provided to contextualize these empirical outcomes within the broader theoretical and managerial landscapes of IT service environments.

---

#### 4.1. Respondent Profile

A total of 245 valid questionnaires were gathered from professionals working in various IT service organizations in Indonesia, including cloud service providers, IT consultancies, software development agencies, and managed service providers (MSPs).

Table 1. Demographic Profile of Respondents (N=245)

| Demographic Variable       | Category                       | Frequency<br>(N=245) | Percentage<br>(%) |
|----------------------------|--------------------------------|----------------------|-------------------|
| Gender                     | Male                           | 142                  | 57.96%            |
|                            | Female                         | 103                  | 42.04%            |
| Experience in IT<br>Sector | 1–3 Years                      | 68                   | 27.76%            |
|                            | 4–7 Years                      | 118                  | 48.16%            |
|                            | > 7 Years                      | 59                   | 24.08%            |
| Organization Type          | Managed Service Provider (MSP) | 84                   | 34.29%            |
|                            | Cloud & Software Development   | 92                   | 37.55%            |
|                            | IT Consulting & Cybersecurity  | 69                   | 28.16%            |

Table 1 presents the demographic characteristics of the 245 respondents working across various IT service organizations in Indonesia. The respondents were distributed across managed service providers, cloud and software development organizations, and IT consulting and cybersecurity organizations. The largest group consisted of respondents with 4–7 years of IT experience (48.16%), indicating that most participants had substantial professional exposure to IT service environments. This respondent composition supports the relevance of the sample to the research context because the participants were sufficiently exposed to digital systems, cybersecurity practices, and organizational operations required to assess Digital Leadership, Employee Cybersecurity Capability, and Organizational Cyber Resilience.

#### 4.2. Measurement Model Assessment (Outer Model)

Evaluating the reflective measurement model involved assessing internal consistency reliability, indicator reliability, convergent validity, and discriminant validity.

- **Indicator Reliability and Convergent Validity** Convergent validity was established as all indicator factor loadings exceeded the standard threshold of 0.70. Construct reliability was confirmed since Cronbach's alpha and Composite Reliability ( $\rho_a$ ,  $\rho_c$ ) values exceeded 0.70. Furthermore, the Average Variance Extracted (AVE) for all latent variables exceeded the 0.50 benchmark.

Table 2. Measurement Model Evaluation (Outer Model Results)

| Construct                               | Indicator | Outer Loading | Cronbach's Alpha | Composite Reliability | AVE   |
|-----------------------------------------|-----------|---------------|------------------|-----------------------|-------|
| Digital Leadership (DL)                 | DL1       | 0.812         | 0.884            | 0.918                 | 0.691 |
|                                         | DL2       | 0.845         |                  |                       |       |
|                                         | DL3       | 0.838         |                  |                       |       |
|                                         | DL4       | 0.829         |                  |                       |       |
| Employee Cybersecurity Capability (ECC) | ECC1      | 0.798         | 0.892            | 0.921                 | 0.699 |
|                                         | ECC2      | 0.842         |                  |                       |       |
|                                         | ECC3      | 0.851         |                  |                       |       |
|                                         | ECC4      | 0.852         |                  |                       |       |
| Organizational Cyber Resilience (OCR)   | OCR1      | 0.831         | 0.905            | 0.930                 | 0.726 |
|                                         | OCR2      | 0.864         |                  |                       |       |
|                                         | OCR3      | 0.871         |                  |                       |       |
|                                         | OCR4      | 0.841         |                  |                       |       |

Table 2 demonstrates the measurement quality of the three constructs examined in this study: Digital Leadership, Employee Cybersecurity Capability, and Organizational Cyber Resilience. The outer loading

values ranging from 0.798 to 0.871 indicate that each indicator consistently represents its corresponding construct. At the construct level, Cronbach's alpha and Composite Reliability values above 0.70 indicate satisfactory internal consistency. The AVE values of 0.691–0.726 further show that the constructs capture an adequate proportion of variance from their respective indicators. Overall, these results establish the adequacy of the measurement instrument and provide a sound basis for examining the structural relationships in the proposed model.

#### 4.3. Discriminant Validity

Discriminant validity was assessed to determine whether Digital Leadership, Employee Cybersecurity Capability, and Organizational Cyber Resilience represent distinct constructs within the proposed research model. Given that these constructs are related to organizational cybersecurity and resilience, it is important to establish that each construct captures a different conceptual dimension. The Heterotrait–Monotrait (HTMT) ratio was used to evaluate the degree of similarity between the constructs, with values below 0.85 indicating adequate discriminant validity. Table 3 presents the HTMT values among the three constructs for this assessment.

| Construct | Digital Leadership (DL) | Employee Cybersecurity Capability (ECC) | Organizational Cyber Resilience (OCR) |
|-----------|-------------------------|-----------------------------------------|---------------------------------------|
| DL        | -                       | -                                       | -                                     |
| ECC       | 0.712                   | -                                       | -                                     |
| OCR       | 0.684                   | 0.792                                   | -                                     |

Table 3 illustrates the extent to which Digital Leadership, Employee Cybersecurity Capability, and Organizational Cyber Resilience remain empirically distinguishable. The HTMT values range from 0.684 to 0.792, with the highest value observed between Employee Cybersecurity Capability and Organizational Cyber Resilience. Although these two constructs show a relatively stronger association, the value remains within the acceptable range. This indicates that the relationships among the constructs do not compromise their conceptual distinctiveness. Accordingly, the three constructs can be treated as empirically distinct variables in the subsequent structural model assessment.

#### 4.4. Structural Model Assessment (Inner Model)

Prior to hypothesis testing, collinearity was checked. All inner Variance Inflation Factor (VIF) values ranged between 1.421 and 1.854, well below the maximum limit of 3.0, confirming no multicollinearity issues.

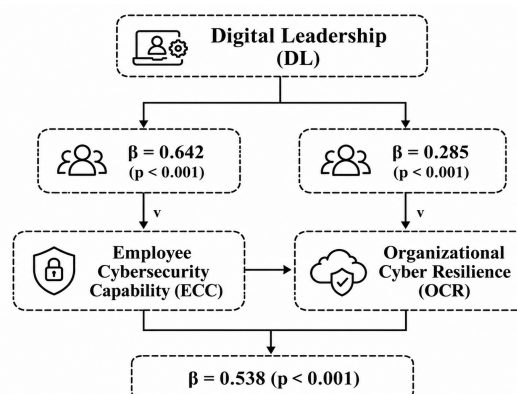


Figure 1. Structural Model Results (PLS-SEM Path Analysis)

Figure 1 illustrates the PLS-SEM structural model linking Digital Leadership, Employee Cybersecurity Capability, and Organizational Cyber Resilience. The results indicate that Digital Leadership positively affects Employee Cybersecurity Capability ( $\beta = 0.642$ ) and Organizational Cyber Resilience ( $\beta = 0.285$ ), while Employee Cybersecurity Capability has a stronger positive effect on Organizational Cyber Resilience ( $\beta =$

0.538). The model also shows that Digital Leadership explains 41.2% of the variance in Employee Cybersecurity Capability, whereas the combined influence of Digital Leadership and Employee Cybersecurity Capability explains 62.8% of the variance in Organizational Cyber Resilience. These findings indicate that strengthening cyber resilience depends not only on the strategic role of digital leadership but also substantially on employees' cybersecurity capability to apply secure practices in daily IT service operations.

#### 4.5. Explanatory and Predictive Power

To provide a more comprehensive evaluation of the proposed structural model, the analysis was further conducted by examining its explanatory and predictive performance. Beyond assessing the significance and strength of the hypothesized relationships, this evaluation considers the proportion of variance explained by the model, the relative contribution of each predictor, and the overall adequacy of the model. These assessments are important for determining how effectively Digital Leadership and Employee Cybersecurity Capability explain Organizational Cyber Resilience and for identifying the substantive importance of the relationships within the model. The results of the explanatory and predictive assessment are presented as follows.

- Coefficient of Determination (R<sup>2</sup>): Digital Leadership explained 41.2% of the variance in Employee Cybersecurity Capability (R<sup>2</sup> = 0.412). Together, Digital Leadership and Employee Cybersecurity Capability explained 62.8% of the variance in Organizational Cyber Resilience (R<sup>2</sup> = 0.628), representing strong explanatory power.
- Effect Size (f<sup>2</sup>) DL had a large effect on ECC (f<sup>2</sup> = 0.701). In predicting OCR, ECC demonstrated a medium-to-large effect (f<sup>2</sup> = 0.384), whereas DL had a moderate direct effect (f<sup>2</sup> = 0.118).
- Model Fit: The Standardized Root Mean Square Residual (SRMR) was 0.058, below the cutoff of 0.08, indicating good model fit.
- Hypothesis Testing: Hypotheses were tested using bootstrapping with 5,000 resamples at a 5% significance level.

Table 4. Structural Model Hypothesis Testing Results

| Hypotheses     | Path           | Path<br>Coeff.( $\beta$ ) | t-Statistic | p-Value | 95% CI         | Decision  |
|----------------|----------------|---------------------------|-------------|---------|----------------|-----------|
| H1             | DL → ECC       | 0.642                     | 12.841      | < 0.001 | [0.542, 0.738] | Supported |
| H2             | DL → OCR       | 0.285                     | 4.112       | < 0.001 | [0.151, 0.422] | Supported |
| H3             | ECC → OCR      | 0.538                     | 8.924       | < 0.001 | [0.418, 0.654] | Supported |
| H4 (Mediation) | DL → ECC → OCR | 0.345                     | 7.182       | < 0.001 | [0.252, 0.441] | Supported |

Table 4 presents the hypothesis testing results based on bootstrapping with 5,000 resamples. All proposed relationships are positive and statistically significant at  $p < 0.001$ , with the 95% confidence intervals remaining above zero. Digital Leadership demonstrates the strongest direct effect on Employee Cybersecurity Capability ( $\beta = 0.642$ ), while Employee Cybersecurity Capability has a stronger effect on Organizational Cyber Resilience ( $\beta = 0.538$ ) than the direct effect of Digital Leadership on Organizational Cyber Resilience ( $\beta = 0.285$ ). In addition, the indirect effect of Digital Leadership on Organizational Cyber Resilience through Employee Cybersecurity Capability is significant ( $\beta = 0.345$ ), confirming the mediating role of Employee Cybersecurity Capability. Because both the direct and indirect effects are significant, the findings support the complementary mediation pattern discussed in the study.

#### 4.6. Discussion

##### 4.6.1. The Direct Impact of Digital Leadership on Employee Cybersecurity Capability (H1)

The structural analysis confirms that Digital Leadership significantly enhances Employee Cybersecurity Capability ( $\beta = 0.642, p < 0.001$ ). This finding indicates that when leaders integrate cybersecurity priorities into strategic planning, provide organizational support, and promote continuous digital learning, employees are more capable of applying cybersecurity knowledge, maintaining secure practices, and responding to potential cyber threats.

This finding is consistent with previous research emphasizing that leadership plays an important role in developing organizational digital capabilities, employee learning, and cybersecurity oriented practices [35]. However, the present study extends this perspective by demonstrating that Digital Leadership is directly associated with Employee Cybersecurity Capability in IT service organizations. The result suggests that digital leadership should not be viewed solely as a driver of technological transformation but also as an organizational mechanism through which cybersecurity capabilities can be developed among employees [36]. Thus, the finding provides a more specific explanation of how leadership can influence the human capability required to support secure digital operations.

#### 4.6.2. The Influence of Leadership and Capability on Cyber Resilience (H2 and H3)

Digital Leadership ( $\beta = 0.285, p < 0.001$ ) and Employee Cybersecurity Capability ( $\beta = 0.538, p < 0.001$ ) both positively affect Organizational Cyber Resilience. The positive effect of Digital Leadership is consistent with previous studies linking strategic leadership, governance, and organizational preparedness with the ability to manage digital disruptions [37]. This finding confirms that leadership contributes to resilience by establishing cybersecurity priorities, supporting resource allocation, and creating organizational conditions for preparedness and response.

The stronger effect of Employee Cybersecurity Capability on Organizational Cyber Resilience is also consistent with previous cybersecurity research emphasizing the importance of human factors in organizational security and resilience [37]. Employees with adequate cybersecurity knowledge, technical competence, security awareness, and policy compliance can contribute to threat recognition, preventive practices, incident response, and organizational recovery. However, the present study extends previous perspectives by positioning employee cybersecurity capability as an operational organizational capability rather than only an individual security characteristic. This finding indicates that employees' cybersecurity capabilities can directly contribute to the organization's broader ability to maintain and restore digital service operations during cybersecurity disruptions [38].

The comparison between H2 and H3 also provides an important theoretical insight. Although both Digital Leadership and Employee Cybersecurity Capability significantly contribute to Organizational Cyber Resilience, the stronger coefficient for Employee Cybersecurity Capability ( $\beta = 0.538$ ) suggests that the human capability component has a particularly important role in translating cybersecurity practices into resilience outcomes [39]. This result complements leadership-based explanations of resilience by indicating that strategic direction needs to be supported by employees who are capable of implementing cybersecurity practices in daily IT service operations.

The empirical findings also provide practical implications for cybersecurity strategies in IT service organizations, particularly in security governance, employee capability development, and cyber risk mitigation. The significant effect of Digital Leadership on Organizational Cyber Resilience ( $\beta = 0.285, p < 0.001$ ) indicates that security governance should be integrated into digital leadership and organizational decision-making. Leaders can establish clear cybersecurity priorities, assign responsibility for cyber risks, allocate resources for security controls, and incorporate cybersecurity considerations into IT service planning and continuity decisions [40]. This approach can strengthen governance mechanisms that support secure and resilient digital service operations.

The significant effect of Employee Cybersecurity Capability on Organizational Cyber Resilience ( $\beta = 0.538, p < 0.001$ ) further indicates the importance of employee training as part of cybersecurity strategy. IT service organizations can implement continuous and scenario-based training focused on threat recognition, secure system usage, credential protection, incident reporting, and appropriate incident response. Such training can strengthen employees' ability to apply cybersecurity practices during routine operations and respond effectively when cyber incidents occur.

The findings also have implications for cyber risk mitigation. Because Employee Cybersecurity Capability demonstrates a stronger relationship with Organizational Cyber Resilience than Digital Leadership, organizations should complement governance and technological controls with human-centered risk mitigation practices [10]. Regular cybersecurity risk assessments can be used to identify employee-related vulnerabilities and critical service risks, while the results can inform targeted training, preventive controls, monitoring, incident response, and recovery measures. Accordingly, integrating security governance, continuous employee capability development, and risk mitigation practices can help IT service organizations strengthen their capacity to maintain, respond to, and recover digital services during cybersecurity disruptions.

#### 4.6.3. The Mediating Role of Employee Cybersecurity Capability (H4)

Employee Cybersecurity Capability significantly mediates the relationship between Digital Leadership and Organizational Cyber Resilience ( $\beta = 0.345, p < 0.001$ ). This result indicates that Digital Leadership contributes to organizational cyber resilience both directly and indirectly through employee capability development. The finding is consistent with the broader theoretical view that organizational resilience is strengthened through the interaction between strategic organizational mechanisms and human capabilities [41].

More importantly, the mediation result provides a deeper explanation of the relationship between leadership and cyber resilience. Previous studies have often examined leadership as a direct organizational determinant or focused on employee cybersecurity awareness and behavior as separate outcomes [42]. In contrast, the present study demonstrates that Employee Cybersecurity Capability functions as an intermediate mechanism through which leadership practices are translated into resilience outcomes. This finding therefore extends previous research by connecting strategic Digital Leadership with the human capabilities required for cybersecurity implementation and organizational resilience [43].

The significant direct effect of Digital Leadership on Organizational Cyber Resilience together with the significant indirect effect through Employee Cybersecurity Capability indicates a complementary mediating relationship [44]. This suggests that leadership contributes to resilience through both organizational level mechanisms and employee capability development. Consequently, the findings provide a more integrated theoretical explanation of how Digital Leadership, Employee Cybersecurity Capability, and Organizational Cyber Resilience are interconnected within IT service organizations.

### 5. MANAGERIAL IMPLICATIONS

IT service managers should embed cybersecurity priorities within strategic planning and operational decision-making by establishing clear security responsibilities, allocating appropriate resources, and maintaining accountability for cybersecurity-related activities. Such leadership practices can create organizational conditions that support employees in applying secure practices consistently across digital service operations.

Employee capability development should be treated as a continuous organizational activity rather than a one-time training requirement. Organizations can strengthen this capability through scenario-based programs addressing threat recognition, secure system usage, credential protection, incident reporting, and response practices. These activities can improve employees' readiness to apply cybersecurity knowledge when performing routine tasks and handling potential security incidents.

A closer alignment between employee capability and cyber risk management can further improve organizational preparedness. Periodic risk assessments can identify employee-related vulnerabilities and risks affecting critical digital services, while the resulting information can be used to prioritize training, preventive controls, monitoring, and incident response activities [45]. This approach allows managerial interventions to be directed toward areas with greater cybersecurity exposure.

The stronger relationship between Employee Cybersecurity Capability and Organizational Cyber Resilience highlights the importance of developing employees as active contributors to organizational resilience. Accordingly, managerial strategies should combine leadership support, continuous capability development, and risk management rather than relying predominantly on technological safeguards. Strengthening employees' ability to prevent, recognize, and respond to cybersecurity disruptions can help sustain more reliable and resilient IT service operations.

### 6. CONCLUSION

This study presents an integrated perspective on organizational cyber resilience by connecting Digital Leadership, Employee Cybersecurity Capability, and Organizational Cyber Resilience within the IT service context. The proposed framework highlights that organizational resilience is shaped by the relationship between strategic leadership and the human capabilities required to support secure digital operations. In this relationship, Employee Cybersecurity Capability provides an important organizational mechanism for translating leadership support into resilient cybersecurity practices.

The study contributes to the literature by integrating these three dimensions into a unified empirical framework and by emphasizing the organizational role of employee cybersecurity capability in cyber resilience. This perspective extends the understanding of cyber resilience beyond technological protection by recognizing the combined importance of leadership direction, employee capability, and organizational conditions in

sustaining digital service operations.

Several limitations should be considered when interpreting the contribution of this study. The cross-sectional design limits the ability to examine changes in organizational cyber resilience over time, while purposive sampling and the focus on Indonesian IT service organizations may constrain the transferability of the findings to other settings. In addition, the use of self-reported data may introduce respondent related bias. Future research should therefore consider longitudinal approaches, broader organizational and geographical contexts, and additional organizational or technological factors to further develop the understanding of organizational cyber resilience.

## 7. DECLARATIONS

### 7.1. About Authors

Rasyid Tarmizi (RT)  <https://orcid.org/0000-0003-0528-4623>

Andriyansah (AN)  <https://orcid.org/0000-0002-4851-2617>

Mohd Faiz Hilmi (MF)  <https://orcid.org/0000-0003-4548-0565>

Yuce Sariningsih (YS)  <https://orcid.org/0000-0001-8460-3375>

Richard Evans (RE)  <https://orcid.org/0009-0007-7280-8323>

### 7.2. Author Contributions

Conceptualization: RT; Methodology: AN; Software: MF; Validation: YS and RE; Formal Analysis: RT; Investigation: AN; Resources: MF; Data Curation: YS; Writing Original Draft Preparation: RT and AN; Writing Review and Editing: MF and YS; Visualization: RE; All authors, RT, AN, MF, YS, and RE, have read and agreed to the published version of the manuscript.

### 7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

### 7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

### 7.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

## REFERENCES

- [1] M. F. Safitra, M. Lubis, and H. Fakhurroja, "Counterattacking cyber threats: A framework for the future of cybersecurity," *Sustainability*, vol. 15, no. 18, p. 13369, 2023.
- [2] A. M. AL-Hawamleh, "Securing the future: Framework fundamentals for cyber resilience in advancing organizations," *Journal of System and Management Sciences*, vol. 14, no. 10, pp. 130–150, 2024.
- [3] B. A. Massa, "Navigating cyber threats: Practitioner insights on building cyber-resilient organizations," Ph.D. dissertation, Robert Morris University, 2025.
- [4] M. MADANCHIAN, "Strengthening cybersecurity through effective leadership," *Cybersecurity Leadership and Strategy for Resilience Innovation and Sustainable Protection*, p. 234, 2026.
- [5] R. Lesmana, I. Wijaya, E. A. Nabila, H. Agustian, S. Audiah, and A. Faturahman, "Enhancing market trend analysis through ai forecasting models," *International Journal of Cyber and IT Service Management (IJCITSM)*, vol. 4, no. 2, pp. 105–113, 2024.
- [6] A. Alwazrah, C. Rouissi, M. D. Alshammari, K. Al-Qahtani, H. Wahsheh, A. Sulieman, H. Alodan, and M. Alazzam, "Digital leadership as a catalyst for enhancing organizational information security," *EDPACS*, pp. 1–24, 2025.
- [7] B. G. Mujtaba, "Operational sustainability and digital leadership for cybercrime prevention," *International Journal of Internet and Distributed Systems*, vol. 5, no. 2, pp. 19–40, 2023.

- [8] S. L. Burton, D. N. Burrell, C. Nobles, and L. A. Jones, "Exploring the nexus of cybersecurity leadership, human factors, emotional intelligence, innovative work behavior, and critical leadership traits," *Scientific Bulletin*, vol. 28, no. 2, pp. 162–175, 2023.
- [9] Y. Wang, "Impact of digital leadership on corporate cybersecurity governance," *Finance Research Letters*, p. 110519, 2026.
- [10] A. M. Al-Momani, M. Sarram, S. M. Zighan, R. T. Al-Majali, N. Al-shanableh, S. G. Saatchi, T. M. Shatnawi, N. S. Alajarmeh, S. I. S. Al-Hawary, and A. A. S. Mohammad, "The influence of cybersecurity leadership on the resilience of jordanian businesses: a study on the role of cybersecurity measures in entrepreneurial success," in *Business Analytical Capabilities and Artificial Intelligence-enabled Analytics: Applications and Challenges in the Digital Era, Volume 2*. Springer, 2024, pp. 1–15.
- [11] C. Z. Oroni and F. Xianping, "Structural evaluation of management capability and the mediation role of cybersecurity awareness towards enterprise performance," *Journal of Data, Information and Management*, vol. 5, no. 4, pp. 345–361, 2023.
- [12] A. Björck, B. Vogel, C. Pugnetti, and M. Lopez, "Advancing cyber crisis readiness: context, microfoundations and the role of leadership," *Journal of Communication Management*, vol. 30, no. 3, pp. 322–341, 2026.
- [13] P. M. Tandon, "Navigating crisis situations: The role of digital resilience in effective leadership and organizational continuity," in *Impact of New Technology on Next-Generation Leadership*. IGI Global Scientific Publishing, 2024, pp. 51–75.
- [14] R. K. Narayan, "Cybersecurity challenges in cloud-edge computing convergence: A systematic analysis and adaptive defense framework," *International Journal of Cyberspace Security*, vol. 1, no. 1, pp. 38–50, 2025.
- [15] B. Rawat, A. S. Bist, U. Rahardja, E. P. Harahap, and R. A. D. Septian, "Novel framework to define extended & mixed reality for online learning," in *2022 4th International Conference on Cybernetics and Intelligent System (ICORIS)*. IEEE, 2022, pp. 1–4.
- [16] D. Ezeagwuna, "Enhancing organizational cyber resilience through the nist cybersecurity framework," *International Journal of Technology, Management and Humanities*, vol. 12, no. 01, pp. 124–140, 2026.
- [17] E. K. ThankGod, O. O. Immanuel, S. A. Muhammed, N. Ikechukwu, O. I. C. Frank, and O. U. Victor, "Reshaping global warfare through cyber security and technology: A critical review," *Technology (IKRJET)*, vol. 2, no. 4, pp. 41–44, 2026.
- [18] A. AL-Hawamleh, "Cyber resilience framework: Strengthening defenses and enhancing continuity in business security," 2024.
- [19] T. Chavarnakul, L. D. Xu, Z. Bi, A. Shankar, G. Dhiman, W. Viriyasitavat, and D. Hoonsoon, "A systematic literature review on resilient digital transformation, examining how organizations sustain digital capabilities," *HighTech and Innovation Journal*, vol. 6, no. 2, 2025.
- [20] R. Sivaraman, M.-H. Lin, M. I. C. Vargas, S. I. S. Al-Hawary, U. Rahardja, F. A. H. Al-Khafaji, E. V. Golubtsova, and L. Li, "Multi-objective hybrid system development: To increase the performance of diesel/photovoltaic/wind/battery system." *Mathematical Modelling of Engineering Problems*, vol. 11, no. 3, p. 837, 2024.
- [21] K. Shatila, "Artificial intelligence and organizational resilience: The mediating role of agility, innovation, and digital leadership," *Strategy & Leadership*, pp. 1–25, 2025.
- [22] J. Ebuzor, "Good governance and cybersecurity: Enhancing digital resilience," in *Corporate Cybersecurity in the Aviation, Tourism, and Hospitality Sector*. IGI Global Scientific Publishing, 2024, pp. 112–136.
- [23] S. Watini, N. Ramadhona *et al.*, "Predicting patient satisfaction levels using artificial intelligence technology for food service at eri soedewo rs pad gatot soebroto," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 2sp, pp. 124–134, 2023.
- [24] P. Verma, T. Newe, G. D. O'Mahony, D. Brennan, and D. O'Shea, "Toward a unified understanding of cyber resilience: Concepts, strategies, and future directions," *IEEE Access*, vol. 13, pp. 49 945–49 965, 2025.
- [25] D. S. S. Wuisan, R. A. Sunardjo, Q. Aini, N. A. Yusuf, and U. Rahardja, "Integrating artificial intelligence in human resource management: A smartpls approach for entrepreneurial success," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 334–345, 2023.
- [26] L. Adewole, "Persistent threats, fragile defenses: An analysis of cybersecurity vulnerabilities in nigeria's

- government and banking sectors (2024-2026),” *Fragile Defenses: An Analysis of Cybersecurity Vulnerabilities in Nigeria’s Government and Banking Sectors (2024-2026)*(June 07, 2026), 2026.
- [27] S. Kosasi, C. Lukita, M. H. R. Chakim, A. Faturahman, and D. A. R. Kusumawardhani, “The influence of digital artificial intelligence technology on quality of life with a global perspective,” *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 240–250, 2023.
- [28] S. Akter, M. R. Uddin, S. Sajib, W. J. T. Lee, K. Michael, and M. A. Hossain, “Reconceptualizing cybersecurity awareness capability in the data-driven digital economy,” *Annals of operations research*, vol. 350, no. 2, pp. 673–698, 2025.
- [29] M. D. Johnson and W. Robert, “Self-healing mechanisms for autonomous cybersecurity systems using reinforcement learning,” *Stout in Computer Science and Technology Studies*, vol. 1, no. 1, pp. 21–30, 2025.
- [30] O. I. Falowo and J. B. Abdo, “2019–2023 in review: Projecting ddos threats with arima and ets forecasting techniques,” *IEEE Access*, vol. 12, pp. 26 759–26 772, 2024.
- [31] J. Kim and S. Y. Lee, “Cyber resilience of ships: An evaluation of guideline and frameworks,” *IEEE Access*, vol. 13, pp. 97 337–97 347, 2025.
- [32] M. T. O. Nyamboga, “Strategic leadership in the digital age: Navigating cybersecurity risks and digital transformation,” *DARSHAN: THE INTERNATIONAL JOURNAL OF COMMERCE AND MANAGEMENT : Darshan University*, vol. 4, no. 2, pp. 95–109, 2024.
- [33] Y. Kristiana, V. A. H. Goeltom, and T. C. Nathalia, “Ai-driven pos, adaptable workload, and service culture influence on frontline employee performance,” *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 1, pp. 217–227, 2025.
- [34] U. Awan, A. Keprate, and P. Braathen, “A conceptual framework of an integrative leadership for cybersecurity management and designing digital road map for organizations,” in *Digital Transformation*. Routledge India, 2025, pp. 47–59.
- [35] O. SUSTAINABILITY, D. KUMAR, and N. SUTHAR, “Resilient cybersecurity culture: Strategies for leadership and,” *Cybersecurity Leadership and Strategy for Resilience Innovation and Sustainable Protection*, p. 104, 2026.
- [36] R. Netrebko, “A risk-oriented framework for forming and modelling information security profiles in modern cyberspace,” *Political Science and Security Studies Journal*, vol. 6, no. 4, pp. 52–63, 2025.
- [37] C. Aksoy, “Building a cyber security culture for resilient organizations against cyber attacks,” *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, vol. 7, no. 1, pp. 96–110, 2024.
- [38] A. Kanaan, A. AL-Hawamleh, M. Aloun, A. Alorfi, and M. A. Alrawashdeh, “Fortifying organizational cyber resilience: an integrated framework for business continuity and growth amidst escalating threat landscapes,” 2024.
- [39] D. Cahyono, A. Susbiyani, E. Lestari, F. Fauziyah, N. Qomariah, and Y. S. Guntur, “Role of personal savings in financial tech impact on family planning in indonesia,” *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 1, pp. 120–131, 2025.
- [40] X. Lin, O. Sivarak, T.-H. Chou, Y.-T. Lin, U. Rahardja, A. Ruangkanjanases, Y.-C. Lin, and S.-C. Chen, “Exploring the effect of team-environment fit in the relationship between team personality, job satisfaction, and performance,” *Frontiers in Public Health*, vol. 10, p. 897482, 2022.
- [41] S. S. Iyer and B. Raji, “Cybersecurity culture and organizational resilience: A human-centered approach to digital risk management,” *American Journal of Industrial and Business Management*, vol. 15, no. 5, pp. 748–766, 2025.
- [42] T. O. Abrahams, O. A. Farayola, S. Kaggwa, P. U. Uwaoma, A. O. Hassan, and S. O. Dawodu, “Cybersecurity awareness and education programs: a review of employee engagement and accountability,” *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 100–119, 2024.
- [43] Y. Shino, F. Utami, and S. Sukmaningsih, “Economic preneur’s innovative strategy in facing the economic crisis,” *IAIC Transactions on Sustainable Digital Innovation (ITS DI)*, vol. 5, no. 2, pp. 117–126, 2024.
- [44] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and Y.-M. Li, “Understanding behavioral intention to use of air quality monitoring solutions with emphasis on technology readiness,” *International Journal of Human–Computer Interaction*, vol. 41, no. 8, pp. 5079–5099, 2025.
- [45] S. Pranata, F. Fanani, D. Hidayati, R. Lesmana, and Z. Ndlovu, “Implementation of smart contracts in tiktok influencer marketing,” *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 84–97, 2025.