Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

A cybersecurity framework for Jordanian express delivery service companies: Analyzing the impact of organizational culture and project team skills

Ahmad AlArabiat [1], Umi Kalsum Zolkafli [2,*]

[1]Faculty of Built Environment, University of Malaya, Kuala Lumpur, Malaysia
[2]Department of Quantity Surveying, University of Malaya, Kuala Lumpur, Malaysia

ARTICLE INFO

Article history:
Received 11 January 2025
Received in revised form
23 May 2025
Accepted 2 October 2025

Keywords:
Cybersecurity
Organizational culture
Team skills
Cyberattacks
Express delivery

ABSTRACT

In the rapidly changing digital environment, cybersecurity has become a major challenge for express delivery service companies, which rely on digital systems and handle sensitive customer data. This study explores how organizational culture influences the development of project team skills in responding to cyberattacks, aiming to improve company performance in Jordan. Using Structural Equation Modeling (SEM) and survey data from 274 operations and IT managers, the study examines the impact of cyberattack factors—such as software vulnerabilities, human error, weak passwords, and insider threats—on organizational responses and team skill development. The results show that these threats significantly affect response mechanisms, which in turn enhance team capabilities. Key elements such as incident response planning, cybersecurity expertise, and fast threat detection are essential for reducing risks. Furthermore, a supportive and flexible organizational culture strengthens these effects by promoting teamwork, learning, and innovation. The study provides practical guidance for improving cybersecurity management in the express delivery sector and offers a foundation for future research in other high-risk industries.

1. Introduction

The rapid pace of digital transformation across industries has profoundly influenced express delivery service companies (EDSCs), which now serve as integral components of contemporary logistics and e-commerce ecosystems (Chatterjee, 2021; Pavlova, 2020). These companies are pivotal in ensuring prompt and dependable goods delivery, utilizing sophisticated logistics frameworks and digital technologies to meet increasing customer expectations. Despite representing only 5% of global trade volume, EDSCs contribute a substantial 35–40% of trade value, underscoring their critical role in managing high-value and time-sensitive shipments (Alqudhaibi et al., 2023; Rejeb et al., 2021). In Jordan, the sector has expanded significantly due to its strategic position as a logistics hub and the rise of e-commerce, spurring demand for faster, more efficient delivery services. However, this rapid growth has also exposed these companies to escalating cybersecurity threats, posing risks to operational stability and customer confidence (Georgiadou et al., 2022; Kosutic and Pigni, 2020). Despite the increasing significance of cybersecurity in logistics and e-commerce, existing cybersecurity frameworks primarily focus on broad industry applications and fail to address the unique vulnerabilities faced by EDSCs. This research aims to bridge this gap by proposing a cybersecurity framework tailored to the express delivery sector, integrating technical and human-centric security measures.

The increasing dependence on interconnected digital systems for real-time tracking, online payments, and logistics management has made EDSCs vulnerable to cyber-attacks (Nkomo and Kalisz, 2023; Georgiadou et al., 2022; Tariq et al., 2023). Threats such as ransomware, phishing, and advanced persistent attacks exploit system vulnerabilities, resulting in financial losses, operational disruptions, and damage to reputation (Abbad et al., 2011). Jordanian EDSCs face distinct challenges, including inadequate cybersecurity frameworks, a shortage of skilled cybersecurity professionals, and weak regulatory enforcement

* Corresponding Author.
Email Address: umi@um.edu.my (U. K. Zolkafli)
https://doi.org/10.21833/ijaas.2025.10.018
Corresponding author's ORCID profile:
https://orcid.org/0000-0001-5061-1019

mechanisms (AlHadid et al., 2023). Compounding these challenges is the lack of a security-centric organizational culture and insufficiently skilled project teams, which further hinder the effectiveness of cybersecurity measures (Abulhaija et al., 2022; Sharma and Patel, 2018). Existing cybersecurity models, such as the NIST Cybersecurity Framework and ISO/IEC 27001, focus primarily on compliance, risk assessment, and technical solutions. However, these frameworks do not sufficiently incorporate organizational behavior and workforce competencies, which are crucial for mitigating cybersecurity threats in EDSCs. Therefore, this study introduces a cybersecurity framework designed for EDSCs that integrates cybersecurity response mechanisms, project team skills, and organizational culture to enhance cyber resilience in the sector.

The types of cyber-attacks targeting EDSCs in Jordan include data breaches, system infiltration, and focused attacks on real-time logistics and payment systems (Safitra et al., 2023; Georgiadou et al., 2022; Kosutic and Pigni, 2020). Combating these threats requires a robust approach encompassing early detection, mitigation strategies, and recovery protocols, which remain underdeveloped in many Jordanian companies (Srinivasan et al., 2018; Naseer et al., 2023). Competent project teams play a crucial role in these defenses, ensuring the proper implementation of security measures and swift responses to emerging threats (Berényi and Soltész, 2022; Skilton and Dooley, 2010; Naseer et al., 2023). Unfortunately, many Jordanian EDSCs lack the expertise and resources to establish and sustain such teams, making them susceptible to evolving cybersecurity threats (Tariq et al., 2023). Recognizing the role of human factors in cybersecurity, this study proposes a cybersecurity resilience framework that emphasizes the development of cybersecurity competencies among project teams. It highlights the importance of continuous training, cross-functional collaboration, and adaptive learning in mitigating cyber threats within EDSCs.

Organizational culture significantly influences the success of cybersecurity strategies by shaping how employees perceive and react to security challenges (Georgiadou et al., 2022). A collaborative and proactive culture promotes shared accountability, encouraging employees to prioritize security practices and promptly report potential threats (Sharma and Patel, 2018). However, hierarchical structures and limited upward communication, common in Jordanian organizations, often impede these efforts by discouraging employees from escalating security concerns (Tariq et al., 2023). Integrating cultural considerations into cybersecurity strategies is essential for bolstering organizational resilience and aligning security initiatives with broader business goals (Georgiadou et al., 2022; Sharma and Patel, 2018; Al-Hawamleh, 2024). This study argues that organizational culture moderates cybersecurity preparedness by shaping employee attitudes and behaviors toward security compliance. By incorporating organizational culture as a key component, the proposed cybersecurity framework aims to ensure that cybersecurity is not just a technical concern but a core aspect of corporate strategy and workforce engagement.

This research addresses these challenges by exploring the interconnections between organizational culture, project team competencies, and cybersecurity practices in Jordanian EDSCs. It aims to identify cyber-attack characteristics impacting these companies and assess their existing response mechanisms. Additionally, the study investigates how project team expertise can enhance cybersecurity measures and examines the moderating effect of organizational culture on these skills. By analyzing the interplay between organizational culture, project team capabilities, and cybersecurity strategies, the research seeks to establish a holistic framework for mitigating cyber risks and fortifying the resilience of Jordanian EDSCs (Georgiadou et al., 2022; Naseer et al., 2023; Cheung and Bell, 2021). The introduction of the Cybersecurity Resilience Framework for Express Delivery Service Companies (CRF-EDS) serves as a novel contribution to the cybersecurity field, providing a structured approach to integrating technical defenses with human-centric security strategies. This framework addresses industry-specific threats and offers practical insights into strengthening cybersecurity governance in express delivery services.

In summary, the growing reliance of Jordanian EDSCs on digital technologies has amplified their exposure to cyber-attacks, posing significant risks to operational continuity and customer trust (Alqudhaibi et al., 2023; Kosutic and Pigni, 2020). Limited access to skilled teams, insufficient organizational awareness, and weak regulatory frameworks exacerbate these vulnerabilities, underscoring the need for tailored cybersecurity solutions (Davis et al., 2021; Tariq et al., 2023). By introducing the CRF-EDS framework, this study advances the discourse on cybersecurity in the express delivery sector and provides a structured, industry-relevant approach to mitigating cyber risks. The findings of this research are expected to guide industry practitioners and policymakers in strengthening cybersecurity measures within the logistics and express delivery domain.

2. Literature review

The adoption of digital technologies has revolutionized the operational structures of express delivery service companies (EDSCs), enabling quicker and more reliable service delivery. However, these advancements have also introduced significant cybersecurity challenges, particularly in data-driven industries such as express delivery, where protecting sensitive customer data and maintaining operational security is paramount (Georgiadou et al., 2022; Kosutic and Pigni, 2020). Cyber threats, including ransomware, phishing, and data breaches,

continue to escalate globally, posing a growing risk to EDSCs, including those in Jordan. The rapid expansion of Jordan's express delivery sector, driven by its strategic location as a logistics hub and the growing influence of e-commerce, has made these companies attractive targets for increasingly complex cyber-attacks.

Effectively addressing cybersecurity issues within Jordanian EDSCs requires a detailed understanding of the sector's unique vulnerabilities, such as weak regulatory oversight, a shortage of skilled cybersecurity personnel, and insufficient organizational support for security initiatives (Tariq et al., 2023). This literature review delves into the key variables of the study, including the characteristics of cyber-attacks, response strategies, the significance of project team expertise, and the influence of organizational culture in strengthening cybersecurity measures. By synthesizing existing research, the review identifies gaps in knowledge and provides a foundation for crafting a cybersecurity framework tailored to Jordanian EDSCs. It systematically explores cyber-attack characteristics, mitigation mechanisms, project teams' roles, and organizational culture's moderating impact in reducing cyber risks (Cheung and Bell, 2021; Georgiadou et al., 2022).

2.1. Cyber-attack features in express delivery service companies

The increasing reliance on digital technologies has exposed express delivery service companies (EDSCs) to a growing number of sophisticated cyber-attacks. These threats disrupt operational processes and compromise data security by exploiting vulnerabilities specific to the sector (Safitra et al., 2023; Kosutic and Pigni, 2020). Identifying the distinctive features of these attacks is essential for developing effective countermeasures tailored to the unique challenges of EDSCs.

The complexity and frequency of cyber-attacks have grown significantly, creating major obstacles for industries worldwide. Common attack methods include phishing, ransomware, and advanced persistent threats (APTs), which target vulnerabilities in software, human behavior, and network configurations. Phishing often employs deceptive emails or fraudulent websites to extract sensitive data, while ransomware encrypts critical organizational information to demand payments for its release (Benavides-Astudillo et al., 2023; Hyslip and Burruss, 2023). High-profile ransomware incidents like WannaCry and NotPetya have inflicted significant financial and operational damage across industries, including logistics and delivery services (Chen and Bridges, 2017; Sharmeen et al., 2020). These developments highlight the increasing sophistication of cyber threats and the pressing need for advanced detection and response strategies (Jadhav et al., 2023).

The interconnected nature of systems used by EDSCs introduces additional cybersecurity challenges. Digital platforms supporting real-time tracking, online payments, and supply chain coordination are prime targets for cybercriminals seeking to disrupt services or steal sensitive information (Tariq et al., 2023; Alqudhaibi et al., 2023). Vulnerabilities in Internet of Things (IoT) devices, which are extensively utilized in logistics, exacerbate these risks (Alnaeli et al., 2017; Seghezzi et al., 2020). Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, which overwhelm systems with excessive traffic to render them inoperative, can significantly disrupt delivery operations and impair customer services (Jadhav et al., 2023). Addressing these threats requires advanced tools for traffic monitoring and anomaly detection to strengthen system resilience (Jegatheswaran and Juremi, 2022; Zlomislić et al., 2017).

In Jordan, systemic and infrastructural limitations heighten cybersecurity risks for EDSCs. Many companies rely on outdated IT systems and third-party service providers, creating multiple points of vulnerability. Phishing schemes often exploit the low level of cybersecurity awareness among employees, leading to data breaches and financial setbacks (Abulhaija et al., 2022). Additionally, the sector's reliance on limited investments in modern technology and the shortage of cybersecurity professionals expose organizations to risks such as ransomware and insider threats. Human error, including weak password management and vulnerability to social engineering tactics, remains a persistent issue, further undermining the effectiveness of cybersecurity defenses (Alsharif et al., 2022; Amorosa and Yankson, 2023).

The dependence on third-party systems for logistics and data management introduces further vulnerabilities, as attackers can exploit weaknesses in vendor networks to infiltrate critical systems (Tariq et al., 2023). Moreover, Jordan's lack of stringent regulatory frameworks fails to enforce comprehensive data protection measures, leaving EDSCs inadequately prepared to address the evolving cyber threat landscape (Alhejaili, 2024).

2.2. Cyber-attack response mechanisms

Effective response mechanisms are essential for maintaining the resilience of express delivery service companies (EDSCs) against cyber-attacks. These mechanisms focus on promptly detecting threats, mitigating damage, and ensuring comprehensive recovery to minimize disruptions and prevent future incidents (Srinivasan et al., 2018; Naseer et al., 2023). Detection systems, such as real-time monitoring tools and intrusion detection software, play a pivotal role in identifying potential threats before they can inflict significant harm, enabling rapid responses (Gelenbe and Nakip, 2023). However, to contain threats, mitigation strategies like network segmentation, access control protocols, and endpoint security are deployed to isolate

compromised systems and limit the extent of the attack (Sistla et al., 2014). Recovery processes, including restoring data from secure backups and repairing affected systems, aim to resume normal operations efficiently. These processes also integrate lessons from post-incident evaluations to bolster defenses. Advanced technologies such as artificial intelligence (AI) and machine learning (ML) are increasingly used to automate detection and response efforts, providing adaptive solutions to emerging threats (Deyannis et al., 2022). Additionally, blockchain technology has gained traction for facilitating secure and transparent data management during recovery (Gelenbe and Nakip, 2023).

The effectiveness of these mechanisms varies based on organizational size and available resources. Larger companies often have the advantage of advanced systems, robust budgets, and skilled personnel, enabling them to respond swiftly and efficiently to cyber threats (Davis et al., 2021). In contrast, many Jordanian EDSCs struggle with outdated IT infrastructure, limited cybersecurity budgets, and inadequate training for their workforce, which hinder timely and effective responses (Tariq et al., 2023). These constraints often lead to prolonged recovery times, operational disruptions, and increased vulnerability to repeat attacks (Davis et al., 2021; Srinivasan et al., 2018). Addressing these issues requires targeted investments in cybersecurity tools, workforce development, and adaptable response frameworks tailored to the needs of Jordanian EDSCs (Alsharif et al., 2022; Naseer et al., 2023).

Regulatory and institutional factors also play a crucial role in determining the success of cyber-attack response mechanisms. In Jordan, weak enforcement of cybersecurity regulations and the lack of a cohesive regulatory framework have hampered the development of effective incident response strategies. Collaborative initiatives, such as partnerships between public and private sectors and capacity-building programs, can help address these gaps by encouraging knowledge-sharing and pooling resources (Oriola et al., 2021; Hawkins, 2017). Internationally, adherence to established standards has proven effective in promoting timely incident reporting and standardizing response protocols, enhancing organizational resilience (Riebe et al., 2021; Oriola et al., 2021).

2.3. Role of project team skills in cybersecurity

The skills and expertise of project teams are critical to successfully implementing and maintaining cybersecurity frameworks. These teams blend technical knowledge, strategic planning, and collaborative abilities to tackle evolving cyber threats and safeguard organizational assets (Berényi and Soltész, 2022; Skilton and Dooley, 2010). By leveraging their expertise, project teams design, deploy, and manage essential security systems, such as firewalls, encryption technologies, and intrusion detection mechanisms, ensuring a robust defense against potential threats (Back and Guerette, 2021; Jiang et al., 2020). Beyond technical capabilities, skilled teams enhance organizational agility by facilitating swift decision-making and adapting to dynamic threat environments. They can promptly assess and neutralize emerging risks, minimizing disruptions and associated costs (Dreibelbis et al., 2018). Furthermore, these teams foster a proactive approach to cybersecurity by conducting regular vulnerability assessments, system audits, and simulation exercises to identify and address weaknesses (Sawyer and Hancock, 2018).

Project teams also play a vital role in aligning cybersecurity initiatives with broader organizational objectives. Incorporating business goals into security strategies ensures that protective measures support overall operational priorities and maintain customer trust (Pharris and Perez-Mira, 2022; Sharma and Patel, 2018). This alignment is particularly important in industries like express delivery, where uninterrupted operations and trust are crucial (Naseer et al., 2023). Moreover, skilled teams promote collaboration across departments and with external stakeholders, facilitating threat intelligence sharing, coordinating incident responses, and ensuring compliance with regulatory standards. Cross-functional teamwork allows organizations to address vulnerabilities comprehensively, leveraging diverse expertise and perspectives (Steinke et al., 2015). Additionally, project teams contribute to workforce training and awareness, bridging knowledge gaps by leading workshops, simulations, and real-world exercises. These efforts improve organizational preparedness, reducing risks associated with human error and insider threats (Carlton and Levy, 2015; Sharma and Patel, 2018).

However, building skilled project teams poses significant challenges. In Jordan, limited resources, a scarcity of cybersecurity professionals, and a lack of advanced training opportunities hinder progress. The rapid evolution of cyber threats necessitates ongoing learning and skill development, which many organizations struggle to provide due to budget constraints and outdated infrastructure (Sawyer and Hancock, 2018). Despite these barriers, organizations investing in team development notably improved cybersecurity resilience. For instance, companies adopting agile practices and fostering multidisciplinary collaboration report quicker incident resolution and fewer vulnerabilities (Sharma and Patel, 2018). Similarly, organizations emphasizing continuous professional development through certifications and specialized training programs have effectively enhanced their ability to combat emerging threats (Naseer et al., 2023).

2.4. Organizational culture and its moderating role in cybersecurity

Organizational culture, encompassing a company's shared values, beliefs, and practices, is pivotal in shaping employee behavior and decision-

making, particularly in cybersecurity (Georgiadou et al., 2022). Leadership, communication, empowerment, and continuous learning profoundly influence how effectively an organization manages cybersecurity risks and fosters secure practices (Sharma and Patel, 2018). Leadership is instrumental in embedding cybersecurity as a core organizational value. Leaders who model secure behaviors and emphasize the importance of cybersecurity set a strong example, creating a culture of accountability and vigilance (Mwim and Mtsweni, 2022). By allocating resources and visibly prioritizing cybersecurity initiatives, leaders can inspire confidence and commitment among employees, motivating them to adopt proactive security practices (Uchendu et al., 2021). Leadership approaches that encourage inclusiveness and participation, such as transformational or participative leadership styles, further enhance cybersecurity efforts by empowering employees to contribute to risk management (Huang and Pearlson, 2019).

Open communication is another critical factor in promoting effective cybersecurity. Clear and transparent communication about security policies, responsibilities, and potential risks ensures that employees understand their roles and feel confident reporting threats (Granova et al., 2023). By aligning employee actions with organizational security objectives, open communication reduces the likelihood of errors and non-compliance (Georgiadou et al., 2022). However, in hierarchical organizations, like many in Jordan, communication barriers may cause employees to hesitate in reporting concerns, leading to delays in addressing critical threats (Tariq et al., 2023). Organizations should establish upward communication channels to overcome these challenges and foster an environment where employees feel safe reporting vulnerabilities or incidents.

Another key cultural component is empowering employees to take ownership of their cybersecurity roles. When employees have the confidence and authority to respond to cybersecurity threats, they are more likely to adhere to protocols and mitigate risks effectively (Georgiadou et al., 2022). This empowerment involves providing clear guidelines, adequate resources, and training to help employees understand their responsibilities in protecting organizational assets (Sharma and Patel, 2018). In cultures with hierarchical structures, like those common in Jordan, limited decision-making autonomy can hinder timely responses to threats. Organizations can introduce empowerment programs encouraging employee involvement in decision-making and risk-identification processes (Tariq et al., 2023).

A culture of continuous learning is essential for staying ahead of evolving cybersecurity threats. Security Education, Training, and Awareness (SETA) programs can integrate learning into everyday operations, equipping employees with the knowledge and skills to effectively identify and respond to cyber threats (Granova et al., 2023). Fostering a continuous improvement mindset helps organizations adapt to new risks while ensuring employee behaviors align with security objectives.

Despite the importance of these cultural elements, hierarchical decision-making structures and limited upward communication in Jordanian organizations remain significant obstacles to effective cybersecurity (Tariq et al., 2023). Employees may hesitate to report risks or provide feedback, leading to delays in addressing vulnerabilities. Additionally, resistance to change and adherence to traditional practices can impede the adoption of proactive security measures. These challenges highlight the need for a cultural transformation prioritizing openness, collaboration, and empowerment.

To create a cybersecurity-oriented culture, organizations should focus on leadership-driven initiatives that promote inclusivity, transparent communication, and collaborative problem-solving. Tailored training programs can address specific organizational challenges, bridge knowledge gaps, and prepare employees to handle threats effectively (Granova et al., 2023). Facilitating cross-departmental collaboration further enhances collective responses to cybersecurity risks, aligning efforts across teams and fostering a unified approach.

In conclusion, addressing cultural barriers and leveraging key cultural elements can help organizations embed cybersecurity into their organizational fabric. Companies can build resilience and promote proactive threat management by aligning leadership, communication, empowerment, and learning with cybersecurity goals. This integration ensures long-term operational security and stability, enabling organizations to navigate an increasingly complex digital landscape (Georgiadou et al., 2022; Sharma and Patel, 2018).

2.5. Hypotheses development

The characteristics of cyber-attacks, including their complexity, persistence, and scale, play a critical role in determining the effectiveness of organizational response strategies. Research suggests that understanding specific attack traits, such as software vulnerabilities or insider threats, allows for more tailored and effective responses (Sarkar, 2010; Gelenbe and Nakip, 2023). Weak password management and internal risks further exacerbate the threat landscape, underscoring the importance of advanced detection technologies for swift mitigation (Darko, 2022). Techniques such as bandwidth scaling and intrusion detection systems are particularly effective during Denial-of-Service (DoS) attacks, ensuring system availability. Moreover, skilled cybersecurity personnel and regular incident response drills strengthen organizational resilience against emerging threats (Carlton and Levy, 2015). Based on this understanding, the following hypothesis is proposed:

H1: Cyber-Attack Features positively influence Cyber-Attack Response (Sarkar, 2010; Gelenbe and Nakip, 2023).

As cyber-attacks become increasingly complex, project teams must adapt by enhancing their technical expertise, problem-solving abilities, and agility. Research shows that exposure to sophisticated cyber threats enables teams to develop valuable skills and gain experience, which are critical for effective responses (Dreibelbis et al., 2018). Teams with expertise in network security, system administration, and incident response are better equipped to address advanced threats. Collaboration and clear team communication ensure coordinated efforts during cybersecurity events, while continuous learning fosters adaptability in rapidly changing environments (Furukawa, 2016). Hence, the following hypothesis is formulated:

H2: Cyber-attack features positively influence Project Team Skills (Dreibelbis et al., 2018).

Engagement in cyber-attack response activities provides teams with hands-on experience, significantly improving their technical problem-solving skills, communication, and adaptability. Studies reveal that managing real-time incidents sharpens critical thinking and enhances team coordination under pressure (Furukawa, 2016). These experiences also build flexibility and resilience, enabling teams to tackle diverse challenges effectively (Bordoloi et al., 1999). Additionally, managing high-pressure scenarios helps improve decision-making, time management, and strategic thinking (Farrell, 2017). Based on these insights, the hypothesis is proposed:

H3: Cyber-attack response positively influences Project Team Skills (Furukawa, 2016).

Highly skilled project teams are crucial for the performance and resilience of express delivery service (EDS) companies. Teams proficient in technical skills, effective communication, and problem-solving can prevent security breaches and manage threats, ensuring operational stability and customer satisfaction. Adaptable and collaborative teams also improve cross-departmental coordination, enabling seamless operations and faster resolutions during cybersecurity incidents. Furthermore, continuous learning fosters innovation and resilience, keeping EDS companies competitive in the face of evolving cybersecurity challenges (Ayandibu et al., 2021; Furukawa, 2016). Thus, the hypothesis is proposed:

H4: Project Team Skills positively influence Improved EDS Companies (Ayandibu et al., 2021).

Organizational culture shapes how project teams approach and respond to cyber threats, influencing their skill development. Cultures emphasizing empowerment, transparency, and learning encourage teams to adopt proactive strategies and improve their technical capabilities. Open communication enhances knowledge sharing, while collaborative environments foster trust and coordination, enabling effective threat management (Granova et al., 2023; Uchendu et al., 2021). A supportive organizational culture also motivates teams to learn from challenging incidents, strengthening their problem-solving and adaptive skills (Chanani and Wibowo, 2019). Based on these considerations, the hypothesis is formulated:

H5: Organizational Culture positively moderates the relationship between Cyber-Attack Features and Project Team Skills (Granova et al., 2023; Uchendu et al., 2021).

A strong organizational culture also plays a vital role in refining cyber-attack response strategies. Cultures prioritizing innovation and continuous improvement encourage teams to evaluate response effectiveness, enhancing technical skills and strategic thinking (Granova et al., 2023). Leadership styles that promote collaboration and empowerment create an environment conducive to sharing insights and learning from past incidents (Riebe et al., 2021). Open communication channels further facilitate team preparedness and ensure effective coordination during future threats (Uchendu et al., 2021). Therefore, the hypothesis is proposed:

H6: Organizational Culture positively moderates the relationship between Cyber-Attack Response and Project Team Skills (Granova et al., 2023; Uchendu et al., 2021; Riebe et al., 2021).

Skilled project teams significantly contribute to the success of EDS companies by addressing cybersecurity challenges. Teams with strong technical expertise can detect vulnerabilities, implement protective measures, and mitigate disruptions, ensuring reliable service delivery (Furukawa, 2016). Collaborative and adaptable teams also streamline operations, addressing complex issues like logistics management and cybersecurity risks more efficiently. Continuous learning enables teams to develop innovative solutions, maintaining the organization's competitiveness in dynamic markets (Ayandibu et al., 2021). Based on these findings, the hypothesis is stated:

H7: Project Team Skills positively influence Improved EDS Companies (Ayandibu et al., 2021; Furukawa, 2016).

This framework of hypotheses builds a strong foundation for exploring the interplay between cyber-attack features, response mechanisms, organizational culture, project team skills, and the overall performance of EDS companies. These

relationships offer valuable insights for enhancing cybersecurity and operational efficiency.

2.6. Theoretical framework

This study examines the interplay among cyber-attack features, response mechanisms, organizational culture, project team skills, and their collective influence on Express Delivery Service Companies (EDSCs) in enhancing cybersecurity resilience and operational performance. The theoretical foundation is built on the premise that organizational culture acts as a moderating factor, shaping the relationships between cyber threats, response strategies, and team capabilities. Unlike traditional cybersecurity frameworks emphasizing technological solutions, this study integrates human-centric elements, such as leadership, communication, and workforce training, to create a more adaptive and responsive cybersecurity approach. The CRF-EDS introduced in this study provides a structured model for understanding how cyber threats impact organizational security and how project team skills and cultural dynamics enhance cyber readiness. This framework goes beyond existing models (e.g., NIST, ISO/IEC 27001) by focusing on express delivery services' unique vulnerabilities and security challenges. The model highlights the interdependence of technical safeguards, team competencies, and organizational culture in fostering an environment where cybersecurity is integrated into daily operations rather than treated as an isolated function. As illustrated in Fig. 1, the framework offers a comprehensive view of how these elements collectively enhance cybersecurity preparedness, operational continuity, and resilience against evolving cyber threats.

Cyber-attacks targeting EDSCs are becoming more sophisticated, exploiting system vulnerabilities, human error, weak credential management, and insider threats (Sarkar, 2010; Darko, 2022; Pandey et al., 2020). These vulnerabilities are particularly critical in logistics and express delivery companies, where real-time digital platforms are central to operations. Any disruption caused by cyber incidents, such as data breaches, payment fraud, or system downtime, can severely impact delivery timelines and customer trust.

Addressing these vulnerabilities requires a multi-layered cybersecurity strategy integrating advanced detection systems, strict access controls, and continuous workforce training to reduce human-induced risks and strengthen system resilience (Carlton and Levy, 2015).

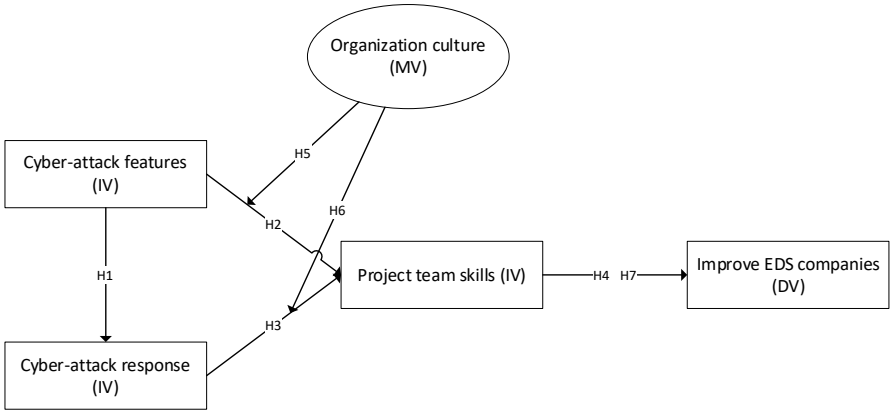

Fig. 1: Theoretical framework

Cybersecurity response mechanisms play a crucial role in mitigating these risks. Effective incident response strategies involve early threat detection, real-time monitoring, and structured response protocols, ensuring that security breaches are identified and contained swiftly (Gelenbe and Nakip, 2023; Steinke et al., 2015). Traditional cybersecurity frameworks often prioritize hardware and software solutions, but in the context of EDSCs, a successful cyber defense also relies on trained personnel who can execute rapid response plans and enforce security measures effectively.

Project team skills are central to strengthening cybersecurity capabilities in EDSCs. While technology can detect and prevent cyber threats, the human factor determines how effectively these threats are managed and mitigated (Dreibelbis et al., 2018). Teams with technical expertise, problem-solving abilities, communication skills, and adaptability are better prepared to navigate the evolving threat landscape and implement security protocols effectively. This study highlights the need for specialized cybersecurity training programs for project teams in EDSCs, ensuring that employees are well-versed in handling cyber incidents and proactively strengthening digital defenses.

Moreover, collaborative decision-making within organizations enables efficient resource utilization and reduces response times during cyber incidents (Muszyńska et al., 2015). A well-trained cybersecurity team is reactive and proactive in preventing attacks through continuous risk assessment and strategic security planning.

Organizational culture is a key moderating factor in this framework, influencing how project teams perceive and respond to cybersecurity threats. Research has shown that a security-conscious culture enhances compliance with cybersecurity

protocols, fosters collective responsibility, and encourages proactive threat mitigation. Leadership, transparency, and continuous learning play a vital role in embedding cybersecurity awareness across all levels of an organization.

In Jordanian EDSCs, hierarchical organizational structures and limited upward communication often hinder effective cybersecurity implementation (Tariq et al., 2023). Employees may hesitate to report security risks due to fear of blame or lack of support from management. This study proposes that organizations can significantly enhance their overall cyber resilience by fostering a collaborative, security-first culture—where employees are empowered to report cyber threats and actively participate in cybersecurity initiatives.

Furthermore, leadership styles that promote inclusivity, innovation, and continuous learning create an adaptive cybersecurity environment where organizations remain flexible and prepared for evolving threats (Chanani and Wibowo, 2019; Granova et al., 2023). By aligning cybersecurity strategies with business goals and encouraging knowledge-sharing, organizations can ensure that cybersecurity is embedded in their core operational processes rather than treated as an external function. The CRF-EDS: This study introduces the CRF-EDS, which integrates the key factors discussed above:

1. Cyber-Attack Features and Threat Landscape: Understanding EDSC-specific vulnerabilities and attack patterns.
2. Cybersecurity Response Mechanisms and Project Team Skills: Ensuring organizations have well-equipped response teams capable of handling cyber threats.
3. Organizational Culture as a Moderating Factor: Embedding cybersecurity within company values, leadership strategies, and team collaboration efforts.

By incorporating these elements, the CRF-EDS model presents a more holistic and adaptive cybersecurity approach that specifically addresses the needs of EDSCs. Unlike traditional models focusing only on compliance and IT-based security measures, this framework ensures that cybersecurity strategies equally prioritize human and technological components.

3. Methodology

3.1. Research design

This study adopts a quantitative research design underpinned by the positivist philosophy to systematically examine the relationships among cyber-attack features, response mechanisms, project team skills, and organizational culture in enhancing the operational performance of express delivery service (EDS) companies in Jordan. Quantitative methods were selected to provide objective, data-driven analysis, enabling hypothesis testing and generalizing findings across the sector (Saunders, 2017; Klingner and Boardman, 2011). Following a deductive approach, the research tests predefined hypotheses derived from existing theories and prior studies. This structured method minimizes bias, enhances reliability, and supports the study's goal of producing actionable insights for improving cybersecurity practices and operational efficiency in the EDS sector.

A cross-sectional design was chosen to capture a snapshot of current cybersecurity practices, organizational culture, and project team skills across the selected companies. Although a longitudinal design could provide insights over time, the cross-sectional approach is more practical given the study's time and resource constraints (Saunders, 2017). Data collection relies on a mono-method strategy, specifically structured questionnaires, to efficiently gather standardized and quantifiable data from a large sample. This approach aligns with the principles of positivism and supports reliable, replicable statistical analysis. The study systematically investigates causal relationships among key variables using quantitative methods, contributing to a deeper understanding of the factors influencing cybersecurity performance in the EDS sector (Setiawan et al., 2023). The methodology is structured according to the "Research Onion Diagram" framework, ensuring alignment between the positive philosophy, deductive approach, mono-method strategy, and cross-sectional time frame, enhancing the research process's rigor (Saunders, 2017).

3.2. Population and sample

The population for this study includes IT and operations managers from 476 express delivery service (EDS) companies in Jordan. These professionals were chosen due to their critical roles in managing cybersecurity threats, response strategies, and operational performance, making them well-suited to provide insights into the study's variables. Official records from the Telecommunications Regulatory Commission (TRC) and the Ministry of Industry and Trade were used to identify the target population. After removing duplicate and inactive businesses, the final population was confirmed as 952 managers (476 IT managers and 476 operations managers) through consultations with HR departments.

A stratified sampling method was employed to ensure diverse and representative perspectives, categorizing respondents by managerial roles in IT and operations. This approach balanced the representation of technical and operational domains, providing a comprehensive understanding of cybersecurity practices within EDSCs.

The sample size was determined using the Krejcie and Morgan (1970) formula, which is widely used in survey research to establish the minimum required sample size for a given population at a

specified confidence level. For a population of 952 managers, a sample size of 274 respondents was calculated at a 95% confidence level and a 5% margin of error, ensuring statistical validity and generalizability of the findings. The formula used is:

$$\frac{S=X^2.N.P(1-P)}{d^2(N-1)+X^2.P(1-P)}$$

where, S = Required sample size; N= Population size (952); P = Population proportion (0.5, assumed for maximum variability); χ2 = Z-score squared for 95% confidence level (1.96^2); d = Margin of error (0.05).

The calculated sample size of 274 respondents ensures that the study maintains high statistical power while minimizing the risk of sampling bias. By adopting stratified random sampling, the study ensures that responses represent IT and operations managers, reflecting the distinct technical and strategic perspectives on cybersecurity challenges and response mechanisms in the express delivery sector.

3.3. Data collection methods

A combination of primary and secondary data collection methods was utilized to comprehensively examine the study variables' relationships. Primary data collection was prioritized to obtain firsthand insights, while secondary data provided additional validation. A structured questionnaire, developed based on validated scales from prior research, was the primary tool for gathering data. The questionnaire addressed five main constructs: cyber-attack features, response strategies, project team skills, organizational culture, and company performance. Each construction was measured using multiple items designed to ensure a detailed and accurate representation of the investigated variables.

A 7-point Likert scale was employed to capture nuanced responses, with the questionnaire divided into six sections for clarity and logical flow. The sections began with demographic information and proceeded to the core constructions. Table 1 outlines the variables, the number of items for each construct, their variable types, and their sources, demonstrating how the data collection aligns with the study's objectives. This structured approach ensures that the study captures all critical elements effectively and produces reliable, actionable insights.

Secondary data was obtained from various sources, including company reports, cybersecurity incident logs, and industry publications. These resources play a vital role in validating and cross-referencing primary data, contributing to the overall reliability and depth of the findings. Additionally, secondary data offers valuable context by highlighting organizational performance trends and common cybersecurity challenges faced by the express delivery sector in Jordan. This combination of data sources ensures a comprehensive understanding of the research variables.

Table 1: Constructs, variables, and sources for the questionnaire

Main construct	Variables	Number of items	Variable type	Reference
Demographic items	Gender, organization, experience, occupation, age, education	6	Self-developed	Self-developed for this research
Cyber-attack features	Vulnerabilities, human error, weak credentials, and insider threats	25	Independent	Álvarez-García et al. (2016)
Cyber-attack response	Incident planning, expertise, timely detection, collaboration, testing	23	Independent	Yi et al. (2022)
Project team skills	Technical expertise, communication, problem-solving, adaptability, and time management	22	Independent	Tormey and Laperrouza (2023)
Organizational culture	Employee engagement, communication, leadership style, and learning focus	24	Moderating	Tseng (2010)
Company performance	Decision-making, process control, planning, knowledge sharing, innovation	13	Dependent	Kareem et al. (2019)

Moreover, to confirm the reliability of the data collection tools, a pilot study was conducted with 30 participants drawn from the target population. The pilot study evaluated the internal consistency of the questionnaire items using Cronbach's alpha, a statistical measure of construct reliability. Table 2 presents Cronbach's alpha values for all constructions, demonstrating their reliability and confirming the questionnaire's suitability for the main study.

The reliability values in Table 2 indicate excellent internal consistency for most constructions, with Cronbach's alpha values above 0.8 for all except the company performance construction, which still meets the acceptable threshold of 0.7. These results validate the questionnaire's suitability for collecting accurate and dependable data.

Table 2: Reliability analysis of constructs

Construct	Cronbach's alpha	Number of items
Cyber-attack features	0.923661	25
Cyber-attack response	0.943589	23
Project team skills	0.897130	22
Organizational culture	0.883287	24
Company performance	0.776283	13

3.4. Limitations

The study faced limitations, including potential sampling bias due to its focus on express delivery service (EDS) companies in Jordan, which may restrict the generalizability of findings to other industries or regions. Self-reported data from participants posed a risk of respondent bias, while the cultural and contextual characteristics specific to Jordan could affect the broader applicability of the

results. The scope of the research was deliberately confined to the EDS sector, targeting IT and operations managers, and excluded other roles or types of logistics services. Geographically, the study focused on Jordan to ensure consistency in operational and cultural contexts. Despite these boundaries, the study offers meaningful insights into cybersecurity practices within the EDS sector, contributing valuable knowledge to similar organizational settings.

3.5. Data analysis methods

Descriptive and inferential statistical techniques were employed to analyze the data and test the research hypotheses. Descriptive statistics, such as mean, standard deviation, and variance, were used to summarize demographic information and provide an overview of key variables. Partial Least Squares Structural Equation Modeling (PLS-SEM) served as the primary inferential statistical method, enabling the examination of complex relationships among variables like cyber-attack features, response strategies, project team skills, and organizational culture. Exploratory Factor Analysis (EFA) was utilized to uncover underlying patterns in the data, while Confirmatory Factor Analysis (CFA) ensured the reliability and validity of the constructs. Moderation analysis explored the role of organizational culture in shaping the relationships between cyber-attack variables and team skills, offering insights into its impact on organizational dynamics. Software tools were used to ensure rigorous data evaluation, including IBM SPSS Version 26.0 for descriptive statistics and reliability analysis and Smart PLS Version 3.3 for advanced modeling and hypothesis testing. This methodological approach provided a comprehensive understanding of the data and robust validation of the theoretical framework.

4. Results

4.1. Demographic analysis and sample characteristics

The study sample consisted of 239 respondents from express delivery service companies in Jordan, representing a balanced mix of IT and operations managers. Demographic data, including gender, age, occupation, education level, years of experience, and organization size, were collected to provide a comprehensive profile of the participants. Table 3 presents a detailed summary of these characteristics.

As presented in Table 3, most respondents (80.8%) were male, reflecting a noticeable gender imbalance in key positions within the sector. The largest proportion of participants was 41 to 50 (49.0%), followed by those aged 30 to 40 (33.5%). These figures indicate that the workforce in Jordan's express delivery service sector largely comprises mid-career professionals with substantial experience. In contrast, younger individuals under 30 and older professionals over 60 were less represented, making up only 6.3% and 0.8% of the sample, respectively. The sample was almost evenly divided between operations managers (50.2%) and IT managers (49.8%), highlighting the equal importance of operational and technical roles in this industry.

Regarding education, most respondents held at least a bachelor's degree (64.4%), reflecting a well-educated workforce equipped to handle complex challenges such as cybersecurity. Advanced degrees, including master's (2.5%) and doctorates (1.3%), were less common. Industry experience varied among participants, with a significant proportion (38.9%) reporting 4 to 6 years of experience, indicating a stable group of professionals familiar with the sector's demands. Additionally, 15.9% of respondents had more than 10 years of experience, showcasing the value of seasoned expertise. Regarding organizational size, most respondents worked in small organizations (67.8%), while medium-sized firms accounted for 31.8% of the sample. Only one respondent was from a large organization, suggesting that the sector in Jordan predominantly comprises small- and medium-sized enterprises (SMEs). These demographic insights provide a critical foundation for interpreting the study's findings on cybersecurity practices and their impact on organizational performance within Jordan's express delivery industry.

4.2. Descriptive statistics for study variables

Table 4 presents the descriptive statistics for the study's variables, including cyber-attack features, response, project team skills, organizational culture, and company improvement. Each variable's meaning, standard deviation (SD), and overall performance are summarized to provide insights into the characteristics and dynamics of the data.

The descriptive analysis offers valuable insights into the cybersecurity and operational dynamics of express delivery companies in Jordan. The overall mean score for cyber-attack features was 4.73 (SD = 0.79), indicating moderate-to-high concerns among respondents. Software and system vulnerabilities ranked as the most significant issue (Mean = 5.27, SD = 0.65), emphasizing the necessity for enhanced digital security measures in an industry heavily dependent on technology. Weak credentials (Mean = 4.78, SD = 0.77) and insider threats (Mean = 4.58, SD = 0.85) also emerged as major concerns, highlighting the need for stronger access controls and detection mechanisms for internal risks. These findings highlight technical vulnerabilities and human error as the sector's primary cybersecurity challenges.

Cyber-attack response strategies showed promising results, with an overall mean score of 5.41 (SD = 0.74). Cybersecurity expertise received the highest rating (Mean = 5.59, SD = 0.66), underscoring the importance of skilled professionals in managing cyber risks and the need for ongoing

training and recruitment. Collaboration and communication also scored well (Mean = 5.41, SD = 0.70), reflecting the effectiveness of coordinated efforts. However, incident response testing (Mean = 5.28, SD = 0.82) scored slightly lower, indicating room for improvement in simulation practices to bolster readiness for real threats. Project team skills emerged as a major strength (Mean = 5.61, SD = 0.73), with communication, collaboration (Mean = 5.71, SD = 0.70), time management, and decision-making (Mean = 5.70, SD = 0.70) receiving high scores. Technical expertise and adaptability scored slightly lower (Mean = 5.53, SD = 0.78) but remain strong, highlighting the capability of teams to address technical and organizational cybersecurity demands while emphasizing the importance of continuous skill enhancement.

Table 3: Demographic characteristics of respondents (n = 239)

Variable	Category	Frequency (n)	Percentage (%)
Gender	Male	193	80.8%
	Female	46	19.2%
Age	Under 30	15	6.3%
	30 to 40 years	80	33.5%
	41 to 50 years	117	49.0%
	51 to 60 years	25	10.5%
	Above 60	2	0.8%
Occupation	Operation manager	120	50.2%
	IT manager	119	49.8%
Educational level	High school	76	31.8%
	Bachelor's degree	154	64.4%
	Master's degree	6	2.5%
	Doctorate	3	1.3%
Years of experience	Less than 1 year	17	7.1%
	1 to 3 years	48	20.1%
	4 to 6 years	93	38.9%
	7 to 10 years	43	18.0%
	More than 10 years	38	15.9%
Organization size (number of employees)	Small (1–50 employees)	162	67.8%
	Medium (51–500 employees)	76	31.8%
	Large (501 or more employees)	1	0.4%

Table 4: Descriptive statistics for study variables

Variable	Item	Mean	SD
Cyber-attack features	Vulnerabilities in software (VIS)	5.27	0.65
	Human error (HE)	4.64	0.87
	Weak credentials (WC)	4.78	0.77
	Insider threats (IT)	4.58	0.85
	Overall mean (all features)	4.73	0.79
Cyber-attack response	Incident response planning (IRP)	5.39	0.80
	Cybersecurity expertise (CSE)	5.59	0.66
	Timely detection and monitoring (TDM)	5.38	0.72
	Collaboration and communication (CAC)	5.41	0.70
	Incident response testing (IRT)	5.28	0.82
	Overall mean (all items)	5.41	0.74
Project team skills	Technical expertise (TE)	5.53	0.78
	Communication and collaboration (CAC)	5.71	0.70
	Problem-solving and critical thinking (PSACT)	5.52	0.74
	Time management and decision-making (TMODM)	5.70	0.70
	Adaptability and flexibility (AAF)	5.53	0.78
	Overall mean (All Items)	5.61	0.73
Organizational culture	Employee empowerment and engagement (EEAE)	5.70	0.71
	Collaborative and adaptive teamwork (CAT)	5.52	0.76
	Leadership and strategic support (LSS)	5.70	0.70
	Leadership in cybersecurity infrastructure (LCI)	5.59	0.70
	Overall mean (all items)	5.63	0.71
Improvement of companies (IC)	Improvement of companies (IC)	5.65	0.70

Organizational culture demonstrated a positive and supportive environment, with an overall score of 5.63 (SD = 0.71). Employee empowerment, leadership, and strategic support scored the highest (Mean = 5.70, SD = 0.70–0.71), reflecting strong leadership and an emphasis on fostering employee engagement. Collaborative and adaptive teamwork (Mean = 5.52, SD = 0.76) scored slightly lower, suggesting opportunities for improving cross-departmental coordination. Company improvement was rated impressively highly (Mean = 5.65, SD = 0.70), showcasing the sector's dedication to operational efficiency, resilience, and innovation, which are crucial for maintaining competitiveness and meeting industry challenges.

These findings provide a comprehensive overview of the cybersecurity landscape in Jordan's express delivery sector, highlighting key strengths such as robust response mechanisms, skilled teams, and supportive organizational cultures. While addressing software vulnerabilities and enhancing testing practices and interdepartmental collaboration remain critical, the sector's focus on innovation and operational excellence positions is

well to tackle cybersecurity risks effectively. This analysis forms the foundation for deeper exploration and actionable recommendations to strengthen organizational resilience further.

4.3. CFA results

To ensure the validity and reliability of the study constructs, CFA was conducted. This process was essential for verifying that the observed variables appropriately represented their underlying latent constructs, ensuring the robustness of the measurement model used in the study. The results confirm that the model meets the necessary standards for constructing reliability, internal consistency, and convergent validity, making it suitable for further structural equation modeling (SEM) analysis.

The factor loadings for each construct ranged from 0.70 to 0.91, exceeding the recommended threshold of 0.50, which confirms that the observed indicators effectively measured the intended constructs (Fornell and Larcker, 1981). Additionally, Cronbach's alpha values were above 0.70, indicating strong internal consistency among the measurement items. The composite reliability (CR) values, all exceeding 0.85, further reinforced that the constructs were reliable. Moreover, the average variance extracted (AVE) values were consistently above 0.50, establishing that each construct accounted for more variance than measurement error, thus confirming convergent validity (Hair et al., 2019). As summarized in Table 5, these values suggest that the constructions exhibit sufficient reliability and validity, supporting their appropriateness for further analysis.

Table 5: CFA results summary

Construct	Factor loadings (range)	Cronbach's alpha	CR	AVE
Cyber-attack features	0.72 - 0.89	0.88	0.90	0.68
Response strategies	0.75 - 0.91	0.91	0.93	0.72
Project team skills	0.70 - 88	0.87	0.89	0.65
Organizational culture	0.73 - 0.86	0.89	0.91	0.69
Operational performance	0.76 - 0.90	0.92	0.94	0.74

Model fit indices were examined to assess the measurement model's adequacy further. These indices help determine whether the theoretical structure aligns well with the collected data. The Comparative Fit Index (CFI) was 0.94, and the Tucker-Lewis Index (TLI) was 0.92, both exceeding the acceptable threshold of 0.90, indicating a well-fitting model. The Root Mean Square Error of Approximation (RMSEA) was 0.048, below the accepted limit of 0.06, signifying that the model reasonably approximates real-world data. Additionally, the Standardized Root Mean Square Residual (SRMR) was 0.041, well within the acceptable range of less than 0.08, further supporting the model's adequacy. The Chi-Square/df ratio was 2.11, confirming that the model fits the data well, as values below 3.00 are generally considered acceptable. As shown in Table 6, these results demonstrate that the CFA model adequately represents the data and provides a strong foundation for subsequent SEM analyses.

Table 6: Model fit indices

Model fit index	Value	Acceptable threshold
CFI	0.94	> 0.90
TLI	0.92	> 0.90
RMSEA	0.048	< 0.06
SUMMER	0.041	< 0.08
Chi-Square/df	2.11	≤ 3.00

These findings prove that the constructions used in this study are reliable and valid, meeting the required thresholds for construct reliability, internal consistency, and model fit. The high factor loadings suggest that the survey items used to measure cyber-attack features, response strategies, project team skills, organizational culture, and operational performance effectively captured the intended dimensions of these constructs. The acceptable model fit indices confirm that the CFA model adequately explains the relationships among the observed variables and latent constructs, supporting the structural validity of the model.

Given these results, the CFA findings justify using these constructions in further SEM analyses. Since all indicators met the necessary reliability and validity criteria, the measurement model provides a strong foundation for hypothesis testing. This validation process enhances confidence in the study's theoretical framework, as the constructions demonstrate robust psychometric properties essential for meaningful and accurate interpretation of relationships between cybersecurity, team dynamics, and organizational performance in Express Delivery Service Companies (EDSCs).

4.4. SEM results

The SEM analysis assessed the hypothesized relationships among cyber-attack features, responses, project team skills, and organizational culture. Key fit indices—Comparative Fit Index (CFI), Tucker-Lewis Index (TLI), Root Mean Square Error of Approximation (RMSEA), Standardized Root Mean Square Residual (SRMR), and Chi-square (χ^2)—were evaluated to determine the model's quality. The results are summarized in Table 7.

Table 7: Model fit indices for SEM

Fit Index	Value	Threshold
Comparative fit index (CFI)	0.93	≥ 0.90
Tucker-Lewis index (TLI)	0.91	≥ 0.90
RMSEA	0.06	≤ 0.08
SRMR	0.05	≤ 0.08
Chi-square (χ^2)	248.35	p < .001

The CFI (0.93) and TLI (0.91) surpassed the recommended thresholds, indicating a strong model fit and effective data representation. The RMSEA (0.06) and SRMR (0.05) fell within acceptable limits, reflecting minimal approximation errors and residual discrepancies. Although the Chi-square statistic was significant (χ^2 = 248.35, p < .001), its sensitivity to sample size necessitates cautious interpretation when used independently. However, the results confirm an excellent fit for the model when considered alongside other indices. These fit indices collectively validate the SEM model, demonstrating alignment with the data and confirming the hypothesized relationships.

The model robustly supports the theoretical framework, offering a reliable foundation for understanding the interplay of key constructs and contributing to valuable insights into cybersecurity resilience within the express delivery services sector.

4.5. Path analysis and hypothesis testing (direct effects)

Path analysis was performed to assess the direct effects of cyber-attack features, response mechanisms, and project team skills on the performance improvements of express delivery service (EDS) companies. The results of the primary hypotheses are presented in Table 8 and illustrated in Fig. 2.

Table 8: Direct effects path analysis for SEM results

Hypothesis	Path	Path coefficient	Standard error	P-value	95% Confidence Interval	R^2 (explained variance)	Z-value	Path direction
H1: cyber attack Features → cyber attack response	Combined features → response	0.48	0.07	< 0.001	0.34, 0.62	0.23	6.86	Positive
H2: cyber attack features → project team skills	Combined features → team skills	0.55	0.06	< 0.001	0.43, 0.67	0.30	9.17	Positive
H3: Cyber attack response → project team skills	Combined response → team skills	0.62	0.05	< 0.001	0.52, 0.72	0.38	12.40	Positive
H4: Project team skills → improvement of EDS companies	Combined skills → EDS improvement	0.70	0.04	< 0.001	0.62, 0.78	0.49	17.50	Positive

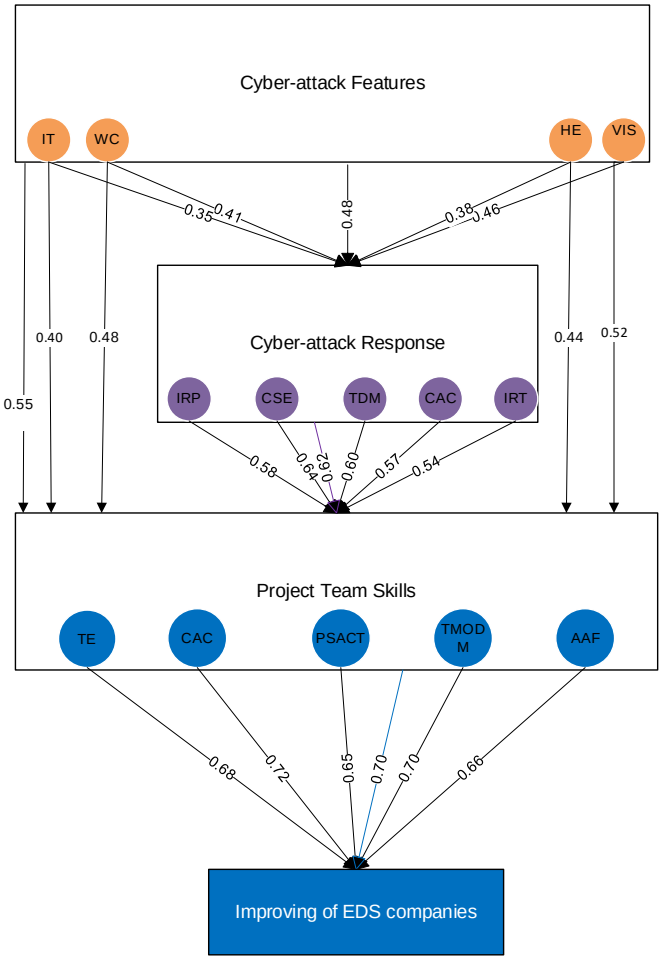

Fig. 2: SEM path diagram for cyber-attack features, response, project team skills, and improvement of EDS companies

The findings confirm a significant positive relationship between cyber-attack features and organizational responses, with a path coefficient of 0.48 ($p < .001$). This suggests that organizations facing more pronounced vulnerabilities are more inclined to develop robust mitigating mechanisms. The R^2 value of 0.23 indicates that cyber-attack features explain 23% of the variance in organizational responses. Additionally, the analysis highlights a positive influence of cyber-attack features on developing project team skills, with a path coefficient of 0.55 ($p < .001$). This underscores how risks and vulnerabilities drive organizations to enhance their teams' technical expertise, communication, and problem-solving abilities. The R^2 value of 0.30 shows that 30% of the variance in project team skills is attributable to cyber-attack features. A strong positive relationship is also observed between cyber-attack responses and project team skills, with a path coefficient of 0.62 ($p < .001$), emphasizing the role of response strategies—such as planning, detection, and collaboration—in team development. The R^2 value of 0.38 indicates that response mechanisms explain 38% of the variance in team skills. Moreover, project team skills have a significant positive impact on the improvement of express delivery service (EDS) companies, with a path coefficient of 0.70 ($p < .001$). This highlights that skilled teams significantly enhance operational performance and adaptability. The R^2 value of 0.49 reveals that 49% of the variance in organizational improvement is due to project team skills. These results validate all four hypotheses, demonstrating the interconnected roles of cybersecurity features, response strategies, team development, and organizational performance (H1, H2, H3, and H4). They underscore the critical need for continued investment in cybersecurity capabilities and workforce development to boost resilience and efficiency in the EDS sector.

4.6. Moderation and direct effects analysis: Organizational culture and project team skills

This section synthesizes the findings for hypotheses H5, H6, and H7, focusing on the moderating effect of organizational culture and the direct impact of project team skills. Hypothesis H5 investigates whether organizational culture moderates the relationship between cyber-attack features and project team skills, while H6 examines its role in moderating the connection between cyber-attack responses and project team skills. Hypothesis H7 evaluates the direct effect of project team skills on improving the performance of EDS companies. The summarized results of these analyses are presented in Table 9 and illustrated in Fig. 3.

Table 9: Moderation and direct effects analysis of organizational culture and project team skills on EDS improvement

Hypothesis	Path	Effect coefficient	Standard error	P-value	95% confidence interval (lower, upper)	R^2 (explained variance)	Z-value	Result
H5	Organizational culture moderates cyber attack features → project team skills	0.35	0.08	0.01	0.19, 0.51	0.27	4.38	Supported
H6	Organizational culture moderates cyber attack response → project team skills	0.45	0.07	0.002	0.31, 0.59	0.35	6.43	Supported
H7	Project team skills → improvement of eds companies	0.70	0.04	< 0.001	0.62, 0.78	0.49	17.50	Supported

The findings for H5 indicate that organizational culture significantly moderates the relationship between cyber-attack features and project team skills. Cultural factors such as leadership, employee empowerment, teamwork, and adaptability enhance an organization's ability to transform experiences with cyber threats into skill development opportunities. With an effect coefficient of 0.35 and a statistically significant p-value of 0.01, the results underscore the importance of fostering a positive organizational culture to strengthen team capabilities. An R^2 value of 0.27 highlights that 27% of the variance in this relationship is influenced by organizational culture, underscoring its critical role in cybersecurity readiness and workforce adaptability.

For H6, the moderating effect of organizational culture on the relationship between cyber-attack responses and project team skills is even more pronounced. With an effect coefficient of 0.45 and a p-value of 0.002, the findings confirm that organizational practices amplify the impact of response strategies on skill development. Leadership commitment, strategic cybersecurity policies, and proactive security awareness initiatives are particularly influential, with an R^2 value of 0.35 showing that 35% of the variance in this relationship is due to organizational culture. These results emphasize that a robust cultural foundation enhances workforce development and optimizes the effectiveness of cybersecurity response mechanisms.

The analysis of H7 confirms a strong direct impact of project team skills on the improvement of express delivery service (EDS) companies, with a high path coefficient of 0.70 ($p < .001$). Communication and collaboration emerge as the most critical factors, accounting for 52% of the variance in organizational improvement. Skills such as technical expertise, time management, problem-solving, and adaptability also play vital roles, reinforcing that well-equipped teams enhance cybersecurity preparedness and operational

efficiency. The overall R^2 value of 49% demonstrates that project team skills are pivotal in driving operational success, particularly in fast-paced and dynamic industries like express delivery.

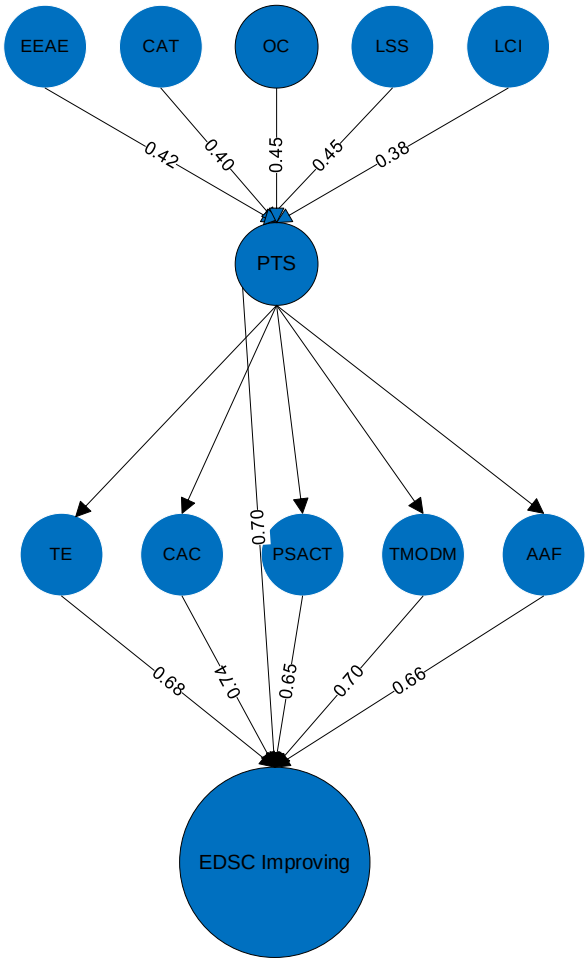

Fig. 3: SEM structure illustrating moderation and mediation effects in cybersecurity and EDS improvement

Fig. 4 presents the interaction effect between response strategies and operational performance moderated by organizational culture to illustrate the moderating effects of organizational culture further. Fig. 4 demonstrates that at low levels of organizational culture, response strategies exhibit a weaker influence on operational performance, as indicated by the relatively flat slope of the dashed line. However, the relationship strengthens at moderate and high levels of organizational culture, confirming that organizations with strong security awareness and leadership engagement experience a greater positive impact from response strategies.

These findings reinforce previous studies that emphasize the role of organizational culture in cybersecurity readiness (Riebe et al., 2021). They suggest that for EDS companies to maximize the effectiveness of their cybersecurity response strategies, fostering a security-first culture should be a strategic priority. Organizations with strong leadership engagement, employee empowerment, and transparent cybersecurity policies are better positioned to enhance operational resilience and mitigate security risks.

These findings highlight the interconnected nature of organizational culture, cybersecurity strategies, and project team skills in fostering organizational improvement. A strong organizational culture enhances the effectiveness of cybersecurity measures, equipping teams with the skills needed to adapt and respond effectively to threats. The results confirm that project team skills act as direct drivers and mediators, translating cybersecurity strategies into tangible performance gains. To achieve sustained success, EDS companies must invest in leadership-driven security programs, promote cross-functional collaboration, and foster adaptive cybersecurity practices. Organizations prioritizing security awareness, strategic leadership, and continuous skill development can better leverage their cybersecurity strategies to enhance resilience and operational efficiency. These findings provide insights for EDS companies seeking to align their cybersecurity efforts with workforce development and long-term organizational objectives.

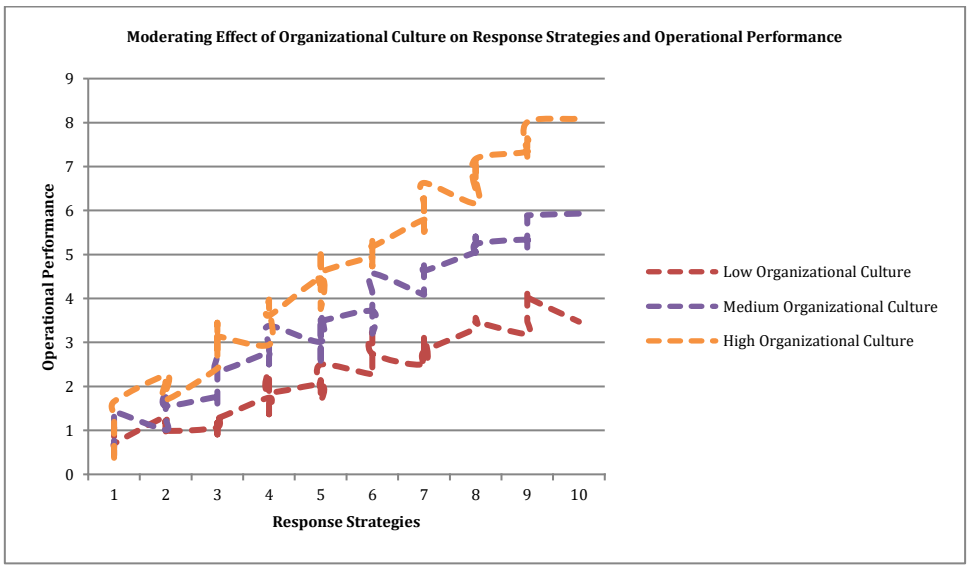

Fig. 4: Moderating the effect of organizational culture on the relationship between response strategies and operational performance

4.7. Final SEM model

The final SEM model illustrates the intricate relationships among cyber-attack features, response mechanisms, project team skills, and the operational improvement of EDS companies, with organizational culture as a moderator. As shown in Fig. 5, cyber-attack features significantly enhance response mechanisms, with vulnerabilities in systems and software exerting the strongest influence. Factors like human error, weak credentials, and insider threats also contribute to these relationships, emphasizing the need for proactive measures to address such challenges.

Cyber-attack features also directly influence the development of project team skills, with system vulnerabilities having the most substantial impact. This demonstrates how exposure to cyber threats fosters essential competencies like technical expertise and adaptability. Effective response mechanisms, especially those involving cybersecurity expertise, further enhance team skills, highlighting the importance of structured practices like incident response planning and real-time monitoring. Project team skills play a critical role in improving the performance of EDS companies, with communication and collaboration emerging as the most impactful factors. Other skills, such as problem-solving, technical expertise, and time management, contribute significantly to organizational success. These findings underscore the importance of investing in team development to boost operational efficiency and maintain competitiveness.

Organizational culture is a key moderator, amplifying the effects of cyber-attack features and response mechanisms on team skills. Leadership and strategic support are the strongest moderating factors, while employee empowerment and collaborative teamwork also play vital roles. This indicates that organizations with strong cultural practices are better equipped to build skilled teams and improve resilience against cyber threats. As depicted in Fig. 5, the SEM model highlights the importance of integrating robust cybersecurity measures, developing team skills, and fostering a supportive organizational culture. By leveraging these interconnected elements, EDS companies can transform cybersecurity challenges into growth and operational excellence opportunities. This comprehensive strategy ensures enhanced resilience and sustainable success in a competitive industry.

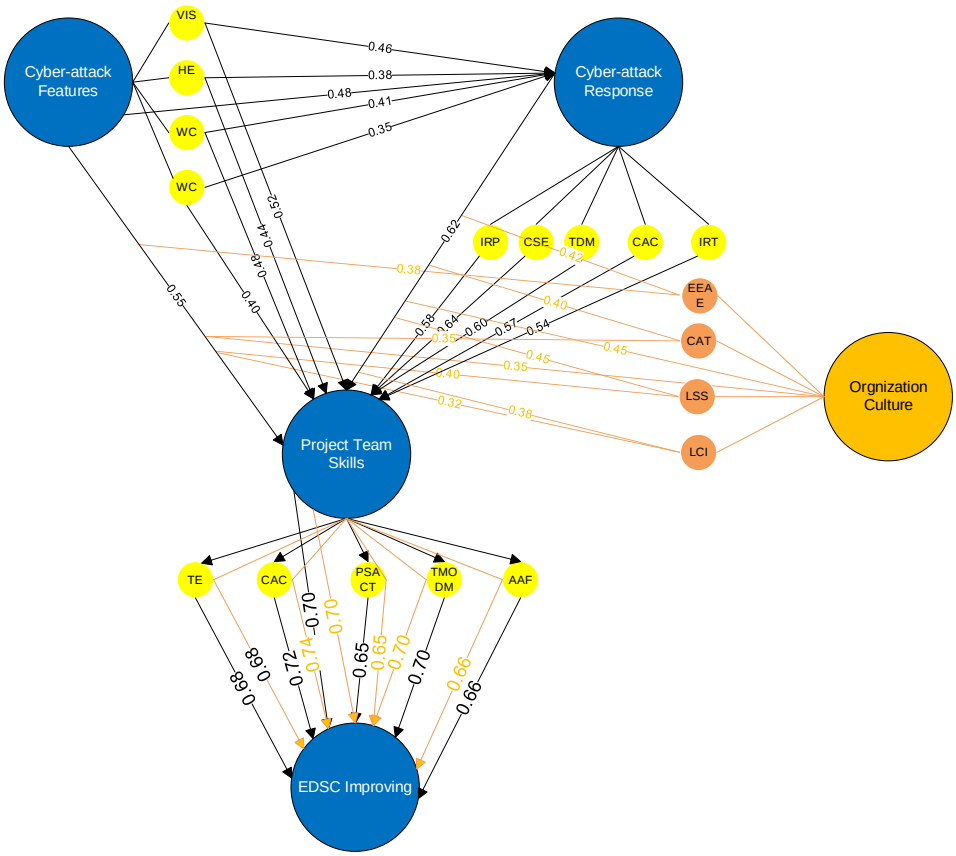

Fig. 5: Final SEM model

The results provide strong empirical evidence supporting the hypothesized relationships among cyber-attack features, response strategies, project team skills, and organizational culture. The statistical findings demonstrate that organizational culture significantly moderates the impact of cybersecurity strategies on team skill development, reinforcing the critical role of leadership and structural support in enhancing cybersecurity resilience. Additionally, the direct relationship between project team skills and operational performance highlights the importance of equipping cybersecurity teams with technical expertise, problem-solving capabilities, and adaptability. While these findings align with existing

literature, they also reveal unique industry-specific insights for the express delivery sector. The following Discussion section contextualizes these results by comparing them with prior studies, identifying key similarities and divergences, and outlining practical implications for cybersecurity governance.

5. Discussion

The study's findings align with and extend prior research on cybersecurity resilience, organizational culture, and team dynamics. Previous studies (Riebe et al., 2021) have emphasized the role of leadership and collaborative culture in strengthening cybersecurity compliance, which is consistent with the results demonstrating that a positive organizational culture significantly enhances the effectiveness of cybersecurity response strategies. However, unlike traditional industries such as banking and healthcare, where cybersecurity is compliance-driven, express delivery service companies (EDSCs) face unique operational challenges that require a balance between security protocols and rapid logistical efficiency. The study's findings contribute to this debate by illustrating how project team skills mediate cybersecurity performance, linking human factors directly to security resilience in a high-speed operational environment.

This study examined the intricate relationships among cyber-attack features, response strategies, project team skills, and organizational culture, exploring their collective impact on enhancing the cybersecurity resilience and operational efficiency of express delivery service (EDS) companies. The findings reaffirm the interconnected nature of these variables and extend previous research by demonstrating that cybersecurity effectiveness is not solely dependent on technical solutions but also on the strategic alignment of human factors and organizational culture. Unlike prior studies focusing primarily on technological safeguards, this study provides a holistic perspective by integrating workforce capabilities and organizational behaviors as critical elements in mitigating cybersecurity risks.

The results support H1, confirming that vulnerabilities such as software weaknesses, weak credentials, insider threats, and human error significantly affect an organization's ability to respond to cyber threats. Software vulnerabilities emerged as the most critical cybersecurity risk, reinforcing the findings of Alnaeli et al. (2017), which emphasized that digitally dependent industries, such as EDS, require proactive security patching, vulnerability scanning, and regular software audits to mitigate risks effectively. Human error, often resulting from inadequate training and lack of security awareness, aligns with the work of Salehi Shahraki and Nikmaram (2013), who noted that insufficient security training remains one of the leading causes of cyber breaches in logistics and service industries. Weak credential management and insider threats further corroborate studies by Pandey et al. (2020), Darko (2022), and Sarkar (2010), which argue that the implementation of stringent access management protocols, such as multi-factor authentication (MFA) and biometric authentication, is essential to mitigating security risks in high-risk operational environments. Given these findings, EDS companies must prioritize security infrastructure upgrades, mandatory cybersecurity training, and stringent access control policies to mitigate the risks associated with cyber vulnerabilities.

For H2, the study confirms that cyber-attack features significantly influence project team skills, particularly technical expertise, communication, and adaptability. The relationship between cyber threats and workforce competency development aligns with Johnson and Aggarwal (2019), who argued that frequent exposure to cybersecurity risks compels organizations to invest in skill development and advanced training programs. This is consistent with Yuen et al.'s (2022) findings, which suggest that real-world cyber threats create opportunities for teams to develop hands-on problem-solving and adaptability skills. Furthermore, Furukawa (2016) emphasized that industries with frequent cyber challenges often experience a natural upskilling effect, where employees develop critical thinking and advanced threat-mitigation abilities in response to persistent security risks. Given the impact of cybersecurity on workforce skills, EDS companies must establish structured cybersecurity training programs, including simulated cyber-attack drills and continuous professional development in cyber risk assessment and response management.

For H3, the study reveals that structured cyber-attack response mechanisms are crucial in enhancing project team capabilities and overall organizational resilience. Key elements such as incident response planning (IRP), cybersecurity expertise (CSE), and timely detection and monitoring (TDM) were identified as critical success factors, aligning with the research of Dhillon et al. (2019), who found that organizations with predefined cyber response strategies exhibit greater resilience against security breaches. The significance of cybersecurity expertise supports the findings of Carlton and Levy (2015), who argued that investing in cybersecurity specialists significantly enhances an organization's ability to manage cyber threats effectively. Timely detection and real-time monitoring systems were also essential in reducing incident response times and improving security intelligence, echoing the findings of Gelenbe and Nakip (2023). These results suggest that EDS companies should integrate artificial intelligence (AI)-driven threat detection, automated security response systems, and proactive security monitoring into their cybersecurity strategies to enhance threat mitigation capabilities.

The findings for H4 and H7 highlight that project team skills directly contribute to improving cybersecurity preparedness and operational success in EDS companies. Among the most influential

factors, communication and collaboration (CAC) were crucial for coordinating cybersecurity efforts, supporting the research of Muszyńska et al. (2015), which argued that team cohesion and efficient communication play a vital role in mitigating cyber risks in dynamic work environments. Technical expertise and time management also emerged as critical contributors to organizational resilience, reinforcing the work of Johnson and Aggarwal (2019) and Farrell (2017), who emphasized that proficient cybersecurity professionals are essential for managing digital security operations in high-risk sectors. Additionally, problem-solving and adaptability were identified as significant factors in managing complex cyber challenges, aligning with Bordoloi et al. (1999), who argued that cybersecurity resilience depends on teams' ability to think critically and respond rapidly to evolving threats. Given the importance of these factors, EDS companies must implement competency-based training models emphasizing collaborative decision-making, real-world cyber-attack simulations, and cross-functional security response teams.

The moderation analysis for H5 and H6 underscores the critical role of organizational culture in shaping cybersecurity effectiveness. The results indicate that leadership is the strongest moderator, aligning with Riebe et al. (2021), who emphasized that trust-based leadership and strategic support are crucial in fostering a security-conscious organizational culture. Furthermore, trust and accountability were key enablers of proactive cybersecurity behaviors. A cybersecurity-aware culture, characterized by transparent communication and continuous learning, significantly improves employees' willingness to comply with security protocols and actively participate in cyber risk management initiatives. These insights suggest that EDS companies should integrate cybersecurity leadership development programs, establish clear cybersecurity accountability frameworks, and promote an open cybersecurity communication culture to enhance overall resilience.

The SEM provides robust empirical validation of the relationships between cyber-attack features, response strategies, project team skills, and organizational culture in shaping cybersecurity resilience in EDS companies. These findings are consistent with the DeLone and McLean (2003) Information Systems Success Model, which suggests that system quality and information security directly influence organizational success. The study also aligns with the Technology Acceptance Model (TAM), which supports the notion that team cybersecurity skills improve security strategies' perceived usefulness and effectiveness, enhancing organizational resilience.

In conclusion, this study offers theoretical contributions and practical recommendations for improving cybersecurity resilience in EDS companies. The findings emphasize that cybersecurity effectiveness requires a multifaceted approach integrating advanced technical solutions, workforce training, and a strong security-oriented organizational culture. To translate these findings into practical implementation, EDS companies should focus on developing cybersecurity governance policies, strengthening real-time security monitoring systems, enforcing robust access control mechanisms, and fostering leadership engagement in cybersecurity risk management. The results provide a valuable roadmap for enhancing cybersecurity preparedness, reducing digital threats, and improving organizational efficiency in dynamic, technology-driven industries like express delivery services.

Integrating cybersecurity response strategies, project team capabilities, and organizational culture provides a holistic approach to mitigating cyber threats in the express delivery sector. These findings suggest that organizations must move beyond isolated security measures and adopt a more interconnected cybersecurity governance model, where culture, leadership, and workforce training are as critical as technical infrastructure. While the study confirms several cybersecurity theories, it also identifies new perspectives on optimizing cybersecurity within operationally demanding industries. The next section presents the Conclusion, summarizing key contributions, policy recommendations, and avenues for future research.

6. Conclusion

This study comprehensively analyzes how cyber-attack features, response strategies, project team skills, and organizational culture collectively influence cybersecurity resilience and operational performance in express delivery service (EDS) companies. The findings emphasize that cybersecurity management must extend beyond traditional technical safeguards to incorporate human and organizational dimensions. Unlike previous research focusing on technical security controls or workforce competencies, this study integrates both perspectives, offering a CRF-EDS that aligns security strategies with team development and organizational culture.

The study confirms that cyber-attack vulnerabilities—such as software weaknesses, weak credentials, insider threats, and human error—necessitate structured and proactive response mechanisms. The effectiveness of cybersecurity interventions depends not solely on technological advancements but also on an organization's ability to cultivate a skilled and adaptive workforce. The results indicate that cybersecurity preparedness is both a technological and a workforce competency challenge, requiring continuous learning programs, crisis simulations, and cross-functional collaboration. By reinforcing these skills through targeted training and practical cybersecurity exercises, EDS companies can develop a proactive security posture that minimizes risks and maximizes operational efficiency.

Furthermore, the study highlights the critical role of organizational culture as a moderating factor in enhancing cybersecurity effectiveness. A security-conscious culture, characterized by strong leadership, transparent communication, and continuous learning, enhances compliance with cybersecurity protocols and fosters proactive threat mitigation behaviors. Organizations that establish a leadership-driven cybersecurity culture experience greater adherence to security policies, faster incident response times, and improved resilience. These findings align with previous studies that emphasize the importance of leadership engagement in cybersecurity risk management. However, unlike industries such as banking and healthcare—where cybersecurity is predominantly compliance-driven—express delivery firms must strike a balance between stringent security protocols and the need for operational agility.

From a practical standpoint, the findings provide several strategic recommendations for improving cybersecurity resilience in EDS companies. Investment in advanced cybersecurity technologies such as AI-driven threat detection, predictive analytics, and automated security response systems is crucial to preemptively identifying and neutralizing cyber threats. Additionally, adopting multi-layered security infrastructures, including cloud-based security solutions and blockchain authentication for secure transactions, can enhance the protection of digital supply chains and logistics operations. Workforce development initiatives must complement these technological advancements. Establishing cybersecurity training programs and cross-functional security teams can ensure that employees across IT, operations, and logistics divisions are equipped to recognize and mitigate cybersecurity risks. This study also underscores the importance of integrating cybersecurity awareness into an organization's leadership framework. Executive training programs should be implemented to educate managers on cyber risk assessment, compliance standards, and incident response best practices, reinforcing cybersecurity as a core strategic function rather than a standalone IT concern.

Beyond organizational efforts, policy-level interventions are necessary to strengthen cybersecurity governance within the express delivery sector. Regulatory agencies should develop cybersecurity compliance frameworks specific to EDS companies, mandating periodic security audits, adherence to ISO/IEC 27001 standards, and alignment with international cybersecurity protocols. Governments should also introduce incentives for companies that proactively invest in workforce cybersecurity training, enhancing industry-wide security resilience. Additionally, national workforce development strategies should incorporate cybersecurity education initiatives to ensure that future professionals in the logistics sector are well-prepared to navigate evolving digital threats.

While this study contributes a novel perspective on cybersecurity resilience in EDS companies, it also opens avenues for further research. Future studies could explore the emerging threats posed by AI-driven cyberattacks, ransomware, and deep-fake social engineering scams, particularly within logistics and e-commerce ecosystems. Comparative studies between express delivery companies operating in different regulatory environments could provide deeper insights into how national cybersecurity policies impact organizational resilience. Furthermore, research into blockchain-based security solutions for digital supply chain protection could offer innovative alternatives for enhancing cybersecurity in the express delivery sector.

In conclusion, this study establishes that cybersecurity in express delivery service companies is not merely a technical challenge but a multi-dimensional issue that demands an integrated approach combining technology, human expertise, and organizational culture. Companies that proactively address cyber-attack vulnerabilities, strengthen response strategies, invest in team skills, and cultivate a security-driven organizational culture will be better positioned to enhance their cybersecurity defenses, improve operational efficiency, and achieve long-term sustainability in the digital economy. By adopting the CRF-EDS introduced in this study, firms can establish a structured and adaptive cybersecurity governance model that aligns security initiatives with broader business objectives. Through strategic investments in technology, workforce development, and leadership-driven security policies, EDS companies can build a resilient cybersecurity foundation that enhances operational agility, customer trust, and competitive advantage in an increasingly interconnected global market.

List of abbreviations

AI	Artificial intelligence
APTs	Advanced persistent threats
AVE	Average variance extracted
CFA	Confirmatory factor analysis
CFI	Comparative fit index
CR	Composite reliability
CRF-EDS	Cybersecurity resilience framework for express delivery service companies
DDoS	Distributed denial-of-service
DoS	Denial-of-service
EDS	Express delivery service
EDSCs	Express delivery service companies
HR	Human resources
IoT	Internet of Things
IRB	Institutional review board
IT	Information technology
ML	Machine learning
RMSEA	Root mean square error of approximation
R^2	Coefficient of determination
SD	Standard deviation
SEM	Structural equation modeling
SRMR	Standardized root mean square residual
TLI	Tucker–Lewis index

TRC Telecommunications Regulatory Commission
χ^2 Chi-square

Compliance with ethical standards

Ethical considerations

This study was conducted in accordance with established ethical standards. All participants were provided with detailed information about the research objectives and procedures, and informed consent was obtained prior to their participation. Data were collected anonymously and treated with strict confidentiality to ensure privacy and protection of participants.

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Abbad M, Abbad R, and Saleh M (2011). Limitations of e-commerce in developing countries: Jordan case. Education Business and Society Contemporary Middle Eastern Issues, 4(4): 280–291. https://doi.org/10.1108/17537981111190060

Abulhaija S, Hattab S, and Qusef A (2022). Cyber security awareness, knowledge and behavior in the banking sector in Jordan. In the 13th International Conference on Information and Communication Systems, IEEE, Irbid, Jordan: 48-53. https://doi.org/10.1109/ICICS55353.2022.9811212

AlHadid I, Abu-Taieh EM, Rawajbeh MA, Alkhawaldeh RS, Khwaldeh S, Afaneh S, Alrowwad A, and Alrwashdeh DF (2023). Evaluating the influence of security considerations on information dissemination via social networks. International Journal of Data and Network Science, 7(4): 1471–1484. https://doi.org/10.5267/j.ijdns.2023.8.015

Al-Hawamleh A (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. International Journal of Computing and Digital Systems, 15(1): 1315–1331. https://doi.org/10.12785/ijcds/150193

Alhejaili MOM (2024). Securing the Kingdom's e-commerce frontier: Evaluation of Saudi Arabia's cybersecurity legal frameworks. Journal of Governance and Regulation, 13(2): 275–286. https://doi.org/10.22495/jgrv13i2siart4

Alnaeli SM, Sarnowski M, Aman S, Abdelgawad A, and Yelamarthi K (2017). Source code vulnerabilities in IoT software systems. Advances in Science, Technology and Engineering Systems Journal, 2(3): 1502–1507. https://doi.org/10.25046/aj0203188

Alqudhaibi A, Deshpande S, Jagtap S, and Salonitis K (2023). Towards a sustainable future: Developing a cybersecurity framework for manufacturing. Technological Sustainability, 2(4): 372-387. https://doi.org/10.1108/TECHS-05-2023-0022

Alsharif M, Mishra S, and Alshehri M (2022). Impact of human vulnerabilities on cybersecurity. Computer Systems Science and Engineering, 40(3): 1153–1166. https://doi.org/10.32604/csse.2022.019938

Álvarez-García D, Barreiro-Collazo A, Núñez JC, and Dobarro A (2016). Validity and reliability of the cyber-aggression questionnaire for adolescents (CYBA). The European Journal of Psychology Applied to Legal Context, 8(2): 69-77. https://doi.org/10.1016/j.ejpal.2016.02.003

Amorosa K and Yankson B (2023). Human error - A critical contributing factor to the rise in data breaches: A case study of higher education. Holistica, 14(1): 110–132. https://doi.org/10.2478/hjbpa-2023-0007

Ayandibu AO, Vezi-Magigaba MF, and Kaseeram I (2021). Innovation as an improvement tool for SMMEs. In: Ayandibu AO (Ed.), Reshaping entrepreneurship education with strategy and innovation: 78-107. IGI Global Scientific Publishing, Hershey, USA. https://doi.org/10.4018/978-1-7998-3171-6.ch005

Back S and Guerette RT (2021). Cyber place management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks. Journal of Contemporary Criminal Justice, 37(3): 427–451. https://doi.org/10.1177/10439862211001628

Benavides-Astudillo E, Fuertes W, Sanchez-Gordon S, Nuñez-Agurto D, and Rodríguez-Galán G (2023). A phishing-attack-detection model using natural language processing and deep learning. Applied Sciences, 13(9): 5275. https://doi.org/10.3390/app13095275

Berényi L and Soltész L (2022). Evaluation of product development success: A student perspective. Administrative Sciences, 12(2): 49. https://doi.org/10.3390/admsci12020049

Bordoloi S, Cooper WW, and Matsuo H (1999). Flexibility, adaptability, and efficiency in manufacturing systems. Production and Operations Management, 8(2): 133–150. https://doi.org/10.1111/j.1937-5956.1999.tb00366.x

Carlton M and Levy Y (2015). Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. In the SoutheastCon 2015, IEEE, Fort Lauderdale, USA: 1-6. https://doi.org/10.1109/SECON.2015.7132932

Chanani UL and Wibowo UB (2019). A learning culture and continuous learning for a learning organization. KnE Social Sciences, 3(17): 591–598. https://doi.org/10.18502/kss.v3i17.4686

Chatterjee D (2021). Cybersecurity readiness: A holistic and high-performance approach. SAGE Publications, Thousand Oaks, USA. https://doi.org/10.4135/9781071837313

Chen Q and Bridges RA (2017). Automated behavioral analysis of malware: A case study of Wannacry ransomware. In the 16th IEEE International Conference on Machine Learning and Applications, IEEE, Cancun, Mexico: 454-460. https://doi.org/10.1109/ICMLA.2017.0-119

Cheung K and Bell MG (2021). Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. European Journal of Operational Research, 291(2): 471–481. https://doi.org/10.1016/j.ejor.2019.10.019

Darko CD (2022). Weak credential information as a threat to online security. Advances in Multidisciplinary and Scientific Research Journal, 1(1): 35–40. https://doi.org/10.22624/AIMS/CRP-BK3-P6

Davis JS, Radhakrishnan A, and Zaveri J (2021). The impact of project team characteristics and client collaboration on project agility and project success: An empirical study. European Management Journal, 40(5): 758–777. https://doi.org/10.1016/j.emj.2021.09.011

Delone WH and McLean ER (2003). The DeLone and McLean model of information systems success: A ten-year update. Journal of Management Information Systems, 19(4): 9–30. https://doi.org/10.1080/07421222.2003.11045748

Deyannis D, Papadogiannaki E, Chrysos G, Georgopoulos KN, and Ioannidis S (2022). The diversification and enhancement of an IDS scheme for the cybersecurity needs of modern supply

chains. Electronics, 11(13): 1944. https://doi.org/10.3390/electronics11131944

Dhillon G, Smith K, and Hedström K (2019). Ensuring core competencies for cybersecurity specialists. In: Vasileiou I and Furnell S (Eds.), Cybersecurity education for awareness and compliance: 1-13. IGI Global, Hershey, USA. https://doi.org/10.4018/978-1-5225-7847-5.ch007 **PMCid:PMC6915323**

Dreibelbis RC, Martin J, Coovert MD, and Dorsey DW (2018). The looming cybersecurity crisis and what it means for the practice of industrial and organizational psychology. Industrial and Organizational Psychology, 11(2): 346–365. https://doi.org/10.1017/iop.2018.3

Farrell M (2017). Time management. Journal of Library Administration, 57(2): 215–222. https://doi.org/10.1080/01930826.2017.1281666

Fornell C and Larcker DF (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1): 39-50. https://doi.org/10.1177/002224378101800104

Furukawa C (2016). Dynamics of a critical problem-solving project team and creativity in a multiple-project environment. Team Performance Management, 22(1-2): 92–110. https://doi.org/10.1108/TPM-04-2015-0021

Gelenbe E and Nakip M (2023). Real-time cyberattack detection with offline and online learning. In the IEEE 29th International Symposium on Local and Metropolitan Area Networks (LANMAN), IEEE, London, UK: 1-6. https://doi.org/10.1109/LANMAN58293.2023.10189812

Georgiadou A, Michalitsi-Psarrou A, and Askounis D (2022). Evaluating the cyber-security culture of the EPES sector: Applying a cyber-security culture framework to assess the EPES sector's resilience and readiness. In the Proceedings of the 17th International Conference on Availability, Reliability and Security, ACM, Vienna, Austria: 1-10. https://doi.org/10.1145/3538969.3543813

Granova V, Mashatan A, and Turetken O (2023). Changing hearts and minds: The role of cybersecurity champion programs in cybersecurity culture. In: Schmorrow DD and Fidopiastis CM (Eds.), Augmented cognition. HCII 2023. Lecture Notes in Computer Science, 14019: 416-428. Springer Nature, Cham, Switzerland. https://doi.org/10.1007/978-3-031-35017-7_26

Hair JF, Risher JJ, Sarstedt M, and Ringle CM (2019). When to use and how to report the results of PLS-SEM. European Business Review, 31(1): 2-24. https://doi.org/10.1108/EBR-11-2018-0203

Hawkins N (2017). Why communication is vital during a cyber-attack. Network Security, 2017(3): 12-14. https://doi.org/10.1016/S1353-4858(17)30028-4

Huang K and Pearlson K (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. In the Proceedings of the 52nd Hawaii International Conference on System Sciences, AIS, Grand Wailea, Hawaii: 6398-6407. https://doi.org/10.24251/HICSS.2019.769

Hyslip TS and Burruss GW (2023). Ransomware. In: Hummer D and Byrne JM (Eds.), Handbook on crime and technology: 86-104. Edward Elgar Publishing, Cheltenham, UK. https://doi.org/10.4337/9781800886643.00013

Jadhav GG, Gaikwad SV, and Bapat D (2023). A systematic literature review: Digital marketing and its impact on SMEs. Journal of Indian Business Research, 15(1): 76-91. https://doi.org/10.1108/JIBR-05-2022-0129

Jegatheswaran RA and Juremi J (2022). Distributed denial of service: Detection method and response strategy. In the IEEE 2nd Mysore Sub Section International Conference, IEEE, Mysuru, India: 1-5. https://doi.org/10.1109/MysuruCon55714.2022.9972744

Jiang H, Choi T, and Ko RK (2020). Pandora: A cyber range environment for the safe testing and deployment of autonomous cyber attack tools. In: Thampi SM, Wang G, Rawat DB, Ko R, and Fan CI (Eds.), International symposium on security in computing and communication: 1-20. Springer, Singapore, Singapore. https://doi.org/10.1007/978-981-16-0422-5_1

Johnson AP and Aggarwal R (2019). Assessment of non-technical skills: Why aren't we there yet? BMJ Quality & Safety, 28: 606-608. https://doi.org/10.1136/bmjqs-2018-008712 **PMid:31129619**

Kareem HM, Aziz KA, Maelah R, Yunus YM, and Dauwed M (2019). Organizational performance in Iraqi SMEs: Validity and reliability questionnaire. Academy of Accounting and Financial Studies Journal, 23(6): 1-16.

Klingner JK and Boardman AG (2011). Addressing the "research gap" in special education through mixed methods. Learning Disability Quarterly, 34(3): 208–218. https://doi.org/10.1177/0731948711417559

Kosutic D and Pigni F (2020). Cybersecurity: Investing for competitive outcomes. Journal of Business Strategy, 43(1): 28–36. https://doi.org/10.1108/JBS-06-2020-0116

Krejcie RV and Morgan DW (1970). Determining sample size for research activities. Educational and Psychological Measurement, 30(3): 607–610. https://doi.org/10.1177/001316447003000308

Muszyńska K, Dermol K, Trunk V, Đakovic A, and Smrkolj G (2015). Communication management in project teams–practices and patterns. In the Joint International Conference, TIIM, Bari, Italy: 1359-1366.

Mwim EN and Mtsweni J (2022). Systematic review of factors that influence the cybersecurity culture. In: Clarke N and Furnell S (Eds.), IFIP advances in information and communication technology: 147–172. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-031-12172-2_12

Naseer A, Naseer H, Ahmad A, Maynard SB, and Siddiqui AM (2023). Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities. Computers and Security, 135: 103525. https://doi.org/10.1016/j.cose.2023.103525

Nkomo L and Kalisz D (2023). Establishing organisational resilience through developing a strategic framework for digital transformation. Digital Transformation and Society, 2(4): 403–426. https://doi.org/10.1108/DTS-11-2022-0059

Oriola O, Adeyemo AB, Papadaki M, and Kotzé E (2021). A collaborative approach for national cybersecurity incident management. Information and Computer Security, 29(3): 457–484. https://doi.org/10.1108/ICS-02-2020-0027

Pandey S, Singh RK, Gunasekaran A, and Kaushik A (2020). Cyber security risks in globalized supply chains: Conceptual framework. Journal of Global Operations and Strategic Sourcing, 13(1): 103–128. https://doi.org/10.1108/JGOSS-05-2019-0042

Pavlova E (2020). Enhancing the organisational culture related to cyber security during the university digital transformation. Information and Security an International Journal, 46(3): 239–249. https://doi.org/10.11610/isij.4617

Pharris L and Pérez-Mira B (2022). Preventing social engineering: A phenomenological inquiry. Information and Computer Security, 31(1): 1–31. https://doi.org/10.1108/ICS-09-2021-0137

Rejeb A, Rejeb K, Simske SJ, and Treiblmaier H (2021). Drones for supply chain management and logistics: A review and research agenda. International Journal of Logistics Research and Applications, 26(6): 708–731. https://doi.org/10.1080/13675567.2021.1981273

Riebe T, Kaufhold MA, and Reuter C (2021). The impact of organizational structure and technology use on collaborative practices in computer emergency response teams: An

empirical study. In the Proceedings of the ACM on human-computer interaction, 5(CSCW2): 478. https://doi.org/10.1145/3479865

Safitra MF, Lubis M, and Fakhrurroja H (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18): 13369. https://doi.org/10.3390/su151813369

Salehi Shahraki A and Nikmaram M (2013). Human errors in computer related abuses. Journal of Theoretical and Applied Information Technology, 47(1): 93-97.

Sarkar KR (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. Information Security Technical Report, 15(3): 112–133. https://doi.org/10.1016/j.istr.2010.11.002

Saunders J (2017). Tackling cybercrime – the UK response. Journal of Cyber Policy, 2(1): 4–15. https://doi.org/10.1080/23738871.2017.1293117

Sawyer BD and Hancock PA (2018). Hacking the human: The prevalence paradox in cybersecurity. Human Factors, 60(5): 597–609. https://doi.org/10.1177/0018720818780472 **PMid:29986155**

Seghezzi A, Mangiaracina R, Tumino A, and Perego A (2020). 'Pony express' crowdsourcing logistics for last-mile delivery in B2C e-commerce: An economic analysis. International Journal of Logistics: Research and Applications, 24(5): 456–472. https://doi.org/10.1080/13675567.2020.1766428

Setiawan I, Fauzi A, and Rohmansyah MS (2023). Epistemology as a scientific methodology foundation for the development of new theories in the field of Islamic education management. International Journal of Asian Business and Management, 2(2): 153–166. https://doi.org/10.55927/ijabm.v2i2.3707

Sharma R and Patel M (2018). Toxic comment classification using neural networks and machine learning. International Advanced Research Journal in Science, Engineering and Technology, 5(9): 47–52. https://doi.org/10.17148/IARJSET.2018.597

Sharmeen S, Ahmed YA, Huda S, Koçer BŞ, and Hassan MM (2020). Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. IEEE Access, 8: 24522–24534. https://doi.org/10.1109/ACCESS.2020.2970466

Sistla AP, Žefran M, Feng Y, and Ben Y (2014). Timely monitoring of partially observable stochastic systems. In the Proceedings of the 17th International Conference on Hybrid Systems: Computation and Control, ACM, Berlin Germany: 61-70. https://doi.org/10.1145/2562059.2562136

Skilton PF and Dooley KJ (2010). The effects of repeat collaboration on creative abrasion. Academy of Management Review, 35(1): 118–134. https://doi.org/10.5465/AMR.2010.45577886

Srinivasan K, Gupta T, Agarwal P, and Nema A (2018). A robust security framework for cloud-based logistics services. In the IEEE International Conference on Applied System Invention, IEEE, Chiba, Japan: 162-165. https://doi.org/10.1109/ICASI.2018.8394557 **PMid:31049321 PMCid:PMC6489043**

Steinke JA, Bolunmez B, Fletcher LS, Wang V, Tomassetti AJ, Repchick KM, Zaccaro SJ, Dalal RS, and Tetrick LE (2015). Improving cybersecurity incident response team effectiveness using teams-based research. IEEE Security and Privacy, 13(4): 20–29. https://doi.org/10.1109/MSP.2015.71

Tariq E, Akour I, Al-Shanableh N, Alquqa EK, Alzboun N, Al-Hawary SIS, and Alshurideh MT (2023). How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks. International Journal of Data and Network Science, 8(1): 69–76. https://doi.org/10.5267/j.ijdns.2023.10.016

Tormey R and Laperrouza M (2023). The development, validation and use of an interprofessional project management questionnaire in engineering education. European Journal of Engineering Education, 48(3): 502-517. https://doi.org/10.1080/03043797.2023.2171854

Tseng SM (2010). The correlation between organizational culture and knowledge conversion on corporate performance. Journal of Knowledge Management, 14(2): 269-284. https://doi.org/10.1108/13673271011032409

Uchendu B, Nurse JR C, Bada M, and Furnell S (2021). Developing a cyber security culture: Current practices and future needs. Computers and Security, 109: 102387. https://doi.org/10.1016/j.cose.2021.102387

Yi B, Sawant A, Chen S, Lee SW, and Zhang B (2022). Readiness for radiation treatment continuity: Survey on contingency plans against cyberattacks. Advances in Radiation Oncology, 7(5): 100990. https://doi.org/10.1016/j.adro.2022.100990 **PMid:36148373 PMCid:PMC9486412**

Yuen KF, Tan L, and Loh HS (2022). Core competencies for maritime business educators in the digital era. Frontiers in Psychology, 13: 915980. https://doi.org/10.3389/fpsyg.2022.915980 **PMid:35903743 PMCid:PMC9315266**

Zlomislić V, Fertalj K, and Sruk V (2017). Denial of service attacks, defences and research challenges. Cluster Computing, 20(1): 661–671. https://doi.org/10.1007/s10586-017-0730-x