Acta logistica - International Scientific Journal about Logistics
Volume: 12 2025 Issue: 3 Pages: 571-594 ISSN 1339-5629

**Enhancing cybersecurity readiness in express logistics: the role of cyber-attack features and project team skills**
Umi Kalsum Zolkafli, Ahmad AlArabiat

*https://doi.org/10.22306/al.v12i3.691* *Received: 09 Mar. 2025; Revised: 03 Aug. 2025; Accepted: 22 Aug. 2025*

# Enhancing cybersecurity readiness in express logistics: the role of cyber-attack features and project team skills

**Umi Kalsum Zolkafli**
University of Malaya, Department of Quantity Surveying, Faculty of Built Environment, Kuala Lumpur 50603, Malaysia, umi@um.edu.my (corresponding author)
**Ahmad AlArabiat**
University of Malaya, Faculty of Built Environment, Kuala Lumpur 50603, Malaysia, s2167521@siswa.um.edu.my

***Keywords*:** logistics cybersecurity, express delivery services, cybersecurity readiness, cyber-attack features, project team skills.
***Abstract:*** The increasing frequency and complexity of cyberattacks pose a significant threat to the express logistics sector, where digital coordination and data integrity are essential for operational continuity. This study examines how specific cyber-attack features influence team-based cybersecurity readiness, focusing on the mediating role of project team skills. The research addresses a practical problem faced by logistics firms in Jordan, many lacking standardized cybersecurity protocols despite rising digital adoption. Using a quantitative, cross-sectional design, data were collected from 310 employees in express delivery service companies. Structural equation modeling (SEM) via SmartPLS was employed to test the proposed relationships. The results demonstrate that cyber-attack features significantly affect cybersecurity readiness, both directly and through the partial mediation of project team skills. Teams with stronger technical and collaborative capabilities were more effective in translating threat exposure into organizational preparedness. The model accounted for 69% of the variance in cybersecurity readiness. This study contributes a novel integration of technical threat dimensions and human-centered readiness within logistics operations. It offers actionable insights for logistics managers aiming to strengthen cyber resilience through targeted skill development and team-based interventions.

## 1 Introduction

The logistics sector has undergone a major shift by adopting digital tools like real-time tracking, smart devices, cloud services, and connected communication platforms to boost efficiency and responsiveness [1-3]. Within this changing environment, express delivery services rely heavily on these digital systems to handle fast and time-sensitive deliveries across wide and often complex areas [4,5]. While these technologies improve speed and visibility, they also create more opportunities for cyberattacks, increasing the risk of digital threats [6,7].

As logistics systems become more connected—linking with external delivery partners, online retailers, and global networks—the risks related to cybersecurity also grow in scale and complexity [8-10]. Many logistics companies, particularly in less developed regions, struggle with old systems, inconsistent security measures, and limited spending on protective tools. These gaps make them easy targets for attacks like ransomware, phishing, service disruptions, and data theft [11,12]. Cybercriminals take advantage of the sector's need for fast responses and heavy reliance on digital connections, knowing that even brief service interruptions can cause widespread problems across supply chains [5,6].

Because of this, cybersecurity preparedness has become a key concern, especially for express delivery services that depend on real-time operations and consistent performance [1-4]. Being prepared goes beyond having the right technology; it also means ensuring teams are trained to recognize threats, respond effectively, and recover quickly [7,8]. Without proper readiness, companies risk financial losses, damage to their reputation, and legal consequences. Therefore, cybersecurity should be treated as an organizational priority, not just a technical task [9,11].

The express delivery sector in Jordan has seen rapid growth, fueled by rising online shopping, urban development, and national plans like Jordan Vision 2025, which support logistics improvements [13-15]. Mobile apps and smart delivery platforms have reshaped how services operate, particularly in cities such as Amman [14,16]. These systems played a vital role during the COVID-19 lockdowns by keeping deliveries running despite movement restrictions [14,17].

Today, delivery firms in Jordan depend on digital tools like GPS tracking, automated dispatching, and centralized data systems to handle operations and customer service [17-20]. However, many small and mid-sized companies face security challenges due to outdated technology, poor cybersecurity management, and a lack of readiness [18,20,21]. Often, they do not have dedicated security staff or formal response plans, leaving general IT workers to handle threats they may not be trained for [19,22]. These issues are made worse by inconsistent risk planning and minimal investment in staff training, especially for project teams that operate without clear cybersecurity guidelines [16,20].

Cyberattacks come with specific patterns and traits—such as their type, how often they happen, how complex they are, and whether they're new or evolving—that affect how a company can respond and recover [23,24]. Knowing these features helps classify threats and understand their potential impact on operations [23,27]. For example, phishing targets human mistakes, ransomware blocks access to data, and denial-of-service attacks make services unavailable [28-30]. When attacks are frequent, complicated, or unexpected, traditional security tools often fail—especially in industries that rely on fast, continuous operations [31-36].

Team-based cybersecurity readiness refers to how well a company's staff—across IT, security, and risk roles—can prepare for, handle, and bounce back from cyber threats [38,39]. This readiness includes access to tools and soft skills like staying aware, making decisions under pressure, and working together in real time [38,42]. Without strong teamwork and clear communication, even advanced technology can fall short during an incident [43-47]. Therefore, it's important to assess readiness through technical systems, team behavior, and organizational culture [40,38].

The skills of project teams—including technical expertise, flexibility, coordination, and problem-solving—play a major role in responding to cyber threats effectively [43,51]. In fast-moving delivery environments, these teams are often the first to deal with an incident [41,52]. Quick, skilled responses are crucial to controlling threats and getting services back on track [48,53]. Technically capable teams can spot weak points and apply the right fixes, while clear communication helps ensure that all efforts are aligned during a crisis [44,47,54]. Adaptability is also key, as it allows teams to adjust quickly in unpredictable situations—a critical strength in high-risk operations [55,56].

Even though interest in cybersecurity is growing, most research still focuses on technical solutions and legal rules, with little attention to the teams' skills [57]. Some studies have looked at individual training or practice exercises, but few explore how the real-world skills of project teams affect security outcomes [58,59]. Often, teams are seen only as parts of the organization, which hides their specific contributions [40,57]. This lack of focus is especially noticeable in the Middle East, where detailed research on cybersecurity in logistics is still limited [19,60]. While the growth of logistics in Jordan has been studied, there's little data on how delivery teams handle cyber threats [14,20,22]. Without this knowledge, it's hard to design effective and tailored strategies [17,22].

To close this gap in understanding, the present study looks at how the skills of project teams influence the relationship between the nature of cyberattacks and overall cybersecurity readiness in Jordan's express delivery sector [61,62]. It adds to academic knowledge by connecting the traits of cyber threats with the abilities of teams, offering a more people-focused view of logistics cybersecurity. The study specifically examines how often attacks occur, how complex or new they are, and how team skills shape the company's ability to respond.

The rest of this paper is organized as follows: Section 2 reviews the existing literature on cyber-attack characteristics, team skills, and cybersecurity preparedness. Section 3 outlines the research method, including how the survey was designed and the data were analyzed. Section 4 presents the study's findings. Section 5 discusses the broader theoretical and practical implications. Finally, Section 6 offers conclusions and suggests areas for future research.

## 2 Literature review

### *2.1 Cyber-attack features in logistics*

Cyberattacks on logistics operations, especially in express delivery service companies (EDSCs), have become more common as the industry becomes increasingly dependent on digital systems and connected technologies. These attacks often take advantage of technical flaws and human mistakes, leading to serious problems such as financial losses, service interruptions, and damage to a company's reputation [63-65]. A major entry point for these attacks is software and IT infrastructure weaknesses, including poor application design, insecure settings, and gaps in Internet of Things (IoT) devices often used in logistics platforms [63-65]. In express delivery companies, these weaknesses frequently affect critical systems like tracking tools, logistics applications, and online data storage platforms, making them prime targets for hacking and service breakdowns [63-65].

Although experts recommend strategies like regular system updates, safe programming methods, and secure software development cycles [69-71], studies show that many logistics companies—particularly small and medium-sized enterprises (SMEs)—struggle to apply these measures consistently [66-68]. SMEs usually lack the funding or expertise to establish strong cybersecurity systems. In contrast to larger organizations that implement complete cybersecurity plans and perform regular testing, SMEs often depend on general IT support and basic security tools, which leaves many gaps open for exploitation [66-68]. This reflects a significant divide between what the literature recommends and what is realistically implemented in day-to-day logistics operations.

Human mistakes are another major source of cybersecurity issues and remain a persistent problem across various sectors [72-74]. In logistics, errors such as incorrect data handling, falling for phishing scams, and misusing systems can compromise security and privacy [72-74]. The high-pressure work environment and frequent staff turnover in express delivery services make it even harder to maintain consistent cybersecurity practices [75-77]. While training and awareness programs are widely encouraged [78-80], research suggests that these efforts often fail to have a long-term impact unless they are supported by regular monitoring and a strong organizational focus on cybersecurity behavior [78-80].

Another common risk is poor authentication habits, like weak or repeated passwords. These practices can make it easier for attackers to gain unauthorized access to systems used for delivery tracking, customer interactions, and payment processing [81-83]. The problem becomes more serious in cloud-based platforms, where poor identity and access controls can expose larger parts of a company's digital infrastructure to attack [84-86]. Although tools like multi-factor authentication (MFA), password managers, and real-time access monitoring are strongly recommended [87-89], many logistics companies—especially those in developing regions like Jordan—struggle to apply these protections due to limited budgets or technical know-how [66-68].

Insider threats—whether intentional or accidental—also pose serious dangers within logistics companies [90-92]. Employees, contractors, or outside service providers with access to sensitive systems can either make errors that compromise security or intentionally misuse their access without being detected by typical security measures [90-92]. To counter these risks, companies need to use a combination of tools like activity monitoring, user behavior analysis, and strict access control policies [93-95]. Although research on detecting insider threats is growing, practical applications in the logistics sector are still rare and not well-documented [93-95].

The cybersecurity risks faced by Jordanian express delivery firms show why it's important to have comprehensive protection strategies that address technical systems, human factors, and access control weaknesses. Even though general guidelines are widely known [63-95], few studies examine how these recommendations are implemented in logistics environments. This lack of research is especially noticeable in the Middle East, where region-specific data is limited. As cyber threats continue to evolve, focused research—especially studies on how teams respond in real situations—is vital for creating effective cybersecurity strategies that improve protection and resilience in logistics [66-68,84-86].

### *2.2 Team-based cybersecurity readiness*

Team-based cybersecurity readiness refers to how well technical and operational teams can work together to prevent and respond to cyber threats quickly and efficiently [43,51]. In express delivery companies, where services depend on fast digital systems and timely operations, having this kind of team coordination is especially important. As cyberattacks become more complex, teams from different departments must maintain a unified and prepared approach to protect the organization [41,55].

This type of readiness involves six connected areas forming a strong defense system. The first is prevention capability, which reflects how effectively a team can identify and reduce threats before they cause harm. This includes hardening systems, ensuring secure configurations, applying updates, and running regular security checks [41,45]. In logistics, these efforts should focus on systems like fleet tracking, order processing, and customer service tools [52]. Teams that follow guidelines such as the NIST Cybersecurity Framework tend to be more resilient [43,51]. However, studies show that while many know these frameworks, small and mid-sized project teams often fail to apply them consistently [41,51].

The second aspect is threat detection readiness, which measures how well teams can monitor systems for unusual activity before a problem escalates. This includes using tools like intrusion detection systems (IDS), event monitoring platforms (SIEM), and analyzing system logs [44,47]. In fast-paced logistics settings, spotting issues early is essential to avoid major disruptions [48]. Regular training and practice scenarios improve this skill, but evidence shows that many logistics teams either don't fully use these tools or struggle with them due to limited skills or system complexity [44,47].

Incident response coordination is the third key area, focusing on how quickly and effectively a team can react during a cyber incident. This involves assigning roles, stopping threats, and analyzing what happened [39,50]. In express delivery services, where delays can affect large networks, well-prepared teams communicate clearly and follow detailed response plans [38,40]. Despite having such plans, many teams don't practice them regularly, which leads to slower and less effective responses when real incidents occur [39,50].

The fourth area, recovery and continuity readiness, relates to how well a team can restore systems and resume normal operations after an attack. This includes executing disaster recovery plans (DRPs), using business continuity procedures (BCPs), and checking data for accuracy [41]. In logistics, delays in restoring key systems can affect deliveries and customer services [39]. While many studies support using DRPs and BCPs, little research shows how well they work in real-world logistics situations, especially in regions like the Middle East [39,41].

Role alignment and task ownership, the fifth component, deals with clearly assigning responsibilities so that every team member knows their duties during a cyber incident. Studies show that when tasks match each person's skills, the team becomes more efficient and accountable [51,55]. Using role charts or skill maps helps with this, but such practices are not consistently applied in logistics project teams [38]. When roles are unclear, teams may duplicate efforts, skip steps, or make slow decisions during a crisis [51,55].

The final area, crisis communication effectiveness, focuses on how well a team shares important information during a cyberattack. Internally, this helps coordinate actions, while externally it helps maintain trust with customers and partners. Both are crucial in express delivery settings where timing is everything [40,45]. However, many logistics teams lack structured communication plans or pre-prepared messages, leading to confusion and mixed messaging when issues occur [38].

In summary, team-based cybersecurity readiness in the logistics sector depends on a combination of technical, organizational, and interpersonal skills. The six main

areas—prevention, detection, response, recovery, clear role assignments, and effective communication—build a team's ability to manage cyber threats. Still, there is a clear need for more real-world research on how these elements work together in logistics, especially in fast-moving environments like Jordan's express delivery industry [41,51]. Future studies should explore how project teams can better integrate these areas to build more practical and effective cybersecurity systems.

### *2.3 Project team skills*

Project teams rely on various skills, including technical ability, clear communication, adaptability, leadership, and effective problem-solving. These skills are especially important in fast-moving and complex environments such as logistics and cybersecurity, where teamwork across departments is essential [96,97]. In express delivery companies that depend heavily on digital tools and tight schedules, a team's capabilities directly affect how well cybersecurity measures are applied, improved, and sustained. When teams combine their skills effectively, they can solve problems quickly, work efficiently under pressure, and maintain high performance even in uncertain situations.

Technical knowledge is a key part of this skill set. Team members must understand topics like computer networks, software systems, data security, and managing cyber risks [98]. In logistics, this means ensuring that tools like routing systems, tracking platforms, and cloud-based databases are secure and work smoothly with operational needs [97]. However, since teams often include logistics professionals and IT experts, differences in technical understanding can make collaboration difficult. To address this, companies should support ongoing training, mentoring, and knowledge-sharing tools that help align everyone's expertise [96].

Strong communication and teamwork are also crucial. These abilities help build trust, promote transparency, and support coordination among team members, especially in logistics companies that operate across different locations and cultures [99,100]. To keep communication clear, teams benefit from using shared digital tools, clear communication protocols, and inclusive practices that support open dialogue [101, 102]. Good communication also ensures that logistics and cybersecurity knowledge are integrated effectively [102].

The ability to think critically and solve problems helps teams respond quickly when issues arise. Project-based learning environments have developed these abilities effectively, helping team members apply what they've learned to real situations [103]. These skills are essential in cybersecurity because threats can appear unexpectedly, requiring fast thinking and quick decisions [104,105]. Teams trained to assess situations under pressure are more capable of preventing problems from escalating.

Time management and sound decision-making are also important, especially in time-sensitive logistics projects. Tools like Gantt charts and time-blocking strategies help teams stay on track and balance cybersecurity tasks with business goals [106,107]. While including diverse viewpoints in decisions can improve judgment, avoiding delays or groupthink is important. In cybersecurity, timely and informed decisions can significantly affect how effectively threats are handled.

Adaptability is another vital skill. Techniques from agile project management—like working in short cycles and holding daily check-ins—help teams adjust their plans as new issues arise [108,109]. In logistics, where conditions often change quickly, adapting is essential. Simulations and training based on different scenarios can help prepare teams to face new cyber threats.

Creative thinking is also becoming more important in cybersecurity work. Finding new solutions—like customized firewalls or unique team-based response plans—depends on a workplace culture that supports experimentation and learning from mistakes [110,111]. Brainstorming sessions, hackathons, and innovation workshops allow teams to test and improve new ideas [112]. Still, such practices are not common in logistics, so companies need to focus more on encouraging innovation in their cybersecurity efforts.

Leadership plays a key role in bringing all these skills together. Effective leaders offer clear direction, boost team morale, and make sure everyone is accountable during stressful or complex situations [113-115]. Good leaders also set a strong example, promote ethical behavior, and encourage a focus on security across all levels of a project. However, many team leaders lack specific training in cybersecurity, which limits their ability to guide teams effectively during a crisis. Conflict resolution is important for keeping the team united and focused alongside leadership. Disputes are likely in high-pressure settings, and handling them constructively requires emotional intelligence, defined roles, and open communication [116,117].

Ongoing learning and professional development help maintain team readiness over time. Opportunities such as certifications, online courses, workshops, and peer learning keep skills current and responsive to new threats [118,119]. When organizations support learning through dedicated time, mentorship programs, and formal training systems, teams are better equipped to keep their skills from becoming outdated [120].

In conclusion, project team skills form the backbone of organizational strength in logistics cybersecurity. Combining technical know-how, leadership, adaptability, and effective teamwork enables teams to respond quickly and work together during cybersecurity incidents. However, many logistics companies fail to fully invest in these skills or support structured training, revealing a gap between what is known to be important and what is practiced in the field.

### *2.4 Theoretical framework*

To understand how cyber-attack characteristics influence team-based cybersecurity readiness—and how

team skills play a role in that relationship—this study uses a blend of theories from cybersecurity, supply chain operations, and organizational behavior. This mixed approach is well-suited to Jordan's express delivery sector, where the rapid shift to digital operations has improved efficiency and increased vulnerability to cyber risks [1,7,11].

The first theory used is Cyber Supply Chain Risk Management (C-SCRM), which focuses on the risks that travel across connected digital supply chains. In express delivery companies, problems can arise from third-party systems, cloud tools, or last-mile technologies like RFID tracking or route optimization software [4,9]. C-SCRM helps explain how these external risks can affect internal systems, making it clear that teams must work together across all parts of the logistics chain to prevent and respond to threats [6,8]. While this framework is gaining attention, it is not yet widely applied in small or medium-sized delivery firms, indicating a need for more localized cybersecurity models.

The second theory, Digital Transformation Theory, examines how businesses adopt modern technologies like cloud systems, data platforms, and blockchain to improve services [1,5]. These tools offer faster, more transparent operations and introduce new security risks. Managing this balance requires teams that are both skilled and flexible. In Jordan, many logistics companies have adopted digital platforms quickly, especially since the pandemic, but their internal security measures have not always kept pace. This gap between technical tools and team readiness highlights the need to strengthen both areas together [11,14,19].

Resilience Engineering Theory adds another perspective by focusing not on avoiding failures but on how organizations respond when problems occur. In logistics, even brief delays or outages can impact entire delivery systems and damage customer trust [6,50]. This theory emphasizes adaptability, showing how teams can maintain service during disruptions by staying flexible and alert. It is a valuable lens for studying how teams in logistics respond to real-time cyber threats, though it has not been widely applied to this field yet [7,41].

Socio-Technical Systems (STS) Theory further broadens the view by examining how people, technology, and company structures interact to affect cybersecurity. In express delivery firms, especially in Jordan, many mid-sized companies rely on informal teamwork and shared practices more than advanced security tools [2,5]. STS Theory shows that even well-designed systems can fail if team roles are unclear or communication breaks down. It supports the growing recognition that human behavior and team coordination are as important as technical tools in keeping systems safe [1,14,19].

Lastly, the Capability-Based View (CBV) looks at how a company's internal strengths—such as team skills, learning capacity, and ability to combine technical and human resources—determine its overall performance [4,12]. CBV helps explain why two firms with similar IT tools may show different readiness levels. The key difference lies in how well their teams apply knowledge, adapt to changes, and learn from experience [7,10]. However, CBV is still rarely used in logistics cybersecurity, even though it highlights the crucial role of project teams in building long-term resilience.

This study's framework combines five theories—C-SCRM, Digital Transformation, Resilience Engineering, STS, and CBV—to provide a well-rounded understanding of how cyber risks, team capabilities, and organizational systems interact. This combined approach offers a strong foundation for studying cybersecurity in Jordan's express delivery sector. Using this theoretical mix, the study develops testable ideas and builds a tailored model for understanding how teams can strengthen cybersecurity in fast-changing logistics environments [1,4,5].

### *2.5 Hypotheses development*

With cyberattacks becoming more frequent, advanced, and damaging, the need for strong cybersecurity preparation has grown, particularly in fast-changing industries like logistics and express delivery. Research increasingly highlights that certain features of cyberattacks—such as how complex they are, how accurately they target systems, and how often they happen—play a major role in shaping how organizations plan for and handle such threats [121,122]. Attacks that are both frequent and damaging often push companies to improve their internal security measures, raise awareness among staff, and build coordinated readiness strategies across departments [45,123].

Different aspects of cyberattacks, such as how they break into systems, the scale of disruption they cause, or the use of new methods, influence how organizations shape their defense strategies [124,125]. The logistics sector is especially at risk because cyberattacks can interrupt key functions like package tracking, route management, and real-time communication. Companies that gain a clear understanding of the nature of these attacks tend to respond more effectively. Their strategies often include team-based simulations, rehearsals based on specific roles, and organized processes for managing incidents [126,127].

These threats also bring about internal changes in how organizations operate, raising risk awareness and encouraging the development of team-based cybersecurity practices [123,128]. Studies across industries such as information technology and finance show that organizations regularly facing complex cyber threats are usually better prepared than those with less exposure [122,124]. Despite this, there's limited research on how these patterns apply to the express logistics industry, especially in developing countries. To address this gap, the first hypothesis is proposed:

**H1: Cyber-attack features positively affect Team-Based Cybersecurity Readiness.**

Additionally, cyber threats put considerable pressure on internal teams, particularly those working on projects with tight deadlines and high technological demands. These

attacks require teams to be quick-thinking, skilled in technology, and strong in collaboration. As attackers increasingly exploit weaknesses between people and systems, teams must become more adaptable, mentally resilient, and clear in communication to respond effectively [96,97].

Facing complex cyber threats often leads to better knowledge sharing, stronger links between departments, and clearer task assignments [98]. Well-functioning teams provide psychological safety, well-defined responsibilities, and shared accountability—all important for handling cybersecurity incidents [99-102]. In addition, the ability to think critically, stay flexible, and make decisions under pressure has become essential for effective cybersecurity teams [103-105]. These qualities are especially important in logistics, where short delays can result in immediate financial and reputational harm.

Because cyber risks are unpredictable, teams must continuously train, practice with realistic scenarios, and use flexible project management approaches to improve their skills [106-109]. While skill development has been widely discussed in academic work, little evidence is focused on logistics cybersecurity. Therefore, the second hypothesis is:

**H2: Cyber-attack features positively influence Project Team Skills.**

Although technical systems remain a key part of cybersecurity, recent studies suggest that the team's abilities—rather than just the technology—play the biggest role in maintaining readiness under pressure. Teams with specialized knowledge and the ability to understand how systems interact tend to perform better in fast-changing threat situations, especially when quick decisions are needed [96,97,130]. These teams can design secure systems, find and fix vulnerabilities, and respond in a coordinated way within strict time limits.

Soft skills also matter greatly. Communication, trust, and planning help teams share information quickly during a crisis and prevent delays in resolving issues [100,101]. How well teams coordinate within their group and with others affects how fast they detect, contain, and recover from attacks. Research also shows that solution-focused, time management, and adaptability contribute to better responses and less system downtime [103-105,131].

Adaptability is crucial in logistics, where operations move quickly and outside factors often change. Because of this, project teams in express delivery need a wide range of skills to handle digital threats effectively. Based on this:

**H3: Project Team Skills positively influence Team-Based Cybersecurity Readiness.**

Lastly, this study focuses on how team skills act as a bridge between external cyber threats and an organization's readiness. While threats come from outside, their impact depends on how internal teams react, adjust, and work together. Even advanced threats like shape-shifting malware or social engineering tactics can overcome strong technical defenses; however, the outcome often depends on human factors like teamwork, communication, and flexibility [4,9,11,29].

Teams that build these abilities respond better during crises and learn and grow from these experiences, turning threats into opportunities to strengthen their resilience [5,7,38,40]. In the logistics industry, research indicates that an organization's readiness often depends more on employee skills than on how much money is spent on technology [6,12,45,51]. This point is especially relevant in Jordan, where technical resources may not be evenly available, making the role of team dynamics even more important [13,14,19,20].

Therefore, the study presents project team skills as a key factor in turning external threats into internal preparedness. Understanding this connection explains differences in readiness and helps identify where improvements can be made at the intersection of people and technology.

**H4: Project Team Skills mediate the relationship between Cyber-Attack Features and Team-Based Cybersecurity Readiness.**

### *2.6 Conceptual framework*

This study presents a conceptual framework (Figure 1) that explores how cyber-attacks influence an organization's ability to prepare for and manage cybersecurity threats. It emphasizes the role of project team skills in shaping effective responses. This model is especially relevant for express delivery service companies (EDSCs) in Jordan, where the shift to digital systems has significantly boosted operational capabilities and increased vulnerability to cyber threats [14,15].

Their digital exposure grows as these companies adopt tools like IoT-enabled tracking, cloud-based logistics platforms, and online customer services. This wider digital presence puts their key systems and sensitive data at risk from more advanced attacks [7,11]. In this context, cyber-attacks stem from weaknesses affecting technology and how people interact with systems. These issues include poor software design, incorrect network settings, weak user access controls, and insider threats that have not been properly addressed—problems that are common causes of breaches across many industries [69,73,77]. In logistics and transport, older IT systems and disconnected digital setups worsen things by limiting visibility into threats and reducing the ability to respond quickly [6,71].

In addition to technical issues, risks are linked to human behavior—such as using the same passwords repeatedly, delaying software updates, or falling victim to phishing and social engineering. These weaknesses weaken an organization's security posture [75,89]. Because threats come from many directions, logistics companies need well-organized responses that do more than react to attacks. Cyber readiness must be fast and dependable in a field where continuous service is essential to remain competitive.

In this framework, team-based cybersecurity readiness means how well a group of employees, usually organized as a project team, can predict, identify, respond to, and recover from cyber incidents under pressure. Unlike older models that focused only on technology, today's understanding of readiness includes a range of elements—like preventive strategies, early warning systems, awareness of current threats, clear communication within teams, and planned recovery procedures [51,55]. These are especially important in the logistics sector, where attacks interrupt vital tasks such as tracking parcels, managing deliveries, and handling payments.

A key part of being ready is having clearly defined roles and the ability to coordinate under stress. Teams with a shared understanding of their responsibilities, take ownership of tasks, and communicate effectively are likelier to catch attacks early and limit their impact [53,102]. Specific challenges in logistics—such as hacked GPS data or stolen customer information—require teams to work quickly and in sync across departments to keep operations running smoothly and maintain customer trust.

At the heart of this framework is the role of project team skills. These include technical know-how—like using cybersecurity tools, managing systems, and analyzing threats—and soft skills, such as adaptability, communication across departments, and making good decisions under pressure [38,96]. In express delivery services, teams often work in different locations, with different systems and responsibilities. Therefore, they must bring together different types of information quickly and create a shared response plan, often while facing time constraints and unclear situations [100,101].

Studies show that teams with strong critical thinking, good time management, and awareness of the situation can turn scattered data into useful information, making their responses quicker and reducing disruptions [104,110]. In many logistics companies, how well a team is prepared—not how advanced their technology—often decides how quickly and effectively they can respond to attacks. This highlights the importance of building team capabilities and positions team skills as a key factor in shifting from reacting to threats to being ready for them ahead of time.

To conclude, the conceptual framework combines three main elements—cyber-attack characteristics, project team skills, and team-based cybersecurity readiness—into one model designed specifically for the logistics industry. It shows how technical weaknesses and human strengths interact and highlights how well-prepared teams help turn outside threats into opportunities for building stronger internal defenses.

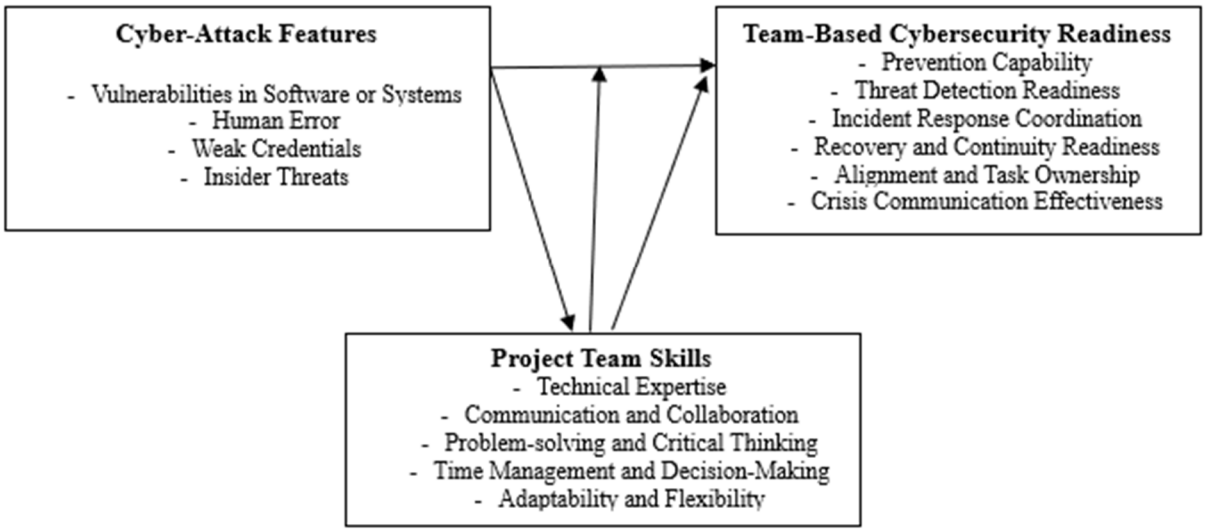


*Figure 1 Conceptual model*

## 3 Methodology

### *3.1 Research design*

This study adopted a quantitative, cross-sectional survey design to investigate how cyber-attack characteristics influence team-based cybersecurity readiness, with project team skills acting as a mediating variable, specifically within the context of Jordanian express delivery service companies [132]. A structured questionnaire was utilized as the primary data collection tool, offering a standardized format for capturing responses efficiently from a broad sample over a limited period [133-134]. The quantitative approach was chosen due to its suitability for testing theoretical models and quantifying abstract constructs using statistical methods [132]. The study's cross-sectional nature enabled data collection at a single point in time, aligning well with the operational realities of the logistics sector [134]. Similar methodologies have been effectively applied in prior research exploring cybersecurity and organizational behavior, where survey designs were instrumental in assessing team capabilities and readiness across organizational environments [135-136]. Moreover, the structured questionnaire allowed the researchers to measure perceptions and attitudes toward cyber threats and

preparedness using validated scales. This approach is widely recognized in empirical cybersecurity research, particularly in studies requiring insight into behavioral and organizational dynamics [133,135,136]. Therefore, using structural equation modeling techniques, the chosen design provided a solid framework for examining the hypothesized relationships and assessing the mediating role of team skills [134].

### *3.2 Population and sampling*

The study targeted IT and operations managers working within express delivery service companies (EDSCs) in Jordan. These professionals were selected based on their integral roles—IT managers are responsible for implementing and maintaining cybersecurity infrastructure, while operations managers oversee service continuity during potential disruptions. Their combined perspectives were essential for evaluating the study's primary constructs: cyber-attack features, project team skills, and cybersecurity readiness. To identify the target population, data were collected from two authoritative sources: the Jordanian Telecommunications Regulatory Commission (TRC), listing 166 express delivery firms, and the Ministry of Industry and Trade, listing 379. After reconciling the records and removing duplicate entries, 476 active companies were identified. Communication with the human resources departments confirmed that each company employed one IT and one operations manager, resulting in a total population of 952 eligible participants. A systematic sampling method was employed to ensure representativeness and minimize selection bias, following a probabilistic approach; every kth participant was selected from the list after a random starting point. An a priori power analysis was conducted using G*Power 3.1.9.7 software to calculate the required sample size. The analysis, based on multiple regression with three predictors—cyber-attack features, project team skills, and cybersecurity readiness—assumed a medium effect size ($f^2 = 0.15$), a significance level of 0.05, and a statistical power of 0.95. The minimum required sample size was determined to be 119 participants. To enhance the robustness of the findings and account for potential non-responses, the target sample size was increased to 310, representing approximately 32.6% of the population. The sampling interval was calculated as $k = N/n \approx 952/310 \approx 3$. Consequently, every third eligible participant was selected after the initial random start.

### *3.3 Instrument development*

A comprehensive questionnaire was developed to measure the constructs specified in the conceptual model (Figure 1) using established and validated instruments from previous research in cybersecurity, team performance, and organizational preparedness. Each construct was measured using four to five items on a 7-point Likert scale, ranging from 1 (strongly disagree) to 7 (strongly agree), a format known for enhancing reliability and response precision in behavioral studies [137].

Cyber-attack features were captured through four dimensions: (1) system or software vulnerabilities, (2) human error, (3) weak access credentials, and (4) insider threats. These indicators were adapted from prior studies focused on risk assessment and threat classification [69, 89, 91], with each item designed to reflect the perceived frequency, exposure, or severity of these risks. The mediating variable, Project Team Skills, comprised five key areas: (1) technical proficiency, (2) communication and collaboration, (3) critical thinking and problem-solving, (4) time and decision management, and (5) adaptability and flexibility. Items representing these skills were adapted from validated frameworks within the literature on team effectiveness and cybersecurity competencies [38,96,102]. Respondents rated the extent to which these skills were demonstrated within their teams. Team-Based Cybersecurity Readiness was assessed across six dimensions: (1) preventive capabilities, (2) threat detection readiness, (3) coordination in incident response, (4) recovery and continuity planning, (5) task ownership and alignment, and (6) effective communication during crises. These elements were informed by widely recognized readiness models and incident management literature [50,51,55].

To ensure instrument validity, a two-phase validation process was conducted. Initially, subject matter experts in cybersecurity and logistics reviewed the items for relevance and clarity. Subsequently, a pilot study involving 30 respondents from the target population was carried out to test internal consistency. Feedback from the pilot was used to make minor refinements, thereby improving the clarity and alignment of items with their respective constructs.

### *3.4 Data collection*

The data for this study were gathered through a structured, self-administered questionnaire aimed at collecting quantitative input from IT and operations managers employed in express delivery service companies across Jordan. The questionnaire was distributed online via Google Forms to facilitate broad and efficient participation, allowing respondents from geographically dispersed locations to access the survey easily [138]. A formal invitation package—including a participant information sheet and a consent form—was initially sent to the human resources departments of the 476 identified companies, who were then responsible for forwarding the survey link to the designated personnel. To improve participation and ensure high response quality, follow-up reminders were sent through email and telephone two weeks after the initial distribution. The survey remained open for a total duration of six weeks. Participation was entirely voluntary, and respondents were assured of the confidentiality of their input, thereby reducing the likelihood of social desirability bias and promoting more accurate responses [139]. Before the full rollout, the questionnaire underwent a pilot test involving 30 managers from the target population. This phase assessed the

questions' clarity, timing, and alignment with the study's objectives. Based on the feedback received, minor revisions were made to enhance the wording and flow of the items.

During the main data collection phase, 310 valid responses were received, yielding a response rate of 32.6% relative to the total population of 952 managers. This figure surpassed the minimum required sample size of 119, calculated through G*Power analysis, and ensured sufficient statistical power and generalizability. The collected data were exported from Google Forms into Microsoft Excel and then transferred to SPSS for data cleaning and initial preparation for analysis. The entire process adhered to ethical research standards, including obtaining informed consent, ensuring participant anonymity, and securing voluntary participation, by institutional research guidelines and international ethical practices [140].

### *3.5 Analysis technique*

The study utilized descriptive analysis, reliability and validity testing, and structural equation modeling (SEM) to examine the hypothesized relationships in the conceptual model. Initial data screening and descriptive statistics were performed using SPSS (v27), while structural modeling and hypothesis testing were conducted using SmartPLS 4.0. The partial least squares SEM (PLS-SEM) approach was selected for its suitability for predictive research involving latent variables and mediation analysis [134,141]. Preliminary data analysis involved evaluating the dataset for missing values, outliers, and deviations from normality to ensure its appropriateness for SEM [142]. Descriptive statistics were used to summarize the demographic characteristics and item-level responses, including means, standard deviations, and frequency distributions. Cronbach's alpha and composite reliability (CR) were calculated to assess measurement reliability, with thresholds of 0.70 or higher considered acceptable [143]. Convergent validity was verified through the average variance extracted (AVE), requiring a minimum value of 0.50. Discriminant validity was tested using the Fornell–Larcker criterion and the Heterotrait–Monotrait ratio (HTMT), following established guidelines [144,145]. Path coefficients and their statistical significance were estimated through bootstrapping with 5,000 resamples for testing the structural model. This enabled the evaluation of both the direct effects of cyber-attack features on team-based cybersecurity readiness and the indirect effects mediated by project team skills. The model's explanatory power was assessed using the coefficient of determination ($R^2$) and effect size ($f^2$) metrics [134]. Additionally, model fit was evaluated using the standardized root mean square residual (SRMR), with values below 0.08 indicating an acceptable level of fit [146].

## 4 Results

### *4.1 Demographic profile of respondents*

Table 1 presents the demographic breakdown across various categories, including gender, age, job role, years of professional experience, geographical region, and organization size. A significant majority of respondents were male (73.2%), which mirrors the existing gender distribution in this sector. The age distribution revealed that 44.5% of participants were between 30 and 39 years old, and 31.6% were between 40 and 49. This indicates that most respondents were mid-career professionals, likely with substantial experience managing technology and operations.

*Table 1 Demographic characteristics of respondents (N = 310)*

| Variable | Category | Frequency (n) | Percentage (%) |
|---|---|---|---|
| Gender | Male | 227 | 73.2 |
| | Female | 83 | 26.8 |
| Age | 20–29 | 42 | 13.5 |
| | 30–39 | 138 | 44.5 |
| | 40–49 | 98 | 31.6 |
| | 50+ | 32 | 10.3 |
| Job Position | IT Manager | 153 | 49.4 |
| | Operations Manager | 157 | 50.6 |
| Years of Experience | 1–5 | 64 | 20.6 |
| | 6–10 | 122 | 39.4 |
| | 11–15 | 89 | 28.7 |
| | 16+ | 35 | 11.3 |
| Region | Northern Jordan | 106 | 34.2 |
| | Central Jordan | 130 | 41.9 |
| | Southern Jordan | 74 | 23.9 |
| Company Size | Small (10–50 employees) | 84 | 27.1 |
| | Medium (51–200) | 179 | 57.7 |
| | Large (201+) | 47 | 15.2 |

The sample was almost evenly split in professional roles: 49.4% of the respondents identified as IT managers, while 50.6% held operations management positions. This balanced representation supports a comprehensive understanding of technical and operational perspectives on cybersecurity readiness. Regarding work experience, 39.4% of participants had been in the field for 6 to 10 years, highlighting a workforce with a solid foundation in industry practices and cybersecurity concerns. An additional 28.7% had between 11 and 15 years of experience, further reinforcing the sample's depth of expertise. In terms of geographical location, respondents were distributed throughout Jordan, with the largest proportion based in the central region (41.9%), followed by those in the north (34.2%) and south (23.9%). This geographical diversity ensures a well-rounded view of practices and challenges across different parts of the country. Company size was also considered. Over half of the participants (57.7%) worked in medium-sized firms employing between 51 and 200 individuals. Smaller companies (10–50 employees) accounted for 27.1% of the sample, while large enterprises (with more than 200 employees) comprised 15.2%. These figures suggest that medium-sized organizations are a prominent segment of Jordan's express delivery sector and will likely play a key role in shaping national cybersecurity readiness.

### *4.2 Descriptive statistics of latent constructs*

The first construct, Cyber-Attack Features, includes four key sub-dimensions: vulnerabilities in software or systems, human error, weak credentials, and insider threats. These represent critical sources of cyber risk within the operational environment of express delivery services. The mean scores for these sub-constructs ranged from 5.15 to 5.31. Specifically, human error received the highest average score (5.31), highlighting it as the most commonly perceived threat. Meanwhile, weak credentials had the lowest mean (5.15), though still above the scale midpoint, indicating a general awareness of credential-related vulnerabilities. The standard deviations, all under 1.00, suggest that perceptions across respondents were relatively consistent, reflecting a shared recognition of cyber risks within the industry. The mediating variable, Project Team Skills, was assessed through five sub-constructs: technical expertise; communication and collaboration; problem-solving and critical thinking; time management and decision-making; and adaptability and flexibility. These skills are essential for ensuring rapid and coordinated responses to cyber threats within team-based structures. The reported mean values ranged from 5.54 to 5.68, indicating a high level of agreement among participants about their teams' capabilities. Notably, adaptability and flexibility received the highest rating (5.68), underscoring the importance placed on agility and responsiveness in dynamic cybersecurity environments. The relatively low standard deviations (below 0.85) across all sub-constructs indicate minimal variance in respondent perceptions, suggesting a widely shared view of team competence and preparedness. The final construct, Team-Based Cybersecurity Readiness, was evaluated using six sub-constructs: prevention capacity, threat detection readiness, incident response coordination, recovery and continuity readiness, alignment and task ownership, and crisis communication effectiveness. These dimensions collectively represent the organization's ability to prevent, identify, respond to, and recover from cyber incidents. The mean scores for these indicators ranged from 5.37 to 5.48. Among them, alignment and task ownership had the highest average (5.48), suggesting strong clarity in roles and responsibilities during cyber incidents. Conversely, recovery and continuity readiness scored lowest (5.37), indicating a slightly more varied level of preparedness in this area. Standard deviations ranged from 0.83 to 0.91, showing that while most organizations demonstrated a generally high level of readiness, some variation exists, possibly reflecting differences in resource allocation, training, or incident experience across companies.

These descriptive results highlight that Jordan's participating express delivery firms generally possess well-developed capabilities in managing cyber threats. High mean values across all constructs suggest strong organizational awareness and team-based preparedness. Table 2 summarizes the average scores and standard deviations for all constructs and their respective sub-dimensions.

*Table 2 Descriptive statistics of constructs and sub-constructs (N = 310)*

| Main Construct | Sub-Construct | Mean | SD |
|---|---|---|---|
| **Cyber-Attack Features** | Vulnerabilities in Software/Systems | 5.24 | 0.91 |
| | Human Error | 5.31 | 0.88 |
| | Weak Credentials | 5.15 | 0.90 |
| | Insider Threats | 5.28 | 0.85 |
| **Project Team Skills** | Technical Expertise | 5.58 | 0.83 |
| | Communication and Collaboration | 5.63 | 0.79 |
| | Problem-Solving and Critical Thinking | 5.61 | 0.82 |
| | Time Management and Decision-Making | 5.54 | 0.78 |
| | Adaptability and Flexibility | 5.68 | 0.80 |
| **Cybersecurity Readiness** | Prevention Capacity | 5.45 | 0.84 |
| | Threat Detection Readiness | 5.39 | 0.87 |

| | | | |
|---|---|---|---|
| | Incident Response Coordination | 5.42 | 0.91 |
| | Recovery and Continuity Readiness | 5.37 | 0.88 |
| | Alignment and Task Ownership | 5.48 | 0.85 |
| | Crisis Communication Effectiveness | 5.41 | 0.83 |

### *4.3 Measurement model evaluation*

Before testing the hypothesized relationships among cyber-attack features, project team skills, and team-based cybersecurity readiness, the measurement model was evaluated to ensure that the latent constructs were measured reliably and validly. This step was critical to confirm that the questionnaire items accurately represented their respective theoretical constructs and could be used confidently in the subsequent structural model analysis. The measurement model was assessed using Partial Least Squares Structural Equation Modeling (PLS-SEM) via SmartPLS 4.0. Four key assessments were performed: internal consistency reliability, convergent validity, discriminant validity, and indicator reliability. The following subsections outline the results of these evaluations, which confirm the measurement model's robustness and suitability for further analysis.

#### 4.3.1 Internal consistency reliability

Internal consistency reliability examines the degree to which multiple items measuring the same construct produce consistent results. Two metrics were used in this study: Cronbach's alpha and composite reliability (CR). While Cronbach's alpha offers a conservative estimate of reliability, composite reliability is considered more appropriate in PLS-SEM as it accounts for the different factor loadings of each indicator [134]. According to the standard criteria suggested by [143], values above 0.70 are deemed acceptable. As reported in Table 3, all constructs exceeded the minimum threshold. Cronbach's alpha values ranged from 0.89 to 0.92, and CR values ranged from 0.91 to 0.94. These results confirm a high level of internal consistency, indicating that the measurement items reliably represent their associated latent constructs.

*Table 3 Internal consistency reliability: Cronbach's alpha and composite reliability (N = 310)*

| Construct | Cronbach's Alpha | Composite Reliability |
|---|---|---|
| Cyber-Attack Features | 0.89 | 0.91 |
| Project Team Skills | 0.92 | 0.94 |
| Team-Based Cybersecurity Readiness | 0.90 | 0.93 |

All values surpass the recommended cutoff, indicating excellent reliability. This suggests that respondents interpreted the items within each construct consistently, reinforcing the validity of the results.

#### 4.3.2 Convergent validity

Convergent validity assesses whether indicators of a given construct share a high proportion of variance, implying they converge on the same underlying concept. This was evaluated using two criteria: the Average Variance Extracted (AVE) and standardized factor loadings. AVE values above 0.50 signify that the construct explains more than half of the variance in its observed indicators [144]. Similarly, factor loadings should exceed 0.70 to be considered statistically meaningful. As summarized in Table 4, all AVE values ranged from 0.64 to 0.76, well above the 0.50 benchmark. Additionally, the standardized loadings for individual items fell between 0.72 and 0.89. These findings confirm that the indicators are strongly associated with their corresponding latent variables, supporting convergent validity.

*Table 4 Convergent validity: standardized loadings and Average Variance Extracted (AVE)*

| Construct | Range of Loadings | AVE |
|---|---|---|
| Cyber-Attack Features | 0.73 – 0.84 | 0.64 |
| Project Team Skills | 0.75 – 0.89 | 0.71 |
| Team-Based Cybersecurity Readiness | 0.72 – 0.88 | 0.76 |

All AVE values exceed the minimum acceptable level, and individual item loadings are robust. This indicates that each construct successfully captures the variance of its indicators, justifying their inclusion in the structural analysis.

#### 4.3.3 Discriminant validity

Discriminant validity evaluates the extent to which a construct is truly distinct from other constructs in the model. This was assessed using two complementary methods: the Fornell–Larcker criterion and the Heterotrait–Monotrait (HTMT) ratio. According to the Fornell–Larcker criterion, the square root of each construct's AVE should be greater than its correlations with any other construct [144]. As presented in Table 5, each construct's diagonal value (√AVE) exceeds the corresponding off-diagonal correlation values, confirming that the constructs are empirically distinct.

*Table 5 Fornell–Larcker criterion matrix*

| Construct | CAF | PTS | TCR |
|---|---|---|---|
| Cyber-Attack Features (CAF) | 0.80 | | |
| Project Team Skills (PTS) | 0.66 | 0.84 | |
| Team-Based Cybersecurity Readiness (TCR) | 0.61 | 0.72 | 0.87 |

*Note: Diagonal values represent the square root of AVE.*

In addition, the HTMT ratio, which provides a more stringent test of discriminant validity, was used. A value below 0.85 suggests adequate discriminant validity [145].

As shown in Table 6, all HTMT values fall within the acceptable range, further supporting the distinctiveness of each construct.

*Table 6 Heterotrait–Monotrait ratio (HTMT)*

| Construct Pair | HTMT Value |
|---|---|
| Cyber-Attack Features – Project Team Skills | 0.76 |
| Cyber-Attack Features – Cybersecurity Readiness | 0.73 |
| Project Team Skills – Cybersecurity Readiness | 0.81 |

The Fornell–Larcker and HTMT assessments confirm that each construct measures a unique theoretical concept, with no significant overlap in meaning. This validation step ensures that the constructs can be independently interpreted in the context of the structural model.

The findings from the measurement model evaluation demonstrate that all constructs used in this study are reliable and valid. Internal consistency is strong, convergent validity is well established, and discriminant validity is supported. In the next section, these results provide a solid foundation for analyzing the structural relationships among cyber-attack features, project team skills, and team-based cybersecurity readiness.

### *4.4 Structural model evaluation - inner model*

Following the confirmation of the measurement model, the structural (inner) model was evaluated to test the proposed theoretical relationships among Cyber-Attack Features (CAF), Project Team Skills (PTS), and Team-Based Cybersecurity Readiness (TCR). The analysis was conducted using SmartPLS 4, applying the Partial Least Squares Structural Equation Modeling (PLS-SEM) approach. The structural evaluation included five key components: assessment of collinearity, estimation of path coefficients and hypothesis testing, evaluation of explained variance ($R^2$), computation of effect sizes ($f^2$), and examination of model fit indicators.

#### 4.4.1 Collinearity assessment

Collinearity diagnostics were performed using the Variance Inflation Factor (VIF) to ensure the reliability of path coefficient estimates. Collinearity occurs when predictor variables are highly correlated, which may distort the model's estimation and reduce interpretability. According to [134], VIF values below 5 are generally acceptable and indicate no critical multicollinearity concerns. As shown in Table 7, all VIF values ranged from 1.38 to 2.03, well within the acceptable range. This confirms that multicollinearity is absent and that the predictor constructs contribute independently to the outcomes.

Low VIF values indicate that each predictor variable has a distinct and independent contribution to the model, ensuring that multicollinearity does not affect the validity of the structural estimates.

*Table 7 Collinearity statistics (VIF)*

| Predictor Construct | Outcome Variable | VIF |
|---|---|---|
| Cyber-Attack Features | Project Team Skills | 1.88 |
| Cyber-Attack Features | Cybersecurity Readiness | 1.79 |
| Project Team Skills | Cybersecurity Readiness | 2.03 |

#### 4.4.2 Path coefficients and hypothesis testing

Path coefficients were estimated using a bootstrapping procedure with 5,000 resamples to evaluate the strength and significance of hypothesized relationships. The results revealed that all proposed paths were statistically significant (Table 8). Cyber-Attack Features positively affected Project Team Skills ($\beta = 0.66$, $t = 11.72$, $p < .001$), suggesting that organizations facing more complex or frequent cyber threats tend to cultivate stronger team competencies. Additionally, Cyber-Attack Features directly influenced Cybersecurity Readiness ($\beta = 0.33$, $t = 6.54$, $p < .001$), indicating that awareness and mitigation of cyber threats enhance organizational preparedness. Project Team Skills also showed a substantial positive effect on Cybersecurity Readiness ($\beta = 0.54$, $t = 10.81$, $p < .001$), highlighting the critical role of team capabilities in enhancing readiness.

*Table 8 Path coefficients, t-values, and significance (bootstrapping results)*

| Path | Coefficient (β) | t-value | p-value |
|---|---|---|---|
| Cyber-Attack Features → Project Team Skills | 0.66 | 11.72 | < .001 |
| Cyber-Attack Features → Cybersecurity Readiness | 0.33 | 6.54 | < .001 |
| Project Team Skills → Cybersecurity Readiness | 0.54 | 10.81 | < .001 |

All path coefficients are statistically significant at the $p < .001$ level, supporting the hypothesized relationships strongly. This confirms that both direct and indirect effects of Cyber-Attack Features on Cybersecurity Readiness are substantial.

#### 4.4.3 Coefficient of determination ($R^2$)

$R^2$ values assess how much variance in the endogenous (dependent) variables is explained by the exogenous (independent) variables. According to common benchmarks, $R^2$ values around 0.25, 0.50, and 0.75 can be considered weak, moderate, and substantial, respectively [134]. As shown in Table 9, Project Team Skills had an $R^2$ of 0.44, indicating that Cyber-Attack Features explain a moderate portion of the variance in team skills. Meanwhile,

the $R^2$ value for Cybersecurity Readiness was 0.62, suggesting a strong level of explanation when both predictors (CAF and PTS) are included.

*Table 9 $R^2$ and adjusted $R^2$ for project team skills and cybersecurity readiness*

| Construct | $R^2$ | Adjusted $R^2$ |
|---|---|---|
| Project Team Skills | 0.44 | 0.44 |
| Cybersecurity Readiness | 0.62 | 0.62 |

The model demonstrates substantial explanatory power, particularly for Cybersecurity Readiness. These values affirm the relevance of Cyber-Attack Features and Project Team Skills in shaping organizational cybersecurity outcomes.

#### 4.4.4 Effect size ($f^2$)

Effect size ($f^2$) measures the contribution of a specific predictor to the $R^2$ value of an endogenous variable. According to Cohen (1988), values of 0.02, 0.15, and 0.35 indicate small, medium, and large effects, respectively. As presented in Table 10, Cyber-Attack Features greatly affected Project Team Skills ($f^2 = 0.79$) and had a medium effect on Cybersecurity Readiness ($f^2 = 0.23$). Project Team Skills greatly affected Cybersecurity Readiness ($f^2 = 0.49$), reinforcing its central role in the model.

*Table 10 Effect size ($f^2$) for predictor constructs*

| Predictor → Outcome | $f^2$ | Effect Size Interpretation |
|---|---|---|
| Cyber-Attack Features → Project Team Skills | 0.79 | Large |
| Cyber-Attack Features → Cybersecurity Readiness | 0.23 | Medium |
| Project Team Skills → Cybersecurity Readiness | 0.49 | Large |

These values indicate that Cyber-Attack Features are a key driver of skill development, and that Project Team Skills are a major determinant of cybersecurity readiness. The practical significance of each predictor is demonstrated.

#### 4.4.5 Model fit indices

To evaluate the overall adequacy of the model, two fit indices were analyzed: the Standardized Root Mean Square Residual (SRMR) and the Normed Fit Index (NFI). An SRMR value below 0.08 indicates a good fit, while an NFI value above 0.90 reflects a strong comparative model fit [145]. As shown in Table 11, the SRMR value was 0.058 and the NFI was 0.93, both meeting the recommended thresholds.

*Table 11 Model fit indices*

| Fit Index | Value | Threshold | Interpretation |
|---|---|---|---|
| SRMR | 0.058 | < 0.08 | Excellent Fit |
| NFI | 0.93 | > 0.90 | Strong Model Fit |

The fit indices confirm that the theoretical model closely aligns with the observed data, supporting the structural relationships proposed in the study.

The results of the structural model evaluation confirm that the research framework is both statistically sound and theoretically meaningful. Cyber-Attack Features significantly influence Team-Based Cybersecurity Readiness both directly and indirectly through the development of Project Team Skills. The model demonstrates strong explanatory power, reliable path estimates, and robust fit indices, validating its application in the context of Jordanian express delivery service companies.

### *4.5 Mediation analysis*

To assess whether Project Team Skills (PTS) mediate the relationship between Cyber-Attack Features (CAF) and Team-Based Cybersecurity Readiness (TCR), a bootstrapping analysis was conducted using SmartPLS with 5,000 resamples. Bootstrapping provides a robust, non-parametric method for testing indirect effects and estimating confidence intervals without assuming normality (Hair et al., 2021). As shown in Table 12, the direct path from CAF to TCR was statistically significant, with a standardized path coefficient of $\beta = 0.33$ ($t = 6.54$, $p < .001$) and a 95% confidence interval [0.22, 0.45]. This confirms that cyber-attack features, such as attack complexity, insider threats, or frequency, directly and positively influence the readiness of express delivery companies to respond to cybersecurity threats. Furthermore, the indirect effect of CAF on TCR through PTS was also significant, with a path coefficient of $\beta = 0.36$ ($t = 8.49$, $p < .001$) and a confidence interval of [0.28, 0.45]. This suggests that cyber-attack features influence team-based cybersecurity readiness directly and indirectly by enhancing project teams' skill sets. These skills—such as adaptability, technical expertise, and collaboration—appear to serve as key mechanisms through which organizations strengthen their cybersecurity posture. The total effect of CAF on TCR, combining both direct and mediated paths, was $\beta = 0.69$ ($t = 14.32$, $p < .001$), with a confidence interval of [0.60, 0.78]. The magnitude of this total effect demonstrates a strong and consistent link between cyber-attack characteristics and organizational readiness.

Since both the direct and indirect effects are significant, the analysis confirms a case of partial mediation. While cyber-attack features directly influence readiness, a significant portion of their impact is channeled through developing project team capabilities. These findings highlight the importance of recognizing cybersecurity threats and developing team-based competencies to manage them effectively. They align with recent research emphasizing the need for an integrated approach combining technical awareness and human capital in enhancing organizational cybersecurity [38,43].

*Table 12 Indirect effects and confidence intervals (bootstrapping for mediation)*

| Effect Type | Path | β | t-value | p-value | 95% CI | Mediation Type |
|---|---|---|---|---|---|---|
| Direct Effect (CAF → TCR) | CAF → TCR | 0.33 | 6.54 | < .001 | [0.22, 0.45] | - |
| Indirect Effect (CAF → PTS → TCR) | CAF → PTS → TCR | 0.36 | 8.49 | < .001 | [0.28, 0.45] | Partial Mediation |
| Total Effect (CAF → TCR via PTS) | CAF → TCR + Indirect | 0.69 | 14.32 | < .001 | [0.60, 0.78] | - |

These results demonstrate that Project Team Skills significantly mediate the relationship between cyber-attack features and cybersecurity readiness. The strong indirect effect affirms that enhancing team skills is a strategic response mechanism that strengthens readiness across the organization. These findings carry practical implications for decision-makers in the logistics and express delivery sectors, suggesting that building team capacity is just as vital as technological threat awareness in fostering digital resilience.

### *4.6 Summary of hypothesis testing*

This section summarizes the results of the hypothesis testing conducted through structural equation modeling using SmartPLS. The study evaluated three direct hypotheses and one mediating hypothesis, all of which were derived from the conceptual model guiding the research. As presented in Table 13, the results strongly support each proposed relationship. Hypothesis H1 proposed that Cyber-Attack Features (CAF) positively influence Cybersecurity Readiness (TCR). This was confirmed by a statistically significant path coefficient ($\beta = 0.33$, $t = 6.54$, $p < .001$), indicating that recognizing and addressing cyber threats contributes directly to enhancing organizational preparedness. Hypothesis H2 suggested that CAF also directly affects Project Team Skills (PTS). The findings supported this relationship ($\beta = 0.44$, $t = 7.22$, $p < .001$), suggesting that increased exposure to cyber risks drives the development of team capabilities, such as technical problem-solving and adaptability, within project environments. Hypothesis H3 examined the direct impact of PTS on TCR. With a path coefficient of $\beta = 0.47$ ($t = 8.01$, $p < .001$), the results confirmed a significant positive relationship. This reinforces the role of skilled, coordinated teams in enabling organizations to respond effectively to cybersecurity incidents. The mediating hypothesis, H4, investigated whether PTS mediates the link between CAF and TCR. As detailed in Section 4.5, both the direct and indirect paths were significant, confirming the presence of partial mediation. The indirect effect ($\beta = 0.36$, $t = 8.49$, $p < .001$) demonstrates that project team capabilities substantially enhance the influence of cyber-attack features on readiness, thereby amplifying the organization's response capacity.

These findings validate the study's theoretical framework and underscore the integrated nature of technical threat factors and internal human competencies. They also offer practical implications for cybersecurity management in express delivery service organizations, highlighting the need for threat recognition and project team development investment to ensure robust cybersecurity readiness.

*Table 13 Summary of hypotheses, paths, and results*

| Hypothesis | Structural Path | Standardized Coefficient (β) | t-value | p-value | Supported |
|---|---|---|---|---|---|
| H1 | Cyber-Attack Features → Cybersecurity Readiness | 0.33 | 6.54 | < .001 | Yes |
| H2 | Cyber-Attack Features → Project Team Skills | 0.44 | 7.22 | < .001 | Yes |
| H3 | Project Team Skills → Cybersecurity Readiness | 0.47 | 8.01 | < .001 | Yes |
| H4 | Cyber-Attack Features → Project Team Skills → Cybersecurity Readiness (Mediating) | 0.36 (Indirect) | 8.49 | < .001 | Yes (Partial Mediation) |

## 5 Discussion

This study's findings clearly show that certain cyber-attack features—especially their complexity, frequency, and advanced nature—significantly affect how well organizations prepare for and manage cybersecurity risks [23,29]. These results are consistent with patterns seen in the logistics and transport industries, where the growing number of complex cyber threats has led companies to strengthen their detection systems and improve their ability to respond. Notable examples, such as the NotPetya attack that heavily impacted operations at Maersk and TNT Express, highlight how repeated cyber incidents can prompt major changes in cybersecurity strategies and infrastructure [147].

In line with earlier research, this study confirms that frequent exposure to advanced cyber threats drives technical upgrades and supports team skills growth. For instance, [38] highlighted that team communication and coordination are essential to managing cybersecurity challenges. The present findings build on this by showing that teams regularly facing complex threats tend to develop stronger response capabilities, increased trust among team members, and improved learning habits [40]. These insights are further supported by studies using simulated environments, where high-pressure situations have been shown to enhance awareness and performance in responding to incidents, as illustrated by Fausett and Keebler (2023).

The strong link between project team skills and cybersecurity readiness points to the crucial role of human expertise in reducing cyber risk. When teams possess the right skills, they can react more effectively to attacks, help maintain organizational stability, and rely on shared mental models that support fast, well-informed decisions [43,51,55]. This evidence reinforces the view that effective cybersecurity plans should not rely solely on technology but should also include investment in workforce development [50,53].

The mediation analysis further revealed that team skills partly explain the connection between cyber-attack features and readiness [134]. This supports the idea from trait-activation theory that external challenges can trigger hidden capabilities within individuals and groups, improving overall organizational performance [43,51]. At the same time, the presence of a direct impact from cyber threats on readiness suggests that external attacks and internal team strengths contribute to building resilience. This dual effect indicates that threat exposure and internal capabilities shape how prepared an organization is [55,144].

These results have clear practical implications for logistics and express delivery firms. Organizations should adopt cybersecurity strategies that balance technology upgrades with continuous team development. Regular cyber drills, encouraging collaboration across departments, and flexible planning should be part of everyday operations to improve adaptability and coordination [38,51]. Embedding these practices into standard procedures can help create a proactive culture about cybersecurity and be ready to handle new and evolving threats [43].

Theoretically, this research also adds to the broader understanding of cybersecurity in organizations. It expands current models by showing how the nature of cyber threats—like how often they happen or how complex they are—can drive improvements in technical systems and human capabilities. While earlier frameworks (e.g., [51]) mainly focused on behavior or organizational culture, this study highlights how external challenges prompt team learning and coordination. Recognizing project team skills as a mediating factor offers a fresh angle on how organizations can become more resilient. Past research, such as [4], often emphasized leadership's role but did not explore how ongoing cyber threats help shape skills within operational teams. This study helps close that gap by showing how real-world pressure activates human potential, resulting in better preparedness.

For those responsible for managing cybersecurity, these insights offer valuable guidance. Understanding the specific traits of cyber threats should influence where resources are allocated—not only in terms of protective tools but also in training and team development. Training programs should reflect the nature of current threats, especially their complexity and frequency, while practice exercises that simulate real attacks can help teams build experience and respond more effectively [38]. After real and simulated events, follow-up reviews can promote learning and improve future processes. Integrating cybersecurity tasks into daily logistics work helps make readiness an ongoing and embedded part of business operations.

At a policy level, these findings suggest that regulators in Jordan and other emerging markets should create cybersecurity frameworks that measure both technology and people-related factors. Adopting models like the one proposed in [51]—which focus on learning, collaboration, and workplace culture—can support better assessment and coordination throughout the logistics sector. Promoting digital skills, running industry-wide drills, and funding training programs can strengthen readiness at both individual and organizational levels. Public agencies can further support these efforts through national strategies, shared knowledge platforms, and real-time monitoring tools across the supply chain. Although this research makes several contributions, it is not without limitations. The study's cross-sectional design means it cannot confirm cause-and-effect relationships or track how skills develop over time. Its focus on Jordan's express delivery sector also limits the extent to which findings can be applied elsewhere. In addition, the use of self-reported survey data may introduce some bias, even though techniques like Harman's single-factor test were used to reduce this risk. Future studies should use longitudinal designs to capture better how threats and team responses change over time. Comparing findings across countries or sectors may also reveal how different systems and cultures affect cybersecurity readiness. Furthermore, using qualitative methods—such as case studies or interviews—could offer deeper insight into how teams work together and learn from cyber events. Future research might also explore other influencing factors, such as leadership approaches, technology maturity, or organizational culture, to understand how cybersecurity resilience develops [51].

In conclusion, this study shows that cybersecurity readiness in logistics depends not only on the nature of external threats but also on the capabilities of internal teams. The partial mediating role of project team skills makes it clear that simply facing threats is not enough—what matters is having skilled and adaptable teams that can turn those challenges into effective responses. By combining analysis of threat features with efforts to build

human expertise, this study adds theoretical insight and practical value for logistics companies facing constant digital risks.

## 6 Conclusion

This research explored how certain cyber-attack features—specifically their sophistication, frequency, and complexity—affect cybersecurity readiness among project teams in Jordan's express delivery sector. A key part of the study was examining the project team skills' role in linking these cyber threats to organizational preparedness. Using a quantitative cross-sectional approach and validating the model with structural equation modeling, the findings showed that cyber-attack traits directly and indirectly impact cybersecurity readiness. The discovery of a partial mediation effect offers a vital takeaway: understanding and identifying threats is important, but having skilled, flexible teams is what truly turns that knowledge into practical readiness. This underlines the importance of human resources in supporting technology and maintaining resilience in cybersecurity.

From a logistics management standpoint, the study offers clear guidance. Companies in the express delivery field should focus on both tracking threats and developing team capabilities. To do this, they should regularly run realistic cybersecurity drills, promote cross-departmental collaboration, and implement clear plans for managing incidents. Because these companies rely heavily on real-time technology and seamless service delivery, it is essential to build technically skilled teams, aware of ongoing risks, and able to work together effectively. This preparation can reduce the impact of cyber incidents and help maintain uninterrupted service.

These insights are useful for logistics managers, IT professionals, and policymakers. In Jordan and similar developing markets, cybersecurity planning should go beyond protecting systems and also focus on strengthening the skills of the people involved. National policies supporting digital training, joint cyber exercises, and knowledge sharing across supply chains can help build stronger, more resilient systems.

That said, the study does have a few limitations. Because it relied on self-reported data, there is a risk of personal bias in responses. Its focus on Jordanian express delivery companies also means the results may not fully apply to other regions or sectors. Additionally, the cross-sectional design only provides a snapshot, making it difficult to track how teams adapt or grow in response to ongoing threats. Future studies should consider using a long-term approach to examine how exposure to cyber threats influences team learning. Comparing data across countries or industries could also reveal how different environments shape readiness. Moreover, exploring additional influencing factors—such as leadership approaches or company culture—could give a more complete picture of what drives cybersecurity resilience.

To conclude, this study adds to the broader understanding of cybersecurity by linking external threats with the internal skills of project teams. It shows how technical challenges and human readiness shape how well logistics organizations respond to cyber risks. The findings offer value for academic research and practical efforts to improve cybersecurity in fast-paced, digitally driven industries like express logistics.

**Acknowledgment**

The authors would like to sincerely thank the participating logistics companies and professionals in Jordan for their valuable contributions to the survey data collection. Their insights were critical to the successful completion of this research. The authors also acknowledge the support of the University of Malaya for providing the academic resources that enabled this study.

## References

[1] MASHALAH, H.A., HASSINI, E., GUNASEKARAN, A., BHATT, D.: The impact of digital transformation on supply chains through e-commerce: Literature review and a conceptual framework, *Transportation Research Part E Logistics and Transportation Review*, Vol. 165, No. September, 102837, 2022. https://doi.org/10.1016/j.tre.2022.102837

[2] NIYAWANONT, N., WANARAT, S.: Structural equation Modelling of digital entrepreneurship, logistics innovation, and digital transformation influence on logistics performance of logistics entrepreneurs in Thailand, *ABAC Journal*, Vol. 41, No. 4, pp. 147-174, 2021.

[3] CUONG, T.H., TIEN, N.H.: Application of ICT in Logistics and Supply Chain in post-Covid-19 economy in Vietnam, *International Journal of Multidisciplinary Research and Growth Evaluation*, Vol. 3, No. 1, pp. 493-451, 2022.

[4] CREAZZA, A., COLICCHIA, C., SPIEZIA, S., DALLARI, F.: Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era, *Supply Chain Management an International Journal*, Vol. 27, No. 1, pp. 30-53, 2021. https://doi.org/10.1108/scm-02-2020-0073

[5] RAUNIYAR, K., WU, X., GUPTA, S., MODGIL, S., DE SOUSA JABBOUR, A.B.L.: Risk management of supply chains in the digital transformation era: contribution and challenges of blockchain technology, *Industrial Management & Data Systems*, Vol. 123, No. 1, pp. 253-277, 2022. https://doi.org/10.1108/imds-04-2021-0235

[6] KECHAGIAS, E.P., CHATZISTELIOS, G., PAPADOPOULOS, G.A., APOSTOLOU, P.: Digital transformation of the maritime industry: A cybersecurity systemic approach, *International Journal of Critical Infrastructure Protection*, Vol. 37, No. July, 100526, 2022. https://doi.org/10.1016/j.ijcip.2022.100526

[7] SINDIRAMUTTY, S.R., JHANJHI, N.Z., TAN, C.E., KHAN, N.A., SHAH, B., MANCHURI, A.R.: *Cybersecurity measures for logistics industry*, In: N. Jhanjhi, I. Shah (Eds.), Navigating Cyber Threats and Cybersecurity in the Logistics Industry, IGI Global Scientific Publishing, pp. 1-58, 2024. https://doi.org/10.4018/979-8-3693-3816-2.ch001

[8] JHANJHI, N.Z., SHAH, I.A.: *Navigating cyber threats and cybersecurity in the logistics industry*, Advances in information security, privacy, and ethics book series, IGI Global Scientific Publishing, 2024. https://doi.org/10.4018/979-8-3693-3816-2

[9] ODIMARHA, N.A.C., AYODEJI, N.S.A., ABAKU, N.E.A.: Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies, *World Journal of Advanced Science and Technology*, Vol. 5, No. 1, pp. 026-030, 2024. https://doi.org/10.53346/wjast.2024.5.1.0030

[10] QUYET, N.X., PHUNG, T.K.: Comparative analysis of information security policies at Big 4 Vietnamese logistics companies, *International Journal of Multidisciplinary Reseach and Growth Evaluation*, Vol. 4, No. 6, pp. 683-690, 2023.

[11] HLYNSKYY, N., DOVHUN, O., POCHOPIEŃ, J.: Digitalization and cybersecurity in companies and supply chains: challenges and opportunities, *Scientific Journal of Bielsko-Biala School of Finance and Law*, Vol. 29, No. 1, pp. 53-59, 2025. https://10.19192/wsfip.sj1.2025.7

[12] NUSEIR, M.T., ALQUQA, E.K., SHRAAH, A.A., ALSHURIDEH, M.T., KURDI, B.A., ALZOUBI, H.M.: *Impact of Cyber Security Strategy and Integrated Strategy on E-Logistics Performance: An Empirical Evidence from the UAE Petroleum Industry*, In: Alzoubi, H.M., Alshurideh, M.T., Ghazal, T.M. (eds), Cyber Security Impact on Digitalization and Business Intelligence, Studies in Big Data, Vol. 117, Springer, Cham., pp. 89-108, 2024. https://doi.org/10.1007/978-3-031-31801-6_6

[13] ALOUN, D.M.: E-Commerce Companies in Jordan, *Journal of the Learning Sciences*, Vol. 32, No. 2, pp. 1-26, 2024. https://10.5281/zenodo.12794277

[14] AL-SHAIKH, M.S., KHANFAR, I.A.A.: *Delivery service via electronic applications and its impact on customers satisfaction at retail stores in Amman City/Jordan*, In: Hamdan, A., Shoaib, H.M., Alareeni, B., Hamdan, R. (eds) The Implementation of Smart Technologies for Business Success and Sustainability. Studies in Systems, Decision and Control, vol 216. Springer, Cham., pp. 827-837, 2022. https://doi.org/10.1007/978-3-031-10212-7_68

[15] HAMED, M.M.: Logistics performance and freight sector in Jordan, *European Journal of Scientific Research*, Vol. 152, No. 4, pp. 516-527, 2019.

[16] ALSHURIDEH, M.T., SHATNAWI, T.M., AL-MOMANI, A., MOHAMMAD, A.A.S., ALZOUBI, A., ALZYOUD, M., AL-SHANABLEH, N., ALAJARMEH, N.S., AL-HAWARY, S.I.S., ALDAIHANI, F.M.F.: *Analysing the impact of online journey determinants on customer digital engagement: an empirical study in Jordan*, In: Musleh Al-Sartawi, A.M.A., Nour, A.I. (eds) Artificial Intelligence and Economic Sustainability in the Era of Industrial Revolution 5.0. Studies in Systems, Decision and Control, Vol. 528, Springer, Cham., pp. 1109-1122, 2024. https://doi.org/10.1007/978-3-031-56586-1_81

[17] ELSHEBLI, A., SWEIS, G., SHARAF, A., JAGHBEER, G.A.: Proposed framework for medication delivery system in the Jordanian public health sector, BMC Medical Informatics and Decision Making, Vol. 24, No. 1, pp. 1-17, 2024. https://doi.org/10.1186/s12911-024-02673-2

[18] IRSHEIDAT, S.A., SHARIFF, D., IRSHEIDAT, A.M., DAOUD, M.K., ABDULLAH, D.: The effect of operational service quality in land cargoes operators on sustainability: the case of Jordanian logistics industry, *International Journal of Entrepreneurship*, Vol. 25, No. Special Issue 1, pp. 1-8, 2021.

[19] JABER, M.Y.: *The Impact of Blockchain on the Digitalizing Courier System of Supply Chain in Jordan*, Doctoral dissertation, Middle East University, 2024.

[20] AL-TUAIMEH, S.F.: *Building a Proposed Model for Supply Chain Decisions Support System in Express Shipping Companies in Jordan*, Doctoral dissertation, Middle East University, 2011.

[21] FRESNER, J., KRENN, C., HADDAD, J., ABDALLAH, R., MATALQA, B., SADA, A.A.: A new approach to motivate micro and small enterprises for Resource-Efficient and cleaner production in Jordan, *Sustainability*, Vol. 17, No. 6, 2404, pp. 1-21, 2025. https://doi.org/10.3390/su17062404

[22] SAMAWI, G.A., BWALIEZ, O.M., DMOUR, W.A., MDANAT, M.F., TA'AMNHA, M.A.: Eco-Smart Economics: Revolutionizing Jordan's Logistics with Sustainable Drone Technology, *International Journal of Energy Economics and Policy*, Vol. 14, No. 5, pp. 49-61, 2024. https://doi.org/10.32479/ijeep.16462

[23] DA PAZ FERRAZ SANTOS, P.R., RESENDE, P.A.A., GONDIM, J.J.C., DRUMMOND, A.C.: Towards Robust Cyber Attack Taxonomies: A Survey with Requirements, Structures, and Assessment, *ACM Computing Surveys*, Vol. 57, No. 8, pp. 1-36, 2025. https://doi.org/10.1145/3717606

[24] ALMASS, S., CHOWDHARY, S.K.: *Comprehensive Study on Cyber Security and Cyber Attacks*, In: 2024 First International Conference on Electronics, Communication and Signal Processing (ICECSP), New Delhi, India, 2024, pp. 1-6, 2024. https://doi.org/10.1109/icecsp61809.2024.10698540

[25] KIM, K., ALFOUZAN, F.A., KIM, H.: Cyber-Attack scoring model based on the Offensive Cybersecurity

Framework, *Applied Sciences*, Vol. 11, No. 16, 7738, pp. 1-21, 2021. https://doi.org/10.3390/app11167738

[26] CHUNG, J.: *Emerging Cyber-Attacks*, In: Emerging Secure Networks, Blockchains and Smart Contract Technologies, Springer, Cham., pp. 1-29, 2024. https://doi.org/10.1007/978-3-031-65866-2_1

[27] YAMIN, M.M., KATT, B.: se of cyber attack and defense agents in cyber ranges: A case study, *Computers & Security*, Vol. 122, No. November, 102892, 2022. https://doi.org/10.1016/j.cose.2022.102892

[28] LEE, J., LEE, Y., LEE, D., KWON, H., SHIN, D.: Classification of attack types and analysis of attack methods for profiling phishing mail attack groups, *IEEE Access*, Vol. 9, pp. 80866-80872, 2021. https://doi.org/10.1109/ACCESS.2021.3084897

[29] PARK, J.H., SINGH, S.K., SALIM, M.M., AZZAOUI, A.E., PARK, J.H.: Ransomware-based cyber attacks: A comprehensive survey, *Journal of Internet Technology*, Vol. 23, No. 7, pp. 1557-1564, 2022. https://doi.org/10.53106/160792642022122307010

[30] ALKHALIL, Z., HEWAGE, C., NAWAF, L., KHAN, I.: Phishing attacks: A recent comprehensive study and a new anatomy, *Frontiers in Computer Science*, Vol. 3, 563060, pp. 1-23, 2021. https://doi.org/10.3389/fcomp.2021.563060

[31] ALGHENAIM, M.F., BAKAR, N.A.A., ABDUL RAHIM, F., VANDUHE, V.Z., ALKAWSI, G.: *Phishing attack types and mitigation: A survey*, In: Wah, Y.B., Berry, M.W., Mohamed, A., Al-Jumeily, D. (eds) Data Science and Emerging Technologies, DaSET 2022, Lecture Notes on Data Engineering and Communications Technologies, Vol. 165, Springer, Singapore, pp. 131-153, 2022. https://doi.org/10.1007/978-981-99-0741-0_10

[32] RANI, S.K., SOUNDARYA, B.C., GURURAJ, H.L., JANHAVI, V.: *Comprehensive analysis of various cyber attacks*, In: 2021 IEEE Mysore sub section international conference (MysuruCon), Hassan, India, pp. 255-262, 2021. https://doi.org/10.1109/MysuruCon52639.2021.9641089

[33] SUN, R., LUO, Q., CHEN, Y.: Online transportation network cyber-attack detection based on stationary sensor data, *Transportation Research Part C: Emerging Technologies*, Vol. 149, No. April, 104058, 2023. https://doi.org/10.1016/j.trc.2023.104058

[34] CHOPRA, A.: Cyberattack-Intangible damages in a virtual world: Property insurance companies declare War on cyber-attack insurance claims, *Ohio State Law Journal*, Vol. 82, No. 1, pp. 121-162, 2021.

[35] BAHADORIPOUR, S., KARIMIPOUR, H., JAHROMI, A.N., ISLAM, A.: An explainable multi-modal model for advanced cyber-attack detection in industrial control systems, *Internet of Things*, Vol. 25, No. April, 101092, 2024. https://doi.org/10.1016/j.iot.2024.101092

[36] AMAL, M.R., VENKADESH, P.: Review of Cyber Attack Detection: Honeypot System, *Webology*, Vol. 19, No. 1, pp. 5497-5514, 2022. https://doi.org/10.14704/web/v19i1/web19370

[37] AUSTIN, G., WITHERS, G.: *Valuation of Reputation Damage for Transport Cyber Attack*, [Online], Available: https://appliedeconomics.com.au/wp-content/uploads/2022/02/Final-Cyber-Report-01-11-2021-5.pdf [10 Jun 2025], 2021.

[38] SINLAPANUNTAKUL, P., FAUSETT, C.M., KEEBLER, J.R.: Exploring team competencies in cybersecurity, *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 66, No. 1, pp. 1110-1114, 2022. https://doi.org/10.1177/1071181322661496

[39] SHINDE, N., KULKARNI, P.: Cyber incident response and planning: a flexible approach, *Computer Fraud & Security*, Vol. 2021, No. 1, pp. 14-19, 2021. https://doi.org/10.1016/s1361-3723(21)00009-9

[40] FAUSETT, C.M., KEEBLER, J.R.: Teamwork in Cybersecurity: Evaluating the Cooperative Board Game [d0x3d!] as an Experimental Testbed, *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 67, No. 1, pp. 1924-1929, 2023. https://doi.org/10.1177/21695067231192665

[41] ALJUMAIAH, O., JIANG, W., ADDULA, S.R., ALMAIAH, M.A.: Analyzing Cybersecurity Risks and Threats in IT Infrastructure based on NIST Framework, *Journal of Cyber Security and Risk Auditing*, Vol. 2025, No. 2, pp. 12-26, 2025. https://doi.org/10.63180/jcsra.thestap.2025.2.2

[42] CHOURASIA, N.R.: AI-Enhanced Cybersecurity Training: Learning Analytics in action, *International Journal of Advanced Research in Science Communication and Technology*, Vol. 5, No. 2, pp. 566-573, 2025. https://doi.org/10.48175/ijarsct-23066

[43] MCBRIDE, D.Y.: *An Analysis of Cybersecurity Curriculum Designs, Workforce Readiness Skills, and Applied Learning Effectiveness*, Doctoral dissertation, Capitol Technology University, Laurel, Maryland, USA, 2021.

[44] WANG, S., LI, Y., CHEN, F.: Optimizing Blue Team Strategies with Reinforcement Learning for Enhanced Ransomware Defense Simulations, *Authorea*, Vol. 2024, pp. 1-9, 2024. https://doi.org/10.22541/au.172356133.30648910/v1

[45] SAFITRA, M.F., LUBIS, M., FAKHRURROJA, H.: Counterattacking Cyber Threats: A framework for the Future of Cybersecurity. Sustainability, Vol. 15, No. 18, 13369, pp. 1-32, 2023. https://doi.org/10.3390/su151813369

[46] STEINGARTNER, W., GALINEC, D., KOZINA, A.: Threat Defense: Cyber Deception approach and Education for Resilience in Hybrid Threats model,

*Symmetry*, Vol. 13, No. 4, 597, pp. 1-25, 2021. https://doi.org/10.3390/sym13040597

[47] NEELI, S.S.S.: Critical cybersecurity strategies for database protection against cyber attacks, *Journal of Artificial Intelligence Machine Learning and Data Science*, Vol. 1, No. 1, pp. 2102-2106, 2023. https://doi.org/10.51219/jaimld/sethu-sesha-synam-neeli/461

[48] LEHTO, M.: *Cyber-Attacks against critical infrastructure*, In: Lehto, M., Neittaanmäki, P. (eds) Cyber Security, Computational Methods in Applied Sciences, Vol. 56, Springer, Cham., pp. 3-42, 2022. https://doi.org/10.1007/978-3-030-91293-2_1

[49] ROY, N.C., PRABHAKARAN, S.: Cyber fraud (CF) in banking: a dual-layer, blockchain-enabled approach for prevention and managerial response, *Managerial Finance*, Vol. 51, No. 5, pp. 765-796, 2025. https://doi.org/10.1108/mf-09-2024-0716

[50] STAVES, A., ANDERSON, T., BALDERSTONE, H., GREEN, B., GOUGLIDIS, A., HUTCHISON, D.: A cyber incident response and recovery framework to support operators of industrial control systems, *International Journal of Critical Infrastructure Protection*, Vol. 37, No. July, 100505, 2022. https://doi.org/10.1016/j.ijcip.2021.100505

[51] GEORGIADOU, A., MOUZAKITIS, S., BOUNAS, K., ASKOUNIS, D.: A Cyber-Security culture framework for assessing organization readiness, *Journal of Computer Information Systems*, Vol. 62, No. 3, pp. 452-462, 2020. https://doi.org/10.1080/08874417.2020.1845583

[52] STADNYK, M., PALAMAR, A.: Project management features in the cybersecurity area, *Scientific Journal of the Ternopil National Technical University*, Vol. 2, No. 106, pp. 54-62, 2022. https://doi.org/10.33108/visnyk_tntu2022.02.054

[53] CRUMPLER, W., LEWIS, J.A.: *Cybersecurity workforce gap*, Center for Strategic and International Studies (CSIS), [Online], Available: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf [10 Jun 2025] 2019.

[54] SALIN, H., LUNDGREN, M.: Towards agile cybersecurity risk management for autonomous software engineering teams, *Journal of Cybersecurity and Privacy*, Vol. 2, No. 2, pp. 276-291, 2022. https://doi.org/10.3390/jcp2020015

[55] CHAPMAN, T.A., REITHEL, B.J.: Perceptions of cybersecurity readiness among workgroup IT managers, *Journal of Computer Information Systems*, Vol. 61, No. 5, pp. 438-449, 2021. https://doi.org/10.1080/08874417.2019.1703224

[56] HOSSAIN, M.A., RAZA, M.A., RAHMAN, T.Y.: Resource allocation and budgetary constraints for cybersecurity projects in small to medium sized banks, *Journal of Multidisciplinary Research*, Vol. 9, No. 1, pp. 135-157, 2023.

[57] ECK, C.A.: *Examining US Organizations' Information Security: A Quantitative Study of Employee Job Role Effects on Cybersecurity Measures Employed*, Doctoral dissertation, Robert Morris University, 2024.

[58] FLOROS, E., STAVROU, E., SMYRLIS, M., NIKOLOUDAKIS, N., POTAMOS, G., APOSTOLIDIS, A., BEMPIS, P., GRIGORIADIS, A., MAGKOS, K., MERKOURIS, D., SPANOUDAKIS, G., STAVROU, S., TRIKOS, S., PAPADAKIS, S.E.: *Towards the Design of Cyber Range Training Programs for Enhanced Preparedness: Investigating the Training Needs in Critical Infrastructures*, In: 2025 IEEE Global Engineering Education Conference (EDUCON), London, United Kingdom, pp. 1-10, IEEE, 2025. https://doi.org/10.1109/EDUCON62633.2025.11016646

[59] JORDAN, K.A.: *Quantitative Effects of Simulation-Based User Training on Overall Cyber Resilience in Department of Defense (DoD) Systems*, Capitol Technology University, 2022.

[60] ELENDU, C., OMELUDIKE, E.K., OLOYEDE, P.O., OBIDIGBO, B.T., OMELUDIKE, J.C.: Legal implications for clinicians in cybersecurity incidents: A review, *Medicine*, Vol. 103, No. 39, e39887, 2024. https://doi.org/10.1097/md.0000000000039887

[61] KLINDIENST, J., AYANIAN, S., SCHLEGELMILCH, J., AKSELROD, H.: Preparing for compounding crises: Staff shortages and cyber-attack vulnerability in the era of COVID-19, *Journal of Business Continuity & Emergency Planning*, Vol. 16, No. 2, pp. 103-120, 2022. https://doi.org/10.7916/6ya3-x453

[62] HOWELL JR, J.W.: *Exploring the Perceptions of Perceived and Actual Cyber Readiness*, Doctoral dissertation, Capella University, 2021.

[63] SHAHZAD, M., SHAFIQ, M.Z., LIU, A.X.: *A large scale exploratory analysis of software vulnerability life cycles*, 2012 34th International Conference on Software Engineering (ICSE), pp. 771-781, 2012. https://doi.org/10.1109/ICSE.2012.6227141

[64] VÄLJA, M., KORMAN, M., LAGERSTRÖM, R.: *A Study on Software Vulnerabilities and Weaknesses of Embedded Systems in Power Networks*, 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, CPSR-SG 2017, 21 April 2017, pp. 47-52, 2017. https://doi.org/10.1145/3055386.3055397

[65] BAYRAMOVA, T.: *Analysis of modern methods for detecting vulnerabilities in software for industrial information systems*, In: NATO science for peace and security series, D, Information and communication security, Vol. 62, pp. 160-162, 2022. https://doi.org/10.3233/nicsp220050

[66] XU, D., WONG, T., SCULLI, D.: A software platform to support collaboration in express delivery services, *Journal of International Technology and*

*Information Management*, Vol. 22, No. 2, pp. 19-34, 2013. https://doi.org/10.58729/1941-6679.1008

[67] SEGHEZZI, A., MANGIARACINA, R., TUMINO, A., PEREGO, A.: 'Pony express' crowdsourcing logistics for last-mile delivery in B2C e-commerce: an economic analysis, *International Journal of Logistics Research and Applications*, Vol. 24, No. 5, pp. 456-472, 2021. https://doi.org/10.1080/13675567.2020.1766428

[68] ZHAO, C., ZHOU, B.: Impact of Express Delivery Industry's Development on Transportation Sector's Carbon Emissions: An Empirical Analysis from China, *Sustainability*, Vol. 13, No. 16, 8908, pp. 1-21, 2021. https://doi.org/10.3390/su13168908

[69] ALHAZMI, O., MALAIYA, Y., RAY, I.: *Security Vulnerabilities in software Systems: A Quantitative perspective*, In: Jajodia, S., Wijesekera, D. (eds) Data and Applications Security XIX, DBSec 2005, Lecture Notes in Computer Science, Vol. 3654, Springer, Berlin, Heidelberg, pp. 281-294, 2025. https://doi.org/10.1007/11535706_21

[70] NOWAKOWSKI, T., WERBIŃSKA-WOJCIECHOWSKA, S.: *Problems of logistic Systems vulnerability and resilience assessment*, In: Golinska, P. (eds) Logistics Operations, Supply Chain Management and Sustainability, EcoProduction. Springer, Cham., pp. 171-186, 2014. https://doi.org/10.1007/978-3-319-07287-6_12

[71] ALNAELI, S.M., SARNOWSKI, M., AMAN, M.S., ABDELGAWAD, A., YELAMARTHI, K.: Source code vulnerabilities in IoT software systems, *Advances in Science Technology and Engineering Systems Journal*, Vol. 2, No. 3, pp. 1502-1507, 2017. https://doi.org/10.25046/aj0203188

[72] CORREA, G.: *To err is human, or is it?*, Process Safety Progress, Special Issue: Latin American Process Safety Conference Nov 3–5, 2020, Vol. 40, No. S1, pp. S4-S7, 2021. https://doi.org/10.1002/prs.12225

[73] AMORESANO, K., YANKSON, B.: Human error - a critical contributing factor to the rise in data breaches: A case study of higher education, *HOLISTICA – Journal of Business and Public Administration*, Vol. 14, No. 1, pp. 110-132, 2023. https://doi.org/10.2478/hjbpa-2023-0007

[74] HANSEN, F.D.: Human Error: a Concept analysis, *Journal of Air Transportation*, Vol. 11, No. 3, pp. 61-77, 2006. https://ntrs.nasa.gov/citations/20070022530

[75] NCUBUKEZIT, T.: *Human errors: a cybersecurity concern and the weakest link to small businesses*, Proceedings of the 17th International Conference on Cyber Warfare and Security (ICCWS 2022), Vol. 17, No. 1, pp. 395-403, 2022. https://doi.org/10.34190/iccws.17.1.51

[76] BOYCE, M.W., DUMA, K.M., HETTINGER, L.J., MALONE, T.B., WILSON, D.P., LOCKETT-REYNOLDS, J.: Human Performance in Cybersecurity: a research agenda, *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 55, No. 1, pp. 1115-1119, 2011. https://doi.org/10.1177/1071181311551233

[77] ALSHARIF, M., MISHRA, S., ALSHEHRI, M.: Impact of human vulnerabilities on cybersecurity, *Computer Systems Science and Engineering*, Vol. 40, No. 3, pp. 1153-1166, 2021. https://doi.org/10.32604/csse.2022.019938

[78] SHAHRAKI, A.S., NIKMARAM, M.: Human errors in computer related abuses, *Journal of Theoretical and Applied Information Technology*, Vol. 47, No. 1, pp. 93-97, 2013. https://eprints.qut.edu.au/74466/

[79] NOBLES, C., ROBINSON, N., CUNNINGHAM, M., ROBINSON, N., CUNNINGHAM, M., CUNNINGHAM, M.: *Straight from the Human Factors Professionals' Mouth: The Need to Teach Human Factors in Cybersecurity*, SIGITE´2022: Proceedings of the 23rd Annual Conference on Information Education, pp. 157-158, 2022. https://doi.org/10.1145/3537674.3555782

[80] ROSYIDI, E., YUSELIN, N., YAHYA, K.: Analysis of factors causing errors in issue of goods at PT Dunia Express Transindo's warehouse, *Jurnal Syntax Transformation*, Vol. 4, No. 2, pp. 165-182, 2023. https://doi.org/10.46799/jst.v4i2.694

[81] YOU, J., LIU, B., WANG, Y., LIU, J.: *Tracking the prevalence of compromised passwords using long-term honeypot data*, In: Proceedings SPIE 12700, International Conference on Electronic Information Engineering and Data Processing (EIEDP 2023), 127000K (26 May 2023), 2023.

[82] DARKO, C.D.: *Weak credential information as a threat to online security*, SMART-IEEE-Creative Research Publications Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensic, pp. 35-40, 2022. https://doi.org/10.22624/aims/crp-bk3-p6

[83] HAJNÝ, J., MALINA, L.: *Anonymous credentials with practical revocation*, 2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL), Rome, Italy, 2012, pp. 1-6, 2012. https://doi.org/10.1109/ESTEL.2012.6400081

[84] SINGH, V., PANDEY, S.K.: *Revisiting cloud security attacks: Credential attack*, In: Rathore, V.S., Dey, N., Piuri, V., Babo, R., Polkowski, Z., Tavares, J.M.R.S. (eds) Rising Threats in Expert Applications and Solutions. Advances in Intelligent Systems and Computing, Vol. 1187, Springer, Singapore, pp. 339-350, 2021. https://doi.org/10.1007/978-981-15-6014-9_39

[85] NATHAN, M.: Credential stuffing: new tools and stolen data drive continued attacks, *Computer Fraud & Security*, Vol. 2020, No. 12, pp. 18-19, 2020. https://doi.org/10.1016/s1361-3723(20)30130-5

[86] JOHNSEN, J.W., FRANKE, K.: *Identifying Proficient Cybercriminals Through Text and Network*

*Analysis*, In: 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), Arlington, VA, USA, 2020, pp. 1-7, 2020. https://doi.org/10.1109/ISI49825.2020.9280523

[87] KENNISON, S.M., CHAN-TIN, E.: Taking Risks with Cybersecurity: Using knowledge and personal characteristics to predict Self-Reported Cybersecurity Behaviors, *Frontiers in Psychology*, Vol. 11, pp. 1-9, 2020. https://doi.org/10.3389/fpsyg.2020.546546

[88] GRIFFIN, P.H.: *Biometric-Based cybersecurity techniques*, In: Nicholson, D. (eds) Advances in Human Factors in Cybersecurity, Advances in Intelligent Systems and Computing, Vol. 501, Springer, Cham., pp. 43-53, 2016. https://doi.org/10.1007/978-3-319-41932-9_5

[89] PELCHEN, C., JAEGER, D., CHENG, F., MEINEL, C.: *The (Persistent) threat of weak passwords: implementation of a semi-automatic Password-Cracking algorithm*, In: Heng, SH., Lopez, J. (eds) Information Security Practice and Experience, ISPEC 2019, Lecture Notes in Computer Science(), Vol. 11879, Springer, Cham., pp. 464-475, 2019. https://doi.org/10.1007/978-3-030-34339-2_27

[90] SARKAR, K.R.: Assessing insider threats to information security using technical, behavioural and organisational measures, *Information Security Technical Report*, Vol. 15, No. 3, pp. 112-133, 2010. https://doi.org/10.1016/j.istr.2010.11.002

[91] PROBST, C.W., HUNKER, J., GOLLMANN, D., BISHOP, M.: *Insider threats in cyber security*, Advances in Information Security, Vol. 49, Springer, 2010. https://doi.org/10.1007/978-1-4419-7133-3

[92] VILLARREAL-VASQUEZ, M., MODELO-HOWARD, G., DUBE, S., BHARGAVA, B.: Hunting for insider threats using LSTM-Based anomaly detection, *IEEE Transactions on Dependable and Secure Computing*, Vol. 20, No. 1, pp. 451-462, 2021. https://doi.org/10.1109/tdsc.2021.3135639

[93] STOLFO, S.J., BELLOVIN, S.M., HERSHKOP, S., KEROMYTIS, A., SINCLAIR, S., SMITH, S.W.: *Insider Attack and Cyber Security: Beyond the Hacker*, Springer US, 2008.

[94] SINGH, A.P., SHARMA, A.: A systematic literature review on insider threats, *arXiv*, Cornell University, Vol. 2022, pp. 1-9, 2022. https://doi.org/10.48550/arxiv.2212.05347

[95] HONG, J., KIM, J., CHO, J.: *The trend of the security research for the insider cyber threat*, In: Ślęzak, D., Kim, Th., Fang, WC., Arnett, K.P. (eds) Security Technology, SecTech 2009, Communications in Computer and Information Science, Vol. 58, Springer, Berlin, Heidelberg, pp. 100-107, 2009. https://doi.org/10.1007/978-3-642-10847-1_13

[96] GILLARD, S.: Soft skills and technical expertise of effective project managers, *Issues in Informing Science and Information Technology*, Vol. 6, pp. 723-729, 2009.

[97] BARRETT, M.J., MARRON, J., PILLITTERI, V., BOYENS, J.M., QUINN, S., WITTE, G., FELDMAN, L.: *Approaches for Federal Agencies to Use the Cybersecurity Framework*, NIST, National Institute of Standards and Technology, U.S. Department of Commerce, NISTIR 8170, 2020. https://doi.org/10.6028/NIST.IR.8170-upd

[98] KLEIN, G., JIANG, J.J., TESCH, D.: Wanted: project teams with a blend of is professional orientations, *Communications of the ACM*, Vol. 45, No. 6, pp. 81-87, 2002. https://doi.org/10.1145/508448.508452

[99] HILLIARD, D.: *The communicator's role in project teams*, Proceedings Professional Communication Conference the New Face of Technical Communication: People, Processes, Products', Philadelphia, PA, USA, 1993, pp. 315-319, 1993. https://doi.org/10.1109/IPCC.1993.593881

[100] MUSZYŃSKA, K.: *Patterns of Communication Management in Project Teams*, In: Ziemba, E. (eds) Information Technology for Management: New Ideas and Real Solutions, ISM AITM 2016, Lecture Notes in Business Information Processing, Vol. 277, Springer, Cham., pp. 202-221, 2017. https://doi.org/10.1007/978-3-319-53076-5_11

[101] SWART, K., BOND-BARNARD, T.J., CHUGH, R.: Challenges and critical success factors of digital communication, collaboration and knowledge sharing in project management virtual teams: a review, *International Journal of Information Systems and Project Management*, Vol. 10, No. 4, pp. 59-75, 2022. https://doi.org/10.12821/ijispm100404

[102] STEINKE, J.A., BOLUNMEZ, B., FLETCHER, L.S., WANG, V., TOMASSETTI, A.J., REPCHICK, K.M., ZACCARO, S.J., DALAL, R.S., TETRICK, L.E.: Improving cybersecurity incident response team effectiveness using Teams-Based research, *IEEE Security & Privacy*, Vol. 13, No. 4, pp. 20-29, 2015. https://doi.org/10.1109/MSP.2015.71

[103] FURUKAWA, C.: Dynamics of a critical problem-solving project team and creativity in a multiple-project environment, *Team Performance Management: An International Journal*, Vol. 22, No. 12, pp. 92-110. https://doi.org/10.1108/TPM-04-2015-0021

[104] ARISTIN, N.F., PURNOMO, A.: Improving Critical Thinking Skill Through Team-based Projects, is it Effective?, *Journal of Education Research and Evaluation*, Vol. 6, No. 4, pp. 586-594, 2022. https://doi.org/10.23887/jere.v6i4.48090

[105] CHAIDIR, J., HIDAYATI, P.P., HARNADI, K.K.: The Relationship between Critical Thinking Ability and Problem-Based Learning with a Causality Pattern in Learning Improvement, *Mix: Jurnal Ilmiah Manajemen*, Vol. 13, No. 1, pp. 122-137, 2023. http://dx.doi.org/10.22441/jurnal_mix.2023.v13i1.00

[106] VARLAMOVA, V.: *The Relationship between Time Management and Decision-Making Processes*, University of Canterbury, 2008.

[107] SRINIVASAN, K., GUPTA, T., AGARWAL, P., NEMA, A.: *A robust security framework for cloud-based logistics services*, 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, Japan, 2018, pp. 162-165, 2018. https://doi.org/10.1109/ICASI.2018.8394557

[108] ALMUKHAMETOV, A.I., DMITRIEV, A.G.: Flexible project management methodologies, *Scientific notes of the Russian academy of entrepreneurship*, Vol. 22, No. 2, pp. 11-17, 2023. https://doi.org/10.24182/2073-6258-2023-22-2-11-17

[109] CHAN, H.K., CHAN, F.T.: Comparative study of adaptability and flexibility in distributed manufacturing supply chains, *Decision Support Systems*, Vol. 48, No. 2, pp. 331-341, 2010. https://doi.org/10.1016/j.dss.2009.09.001

[110] HUGHES, T.R., CASLIN, J., FOSS, C., LARSEN, A.K., LOFFER, J., SACCO, K.: Leading Through Conflict with Critical Thinking and Creative Problem-Solving, *International Journal for Cross-Disciplinary Subjects in Education*, Vol. 10, No. 4, pp. 4142-4146, 2019. http://dx.doi.org/10.20533/ijcdse.2042.6364.2019.0505

[111] WAHYUDIATI, D., IRWANTO, I., NINGRAT, H.K.: Improving pre-service chemistry teachers' critical thinking and problem-solving skills using project-based learning, *World Journal on Educational Technology: Current Issues*, Vol. 14, No. 5, pp. 1291-1304, 2022. https://doi.org/10.18844/wjet.v14i5.7268

[112] SÁNCHEZ-SILVA, M., CALDERÓN-GUEVARA, W.: Flexibility and adaptability within the context of decision-making in infrastructure management, *Structure and Infrastructure Engineering*, Vol. 18, No. 7, pp. 950-966, 2022. https://doi.org/10.1080/15732479.2022.2038642

[113] FARRELL, M.: Time management, *Journal of Library Administration*, Vol. 57, No. 2, pp. 215-222, 2017. https://doi.org/10.1080/01930826.2017.1281666

[114] FATHIMA, A., DEVI, G.S., FAIZAANUDDIN, M.: Improving distributed denial of service attack detection using supervised machine learning, *Measurement: Sensors*, Vol. 30, 100911, pp. 1-8, 2023. https://doi.org/10.1016/j.measen.2023.100911

[115] APENKO, S., ROMANENKO, M.: *Leadership competencies of flexible teams of innovative projects of enterprises*, 5th International Scientific Conference – EMAN 2021 – Economics and Management: How to Cope With Disrupted Times, Online/Virtual, March 18, 2021, Conference Proceedings published by: Association of Economists and Managers of the Balkans, Belgrade, Serbia, pp. 311-318, 2021. https://doi.org/10.31410/eman.2021.311

[116] THOMAS, G., SULE, M.: A service lens on cybersecurity continuity and management for organizations' subsistence and growth, *Organizational Cybersecurity Journal Practice Process and People*, Vol. 3, No. 1, pp. 18-40, 2023. https://doi.org/10.1108/ocj-09-2021-0025

[117] MOKHOR, V., KORCHENKO, O., HONCHAR, S., KOMAROV, M., ONYSKOVA, A.: *Research of the impact on the ecology of the state of cybersecurity of the critical infrastructure objects*, E3S Web of Conferences, Vol. 280, 09009, pp. 1-6, 2021. https://doi.org/10.1051/e3sconf/202128009009

[118] SAWYER, B.D., HANCOCK, P.A.: Hacking the human: The prevalence paradox in cybersecurity, *Human Factors: The Journal of the Human Factors and Ergonomics Society*, Vol. 60, No. 5, pp. 597-609, 2018. https://doi.org/10.1177/0018720818780472

[119] BURRELL, D.N.: *Teaching graduate technology management students with innovative learning approaches around cybersecurity*, In: Research Anthology on Advancements in Cybersecurity Education, edited by Information Resources Management Association, IGI Global Scientific Publishing, pp. 491-500, 2022. https://doi.org/10.4018/978-1-6684-3554-0.ch024

[120] WANG, Q., LU, S., LIN, J., WANG, C., FAN, H.: Sentiment analysis for the customer feedback in the Express Delivery Enterprise Evaluation System, *Learning & Education*, Vol. 9, No. 3, pp. 57-59, 2020. https://doi.org/10.18282/l-e.v9i3.1574

[121] QUADER, F., JANEJA, V.P.: Insights into organizational security readiness: Lessons learned from cyber-attack case studies, *Journal of Cybersecurity and Privacy*, Vol. 1, No. 4, pp. 638-659, 2021. https://doi.org/10.3390/jcp1040032

[122] HASAN, M.F., AL-RAMADAN, N.S.: Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case, *Social Science and Humanities Journal*, Vol. 5, No. 8, pp. 2312-2323, 2021.

[123] AHMED, S.A.A.S., ISAK, M.A.: Factors Affect Cyber Security Readiness and Performance of SMEs: A Case Study of Mogadishu, Somalia, *International Journal of Innovative Science and Research Technology*, Vol. 9, No. 7, pp. 1059-1069, 2024. https://doi.org/10.38124/ijisrt/IJISRT24JUL264

[124] NERI, M., NICCOLINI, F., MARTINO, L.: Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment, *Information & Computer Security*, Vol. 32, No. 1, pp. 38-52, 2024. https://doi.org/10.1108/ICS-05-2023-0084

[125] ALHARBI, F., ALSULAMI, M., AL-SOLAMI, A., AL-OTAIBI, Y., AL-OSIMI, M., AL-QANOR, F.,

AL-OTAIBI, K.: The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia, *Sensors*, Vol. 21, No. 20, 6901, pp. 1-14, 2021. https://doi.org/10.3390/s21206901

[126] WHITE, G.: Generation Z: cyber-attack awareness training effectiveness, *Journal of Computer Information Systems*, Vol. 62, No. 3, pp. 560-571, 2022. https://doi.org/10.1080/08874417.2020.1864680

[127] AKTER, S., UDDIN, M.R., SAJIB, S., LEE, W.J.T., MICHAEL, K., HOSSAIN, M.A.: Reconceptualizing cybersecurity awareness capability in the data-driven digital economy, *Annals of Operations Research*, Vol. 350, pp. 673-698, 2025. https://doi.org/10.1007/s10479-022-04844-8

[128] BERLILANA, NOPARUMPA, T., RUANGKANJANASES, A., HARIGUNA, T., SARMINI: Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness, *Sustainability*, Vol. 13, No. 24, 13761, pp. 1-20, 2021. https://doi.org/10.3390/su132413761

[129] NOPARUMPA, T., SAENGCHOTE, K., WANNAKRAIROJ, W.: An Empirical Investigation of Productivity and Corporate Culture Using Textual Analysis, *SSRN*, Vol. 2024, pp. 1-12, 2024.

[130] PESZKO, G., VAN DER MENSBRUGGHE, D., GOLUB, A., CHEPELIEV, M.: *Low-Carbon transition, stranded fossil fuel assets, border carbon adjustments, and international cooperation*, In: The World Bank eBooks, pp. 225-269, 2021. https://doi.org/10.1596/978-1-4648-1590-4_ch10

[131] CLARK, M.E., MCEWAN, K., CHRISTIE, C.J.: The effectiveness of constraints-led training on skill development in interceptive sports: A systematic review, *International Journal of Sports Science & Coaching*, Vol. 14, No. 2, pp. 229-240, 2018. https://doi.org/10.1177/1747954118812461

[132] CRESWELL, J.W., CRESWELL, J.D.: *Research design: Qualitative, quantitative, and mixed methods approaches*, 5th ed., SAGE Publications, 2018.

[133] BRYMAN, A.: *Social research methods*, 5th ed., Oxford University Press, 2016.

[134] HAIR, J.F., HULT, G.T.M., RINGLE, C.M., SARSTEDT, M.: *A primer on partial least squares structural equation modeling (PLS-SEM)*, SAGE Publication, Inc., USA, 2014.

[135] IFINEDO, P.: Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory, *Computers & Security*, Vol. 31, No. 1, pp. 83-95, 2012. https://doi.org/10.1016/j.cose.2011.10.007

[136] ROSADO, D.G., MORENO, J., SÁNCHEZ, L.E., SANTOS-OLMO, A., SERRANO, M.A., FERNÁNDEZ-MEDINA, E.: MARISMA-BiDa pattern: Integrated risk analysis for big data, *Computers & Security*, Vol. 102, No. March, 102155, 2021. https://doi.org/10.1016/j.cose.2020.102155

[137] JOSHI, A., KALE, S., CHANDEL, S., PAL, D.K.: Likert scale: Explored and explained, *Current Journal of Applied Science and Technology*, Vol. 7, No. 4, pp. 396-403, 2015. https://doi.org/10.9734/BJAST/2015/14975

[138] SHANNON, D.M., JOHNSON, T.E., SEARCY, S., LOTT, A.: Using electronic surveys: advice from survey professionals, *Practical Assessment, Research, and Evaluation*, Vol. 8, No. 1, pp. 1-9, 2002. https://doi.org/10.7275/q9xy-zk52

[139] SCHWARZ, N.: The Psychology of Survey Response, Roger Tourangeau, Lance J. Rips, and Kenneth Rasinski. New York: Cambridge University Press, 2000. 401pp, ISBN 0-521-57246-0 (cloth) and 0-521-57629-6 (paper)., *International Journal for Quality in Health Care*, Vol. 13, No. 1, pp. 80-82, 2001. https://doi.org/10.1093/ijpor/13.1.80

[140] ISRAEL, M.A., HAY, I.M.: *Research ethics for social scientists : between ethical conduct and regulatory compliance*, SAGE Publications Ltd, London, UK, 2006.

[141] SARSTEDT, M., RINGLE, C.M., SMITH, D., REAMS, R., HAIR, J.F.: Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers, *Journal of Family Business Strategy*, Vol. 5, No. 1, pp. 105-115, 2014. https://doi.org/10.1016/j.jfbs.2014.01.002

[142] TABACHNICK, B.G., FIDELL, L.S.: *Using multivariate statistics*, 6th ed., Pearson, New York, USA, 2013.

[143] NUNNALLY, J.C., BERNSTEIN, I.H.: *Psychometric theory*, 3rd ed., McGraw-Hill, New York, USA, 1994.

[144] FORNELL, C., LARCKER, D.F.: Evaluating structural equation models with unobservable variables and measurement error, *Journal of Marketing Research*, Vol. 18, No. 1, pp. 39-50, 1981. https://doi.org/10.1177/002224378101800104

[145] HENSELER, J., RINGLE, C.M., SARSTEDT, M.: A new criterion for assessing discriminant validity in variance-based structural equation modeling, *Journal of the Academy of Marketing Science*, Vol. 43, pp. 115-135, 2015. https://doi.org/10.1007/s11747-014-0403-8

[146] HU, L.T., BENTLER, P.M.: Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives, *Structural Equation Modeling: A Multidisciplinary*

*Journal*, Vol. 6, No. 1, pp. 1-55, 1999. https://doi.org/10.1080/10705519909540118

[147] BORKY, J.M., BRADLEY, T.H.: *Protecting Information with Cybersecurity*, In: Effective Model-Based Systems Engineering, Springer, Cham., pp. 345-404, 2019. https://doi.org/10.1007/978-3-319-95669-5_10

**Review process**
Single-blind peer review process.