SSRG International Journal of Recent Engineering Science
ISSN: 2349–7157 / https://doi.org/10.14445/23497157/IJRES-V11I5P105

Volume 11 Issue 5, 40-50, Sep-Oct 2024
© 2024 Seventh Sense Research Group®

Original Article

Enhancing Cybersecurity in Logistics Networks in Oman

Ali S al Kalbani[1], Hajar R al Kalbani[2]

[1]*Department of Management Studies, Middle East College, Muscat, Oman.*
[2]*Department of Foundation Studies, Global College of Engineering and Technology, Muscat, Oman.*

[1]*Corresponding Author : bur3d.x@gmail.com*

Received: 07 August 2024 Revised: 10 September 2024 Accepted: 25 September 2024 Published: 15 October 2024

Abstract* - *The logistics industry in Oman relies heavily on digital networks, increasing its vulnerability to cyber threats. This study examines the current cybersecurity state within Oman's logistics networks, focusing on implementing and assessing cybersecurity measures. The present study combines elements of both qualitative and quantitative research through interviews and surveys with supply chain and logistics professionals. Key areas explored include cybersecurity measures, employee training, adherence to cybersecurity standards, and incident response plans. Findings reveal widespread adoption of essential cybersecurity technologies but highlight the need for increased investment, training, and security audits. This study provides insights and recommendations to enhance cybersecurity resilience in Oman's logistics sector.

Keywords* - *Cybersecurity, Data breaches, Logistics networks, Oman, Supply chain security.

1. Introduction

The logistics industry in Oman is increasingly dependent on digital networks and data exchange for its operations, which has heightened its vulnerability to cyber threats. As the interconnectedness of logistics networks grows, so does the potential for cyber-attacks, making cybersecurity a critical area of focus. Unfortunately, recent scholarship on cybersecurity in Logistics Networks remains limited, especially from the Sultanate of Oman. Most researchers emphasise carrying out cybersecurity studies broadly on Oman's sectors like IT and telecommunication, healthcare, and finance, a practice that overlooks all the cybersecurity challenges the supply chain and logistics sector in the Sultanate experiences. Besides, studies such as [6, 7, and 12] have given too much focus on the state of the cybersecurity sector across developed and only leave [9] as a notable study reviewing the cybersecurity elements in a less developed economy like Oman. Hence, the current research fills this research gap by focusing on the effectiveness of cybersecurity implementation processes for the Logistic Networks sector in Oman, a developing state. The study is valuable because Oman's logistics sector policymakers have struggled to make informed decisions on addressing the challenges of interconnected logistics systems and keeping up with international compliance standards. Thus, this research investigates the present insights and conditions of the state of cybersecurity in Oman's logistics sector. It aims to identify and analyse the measures necessary to safeguard data integrity and prevent data breaches. This will help narrow the industry-specific studies on enhancing cybersecurity in Omani logistics network systems. It also provides evidence-based recommendations on improving the sectors' cybersecurity and IT resilience levels. The research framework addresses four key variables: Cybersecurity Measures Implemented, Employee Training and Awareness Programs, Adoption of Cybersecurity Standards and Frameworks, and Incident Response and Recovery Plans. These variables are crucial for maintaining the integrity of logistics networks. Employee training programs significantly improve cybersecurity awareness, though participation and content coverage vary. Additionally, adopting international standards, particularly ISO/IEC 27001, is prevalent, and incident response plans are well-established but require continuous enhancement. This study provides valuable insights for policymakers, logistics managers, and IT professionals, emphasizing the importance of proactive cybersecurity measures and continuous improvement to protect the integrity of logistics networks in Oman.

2. Objectives

- Identify Cybersecurity Threats: To identify and analyse the various cybersecurity threats faced by logistics networks in Oman, including data breaches, ransomware attacks, and supply chain disruptions.
- Assess Current Practices: To assess the existing cybersecurity practices within Oman's logistics sector, including the adoption of security measures, protocols, and technologies aimed at mitigating cyber risks.
- Develop Recommendations: Based on the findings, develop recommendations and actionable insights tailored to the Omani context to improve country-specific cybersecurity resilience and outcomes.

3. Literature Review

ICT has penetrated the supply chain and logistics sector, with the two providing the best Supply Chain Management (SCM) outcomes by effectively and timely availing products to consumers worldwide. According to a study by [7], integrating ICT into the logistics sector has been a game-changer in SCM. It helps the industry balance the need to satisfy customer needs and manage costs to help accrue profits. Scholars identify that ICT integration into logistics also significantly influences the value chain, considering that it massively links one activity with the other, thereby improving visibility, avails real-time data within the firm and with outside suppliers, customers, and channels, and also helps logistics companies redesign their processes in a bid to achieve competitive advantage and sustainability [1].

However, an article by [3] laments that digitising the sector exposes different stakeholders to ransomware attacks, sabotage, intellectual property theft, and malware that breach the sector's agility and resilience [18]. While it is acknowledgeable that the Sultanate of Oman's Logistics sector has made significant strides in modernising its digital infrastructure, a research article by [23] asserts that the sector is vulnerable and less resilient to cybersecurity and privacy attacks. Studies have indicated that the Omani logistics networks are highly vulnerable because of third-party vendor compromises, outdated and unpatched systems, routine data breaches, embedded hardware flaws, inadequate cybersecurity knowledge and cultures among the Omani workforce, and various insider threats [23]. The literature review assesses the current cybersecurity standards and frameworks and implementation measures to help address the challenges imposed by cybersecurity issues in Oman. It also discusses how cybersecurity employee training and awareness programs help improve cybersecurity compliance and incidence and recovery times to help foster logistic network cybersecurity agility and resilience.

3.1. Implementation of Cybersecurity Measures

New cybersecurity issues have emerged in the logistics industry that have also jeopardized the integrity and security of critical supply chain data. [1] highlights that the 2017 NotPetya malware attack on Maersk's IT systems resulted in various supply chain disruptions, financial losses, and damage to the firm's reputation. Logistics companies are implementing various measures that can protect their companies and IT systems from such attacks. [2] assert that logistics companies are rapidly deploying cryptography and encryption technologies to code information to prevent information from landing in the wrong or unintended hands. Logistics companies have robust training and awareness, firewalls, antivirus software, encryption, automatic updates, and multifactor authentication measures to make these logistics technologies more secure against cyberattacks [1, 2]. Cybersecurity policies help protect digital supply chains by establishing acceptable and safe internal system use, outlining procedures that can identify and report threats, establishing regular updates, and providing software system patches [3]. These policies and measures inform the use of identity and access management (IDP) systems, role-based access control, and least privilege access. [3] holds that logistics companies can also physically secure their network infrastructure by having locked cabinets, deploying encrypted connections, and routinely updating firmware. Similarly, they can complement their passwords with Multifactor Authentication (MFA) like secret codes, cards, or statements [2]. Scholars also call for intensive employee training on security, cybersecurity software investment, backing up vital data, and monitoring and evaluating the entire cybersecurity process [4].

Therefore, it is prudent for logistics industries to conduct Cybersecurity Audits (CSA) to help logistics firms review their organizational cybersecurity policies, risk management, internal controls, data confidentiality, integrity, and availability (CIA) and their susceptibilities to make informed decisions about cybersecurity governance [4]. However, these scholars also acknowledge that conducting CSA is challenging because logistics companies must follow a lack of official schedules to conduct audits. According to [5], companies must conduct CSA audits at least once annually. Interestingly, despite all these cybersecurity risks in the logistics industry, scholars like [6] lament that logistics and supply chains have significantly underinvested in logistics cybersecurity. There is an estimate that cybercrime consumes about 445 billion US Dollars annually globally. [7] add that there is a trade-off for logistic companies when making investment decisions concerning cybersecurity because most are resource-constrained and cannot make considerable investments in cybersecurity.

3.2. Cybersecurity Employee Training and Awareness

Organizations with regular cybersecurity and awareness programs often experience a 70% reduction in security-related incidents [8]. According to [9], the supply chain and logistics industry designs cybersecurity training programs to help identify and manage risk and strengthen project management by having the necessary potential risk forward plans and risk mitigation strategies. Conversely, [10] asserts that it is unfortunate that despite the significant growth in logistics cybersecurity concerns, there are still limited awareness levels in the logistics sector. This comes in the form of low cybersecurity skill shortage even as late as 2020 when COVID-19 struck and compelled logistics firms to have robust cybersecurity staff. Training and raising awareness levels among the logistic industry workforce has been evidenced to help the team recognize and understand how to assess and mitigate the available risks and the impacts they can have on their performance levels and broader enterprise disruptions [9, 10] Training and awareness also involve teaching the logistics and supply chain staff the methodologies recommended for risk assessment, management, and risk mitigation as outlined in the RMPPM - risk management policies and procedures manual [9]. Organizations should not have a generic and fixated period on employee cybersecurity programs because they are ongoing and long-term investment plans enshrined in logistic companies' policies and guidelines [11]. The programs should review the hacking challenges, password protection, phishing identification, incident reporting, and privacy and security elements of logistics cybersecurity. [8] added that cybersecurity awareness training occurs after audits and gap analysis. Cybersecurity awareness training goes beyond protecting the firm from data breaches and attacks; it also attempts to shift employee knowledge, behaviours, and attitudes toward embracing best practices that can protect the firm's IT infrastructure [8, 11]. Scholars also remind organizations to monitor and evaluate their training and awareness programs using awareness scores indicating employees' knowledge of the recommended cybersecurity best practices. The feedback scores measure the knowledge, behaviour, and attitude perceptions before and after the training sessions [10, 11]. Moreover, these cybersecurity awareness and training programs significantly impact employee morale and job satisfaction, eventually increasing the firm's agility and resilience towards such attacks [8].

3.3. Cybersecurity Standards and Frameworks

Cybersecurity Frameworks (CSF) offer industries a common language and outline security standards that policymakers and decision-makers use across different nations, regions, and industries. Ideally, standards are the technical specifications a service facility must meet to enhance the service user's maximum function, purpose, or revenue profits from services offered [13]. The ISO/IEC CSF defines standards as documents or rules designed after a unanimous agreement following a legal entity validation vital in helping realise optimal results as a guideline or model in specific contexts [12, 13]. These CSFs and standards help in the prevention or mitigation of cyberattacks by reducing cyber threat risks. According to [12], implementing CSF and standards helps save organizational costs and time, increases profits, improves user awareness levels, minimizes risks, and offers business continuity. Further, integrating standards into logistics operations helps businesses comply with the best-formulated industry practices. [14] the article also asserts that these CSF standards help logistics firms compare their security systems against the regional or international levels. CSF and standards have significantly protected business assets and processes from cyber threats [13, 14]. These standards can be categorized as either information security standards or information security governance standards [12]. Organizations across industries use several CSFs and standards. They include the ISO/IEC series, NIST CSF, ISF SOGP, IEC, GB/T 22239, COSO, CSA CCM, ITIL, COBIT, and IASME. [13] adds that these CSFs and standards are primarily international, local, and industry-specific. Consequently, the most commonly used internationally recognised CSFs and standards are COBIT, ISO/IEC, ITIL, NIST, and COSO [14]. These scholars also claim that these CSFs and standards have specific cybersecurity components, governance structures, and certification requirements [12, 13, 14].

Additionally, [15] expounds that these CSFs, standards, and policies are applied alone to the relevant regulator areas after acceptance. Despite the striking difference in CSFs, standards, and policy components, scholars call for routine monitoring and evaluation practices to increase efficiency. For instance, [14] stated that reviewing CSFs and standards helps organizations perform gap analyses on their IT governance structures with the existing industry cybersecurity requirements. [12] also added that updating and reviewing these CSFs and standards benefits the company because of its cost-effectiveness structures and efforts to offer more resilient and uninterruptable supply chain and logistic activities. Embracing updates also shows an organization's commitment to evolving with the changing standards and continually improving its cybersecurity activities [14].

3.4. Incident Response and Recovery Planning

Logistics companies must have precise incident management and emergency management plans to provide clear guidelines that can be used to respond to data or firewall breaches, insider threats, or other general security breaches. According to [16], security incident responses occur from security threats in an existing computer system. Most attacks are realizable and lack identifiable signs from a target perspective. Thus, [17] asserts that organizations should have timely precursor detections. The Recovery Time Objective (RTO) denotes the maximum time the cybersecurity team should take to restore and access data or network after an unplanned cybersecurity disruption [19].

Consequently, the higher the RTO, the more the incident disrupts business processes and leads to revenue losses. [18] add that cybersecurity incident management significantly impacts the response and recovery plans since it identifies, manages, records, and analyses security threats or incidents. Effective incident management leads to better organizational cybersecurity incident plans and procedures. It offers a comprehensive view regarding the security issues the IT team encountered during the data breach or any incidence [18]. Scholars suggest that the CSFs and standards are crucial in designing incidence response and recovery plans. For example, the ISO/IEC standard recommends that firms should have robust incident handling preparation plans using the identify, assess, respond, and react aspects.

3.5. Conceptual Model

This model figure presents the study's independent variables as Cybersecurity Measures Implemented (H1), Employee Training and Awareness Programs (H2), Adoption of Cybersecurity Standards and Frameworks (H3), and Incident Response and Recovery Plans (H4), and the dependent variable is the Integrity of Logistics Networks.

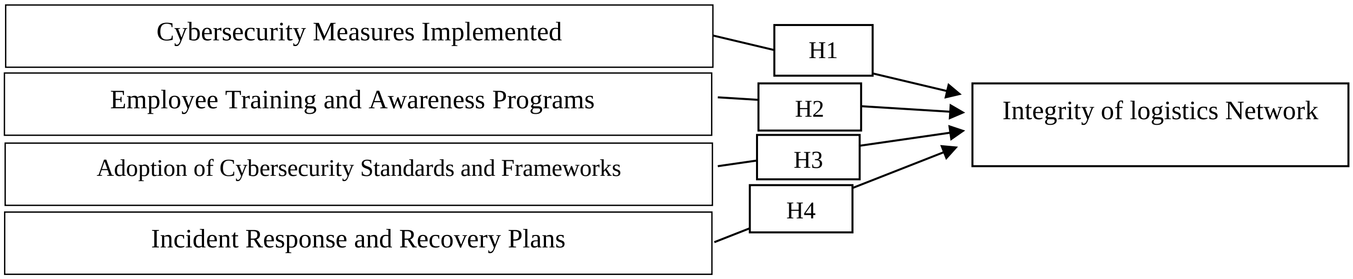
Cybersecurity Measures Implemented
Employee Training and Awareness Programs
Adoption of Cybersecurity Standards and Frameworks
Incident Response and Recovery Plans
H1
H2
H3
H4
Integrity of logistics Network

Fig. 1 Conceptual Model Diagram

Table 1. Independent variables and their measurements,

H1: Cybersecurity Measures Implemented		
Measurements		**Author / Theory**
CM1	Type of Cybersecurity Technologies Adopted	Sobb, Turnbull, and Moustafa (2020), Information Security Theory
CM2	Frequency of Security Audits	Slapničar et al. (2022), Control Theory
CM3	Level of Investment in Cybersecurity	Simon and Omar (2020), Resource-Based View Framework
CM4	Cybersecurity Policy Implementation	Masip-Bruin et al. (2021), Institutional theory
H2: Employee Training and Awareness Programs		
Measurements		**Author / Theory**
ET1	Number of Training Sessions per Year	Munene and Walter (2021), Resource Dependence Theory, Social Learning Theory
ET2	Employee Cybersecurity Awareness Level	Canepa et al. (2020), Dynamic Capability Theory
ET3	Participation Rate in Training Programs	Tolossa (2023), Expectancy Theory
ET4	Content Coverage of Training Programs	Salamah et al. (2023), Cognitive Load Theory
H3: Adoption of Cybersecurity Standards and Frameworks		
Measurements		**Author / Theory**
AC1	Certification in Cybersecurity Standards	Syafrizal, Selama, and Zakaria (2020), System Theory, Legitimacy Theory
AC2	Compliance Score	Mulugeta (2023), Regulatory Focus Framework
AC3	Implementation Level of Frameworks	Taherdoost (2022), Organizational Learning Theory
AC4	Regular Update and Review	Li and Liu (2021), Dynamic Capabilities Theory
H4: Incident Response and Recovery Plans		
Measurements		**Author / Theory**
IR1	Existence of a Formal Incident Response Plan	Zamfiroiu and Sharma (2022), Contingency Theory
IR2	Recovery Time Objective (RTO)	Naseer et al. (2023), Time-Based Competition Theory
IR3	Incident Detection Time	Blum (2020), Signal Detection Theory
IR4	Effectiveness of Incident Management	Patterson, Nurse and Franqueira (2023) Organizational Resilience Theory

4. Methodology

The present study incorporates both insights from quantitative and qualitative research elements to help unearth the factors impacting the effectiveness of cybersecurity in the logistics networks of the Sultanate of Oman. The quantitative literature review helped build the conceptual framework by analysing what previous researchers and studies had to say regarding the cybersecurity enhancement initiatives in Oman's Logistics Networks. Additionally, the researchers interviewed IT experts and firms operating in the field of logistics and supply chain and sent questionnaires to professionals working in the various IT departments of major logistics companies across Oman.

4.1. Population and Sample

The study's target population includes critical stakeholders in Oman's logistics sectors, such as IT professionals, IT managers, logistics network operators, and top-level managers working in different companies across the Sultanate in the logistics sectors. Moreover, the study stratified the sample as either industry experts or logistics professionals. For instance, logistics professionals included logistics coordinators, supply chain management policymakers, and IT support staff to ensure that the population and sample are representative and diverse. Conversely, Industry players included IT managers, climate professionals, and the general consumers selected according to their expertise, professional experiences, and involvement in cybersecurity decision-making. The study targets a sample of 70 participants, with 60 participating in questionnaire research and 10 participating in the interview sessions.

4.2. Data Collection, Analysis and Presentation

The semi-structured interviews with the selected ten experts were conducted according to the participant's feasibility and preferences of either utilising online videoconferencing platforms or through one-on-one physical sessions, with the individual interview sessions taking between 15 and 30 minutes. The major interview focused on the cybersecurity challenges witnessed in Oman's Logistics Networks and the evidence-based measures the companies are leveraging to tackle the existing gaps. On the other hand, the structured questionnaires collecting quantitative data were sent to the 60 participants, and again, they were filled out according to the participant preferences, with others preferring to complete them online rather than filling them in person. According to [20], all data collected from the field must be cleaned because all the collected data from the field cannot achieve accuracy or usefulness. The researchers sorted and charted all the data collected and ensured there were no duplications and that they were consistent, accurate, and complete. All qualitative findings were thematically analysed and coded based on the identified recurring themes [20]. However, all the quantitative data was statistically analysed to highlight the relationships between the variables. The researchers analysed and presented the data collected using Microsoft Excel and Google Forms tools. All quantitative results are presented in tables and graphs, while qualitative results are presented narratively [21]. According to [22], reliability in research assesses the truthfulness of the data collected and the extent to which the measuring tools control random error. On the other hand, a study's validity reviews what instruments measure and how well they do it. The researchers ensured that the collected data through the said instruments met the reliability and validity criteria to help ascertain that the data used for the study are sound and replicable and that the study results exhibit high levels of accuracy.

4.3. Ethical Consideration

Ethical considerations are vital for research processes because the concept helps uphold participant rights and well-being. The researchers ensured that the participants filled out informed consent forms detailing the study procedures, details, and all the benefits they could accrue from the research. Additionally, the researchers upheld data security, confidentiality, and anonymity, ensuring that the participants were not coerced to participate in the study.

5. Results

5.1. Interview Results

The interviews provided insights into the types of cybersecurity technologies adopted, the frequency of security audits, the level of investment in cybersecurity, and the implementation of formal cybersecurity policies. Additionally, the interviews explored employee training and awareness programs, adopting cybersecurity standards and frameworks, and the effectiveness of incident response and recovery plans. The following points summarize the key findings from the 10 interviews conducted.

5.1.1. Cybersecurity Measures Implemented

The logistics companies in Oman have implemented various cybersecurity technologies, including Firewalls, Antivirus software, Encryption technologies, and Intrusion Detection Systems (IDS). Advanced measures such as Multifactor Authentication (MFA) and Security Information and Event Management (SIEM) are also in place. The measures comprehensively help protect firms from all types of risks. Security audits are conducted annually to ensure the effectiveness of these measures. Despite the importance of cybersecurity, less than 5% of the IT budget is allocated to it, indicating a need for increased investment. Formal cybersecurity policies are in place and rated as comprehensive by the respondents.

5.1.2. Employee Training and Awareness Programs

Employee training is a crucial aspect of cybersecurity in Oman's logistics sector. Most companies conduct 1-2 training sessions per year. Before these sessions, the cybersecurity awareness level among employees was generally low, rated at 2 out of 5. However, post-training, this awareness significantly improves to a level of 4. Participation in these training programs varies, with 26% to 50% of employees attending. The training content covers essential topics such as phishing, secure password practices, handling sensitive data, and identifying and reporting security threats.

5.1.3. Cybersecurity Standards and Frameworks Adoption

Cybersecurity standards and frameworks adoption among logistics companies in Oman is on the rise. Many companies are certified in ISO/IEC 27001. Compliance with these standards is rated at 4 on a scale of 1 to 5, indicating high adherence. Cybersecurity frameworks are partially implemented, with annual reviews and updates, to keep up with evolving threats and ensure continuous improvement in cybersecurity practices.

5.1.4. Incident Response and Recovery Plans

Formal incident response plans are a standard among logistics companies in Oman, ensuring preparedness for potential cybersecurity incidents. These plans typically define a Recovery Time Objective (RTO) of 24-48 hours for critical systems, essential for minimizing downtime and maintaining operational continuity. The detection time for cybersecurity incidents usually falls within 1 to 24 hours. The effectiveness of incident management processes is rated as effective, reflecting a well-coordinated approach to handling and mitigating incidents promptly.

5.2. Questionnaire Results

This section presents the findings from the questionnaire distributed to logistics companies in Oman. The questionnaire aimed to gather quantitative data on the logistics sector's cybersecurity practices, challenges, and opportunities.

Dependent Variable (DV):

- Integrity of Logistics Networks
- M1: Frequency of Cybersecurity Incidents: Count the number of cybersecurity incidents reported within a specific timeframe.
- M2: Severity of Cybersecurity Incidents: Assess the impact of incidents on operations using severity levels.
- M3: Incident Response and Recovery Metrics: Measure effectiveness and efficiency of response efforts.
- M4: Customer Satisfaction and Trust: Gauge post-incident customer sentiment and trust levels.
- M5: Financial Impact: Quantify direct and indirect financial losses from incidents.

Table 2. Reliability and validity construct

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
Cybersecurity Measure	0.859	0.880	0.903	0.699
Cybersecurity Standards and Framework	0.852	0.919	0.893	0.679
Employee Training and Awareness Program	0.881	0.886	0.918	0.737
Incident Response and Recovery Plans	0.912	0.914	0.939	0.794
Integrity of LogisticsNetworks	0.942	0.945	0.958	0.852

Table 3. Fornell-Larcker criterion

	Cybersecurity Measure	Cybersecurity Standards and Framework	Employee Training and Awareness Program	Incident Response and Recovery Plans	Integrity of Logistics Networks
Cybersecurity Measure	0.836				
Cybersecurity Standards and Framework	0.263	0.824			
Employee Training and Awareness Program	0.398	0.573	0.858		
Incident Response and Recovery Plans	0.289	0.496	0.628	0.891	
Integrity of Logistics Networks	0.191	0.395	0.426	0.657	0.923

The reliability and validity of measurements are crucial factors in research, ensuring accurate and credible results. The data presented demonstrates robust reliability and validity across several constructs, such as cybersecurity, employee training, incident response, and logistics network integrity. Cronbach's alpha values consistently exceed 0.7, indicating high internal consistency among items within each construct.

Moreover, the composite reliability measures (rho_a and rho_c) and average variance extracted (AVE) values are significantly high, further validating the measurement instruments' robustness. These results suggest that the scales effectively capture the intended constructs, enhancing the credibility and applicability of research findings in logistics, supply chain, and related fields. The Fornell-Larcker criterion is used in checking measurement models' discriminant validity. This criterion assesses the distinctiveness of the constructs, including cybersecurity measures, standards, employee training, incident response, and logistics network integrity. According to the criterion, all average variance extracted (AVE) square roots must always exceed the correlation between a construct and the other. It helps demonstrate the adequacy of the distinctiveness of these constructs. The diagonal elements representing the square roots of the AVE in the provided correlation matrix consistently exceed the off-diagonal correlations. This finding supports the robust discriminant validity of the measurement model, thereby reinforcing confidence in the distinctiveness of the constructs and the validity of the research findings in the fields of logistics, supply chain, and related disciplines.

The Heterotrait-Monotrait (HTMT) ratios in the matrix illustrate the discriminant validity among the constructs under examination. With all of the HTMT ratios falling below the recommended threshold of 0.85, the correlations between different constructs are notably lower than those within the same construct. This observation indicates that the constructs, including cybersecurity measures, standards, employee training, incident response, and logistics network integrity, are empirically distinct and effectively capture different aspects of the phenomenon. As a result, the measurement instruments utilized demonstrate satisfactory discriminant validity, which enhances confidence in the distinctiveness of the constructs and the validity of the research findings in the domains of logistics, supply chain, and related fields.

Table 4. The Discriminant Validity, Heterotrait-monotrait Ration (HTMT) - Matrix

	Cybersecurity Measure	**Cybersecurity Standards and Framework**	**Employee Training and Awareness Program**	**Incident Response and Recovery Plans**	Integrity of Logistics Networks
Cybersecurity Measure					
Cybersecurity Standards and Framework	0.354				
Employee Training and Awareness Program	0.458	0.681			
Incident Response and Recovery Plans	0.322	0.555	0.701		
Integrity of Logistics Networks	0.209	0.414	0.467	0.709	

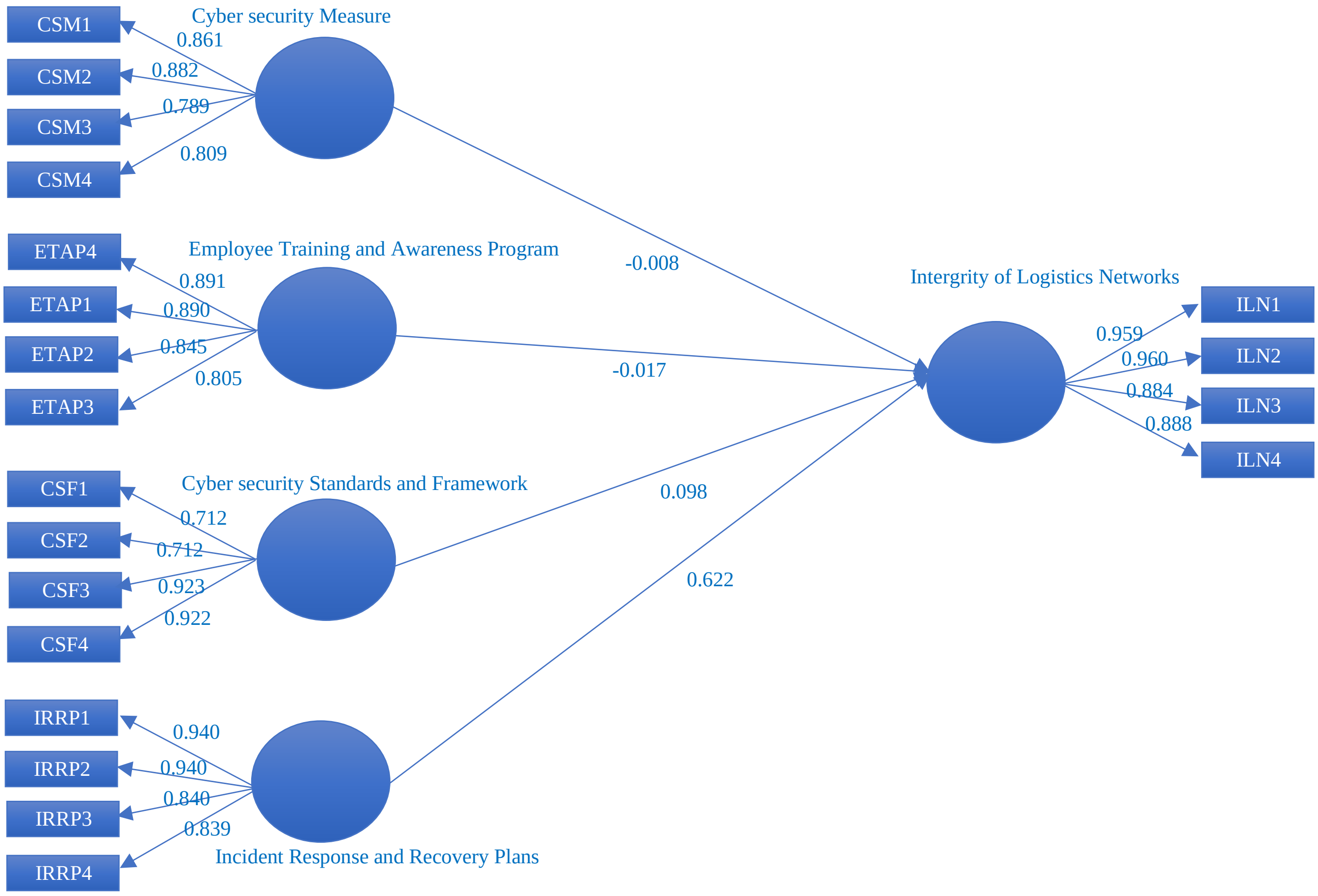

Fig. 2 Factor loading

Table 5. Outer loadings matrix

	Cybersecurity Measure	Cybersecurity Standards and Framework	Employee Training and Awareness Program	Incident Response and Recovery Plans	Integrity of Logistics Networks
CSF1		0.712			
CSF2		0.712			
CSF3		0.923			
CSF4		0.922			
CSM1	0.861				
CSM2	0.882				
CSM3	0.789				
CSM4	0.809				
ETAP1			0.890		
ETAP2			0.845		
ETAP3			0.805		
ETAP4			0.891		
ILN1					0.959
ILN2					0.960
ILN3					0.884
ILN4					0.888
IRRP1				0.940	
IRRP2				0.940	
IRRP3				0.840	
IRRP4				0.839	

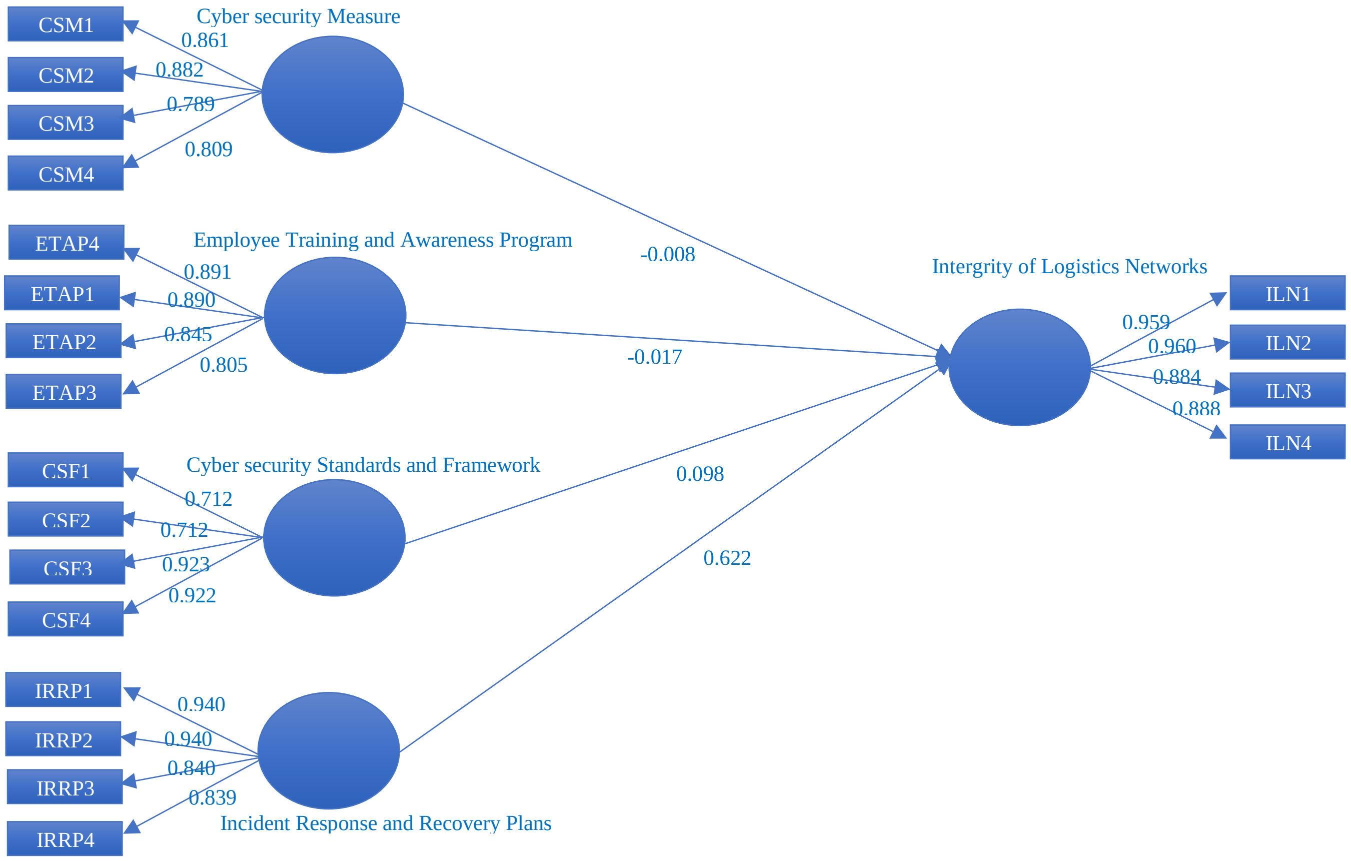

Fig. 3 Factor outer loading

Table 6. Total Effects – Mean STDEV, T-Values, P-Values

	Original sample (O)	**Sample mean (M)**	**Standard deviation (STDEV)**	**T statistics (|O/STDEV|)**
Cybersecurity Measure -> Integrity of Logistics Networks	-0.008	0.001	0.042	0.185
Cybersecurity Standards and Framework -> Integrity of Logistics Networks	0.098	0.100	0.081	1.203
Employee Training and Awareness Program -> Integrity of Logistics Networks	-0.017	-0.018	0.073	0.235
Incident Response and Recovery Plans -> Integrity of Logistics Networks	0.622	0.621	0.077	8.024

The strength of the connection between each indicator and its corresponding latent construct in a structural equation model is represented by the other loadings in the matrix table above. The outer loadings consistently display strong associations with the indicators for all five constructs, including cybersecurity standards and framework, cybersecurity measures, employee training and awareness programs, incident response and recovery plans, and integrity of logistics networks. The outer loadings vary between 0.712 and 0.960, indicating that the indicators effectively measure their respective constructs. This further validates the measurement model and helps foster the study findings' reliability in the fields of logistics, supply chain management, and related disciplines.

The following information presents the collective impact of various factors, namely Cybersecurity Measures, Cybersecurity Standards and Framework, Employee Training and Awareness Development Initiatives, and Incident Response and Recovery Plans, on the Integrity of Logistics Networks. The provided data illustrates the average impact of each factor on the Integrity of Logistics Networks, as indicated by the mean values. Moreover, the standard deviation (STDEV) reflects the extent of variability across the sample. The T statistics, which represent the ratio of the mean effect to its standard deviation, indicate the significance of the effect. A higher T value suggests a more substantial impact, while a lower T value suggests a less significant effect. For instance, the T value of 8.024 for Incident Response and Recovery Plans indicates a highly significant impact on the Integrity of Logistics Networks. Conversely, lower T values for other factors suggest comparatively weaker effects. Additionally, p-values, which are not explicitly provided here, would typically accompany T statistics to determine the statistical significance of the impact.

In conclusion, Incident Response and Recovery Plans have the most substantial and statistically significant impact on the Integrity of Logistics Networks, followed by Cybersecurity Standards and Framework. In contrast, the impact of Cybersecurity Measure and Employee Training and Awareness Program appears less significant. The findings also underscore the different elements of Oman's Logistic sector cybersecurity, detailing the current positions, challenges encountered, and the most viable recommendations that can improve cybersecurity integrity. It is worth acknowledging that the study's robust, comprehensive mixed-methodology approach and country-specific focus make it easily applicable and transferable to the different Logistics companies of the Sultanate. Besides, most existing literature heavily focuses on technical solutions and frameworks without touching on cybersecurity's human and firm-based dimensions. However, the present study evidences various stakeholders' perspectives, including IT professionals, the logistics workforce, customers, and other vital industry players. This helps expound why some variables have significantly more substantial impacts on Logistics Networks than others since the results show an interesting relationship between organisational practices, technology, and human factors.

6. Conclusion

Critical Role of Incident Response and Recovery Plans: The study conclusively finds that having robust incident response and recovery plans significantly enhances logistics networks' integrity. This suggests that logistics companies in Oman should prioritize developing and implementing comprehensive incident management strategies to mitigate cybersecurity risks effectively. Importance of Cybersecurity Standards and Frameworks: While not as impactful as incident response and recovery plans, cybersecurity standards and frameworks still are still vital in upholding the logistic networks' integrity. Adopting internationally recognized standards and frameworks can provide a structured approach to managing cybersecurity risks. Relative Impact of Cybersecurity Measures and Training: The study indicates that cybersecurity measures and employee training and awareness programs have a lesser impact on logistics networks' integrity than other factors. However, this does not undermine their importance. Continuous improvement in cybersecurity practices and ongoing employee training are essential for creating a resilient cybersecurity posture. Recommendation for Focused Investment: Given the varying impact of different cybersecurity initiatives, logistics companies in Oman are advised to allocate resources strategically. Investments should be prioritized to develop and enhance incident response and recovery capabilities, along with adopting relevant cybersecurity standards and frameworks. Need for Oman-specific Cybersecurity Guidelines: The study highlights the necessity for Oman-specific cybersecurity guidelines and best practices. Tailoring cybersecurity measures to the local context can address unique challenges the Omani logistics sector faces and ensure more effective protection against cyber threats. Ongoing Evaluation and Adaptation: The dynamic nature of cyber threats requires that logistics networks in Oman continuously evaluate their cybersecurity measures and adapt to emerging challenges. Regular audits, threat assessments, and updates to cybersecurity policies should be integral components of their cybersecurity strategy.

Recommendations

Implement Robust Cybersecurity Measures: Oman logistics companies should adopt advanced cybersecurity technologies, including encryption and cryptography, to protect sensitive data and IT systems against cyber threats. Also, Conduct Regular Cybersecurity Audits: Organizations should routinely conduct cybersecurity audits to evaluate their cybersecurity policies, risk management, and internal controls. This will help identify vulnerabilities and areas for improvement in their cybersecurity practices. Enhance Employee Training and Awareness: Developing comprehensive employee training and awareness programs is critical. These programs should cover risk assessment, management, mitigation strategies, and best practices for cybersecurity, aiming to build a culture of cybersecurity awareness within the organization. Adopt International Cybersecurity Standards and Frameworks: Adopting and complying with internationally recognized cybersecurity standards and frameworks can help logistics companies in Oman align with best practices and improve their cybersecurity posture. Update and Review Cybersecurity Practices Regularly: Logistics companies should commit to continuously reviewing and updating their cybersecurity measures and policies to adapt to evolving cyber threats and technologies. Invest in Cybersecurity Infrastructure: Despite resource constraints, logistics companies must prioritize investments in cybersecurity infrastructure to protect against cyber incidents' financial and operational impacts. Develop Incident Response and Recovery Plans: Formal incident response and recovery plans will ensure that companies are prepared to respond to and recover from cybersecurity incidents effectively, minimizing potential disruptions and losses.

Funding Statement

The Research Council Oman funded the research and publication of this article under Grant Number [BFP/GRG/EI/23/178]

Acknowledgments

Ali al Kalbani and Hajer al Kalbani contributed equally to this work. The researchers are massively grateful to everyone who helped complete this study, especially those interviewed and those who responded to the questionnaire.

References

[1] Gabriela Ioana Enache, "Logistics Security in the Era of Big Data, Cloud Computing and IoT," *Proceedings of the International Conference on Business Excellence*, vol. 17, no. 1, pp. 188-199, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Theresa Sobb, Benjamin Turnbull, and Nour Moustafa, "Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions," *Electronics*, vol. 9, no. 11, pp. 1-31, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Xavi Masip-Bruin et al., "Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture," *Sensors*, vol. 21, no. 18, pp. 1-24, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Sergeja Slapničar et al., "Effectiveness of Cybersecurity Audit," *International Journal of Accounting Information Systems*, vol. 44, pp. 1-21, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Mário Antunes, Marisa Maximiano, and Ricardo Gomes, "A Client-Centered Information Security and Cybersecurity Auditing Framework," *Applied Sciences*, vol. 12, no. 9, pp. 1-15, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Jay Simon, and Ayman Omar, "Cybersecurity Investments in the Supply Chain: Coordination and a Strategic Attacker," *European Journal of Operational Research*, vol. 282, no. 1, pp. 161-171, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Sebastian Heierhoff, and Nils Hoffmann, "Cybersecurity vs. Digital Innovation: A Trade-off for Logistics Companies?," *Proceedings of the 55th Hawaii International Conference on System Sciences*, pp. 1-10, 2022. [Google Scholar] [Publisher Link]

[8] Dawit Negussie Tolossa, "Importance of Cybersecurity Awareness Training for Employees in Business," *Vidya - A Journal of Gujarat University*, vol. 2, no. 2, pp. 104-107, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Munene Hellen Muthoni, and Karungani Walter, "Effect of Risk Management Strategies on Supply Chain Performance of Cybersecurity Firms in Kenya," *International Journal of Strategic Management*, vol. 4, no. 2, pp. 407-420, 2021. [Google Scholar] [Publisher Link]

[10] Monica Canepa et al., "Effectiveness of Cybersecurity Training and Awareness Raising within the Maritime Logistics Domain," *DEVPORT International Conference*, 2020. [Google Scholar] [Publisher Link]

[11] Fai Ben Salamah et al., "An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work," *Applied Sciences*, vol. 13, no. 17, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Hamed Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards-A Review and Comprehensive Overview," *Electronics*, vol. 11, no. 14, pp. 1-20, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Melwin Syafrizal, Siti Rahayu Selamat, and Nurul Azma Zakaria, “Analysis of Cybersecurity Standard and Framework Components,” *International Journal of Communication Networks and Information Security*, vol. 12, no. 3, pp. 417-432, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Henock Mulugeta Melaku, “A Dynamic and Adaptive Cybersecurity Governance Framework,” *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 327-350, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Yuchong Li, and Qinghui Liu, “A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments,” *Energy Reports*, vol. 7, pp. 8176-8186, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Alin Zamfiroiu, and Ramesh C Sharma, “Cybersecurity Management for Incident Response,” *Romanian Cyber Security Journal*, vol. 4, no. 1, pp. 69-75, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Ayesha Naseer et al., “Moving Towards Agile Cybersecurity Incident Response: A Case Study Exploring the Enabling Role of Big Data Analytics-Embedded Dynamic Capabilities,” *Computers and Security*, vol. 135, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Clare M. Patterson, Jason R.C. Nurse, and Virginia N.L. Franqueira, “Learning from Cyber Security Incidents: A Systematic Review and Future Research Agenda,” *Computers and Security*, vol. 132, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Dan Blum, *Institute Resilience through Detection, Response, and Recovery*, Rational Cybersecurity for Business, pp. 259-295, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] Hamed Taherdoost, “Data Collection Methods and Tools for Research; a Step-by-Step Guide to Choose Data Collection Technique for Academic and Business Research Projects,” *International Journal of Academic Research in Management*, vol. 10, no. 1, pp. 10-38, 2021. [Google Scholar] [Publisher Link]

[21] Judith Schoonenboom, and R. Burke Johnson, “How to Construct A Mixed Methods Research Design,” *KZfSS Cologne Journal for Sociology and Social Psychology*, vol. 69, pp. 107-131, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[22] Haradhan Mohajan, “Two Criteria for Good Measurements in Research: Validity and Reliability,” *Annals of Spiru Haret University. Economic Series*, vol. 17, no. 4, pp. 56-82, 2017. [Google Scholar] [Publisher Link]

[23] Ashraf Mishrif, Alessandro Antimiani, and Asharul Khan, “Examining the Contribution of Logistics and Supply Chain in Boosting Oman's Trade Network,” *Economies*, vol. 12, no. 3, pp. 1-25, 2024. [CrossRef] [Google Scholar] [Publisher Link]