Enhancing Cyber Security Resilience in the Industrial Sector: A Comprehensive Framework for Third-Party Risk Management

***Nadir Aliane*[1*]**
King Faisal University, Saudi Arabia

***Ahmad Zakariya*[2]**
National University of Modern Languages, Lahore Campus

Abstract

The objective of this study is to address the increasing cyberthreats in the industrial sector, particularly those originating from third-party links. The study aims to develop a comprehensive framework for effectively mitigating cyber risks in external relations, specifically through Third Party Risk Management (TPRM). This approach will increase the overall flexibility of industrial systems. In Saudi Arabian organisations, employees were asked to submit their responses related with the operation management division, especially in the domains of supply chain management, procurement, contracting, and IT. A total of 300 questionnaires were gathered, 215 of them being used for the analysis. The data was examined using Structural Equation Modelling (SEM) with Amos. The research findings offer valuable insights into the weaknesses and problems associated with third party engagements. The study centres on the industrial environment and disclose the key factors that significantly influence cybersecurity resilience. A thorough framework has been created to deal with risks discrepancies, draw attention to specific risks, and increase overall resilience based on these results. The part that deals with synthesis of this studies emphasize on the importance of immediate actions and practicing incident response as preventive tactics against cyber threats connected to third-party relationships. This framework focus on its development of a thorough and developing landscape of Third-Party Risk Management. The methodology contains the procedure for cutting down or avoiding an attack and the safety measures for any possible occurrence in the industrial sector. This new technique is applied in the sector so as to eliminate the threat that is proliferating; therefore, it is of great value to the domain.

[1] Department of Management, School of Business, King Faisal University, Al-Ahsa 31982, Saudi Arabia. Email: nhaliane@kfu.edu.sa
[2] Department of Management Sciences, National University of Modern Languages, Lahore Campus. Emails: aaazakariya@numl.edu.pk

Keywords: Industrial Cybersecurity, Critical Infrastructure Protection, Cyber Threat Intelligence, Supply Chain Security, Incident Response Strategies, Cybersecurity Framework.

Introduction

The advancement of digital technology in the industrial sector has added efficiency, connectivity, and operational capability to a fast-changing scenario. However, with digitization being implemented, the risk of cyber threats to the organisation makes it vulnerable. Such risks deserve an advanced strategy in order to safeguard essential resources. It's indispensable in such a context to consider the Cybersecurity Resilience Score (CRS), which exhibits the intricate network of third-party entities that often affect the industry ecosystem. This framework further delves into the strategic management of risks connected with third-party industrial relationships and focuses on designing a flexible organisation. The study focuses on the significance of both structure and adaptability. The initial focus is on the genuineness of cyber resilience policies, especially in dealing with risks from third parties in the industrial sector. Haque et al. (2018) framework further examines the need for more research on cyber resilience within ICSs, emphasising the specific aspects of her work that deal with this task. This aspect is so crucial because external dependencies have the capacity to showcase security vulnerabilities (Keskin et al., 2021).

The study by Lykou, Anagnostopoulou, and Gritzalis (2018) explains how self-assessment tools were found to be helpful in enabling organisations to regularly scrutinise their security levels for any potential vulnerabilities in their systems. Based on Luiijf and Klaver (2015) paper, the author examines the various cyber security threats that threaten both enterprises and society. Hence, when businesses focus on third-party vendors, partners, and service providers to develop their operations, any failures can result in serious concerns. These endeavours focus on addressing intricate cybersecurity resilience challenges through the identification of properties, threat modelling, vulnerability assessments, regulatory compliance, and the improvement of collaborative information sharing. These elements are noteworthy for companies to increase their cyber security, mitigate risks related to third-party relationships, and promote a solid foundation to face the intricacies of cyberattacks in this on-going world.

Industrial cybersecurity needs an effective approach that involves thorough adaptability. Saeed et al. (2023) proposes that the use of CTI can efficiently foster cyber security measures. Whereas Putra et al. (2023b) suggests the use of ISO 27005:2018 and NIST SP 800-30, especially for information security risk management. IIoT has taken a proactive approach to addressing this matter (Buja, Apostolova, & Luma, 2023). In his study, Alqudhaibi et al. (2023) demonstrates the process of identifying network vulnerabilities and their potential for exploitation. Numerous studies have been conducted on resilience in various industries. In a recent study, Ouyang, Chen, and Cao (2024) presents a secure key-insulated signature mechanism that aims to enhance data credibility in the context of the Industrial Internet of Things (IIoT). In his study, Khan (2024) examines the impact of supply chain ambidexterity and agility on the resilience of manufacturing and industrial supply networks. A study conducted by Alassuli (2024) examines the influence of

environmental accounting on corporate social responsibility within industrial enterprises, highlighting its potential to enhance productivity and achieve greater success. Zahid (2024) conducted a study on the resilience of inter-organizational networks in the red bus service. Infrastructures essential for daily life can rapidly lose their capacity to withstand simultaneous shocks.

Keskin et al. (2021) highlights the importance of robust partner cybersecurity risk assessment frameworks. Ani, He, and Tiwari (2017) study, examines the comprehensive security of the industrial vital infrastructure. Meanwhile, Corallo et al. (2022) focuses on the cybersecurity awareness of the Industrial Internet of Things. The highlighted studies highlight the significance of risk assessment, organizational learning, and knowledge building to improve the nature and level of industrial cybersecurity culture. The structure is influenced by the dedication of leaders, thorough staff training and awareness, ongoing monitoring, and the participation of external parties. During the Industrial Revolution, there was a notable increase in the implementation of Information Technology (IT) services. 4.0 has amplified the risks and threats to information systems linked to Information and Communication Technology (ICT) (Putra, Pratiwi, & Arafik, 2023a).

An effective approach to managing cyber risk involves a proactive and adaptive methodology. The application of allowance provision to danger, technology, and organized environments is discussed in a study by Melaku (2023). Implementing a strategic approach to mitigate security breaches caused by cyber threat intelligence (CTI) can greatly enhance the effectiveness of this architecture. There is a need to shift the focus from technology to socio-cultural aspects to establish a solid foundation for cybersecurity culture. Regarding the prevailing cyber threats, it is essential for human resource management training to incorporate cybersecurity awareness (Al-Dulaimi, 2023). Designing a strong cybersecurity culture can effectively handle changing cyber threats, promote employee accountability and critical thinking, and foster industrial resilience.

The following sections of this framework will deal with the strategies and practices employed by each pillar. We will also examine practical scenarios that exhibit the design of a cybersecurity culture in the industrial sector, focusing on meeting compliance standards and strengthening against advanced cyber threats. Several studies have investigated the relationship between technological culture and organisational systems. The Ouyang et al. (2024) cryptographic approach is very impressive because it enables people to guarantee data validity and integrity in the Industrial Internet of Things domains. Alassuli (2024) and Mulyani and Basrowi (2024) have found that incorporating environmental accounting into the supply chain and implementing leadership can enhance supply chain performance. This proves the positive impact of corporate social responsibility (CSR) on supply chain operations. The experiments prove the importance of cultivating a vigorous organizational culture that emphasizes ethics and sustainability. This study explores the influence of various factors on the efficacy of blockchain technology in the banking industry, specifically in Bangladesh, with a focus on UAE Islamic institutions.

First, a lot of assessments should be done when it comes to vendors so as to provide a complete framework for managing third-party risks in an industrial company. Besides, vendors should be subjected to rigorous testing to ensure that they adhere

to the standard cybersecurity procedures for conducting an audit. Vendor security evaluations included both risk evaluations and on-site visits conducted to review vendors' policies and techniques and assess if they were in line with industry standards. Sharing is thus one of the cornerstones of information- and collaboration-based TPRM, entailing real-time threat intelligence and best practice exchange between peer companies and third parties. As in SIEM systems, continuous monitoring of anomaly detection protocols is considered mandatory for the immediate discovery and location of security problems in relation to related industrial processes. Still, the project relies on addressing the challenges of fragmented coordination in incident response by designing dedicated communication channels and performing coordinated drills to counter cyberattacks.

Basically, the key aim of the study will highlight the manner in which the authenticity of the security strategies for cybersecurity, particularly issues in the industrial sector, will lay emphasis on a proactive third-party risk management (TPRM). The major objective behind Vendor Risk Management is to develop an all-inclusive Vendor Assessment Model that includes risk assessment questionnaires and audit. Such a model should be a helping factor in the making of informed decisions relating to the use of outside partners and providing responses to threats from third-party sources. Collaborative information sharing platforms along with continuous surveillance strategies significantly increase the capacity of cybersecurity in the industrial sector. The purpose of the programme is to deal with some of the challenges that emerge from raising the resilience of cyber security in the industrial systems. In such cases, the detailed and rigorous Third-Party Risk Management (TPRM) framework is therefore more needed to be designed in such a way so that such operations remain efficiently managed, and its impacts by the cyber threats are minimized. This, thus, will help in nullifying the risks and guarantee the smooth continuation of workflows.

Literature Review and Hypothesis

Vendor assessment methods, organizational culture of cybersecurity, and cyber resilience score come to be part of the assessment of vendors and are quite interrelated and complex. An organization needs to assess vendors for the establishment of robust cybersecurity frameworks within the organization. This includes a thorough assessment and scrutiny of cybersecurity practices carried out by third-party partners.

'Organizational Cybersecurity Culture' is often called shared values, beliefs, and behaviors related to cybersecurity in the organization. One of the criteria that can make organizational cybersecurity culture strong is the consistent application of strict assessment measures. It has a significant influence on the employees' cognitions and salience to cybersecurity and their agreement with the security policies, and vice versa. A positive and true cybersecurity culture generally comes with increased consciousness, increased security practices, and boosted resilience. The linkage that exists between the vendor assessment methods and the cybersecurity resilience score is not a straightforward one but is rather dictated by the organizational culture. A strong set of influences on the effectiveness of a higher cybersecurity resilience score is the integration of vendor assessment into the wide

and deep cybersecurity culture of the organization. The better the cybersecurity practices, the organization is therefore likely to have a higher cybersecurity resilience score when the assessment methods help to foster a real cybersecurity culture.

Developing a robust cybersecurity culture necessitates proper training, unwavering leadership support, and a sense of responsibility. Enhancing employee knowledge and behavior is achieved through training and awareness, while fostering a culture relies heavily on the crucial support of leadership. Enhancing employee engagement and cybersecurity investment can be achieved through auditing compliance, involving employees in policy design, and recognizing responsible behavior. The report indicates that companies facing cyberattacks have a low level of cyber resilience. They have a limited use of cybersecurity frameworks and lack proper prevention, detection, and recovery procedures. Although there is no direct link between cybersecurity roles and frameworks and the reduction of breaches, investigations, or penalties, implementing robust preventive, detection, and recovery methods can help mitigate these risks. According to a study conducted by Tsen, Ko, and Slapnicar (2022), improving organizational responses can heighten the severity of breaches, but it does not have an impact on investigations, fines, or penalties. The report highlights the challenge of validating qualitative cyber resilience assessment approaches. The assessment approaches for cyber resilience have developed in a manner similar to the methodologies used for assessing infrastructure resilience. The authors present a novel approach for enhancing cyber resilience analysis through a hybrid infrastructure resilience assessment (Vugrin & Turgeon, 2014).

The report discusses the increase in cybercrime and vulnerabilities observed during the COVID-19 pandemic. It also presents the campaign's findings, which revealed shortcomings in security awareness and led to the development of targeted training programmes (Ahmad, Johnson, & Storer, 2015). The study focuses on identifying key human-related security features, developing a security model that can be applied across different domains, creating a tool for evaluating security culture, and adapting the model for various application domains. The paper concludes by applying their instrument to security-critical areas and making a valuable contribution to cybersecurity research through a deeper understanding of the human aspect (Georgiadou, Michalitsi-Psarrou, & Askounis, 2022). The absence of a cohesive approach to cyber resilience has resulted in the fragmentation of the growing body of literature. The paper discusses the process of establishing, assessing, and maintaining cyber resilience within an organisation through the use of knowledge-based cyber security management (Annarelli, Nonino, & Palombi, 2020).

H1: *Organizational Cybersecurity Culture mediated the relationship between Vendor Assessment Methods and Cybersecurity Resilience Score.*

The relationship between CISPs, OCSC, and CSR highlights the complex nature of cybersecurity management. Collaborative Information Sharing Platforms serve as intermediaries that facilitate the exchange of cybersecurity knowledge among different internal and external stakeholders. However, the current OCC has a significant impact on their viability. The extent of employee collaboration using tools can be modified based on the values and behaviours of the organisation. Healthy cybersecurity practice involves information sharing that stem from ordinary human

impulse, when it is seen as positive and desirable culture. Petrenj, Lettieri, and Trucco (2013) highlights the importance of information sharing and collaboration in enhancing the effectiveness of crisis response, especially in the context of critical infrastructure protection and resilience.

In their recent publication, Trocoso-Pastoriza et al. (2022) presents a framework that addresses the imperative need for secure threat intelligence sharing. This framework plays a pivotal role in bolstering cybersecurity resilience. This framework is highly effective in fostering a collaborative cybersecurity culture by utilising privacy-preserving technologies and federated processing. The relationship between organisational cyber resilience and the outcomes of cyberattacks was explored by Tsen et al. (2022) in a recent study. The findings revealed that when organisations show resilience characteristics, they are more likely to handle the issues of stakeholders related to the aftermath of attacks. In another study carried out by Yoo, Goo, and Rao (2020), he emphasises the importance of workgroup mechanisms, specifically collective efficacy and security knowledge coordination, influencing the association between individual self-efficacy and workgroup information security effectiveness. According to Zuhroh et al. (2024), the influence of organisational culture and employee training on performance is noted. This study indicates the strong influence of the sharing economy on the usage of management accounting systems. Need for Collaborative information sharing platforms to decide on the strategy score of an organisation's overall cyber security resilience Such extensive use of these channels ensures detection of threats in time, and reaction to incidents from the very start is rather quick, so a strong cyber defence is being built. Besides, the organisation's cybersecurity culture plays a mediating role between the platforms for collaboration and their performance in the Cyber Resilience Score. The efficiency of information sharing also depends on the language used to share it, and hence on the overall fostering of the cybersecurity stance.

H2: *Organizational Cybersecurity Culture mediated the relationship between Collaborative Information Sharing Platforms and Cybersecurity Resilience Score.*

The efficacy of cyber-management depends on the correlation between Continuous Monitoring Strategies, Organisational Cybersecurity Culture, and Cybersecurity Resilience. Continuous monitoring strategy relates to continuous surveillance and an assessment of the security strategy of the organization in the information systems. It therefore allows for the timely detection of the threats that may emanate from the information system. It is, therefore, suggested that Organisational Cybersecurity Culture would sit at the core of the central factor between the monitoring strategies and the effect on the Cyber Resilience Scores. Influenced by such dimensions as cyber strategy, competent personnel, efficient communication (Vasudevan, Piazza, & Carr, 2022). The degree of cyber resilience varies upon unique attributes of an organization like its sector, size, and level of digital integration (Tsen et al., 2022).

For improved organisational resilience, it is advisable to adopt a cybernetic approach that aligns governance and management models with the organization's purpose and strategic direction (Zouave et al., 2020). Senior management must be

aware of the importance of cyber resilience, as different managerial groups may have varying preferences for approaches to address these challenges (Bagheri, Ridley, & Williams, 2023). Therefore, it is crucial to ensure that the implementation of continuous monitoring strategies for cybersecurity resilience does not negatively impact employee well-being. In a study carried out by Owens et al. (2024), the effectiveness of a brief 3-minute mindful breathing intervention in enhancing the resilience of psychiatric mental health nurses was demonstrated. In a study performed by Zahid (2024), the detrimental effects of routine disruptions on inter-organizational systems were emphasised. It was found that disturbance co-occurrence is inversely related to the resilience of critical infrastructure. Despite the benefits of Continuous Monitoring Strategies in mitigating cyber threats in real-time, there are instances where this approach proves ineffective. However, the effectiveness of these approaches is heavily influenced by the cybersecurity culture within the organisation. The shared values and beliefs regarding cybersecurity have an impact on how engaged employees are in using continuous monitoring tools and how they respond to the information obtained from these tools.

H3: *Organizational Cybersecurity Culture mediated the relationship between Continuous Monitoring Strategies and Cybersecurity Resilience Score.*

The interplay between various factors, including Incident Response Collaboration, becomes crucial in safeguarding organisational assets from cyber threats. Incident Response Collaboration is the collaborative work and communication among different stakeholders within an organisation against cybersecurity incidents. As per the argument made, organisational cybersecurity culture has a pivotal role to play in establishing the link between the key variables, viz., incident response collaboration and the cybersecurity resilience score. This is because conflicting priorities and issues pertaining to communication and coordination can act as barriers to the competence of incident response collaboration (Malviya et al., 2011). It is, therefore, important to face such challenges and design a healthy cybersecurity culture to embrace an organisation's resilience against any cyber threat. Though the development of such a culture can be imposed on difficulties, neat communication, coordination, and cooperation play an imperative role (Ioannou, Stavrou, & Bada, 2019). Correspondingly, Riebe, Kaufhold, and Reuter (2021) study also adds weight to the necessity to further enhance collaborative practices within Computer Emergency Response Teams (CERTs) to ensure their effective coping with these challenges.

In another piece of research, Saeed et al. (2023) delves into the role of cyber threat intelligence in promoting the taking of precautionary measures against security breaches, propounding a framework for its implementation. Similarly, in their research, Woods et al. (2023) proceeds to examine the influence of cyber insurance and breach attorneys on incident response, highlighting a strong collaboration with involved stakeholders. Dornheim and Zarnekow (2023) presents a pragmatic strategy for assessing and enhancing cybersecurity culture maturity by presenting the execution of the framework in a realistic contextual setup. Collaboration in incident response is very significant as it goes along the way of effective mitigation of cybersecurity incidents. Organisational cybersecurity culture notably influences the level of collaboration within organisations during incident response. Shared

organisational values, attitudes, cybersecurity culture, and behaviours notably influence the coordination of operations among individuals and teams in moments of heightened stakes.

H4: *Organizational Cybersecurity Culture mediated the relationship between Incident Response Collaboration and Cybersecurity Resilience Score.*

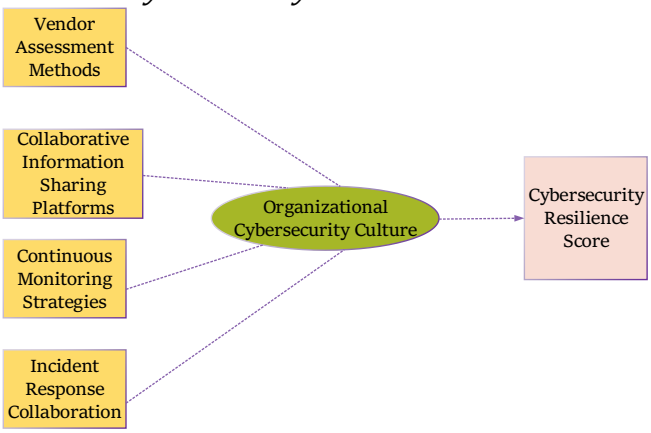

Figure 1: Conceptual Framework.

Methodology and Data Sampling

The interviews were conducted among the operational management, supply chain management, procurement, contracts, IT, and related employees in Saudi Arabia. A well-crafted questionnaire was used to collect data on factors that have been identified in the research objectives. 300 questionnaires were issued to create comprehensive, representative data since the people are so diverse. A total of 215 surveys were done, and this brought out a strong database for analysis. The study, therefore, made use of structural equation modelling (SEM), with the choice of the Amos software for the analysis being based on the accuracy with which it handles simple and advanced analytical techniques. Structure equation modelling (SEM) is important as it helps an organisation that is involved in supply chain management, procurement, contracts, and IT departments evaluate the complex interrelationships among variables. In this regard, the Amos programme helps in the tracing of the correlations that exist between the different variables. This method was an indication of carefulness in the way the researchers employed it to scrutinise all the details so as to have a complete comprehension of the underlying problems in operation management. The findings of this research have been supported by the meticulousness and data collected, which are coupled with the advanced analysis tools.

Factor Loadings Reliability, Convergent Validity

Table 1 provides a summary of factor loadings, reliability coefficients, and convergent validity metrics for each latent variable. The Vendor Assessment Methods factor had an internal consistency reliability at a high level of 0.837 (α). The Average Variance Extracted (AVE) has a value of 0.69, revealing a strong level of convergent validity. Also, the Composite Reliability (CR) is 0.754. The Cronbach's coefficient alpha of 0.733 and a robust alpha value of 0.791 indicate that the construct "Collaborative Information Sharing Platforms" shows a high value. The construct's

high AVE of 0.63 shows its strong convergent validity, which guarantees an accurate measurement of the latent variable. The latent variable "Continuous Monitoring Strategies" has a CR value of 0.822, and the loadings α value of 0.822 is deemed noteworthy. The convergent validity of the construct (AVE = 0.65) indicates that the construct includes the relevant dimensions. Once again, due to the high loading values on the factor, the high internal consistency of the construct "Incident Response Collaboration" is indicated with a CR value of 0.797 and α value of 0.864. The value of 0.62 AVE exhibits convergent validity, showcasing that the construct can measure and calculate the latent variable. An important factor loading is clear in the "Cybersecurity resilience score construct" (CR = 0.819, α = 0.788). An AVE value of 0.60 for its latent variable of interest helps the construct's convergent validity. The construct "Organisational Cybersecurity Culture" exhibits high internal reliability, with a moderate α value of 0.706 and a CR of 0.780. The AVE of 0.62 provides support for the accuracy of the relations in the latent variable of the construct, indicating convergent validity. The validity and reliability of the study measurement model are presented in Table 1, which presents an in-depth analysis of factor loadings, reliability coefficients, and convergent validity across latent constructs.

Table 1: Factor Loadings Reliability, Convergent Validity.

	CR	**AVE**	**α**
Vendor Assessment Methods	0.754	0.69	0.837
Collaborative Information Sharing Platforms	0.733	0.63	0.791
Continuous Monitoring Strategies	0.822	0.65	0.782
Incident Response Collaboration	0.797	0.62	0.864
Cybersecurity Resilience Score	0.819	0.60	0.788
Organizational Cybersecurity Culture	0.780	0.62	0.706

Discriminant Validity

The concept of interlapping and the results of the discriminant validity analysis are presented in Table 2. The table below displays the diagonal correlation squared and correlation off-diagonal values for the pairs of constructs provided. It has been argued that if the AVE values for diabetes exceed the squared correlations between constructs, then discriminant validation is confirmed. The diagonal values of the matrix show that the AVE values for each construct, including Vendor Assessment Methods, Collaborative Information Sharing Platforms, Continuous Monitoring Strategies, Incident Response Collaboration, Cybersecurity Resilience Score, and Organisational Cybersecurity Culture, are higher than the variance explained by squared correlations. The single outcome of this study provides strong evidence of the discriminant validity, as each latent factor accurately captures the variation present in the dataset. The scores on the off diagonal represent the construct pair correlations found in Table 2. The correlations below unity between two constructs indicate that these constructs are separate latent constructs. The data suggests that when constructs are measured together, their discriminant validity is reduced compared to when they are measured separately. This provides evidence of the constructs' discriminant validity. The symbols †, *, **, and *** represent different levels of significance: p = 0.100, p = 0.050, p = 0.010, and p = 0.001. The zero-to-zero legities demonstrate the strength of correlation and the

statistical reliability. The discriminant validity of the measurement model is confirmed in table 2. It shows that each latent construct captures a unique facet of the operational elements of the vendors, including the Vendor Assessment Method, collaborative information sharing platforms, continuous monitoring strategies, incident response collaboration, cybersecurity resilience score, and organisational cybersecurity culture.

Table 2: Discriminant Validity.

	1	2	3	4	5	6	7
VAM	**0.38**						
CISP	0.11**	**0.41**					
CMS	0.26	0.21	**0.51**				
IRC	0.31*	0.18*	0.30	**0.34**			
CRS	0.19**	0.16**	0.28	0.15**	**0.33**		
OCC	0.22	0.28	0.19**	0.24*	0.22**	**0.40**	

Note: values of AVE on diagonal higher than squared correlations values. † p < 0.100; * p < 0.050; ** p < 0.010; *** p < 0.001

Measurement Model Fit

Given the recognised difference between absolute and incremental fit indices, the evaluation of goodness-of-fit involves the use of two distinct measures, consisting of multiple indices. The fitness of the survey model is determined by several indices, including CFI, AGFI, RMSEA, CMIN/df, TLI, and IFI. These indices serve as measures to assess the suitability of the measurement model. The Comparative Fit Index value is 0.93, which is above average and meets the threshold of 0. It is important to note that a value below 0.90 should prompt a re-evaluation of the specification and model. The evaluation of the CFI score is possible as it compares the model to a baseline model, revealing the data representation capacity of the measurement model. When the AGFI exceeds 0.80, it has the potential to reach a value of 0.886. The AGFI validates the appropriateness of the measurement model that utilises paired approaches, with a critical assessment of variance and covariance coverage. The RMSEA value significantly surpasses the threshold of 0.10, indicating a strong Root Mean Square Error of Approximation.

A low RMSEA value indicates a strong alignment between the superior model and the observed data, suggesting a good fit. The CMIN/df represents the ratio of Chi-Square to Degrees of Freedom, and in this case, the ratio is 2.31, which is below 3. The ratio demonstrates that a satisfactory fit between the measurement model and the data has been achieved. Another suitable equation is the measure model, which achieved a Tucker-Lewis Index (TLI) score of 0.92 and an Incremental Fit Index (IFI) objective of 0.90. These values meet the criteria of 0.89 and 0.99, respectively, indicating acceptable performance. The indices propose that the model effectively represents the underlying relationships of the latent constructs it approximates. The results in Table 3 indicate that the fit measures of the assessment model meet the criteria for an acceptable fit, suggesting a satisfactory level of fit. It is clear that the researcher has effectively measured and presented the data structure, considering reliability and validity.

Structural Model Fit

It is important to report multiple indices that suggest the model's ability to capture the relationship between latent constructs and to evaluate the structural model fit. In order to evaluate the accuracy of the structural model fit, it is essential to assess the predictive power of the theoretical framework pertaining to the data. The Comparative Fit Index (CFI) has a value of 0.95, which exceeds the typical industry standard of 0.9. However, the CFI score's magnitude serves as a robust indicator of latent construct interactions when the structural model surpasses the baseline model. The AGFI has a value of 0.88, which is higher than the threshold of 0.80. The AGFI gives an explanation for the variance and covariance in the structural model, hence confirming the achievement of data explanation in this model. The RMSEA value is 0.010, which is clearly lower than the standard index of 0.10. The RMSEA value below 0.05 indicates strong compliance between the theoretical framework and empirical results. Hence it is suggested that the model fits the data well regarding its structure. The ratio of Chi-Square to Degrees of Freedom (CMIN/df) is 1.61. This value suggests an important difference when compared to three other entities, warranting further consideration.

The ratio of chi-square to degree of freedom proposes the degree of fit between the structural model and the empirical data. The Tucker-Lewis Index (TLI) score is 0.93, while the Incremental Fit Index (IFI) score is 0.91. Both scores exceed the acceptable thresholds of 0.89 and 0.90. The indicator values provide proofs for the construct validity of the structural model in clarifying the relationships between latent constructs. The findings presented in Table 4 suggest that it can be concluded that the chi-square test yielded a value of 41.11 with a p-value of less than 0.05. This suggests that there is a well-fitting model of structural latent constructs. Further, the item fit indices propose that the model parameters align well with the data. This position's relevance implies a strong relationship between the theoretical framework and empirical evidence. The high score further suggests a successful alignment between the two. The structural model that explains the research results is supported by its credibility and proven value, which adds complexity to its interpretation.

Summary of Effects

The effects of the variability of the structural model on the analysed constructs can be observed in Table 3. It presents the Direct, indirect, and Total effects. VAM, CISP, CMS, ICR, OSC, and CRS are regarded as facets. The presence of Organisational Cybersecurity Culture (OCC) is determined by the implementation of Vendor Assessment Methods (VAM), which yields a correlation coefficient of 0.214. When considering direct influences, CISP has a direct influence of 0.154 on OCC, whereas CMS has a slightly higher direct influence of 0.201. Incident Response Collaboration (IRC) indirectly contributes 0.167 to the overall outcome. The initial actor (OCC) has a significant impact on the CRS with a coefficient of 0.358. The results are presented in a table that showcases the indirect effects.

It is important to mention that Vendor Assessment Methods (VAM) have an indirect impact of 0.354, as well as an impact of 0.487 in the path between Collaborative Information Sharing Platform (CISP) and Cybersecurity Resilience

Score (CRS). CMS and IRC have indirect effects on CRS, with levels of 0.447 and 0.501, respectively. The total direct and indirect emissions are presented in Table 5. The connections between the Vendor Assessment Method (VAM), Organisational Cybersecurity Culture (OCC), and Cybersecurity Resilience Score are statistically significant. The correlation between VAM and OCC is 0.214, while the correlation between VAM and Cybersecurity Resilience Score is 0.354. The overall impact of CISP, CMS, and IRC on OCC and CRS is significant. The precise structural model suggests the subtle connections depicted in Table 5, as well as the relationships between the independent variables and the Structural Equation Model. A comprehensive analysis within the intricate multi-cultural framework Based on this information, a deeper understanding of the intricate interplay between the examined factors can shed light on the dynamics of cybersecurity within organisations.

Table 3: Summary of Effects.

Variables	Direct Effects	Indirect Effects	Total Effects
VAM → OC:	0.214		0.214
CISP → OCC	0.154		0.154
CMS → OCC	0.201		0.201
IRC → OCC	0.167		0.167
OCC → CRS	0.358		0.358
VAM → CRS		0.354	0.354
CISP → CRS		0.487	0.487
CMS → CRS		0.447	0.447
IRC → CRS		0.501	0.501

Result of Analyses and Hypotheses

Table 4 presents concise summaries of the results and hypotheses, demonstrating the role of OCC in predicting predictors and the Cybersecurity Resilience Score. H1 proposed that OCC functions as a mediator between VAM-CRS. The hypothesis (H1) is derived from the obtained statistical values: a P-value of 0.014 and a t value of 2.36. These values suggest the presence of statistically significant factors that can be explained. It is possible that a strong cultural influence on organisational cybersecurity acts as a mediator for the impact of VAM on CRS. Sections H2, H3, and H4 delve into the hypothesis regarding the mediating role of OCC in the relationship between CISP, CMS, IRC, and CRS. Statistical significance is established for H2, H3, and H4 with p-values of 0.012, 0.010, and 0.031, respectively. The t-values of 3.1, 4.51, and 3.66 provide further confirmation for all three hypotheses. The results indicate that the presence of Organisational Cybersecurity Culture plays a role in mediating the impact of Ivetkov Risk Culture on Cybersecurity Resilience Score. Table 6 further indicates evidence for the correlation between Operational Parameters and Cybersecurity Resilience Score. The result of this study presents valuable insights into the complex nature of corporate cybersecurity, emphasizing the role of culture in shaping resilience strategies and partnerships.

Table 4: Result of Analyses and Hypotheses.

	Hypotheses	P-value	t-value	Accept or Reject
H1	Organizational Cybersecurity Culture mediated the relationship between Vendor Assessment Methods and Cybersecurity Resilience Score	0.014	2.36	Accept
H2	Organizational Cybersecurity Culture mediated the relationship between Collaborative Information Sharing Platforms and Cybersecurity Resilience Score	0.012	3.01	Accept
H3	Organizational Cybersecurity Culture mediated the relationship between Continuous Monitoring Strategies and Cybersecurity Resilience Score	0.010	4.54	Accept
H4	Organizational Cybersecurity Culture mediated the relationship between Incident Response Collaboration and Cybersecurity Resilience Score	0.031	3.66	Accept

p-value <0.05 (Hair et al., 2007), t-value > 1.96 (Othman et al., 2015)"

Discussion

For the protection of the proposed system and to assess cybersecurity practices, vendor evaluation methods are needed. its vulnerabilities and overall risk exposure, these changes have to incorporate conducting systematic reviews and evaluations of external partners. An effective VAM system requires building a strong and trustworthy foundation for third-party transactions. This policy confirms that vendors are adhering to strict cybersecurity standards and policies. Collaborative processing of information is an important part of the process, encouraging a culture of collaborative intelligence within the technology ecosystem. These forums support more effective communication and the exchange of information between internal and external stakeholders. The study highlights the importance of secure business units in improving situational awareness in order to respond proactively to emerging cyber threats. The purpose of the ongoing analysis is to objectively observe and analyse technical outputs for deviations from normality. The suggested framework incorporates a proactive variable, CMS, which plays a vital role in confirming real-time risk detection and response.

The study also aims to increase the overall cyber security posture by incorporating the advanced surveillance technologies, anomaly detection, and automated response mechanisms. Collaborative incident response is an important factor that emphasize on the need for organizations to adopt an extensive and collaborative approach to tackle cybersecurity incidents. IRC uses standard protocols, efficient communication channels, and fosters collaboration among both internal and external stakeholders. The study highlights the significance of coordinated and efficiently implemented joint incident response efforts to mitigate the influence of cyber incidents. The Cybersecurity Resilience Score is a quantifiable metric within the system that reflects

the overall efficacy of the implemented cybersecurity measures. These variables have an important impact on an organization's capacity to mitigate, identify, address, and rebound from emerging cyber threats. The analysis is carried out using an extensive CRS approach that considers both technical factors and the overall organisational culture. The emergence of organisational cybersecurity culture as a peripheral variable has a noteworthy effect on the relationships among other key components. This shift highlights the importance of considering cybersecurity in a comprehensive manner throughout the organisation, supporting a culture that recognises and places importance on cybersecurity. The analysis highlights the significant role of OCC in VAM, CISP, CMS, and the notable enhancements in IRC performance, eventually enhancing the effectiveness of CRS.

The empirical results provide support for the hypothesis that Organisational Cybersecurity Culture acting as a mediator between the VAM and the CRS. The culture of cybersecurity within an organisation plays a vital role in increasing the impact of effective vendor assessment methods on overall cybersecurity resilience. Engaging with vendors can introduce security risks, so it is crucial for the host firm to foster a strong cybersecurity culture. In the long run, a well-informed assessment will be needed, which will eventually lead to an enhanced CRS. The results emphasise the importance of effective execution of strategies for evaluating potential business partners. In addition, developing a cyber culture is essential to enhancing the ability to manage cyberattacks through third-party agreements within the organisation. This perspective suggests that the impact of VAM on CRS is indirect but is affected by OCC. The effectiveness of evaluating vendors to improve cybersecurity adaptation depends on the prevailing organisational culture. Developing a culture of cybersecurity is essential to increasing the efficiency of the VAM. Encouraging a stronger commitment to security measures and strengthening resilience to third-party threats can help achieve this.

To confirm the validity of H2, organisational cybersecurity culture was proposed to act as a mediator between CISP and CRS. Cybersecurity culture influences the effectiveness of information sharing to increase cybersecurity resilience in organizations. Encouraging a platform that encourages information sharing and a culture of effective communication within and between organisations improves the effectiveness of CRS. This study also reveals the intricate relationship between technological solutions and cultural factors, pointing to the need for a comprehensive organisational framework that can enhance cybersecurity resilience. H2 also proposed that OCC plays an important role as a mediator between CISP and CRS. Collaborations are considered most effective when they are seamlessly integrated into a culture that prioritises cybersecurity. A culture that encourages secure information sharing is thought to improve the effectiveness of collaborative meetings, and this hypothesis ultimately leads to developments in CRS that focus on the connection between solutions and organisation between cultures.

Considering all factors: The affirmation of H3 in this case is based on the result that Organisational Cybersecurity Culture plays its role as a mediator between Continuous Monitoring Strategies (CMS) and Cybersecurity Resilience Score (CRS). The effectiveness of continuous monitoring strategies in influencing CRS is strongly connected to the organization's cybersecurity culture. The culture values and

encourages a strong focus on vigilance and monitoring, which provides a notable perspective on the outlined interventions and their potential to increase cybersecurity resilience. The study shows that technological measures and cultural factors work together in the virtual world, offering an in-depth analysis into how organisations can handle and respond to cyber threats. This study explores the role of OCC in mediating the relationship between CMS and CRS. The argument of integrating continuous monitoring techniques into a cybersecurity-conscious lifestyle is optimal. Therefore, Regular vigilance and swift reaction are expected to increase the impact of CMS, leading to a more resilient cybersecurity posture. It is crucial to confirm that technological strategies align with organisational culture to achieve optimal results.

H4 promotes CRS from IRC to OCCC, according to the study. This is supported by empirical data. CRS and incident response collaboration are closely related and can be affected by a cybersecurity culture. A culture that prioritises fast and coordinated incident response emphasises cybersecurity collaboration and resilience. The findings underline the necessity of creating a cybersecurity culture that promotes collaboration and a shared commitment to attack resistance. H4 shows that OCC affects IRC-CRS. A cybersecurity-focused culture that encourages timely and coordinated security issue response improves incident response collaboration. The speculation shows how organisational culture affects collaborative incident response efforts, improving CRS.

Contribution

Industrial cybersecurity has benefited greatly from this study's thorough approach, which successfully integrates technological and cultural considerations. An innovative and comprehensive perspective is provided by the cybersecurity culture of the organisation, which is vital in understanding the connection between cybersecurity velocity scores and business processes. In addition to adding to what is already known, the Framework provides a useful tool for businesses to evaluate and strengthen their cybersecurity resilience, which is particularly important when collaborating with outside parties. Supporting practitioners, legislators, and organisations dealing with cybersecurity dangers in technology, these awards extend beyond the world of research.

Implications

This study has important theoretical implications for understanding cybersecurity resilience in technology, particularly third-party risk management. The vendor assessment process, collaborative information sharing, continuous monitoring, collaborative incident response, cybersecurity resiliency scores, and organisational computing A safety culture supports a complete design framework and illuminates complex relationships. This theoretical model illuminates the dynamic interactions between these variables and provides a platform for industrial cybersecurity research.

This study has several practical implications for IT companies looking to improve their cybersecurity. A framework for improved vendor evaluation, collaborative information exchange, ongoing monitoring, and coordinated incident response is proposed. The focus

on corporate cybersecurity culture also emphasises the need for a broader cybersecurity viewpoint. Organisations can improve their cybersecurity by using modern technologies and promoting a cybersecurity culture. The framework helps industrial practitioners improve their cybersecurity, particularly third-party risk management.

Limitations:

Despite its benefits, this study admits numerous drawbacks. The study stresses Saudi organisations' technical elements, which may limit its application to other industries or situations. Questionnaires may create response bias, and self-reported data may affect conclusions. Additionally, the variables may not adequately represent organisational culture and cybersecurity resilience. External variables like legislative changes or cybersecurity threats may also affect framework implementation. The findings must be carefully considered in context to be completely understood and applied.

Future Directions

Future research on industrial cybersecurity can explore different directions to improve our understanding and implementation of strategies. Examining testimonials in different technological settings and applications can provide valuable insights into the generalizability and adaptability of existing systems. Longitudinal studies can provide valuable insights into the effectiveness of cybersecurity coping mechanisms over time. In addition, conducting in-depth case studies in specific technology sectors to identify and analyse best practices will provide practical insights and valuable guidance for organisations. Additional research is needed to delve into the complexities of organisational culture and its impact on successful cybersecurity efforts.

By integrating advanced technologies such as artificial intelligence and blockchain, current systems can be improved to more effectively counter ever evolving cyber threats. Comparative studies in diverse global contexts have identified the influence of legal environments, cultural characteristics, and geopolitics on the success of vulnerable cybersecurity tactics. An exhaustive economic effect study is essential for making well-informed strategic decisions, as it evaluates the expenses and advantages of investments associated with improved cybersecurity adaptability. Gaining comprehension of user experience and acceptance of cybersecurity policies among employees and stakeholders can provide useful insights into the human elements that influence the effectiveness of implementation. This intelligence enables the ongoing investigation and immediate optimisation of the constantly evolving threat landscape.

Acknowledgment

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant 5814]'.

References

Ahmad, A., Johnson, C., & Storer, T. (2015). An investigation on organisation cyber resilience. *International Journal of Computer and Systems Engineering, 9*(7), 1696-1701. https://doi.org/10.5281/zenodo.1107786

Al-Dulaimi, F. A. (2023). Cyber-Attacks and the Erosion of the Right to Legitimate Defense. *Journal of The Iraqi University, 19*(19), 140-152. https://www.iasj.net/iasj/article/284655

Alassuli, A. (2024). The role of environmental accounting in enhancing corporate social responsibility of industrial companies listed on the Amman Stock Exchange. *Uncertain Supply Chain Management, 12*(1), 125-132. https://doi.org/10.5267/j.uscm.2023.10.012

Alqudhaibi, A., Albarrak, M., Aloseel, A., Jagtap, S., & Salonitis, K. (2023). Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations. *Sensors, 23*(9), 4539. https://doi.org/10.3390/s23094539

Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology, 1*(1), 32-74. https://doi.org/10.1080/23742917.2016.1252211

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & Industrial Engineering, 149*, 106829. https://doi.org/10.1016/j.cie.2020.106829

Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational Cyber Resilience: Management Perspectives. *Australasian Journal of Information Systems, 27*, 1-28. https://doi.org/10.3127/ajis.v27i0.4183

Baksa, R. (2015). Continuous monitoring of enterprise risks: A delphi feasibility study. *Dissertations*, 114. https://digitalcommons.njit.edu/dissertations/114

Buja, A., Apostolova, M., & Luma, A. (2023). Enhancing Cyber Security in Industrial Internet of Things Systems: An Experimental Assessment. In *2023 12th Mediterranean Conference on Embedded Computing (MECO)* (pp. 1-5). IEEE. https://doi.org/10.1109/MECO58584.2023.10155100

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry, 137*, 103614. https://doi.org/10.1016/j.compind.2022.103614

Dornheim, P., & Zarnekow, R. (2023). Determining cybersecurity culture maturity and deriving verifiable improvement measures. *Information & Computer Security*, 1-18. https://doi.org/10.1108/ICS-07-2023-0116

Eilts, D. (2020). *An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses* (Doctoral dissertation, Nova Southeastern University). https://nsuworks.nova.edu/gscis_etd/1106

Georgiadou, A., Michalitsi-Psarrou, A., & Askounis, D. (2022). Cyber-Security Culture Assessment in Academia: A COVID-19 Study: Applying a Cyber-Security Culture Framework to assess the Academia's resilience and readiness. In *Proceedings of the 17th International Conference on Availability, Reliability and Security* (pp. 1-8). ACM Digital Library. https://doi.org/10.1145/3538969.3544467

Hair, J. F., Money, A. H., Samouel, P., & Page, M. (2007). Research Methods for Business. *Education+ Training, 49*(4), 336-337. https://doi.org/10.1108/et.2007.49.4.336.2

Haque, M. A., De Teyou, G. K., Shetty, S., & Krishnappa, B. (2018). Cyber resilience framework for industrial control systems: concepts, metrics, and insights. In *2018 IEEE international conference on intelligence and security informatics (ISI)* (pp. 25-30). IEEE. https://doi.org/10.1109/ISI.2018.8587398

Huang, K., & Pearlson, K. (2019). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. In *Proceedings of the 52nd*

Hawaii International Conference on System Sciences (pp. 6398-6407). HICSS. http://hdl.handle.net/10125/60074

Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-4). IEEE. https://doi.org/10.1109/CyberSecPODS.2019.8885240

Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. *Electronics, 10*(10), 1168. https://doi.org/10.3390/electronics10101168

Khan, M. (2024). Enhancing supply chain resilience: The role of SC-ambidexterity and SC-agility. *Journal of Future Sustainability, 4*(4), 189-214. https://doi.org/10.5267/j.jfs.2024.10.002

Luiijf, E., & Klaver, M. (2015). On the Sharing of Cyber Security Information. In *Critical Infrastructure Protection IX: 9th IFIP 11.10 International Conference, ICCIP 2015, Arlington, VA, USA, March 16-18, 2015, Revised Selected Papers 9* (pp. 29-46). Springer. https://doi.org/10.1007/978-3-319-26567-4_3

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Implementing cyber-security measures in airports to improve cyber-resilience. In *2018 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE. https://doi.org/10.1109/GIOTS.2018.8534523

Malviya, A., Fink, G. A., Sego, L., & Endicott-Popovsky, B. (2011). Situational awareness as a measure of performance in cyber security collaborative work. In *2011 Eighth International Conference on Information Technology: New Generations* (pp. 937-942). IEEE. https://doi.org/10.1109/ITNG.2011.161

Melaku, H. M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. *Risks, 11*(6), 101. https://doi.org/10.3390/risks11060101

Mullaivendan, P., & Morais, D. S. (2022). A Short Review On Vendor Evaluation, Approach, Criteria And Questionnaire.(2022). *International Journal of Life Science and Pharma Research, 12*(3), 1-10. https://doi.org/10.22376/ijpbs/lpr.2022

Mulyani, S., & Basrowi, B. (2024). The effect of environmentally oriented leadership and public sector management quality on supply chain performance: The moderating role of public sector environmental policy. *Uncertain Supply Chain Management, 12*(1), 471-480. https://doi.org/10.5267/j.uscm.2023.9.005

Othman, A. A., Abd Rahman, S., Sundram, V. P. K., & Bhatti, M. A. (2015). Modelling marketing resources, procurement process coordination and firm performance in the Malaysian building construction industry. *Engineering, Construction and Architectural Management, 22* (6), 644-668. https://doi.org/10.1108/ECAM-02-2014-0030

Ouyang, X., Chen, J., & Cao, L. (2024). Threshold effect of ecosystem services in response to human activity in China's urban agglomeration: a perspective on quantifying ecological resilience. *Environmental Science and Pollution Research, 31*, 9671–9684. https://doi.org/10.1007/s11356-024-31865-6

Owens, R. A., Houchins, J., Nolan, S., Smalling, M. M., Attia, E., & Fitzpatrick, J. J. (2024). Feasibility of a 3-Minute Mindful Breathing Intervention for Enhancing Psychiatric Mental Health Nurses' Resilience During COVID: Findings From a 4-Week Pilot Study. *Holistic Nursing Practice, 38*(1), E1-E9.

https://doi.org/10.1097/HNP.0000000000000628

Pang, S., Bao, P., Hao, W., Kim, J., & Gu, W. (2020). Knowledge sharing platforms: An empirical study of the factors affecting continued use intention. *Sustainability, 12*(6), 2341. https://doi.org/10.3390/su12062341

Petrenj, B., Lettieri, E., & Trucco, P. (2013). Information sharing and collaboration for critical infrastructure resilience–a comprehensive review on barriers and emerging capabilities. *International Journal of Critical Infrastructures, 9*(4), 304-329. https://doi.org/10.1504/IJCIS.2013.058171

Putra, A. P., Pratiwi, I., & Arafik, M. (2023a). Development of MOOC Content in Educational Information Communication Technology Courses. In *International Conference on Educational Management and Technology (ICEMT 2022)* (pp. 673-679). Atlantis Press. https://doi.org/10.2991/978-2-494069-95-4_77

Putra, I., Octavian, A., Susilo, A., & Prabowo, A. (2023b). A hybrid AHP-TOPSIS for risk analysis in maritime cybersecurity based on 3D models. *Decision Science Letters, 12*(4), 759-772. https://doi.org/10.5267/j.dsl.2023.6.005

Riebe, T., Kaufhold, M.-A., & Reuter, C. (2021). The impact of organizational structure and technology use on collaborative practices in computer emergency response teams: An empirical study. *Proceedings of the ACM on human-computer interaction, 5*(CSCW2), 1-30. https://doi.org/10.1145/3479865

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors, 23*(16), 7273. https://doi.org/10.3390/s23167273

Trocoso-Pastoriza, J. R., Mermoud, A., Bouyé, R., Marino, F., Bossuat, J.-P., Lenders, V., & Hubaux, J.-P. (2022). Orchestrating collaborative cybersecurity: a secure framework for distributed privacy-preserving threat intelligence sharing. *arXiv preprint arXiv:2209.02676, 1*, 1-31. https://doi.org/10.48550/arXiv.2209.02676

Tsen, E., Ko, R. K. L., & Slapnicar, S. (2022). An exploratory study of organizational cyber resilience, its precursors and outcomes. *Journal of Organizational Computing and Electronic Commerce, 32*(2), 153-174. https://doi.org/10.1080/10919392.2022.2068906

Vasudevan, S., Piazza, A., & Carr, M. (2022). Qualitative Factors in Organizational Cyber Resilience. In *2022 International Conference on Cyber Resilience (ICCR)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICCR56254.2022.9995762

Vugrin, E. D., & Turgeon, J. (2014). Advancing cyber resilience analysis with performance-based metrics from infrastructure assessments. In *Cyber Behavior: Concepts, Methodologies, Tools, and Applications* (pp. 2033-2055). IGI Global. https://doi.org/10.4018/978-1-4666-5942-1

Woods, D. W., Böhme, R., Wolff, J., & Schwarcz, D. (2023). Lessons Lost: Incident Response in the Age of Cyber Insurance and Breach Attorneys. In *Proceedings of the 32nd USENIX Security Symposium, Anaheim, California* (pp. 2259-2273). USENIX Association. https://www.usenix.org/conference/usenixsecurity23/presentation/woods

Yoo, C. W., Goo, J., & Rao, H. R. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *Mis Quarterly, 44*(2), 907-931. https://doi.org/10.25300/MISQ/2020/15477

Zahid, M. S. (2024). Resilience in inter-organizational networks of red buses: dealing with

their daily disruptions in critical infrastructures. *South Asian Journal of Operations and Logistics, 3*(1), 54-71. https://doi.org/10.57044/SAJOL.2024.3.1.2425

Zouave, E., Bruce, M., Colde, K., Jaitner, M., Rodhe, I., & Gustafsson, T. (2020). *Artificially Intelligent Cyberattacks* (FOI-R--4947—SE). Swedish Defence Research Agency (FOI). https://www.statsvet.uu.se/digitalAssets/769/c_769530-l_3-k_rapport-foi-vt20.pdf

Zuhroh, D., Jermias, J., Ratnasari, S. L., Sriyono, S., Nurjanah, E., & Fahlevi, M. (2024). The role of GoJek and Grab sharing economy platforms and management accounting systems usage on performance of MSMEs during covid-19 pandemic: Evidence from Indonesia. *Uncertain Supply Chain Management, 12*(1), 249-262. https://doi.org/10.5267/j.uscm.2023.10.001

Appendix 1: Measurement Scales

Vendor Assessment Methods	
1. The vendor adopted a quality assurance system 2. The vendor is engaged in this Quality Assurance system 3. The vendor is certified as per regulatory bodies like ISO and WHO. 4. The vendor is audited by an independent body (national authority or private organization). 5. The vendor has a valid factory license under Factories Act 6. The vendor is developed a procedure to identify applicable legal and regulatory requirements with respect to Health, Safety & Environment	Mullaivendan and Morais (2022)
Collaborative Information Sharing Platforms	
1. Information output taken from vendor cybersecurity by the Information sharing platform demonstrates high reliability. 2. Information output taken from vendor cybersecurity by the Information sharing platform has a high content quality. 3. Information output taken from vendor cybersecurity by the Information sharing platform is all-dimensional. 4. Information output taken from vendor cybersecurity by the Information sharing platform is easy to understand.	Pang et al. (2020)
Continuous Monitoring Strategies	
1. There is a procedure of monitoring on the basis of availability of digital data 2. There is a procedure of monitoring on the basis of proficiency of human judgment to detect risk 3. The performance of the best predictive monitoring model compared to expert human judgment	Baksa (2015).
Incident Response Collaboration	
1. Not all employees are being kept informed during an incident 2. The right information is not being sent to the right people 3. Functional Areas not collaborating 4. Roles are not clearly defined from Policy 5. Lack of Trust between the teams 6. Not very good relationships between the employees and the managers 7. Fear from an employee that is not approaching the right solution 8. People take roles that are not assigned to them	Ioannou et al. (2019).
Cybersecurity Resilience Score	
1. Decision makers' perceived risk of cyberattack before and after participation in the cyber security assessment of risk management to optimize resilience program 2. Cyber security preparedness activities are implemented after participation in the cybersecurity assessment of risk management to optimize resilience program	Eilts (2020)

Organizational Cybersecurity Culture	
1. Employees would regularly compare notes on Third Party Risk Management and discuss other cyber topics. 2. The core team working with cybersecurity leaders included members from across the enterprise, not just the tech departments 3. Employees indicated that they knew what to do when they received a suspecious email, and knew who to contact should they notice any other potential cyber incident brewing. 4. Employees were regularly told about cyber threats and were encouraged to take steps to both protect the company asset and their own personal assets. 5. The entire organization was continually updated on cybersecurity news and issues through campaigns designed to facilitate long-term retention of cybersecurity practices and behaviors. 6. Employees who got involved in cyber-related activities were praised and given 'status' in the organization.	Huang and Pearlson (2019).