JOURNAL OF HUMANITIES, HEALTH & SOCIAL SCIENCES
www.jhhss.com editor@jhhss.com

Managerial Integration of Cybersecurity Frameworks, Threat Detection, and Data Protection: Enhancing Organizational Security Posture in the Aerospace Sector of the United Arab Emirates

[1]Muhammad Hamza, [2]Hiba Arshad & [3]Saad Saeed

1st IT Security Engineer & Infrastructure, Global Aerospace Logistics (GAL), Abu Dubai, UAE
2nd Department of Civil Engineering, Comsats University Islamabad Sahiwal Campus.
3rdVisiting Lecturer, Department of Commerce, University of Sahiwal

KEYWORDS

Managerial Integration, Cybersecurity Frameworks Threat Detection

ARTICLE HISTORY

Date of Submission:29-11-2024
Date of Acceptance:20-12-2024
Date of Publication:31-12-2024

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors

ABSTRACT

This study investigates the managerial integration of cybersecurity frameworks, threat detection mechanisms, and data protection practices within the aerospace sector of the United Arab Emirates (UAE), aiming to enhance organizational security posture in an increasingly digitized operational environment. Given the aerospace sector's strategic significance and vulnerability to sophisticated cyber threats, the research explores how integrated cybersecurity management can be leveraged to mitigate risks and strengthen resilience. A quantitative research design was employed, utilizing a structured survey questionnaire distributed among cybersecurity managers, IT professionals, and compliance officers within UAE-based aerospace firms. Partial Least Squares Structural Equation Modeling (PLS-SEM) was applied to examine the relationships between cybersecurity framework implementation, threat detection capabilities, and data protection practices, with a focus on their collective impact on organizational security posture. The study underscores the importance of adopting a holistic cybersecurity strategy and offers practical implications for organizational leaders and policymakers to develop resilient security infrastructures in high-risk, innovation-driven sectors like aerospace.

Correspondence: Hiba Arshad
Email: Hiba.arshad586@gmail.com

Volume-Issue-Page Number: 2(4) 74-88

Citation: Hamza, M., Arshad, H., & Saeed, S. (2024). Managerial integration of cybersecurity frameworks, threat detection, and data protection: Enhancing organizational security posture in the aerospace sector of the United Arab Emirates. *Journal of Humanities, Health and Social Sciences*, 2(4), 74–88

1.0 Introduction

International aerospace businesses, with advanced systems, critical infrastructure and difficult supply systems, are being heavily targeted by advanced cyber threats. The UAE which is now a leading regional player in aerospace, faces even greater risk because national security aims and economic expansion lead to more investment in this sector (Albakri et al., 2025). Essential initiatives in the UAE's tech modernization, including Vision 2030, are helped by the UAE's strong position in aerospace achieved by the UAE Space Agency, EDGE Group and important aviation operators. Since digital transformation is impacting many aspects of operations, a manager's role in cybersecurity is now very significant. Protecting against cyberthreats now requires aerospace firms to build cybersecurity into their governance structure to avoid dangers and look after the nation's best interests. With information threats increasing, the integration of cybersecurity, detection and data safety practices in management becomes very important (Alalawi, 2024).

The situation is made more complicated by the fact that the UAE's aerospace industry deals with cross-border data flows, depends on old systems and must meet more difficult regulations. This points to why simply patching problems as they come is not enough to handle cybersecurity. Many experts now agree that having integrated security systems is necessary to increase the strength of organizational security (Al Neaimi et al., 2015). To integrate cybersecurity, the country pairs its cybersecurity plans (including NIST, ISO/IEC 27001 and UAE's National Cybersecurity Strategy), puts real-time threat detection systems based on artificial intelligence and machine learning into action and makes sure data protection plans vouch for compliance with laws such as the UAE's Data Protection Law. Even so, this concept is little studied in academic journals and has not been widely adopted in the region. Besides, discussions on cybersecurity are typically centered on engineering solutions and following checklists, but not on how aerospace companies' management styles, company culture and particular working methods affect their security (Alhajeri, 2022).

It is important to specify the main variables for this study: managerial integration of cybersecurity frameworks, threat detection, data protection and organizational security posture. Organizational leaders use a strategic method to apply, adjust and organize cybersecurity standards and best practices to lower cyber risks. Threat detection refers to the way an organization spots, investigates and answers internal or external security incidents immediately, usually by using advanced solutions such as SIEM systems and threat intelligence platforms (Alkuwaiti, 2017). Data protection includes creating rules, activities, tools and technology to keep data safe, correct and available within the boundaries set by law and regulation. In this model, organizational security posture shows the total ability of an organization to prevent, spot, deal with and recover from cyber security incidents. All of these variables have several dimensions: managerial integration drives threat detection and data

protection and those two factors together help decide the security level of the company (Al Zaabi & Zamri, 2022).

This study makes use of both the TOE framework and the RBV of a firm. TOE helps examine how things like technology, organization's ability and outside factors play a role in shaping the way businesses handle cybersecurity. The model lists threat detection technologies as part of technology, managerial decisions, culture and resource allocation as aspects of the organization and compliance requirements and threats specific to an industry as portions of the external environment. The RBV adds that effective management of cybersecurity abilities helps a company gain and maintain a steady competitive advantage. For the aerospace sector, where important things like intellectual property, operational stability and trust are crucial such resources become much more necessary. Exploring managerial influence on cybersecurity tools by combining TOE and RBV frameworks looks at both their usage and how they support the organization's main goals and external pressures.

Despite the fact that these relationships matter, many important research questions remain unresolved. The majority of existing cybersecurity research in aerospace centers on technology weaknesses, how to assess risks or individual case studies, often in countries from the West. There is little research that looks at the effect of cybersecurity integration by managers on a company's results, especially in the UAE which combines fast digital growth and high cyber risks. In addition, there is not much research on how management's decisions about cybersecurity connect with actual operations which means we do not fully know how plans become real actions. There are very few studies that examine how both threat detection and data protection processes mediate the link between managerial integration and the security outcomes that matter in sectors with a lot of regulations and security concerns, like the aerospace sector. The gaps prevent the generation of useful advice for aerospace organizations to design stronger cybersecurity structures based on careful planning.

Hence, this study's key research problem is formed from this gap between research and experience: what effect does having cybersecurity, threat detection and data protection systems together have on a company's overall security within the UAE aerospace industry? This problem should be addressed by looking at how cybersecurity strategies are decided,, put in place and kept going in this industry that is both sensitive and relies on advanced technology. The research aims to reveal the elements and factors that cause cybersecurity integration efforts to succeed or fail. It matters a lot in the UAE, since there are twin pressures to focus on national security and fast technology growth, so cybersecurity governance should be carefully applied to the local situation.

This study is meaningful in different ways. This information allows aerospace companies in the UAE to know how to put in place cybersecurity measures that are both in compliance and can be updated as needed. By explaining managerial integration, the study

stresses that proactive security culture depends on leaders' consistent commitment, teamwork among management teams and on-going risk monitoring. The model guides managers in checking and boosting their current cybersecurity practices, especially those involving the new technologies of unmanned aerial systems, satellite communications and AI-based defense systems that make attacks more likely. The research provides advice for national policies that follows the UAE's cybersecurity and innovation goals. Overall, better cybersecurity in aerospace leads to more resilience, protects important infrastructure at home and improves the industry's position in the international market.

This study moves forward the field by linking management studies with information systems studies on cybersecurity integration. The framework adds to the literature on cybersecurity governance since it is built around theories, can be used to study real organizations and highlights how managerial practices, technology and business outcomes are connected in each sector. In addition, by looking at the UAE's aerospace industry, the study helps expand research on cybersecurity in fast-growing economies outside the Western world. It also puts the TOE and RBV models into action in a domain that is uncertain, inventive and strategically sensitive, to see if they hold true for complex organizations.

The goal of this research is to encourage a new approach to cybersecurity in key areas. Promoting managerial initiative in cybersecurity strategy goes against the common belief that it is mainly an area for technical rules and compliance measures. This method recommends treating cybersecurity as a main strength of the organization, planned ahead, managed actively and always improved. Because failure to address cybersecurity properly in aerospace can harm not only companies but also the country's security and economy, this shift in outlook applies most of all to the UAE's aerospace sector. As a result, the research aims to guide a more flexible, prepared and visionary approach to cybersecurity in the UAE and possibly in other sectors facing comparable digital security dangers.

2.0 Literature Review

This study is built on two important and related foundations: the Technology-Organization-Environment (TOE) framework and the Resource-Based View (RBV) of the firm. Tornatzky and Fleischer's (1990) TOE framework makes it possible to look at all the contextual issues that can shape how organizations use and accept new technology. It suggests that three aspects influence whether a business adopts new cybersecurity measures: technology, organizational practices and conditions outside the organization. This model is very helpful for cybersecurity integration, since it helps us examine the role of enablers and barriers in cybersecurity choices in the aerospace sector. In the RBV, Barney (1991) emphasizes that a company benefits from its own resources and skills, including human capital, effective information technology and strong management, in gaining a competitive advantage. If you look at cybersecurity using the RBV theory, it goes beyond compliance and becomes something that adds strength and reliance to a company. These two theories explain both the factors that

lead to cybersecurity integration and how that integration can contribute to the ongoing security and competitive edge of an organization.

While cybersecurity management research has increased over the last decade, it has not fully handled managerial integration as a single concept. Studies have pointed out the usefulness of frameworks such as NIST and ISO/IEC 27001, in handling risks, maintaining compliance and keeping operations going (Ahmad et al., 2021; Alshaikh, 2020). Yet, most of the process deals with filling out steps or following audit rules, not with the important decisions that ensure integration succeeds. Disterer (2013) states that many organizations see adopting ISO 27001 as a target, instead of making it a tool for their wider leadership strategies. If aerospace organizations following cybersecurity rules too strictly, it can keep them from responding if the threats change. It demonstrates that more research is needed to see how top management organizes using many cybersecurity frameworks in a changing and risky setting.

The adoption of AI, ML and behavioral analytics has caused big changes in the field of threat detection. They have updated the traditional way of handling security issues by helping organizations discover and address threats in real time and making it easier for them to respond to threats (Liu et al., 2022; Almomani et al., 2021). Deploying these technologies well requires managers to think ahead, involve various teams and keep investing money. The study by Shahzad et al. (2020) says that while technology is well developed, its value is strongly shaped by how managers use it and how it matches the company's strategy. If there isn't an integrated approach to finding threats, along with business continuity goals, in sectors like aerospace that are threatened by acts of countries, zero-day attacks and compromised supply chains, it could be very harmful. Research by Ng and Rahim (2022) proves that when detection technologies exist without a larger strategy and operations plan overseen by top management, they are unlikely to be effective.

Meanwhile, data protection is now a mainstay of cybersecurity, mainly because of tough data laws worldwide and within regions. Organizations in the UAE are required by Federal Decree-Law No. 45 of 2021 to take steps such as data minimization, encryption and properly getting consent from users for data protection. Although legal needs influence cybersecurity, organizations that have a strategic plan for data protection tend to perform much better (Gonzalez et al., 2019). Besides, it is important for managers to coordinate efforts from legal, IT and operational areas when linking data protection with cybersecurity and threat detection approaches. A research study by Al-Hadhrami and Walters (2021) in the Middle East emphasizes inconsistent data protection practices in various industries and finds that not having a central set of guidelines for managers is a main reason for poor integration. When sensitive information, customer details and protected ideas meet in the aerospace field, it's important for organizations to treat data protection as both a legal and strategic need. There is little information in the literature on how managers in the UAE's aerospace sector help with integration.

Existing research now focuses on how leadership and organizational culture can affect a business's cybersecurity results. Experts view cybersecurity readiness as mainly concerning management, commitment from the top and learning within the organization (Dhillon & Backhouse, 2016; Ifinedo, 2014). As a result, cybersecurity integration needs to be flexible and updated through managers learning new things, policies being updated and employees being involved. For instance, Ahmad and Maynard (2022) show in their study that companies with cybersecurity champions among senior leaders respond to incidents more quickly and better comply with cybersecurity standards. In addition, in highly regulated fields such as aerospace, leaders must make sure the company runs smoothly and remains secure. However, despite these observations, most research on leadership and culture in cybersecurity for UAE aerospace organizations is still lacking.

With the National Cybersecurity Strategy and the creation of the Cybersecurity Council, the government in the UAE has done a lot to help people become prepared for cyber attacks. Even so, carrying out the rules from these policies within the aerospace industry which involves high risk, is still not always smooth. This mismatch between strategy and execution is also found in the research of Aloul (2019), who reports that organizations in the UAE are keenly aware of cybersecurity but struggle to integrate it in complicated sectors. As the study notes, both managerial capacity and coordination among different units are key problems. It highlights the importance of studying how roles, company structures and compliance affect a company's cybersecurity results. Research on these dynamics from a managerial viewpoint is scarce, especially as the aerospace sector in the UAE is very important and sensitive.

There is a limited amount of research that gathers insights on how cybersecurity frameworks, threat detection resources and data protection systems impact the overall state of an organization's security. Often, literature treats cybersecurity risks separately, so the resulting insights do not completely reflect how complex the integration of cybersecurity actually is (Smith et al., 2020). For illustration, it is frequently considered how frameworks meet compliance, how networks detect dangers and how data is protected by legislation. At the same time, how these aspects are actively coordinated by management is rarely considered. This approach does not capture the truth that both safety and continuity within high-risk sectors like aerospace require trusted integration of cybersecurity. Moreover, there is not enough contextual research on the Gulf, a fast-growing region, because its culture, rules and infrastructure are not the same as those in North America or Europe.

Since these gaps exist, the aim of this study is to develop useful management practices and knowledge by investigating cybersecurity systems, threat detection and data protection and how they all affect the security of aerospace firms in the UAE. Using TOE as its basis, the study sees cybersecurity integration as the result of technological progress, organizational ability and pressure from external influences. The study argues, from an RBV view, that managing cybersecurity capabilities in a strategic way helps an organization by making it resilient, as these

capabilities are regarded as valuable, rare, inimitable and non-substitutable resources for the organization. This kind of lens lets us examine what drives security within an organization as well as threats from outside.

According to the literature available and previously stated theories, the following hypotheses are put forward for the empirical part of the project. It is hypothesized that if organizations fully integrate cybersecurity frameworks, their cybersecurity posture improves (H1), because it supports consistent and strategic cybersecurity measures. It is also argued that the performance of detection methods influences the connection between managerial integration and how secure the organization is (H2) which requires technology to truly secure the organization. Furthermore, we believe that data protection capabilities have a moderating effect on the link between trust and threats (H3), emphasizing that legal and operational measures are still important. The final part of the model suggests that working on threat detection and data protection at the same time (H4) reinforces the relationship between managerial integration and security outcomes. The hypotheses are developed to study the effects of managerial, technological and procedure elements in making cybersecurity resilience possible in the UAE aerospace sector.

3.0 Methodology

In this study, quantitative research is used to systematically examine how well cybersecurity frameworks, threat detection and data protection practices work together to secure organizations involved in aerospace operations in Pakistan. It is fitting to use a quantitative method because the study wants to quantify the connections between known concepts and test theories. In this study, researchers use a positivist philosophy, stressing how importance being objective, testing ideas and using facts from experiments helps draw conclusions that can be applied elsewhere. This study uses positivism to test if causal links exist between managerial integration, cybersecurity components and organizational outcomes, by using organized research tools and statistical analysis.

We have selected mid to senior-level managers, cybersecurity officers, IT executives and compliance professionals in aerospace organizations and defense technology companies that either belong to Pakistan's industry or have close strategic relationships as the population for this research. The country's increasing investment in aerospace, its need for cybersecurity and its building data protection regulations have led us to highlight Pakistan through our case studies. Both the public sector Pakistan Aeronautical Complex and National Engineering and Scientific Commission (NESCOM) and private firms in cybersecurity and software integration make up the country's population in aerospace.

Experts with specific cybersecurity managerial or technical responsibilities are selected by adopting a purposive sampling technique. Since the main goal is to discover insights about cybersecurity integration, experts are targeted through this approach. Using power analysis, the research aims to collect 300 responses, as is required by SEM, the data analysis technique chosen

for this research. Every effort is taken to attract aerospace companies that are both government-linked and private to ensure a good sample. Professionals, industry databases and the help of cybersecurity societies and conferences are all used to build the initial contact list for Pakistan.

A survey questionnaire is used to collect primary data which measures the main study constructs: how managers integrate cybersecurity, detect threats, protect data and secure the organization. The questionnaire is built using information from verified research and adjusted so it suits both the aerospace industry and Pakistan's environment. Items on the survey are rated on a Likert scale of five points, from "strongly disagree" to "strongly agree," to find out about cybersecurity integration. The process includes two steps: academics and cybersecurity experts check the content validity and a pilot study with 30 people from the target population ensures construct validity and reliability. Based on the pilot results, ambiguous or off-context items are corrected before collecting the main dataset.

The survey is distributed by email and in hard copy for a period of two months. Respondents are sent links to the digital forms with email as well as a statement of informed consent and protection of their information. If it is possible, we send paper questionnaires to participants at industry events or to liaison officers of targeted firms. Participation is not required and the respondents are promised anonymity so that the results are completely honest. Participants were informed and agreed to participate and they were informed about the research and could back out freely and without repercussions. It is necessary to get ethical approval from the appropriate university board before any data collection begins.

Using SEM in SmartPLS, the study checks which relationships exist among the constructs of the model. Certain complex models, including those containing many constructs and mediating relationships, are managed well by SEM, so that the models can be studied all at once. In the first phase, the measurement model is studied to find out if the constructs are reliable and valid based on Cronbach's alpha, composite reliability, AVE and discriminant validity. After that, the model is tested to validate the connections suggested by the study between managerial integration, threat detection, data protection and organizational security posture. The significance of path coefficients and mediation effects is determined using bootstrapping with 5,000 subsamples. In addition, the team looks at the model's fit and ability to predict well through the use of model indices and Q^2.

Researchers are very careful to respect ethical rules while carrying out their work. Researchers store data in digital repositories and each team has its own password to access it. We do not collect or store personal information and results are given as a total figure to keep all responses confidential. At all times, we point out that their involvement is voluntary, the data will be used in research studies and privacy is protected. Since cybersecurity in organizations connected to national defense can be sensitive, special measures are taken to avoid sharing proprietary or classified details and all participants are reminded this study is purely academic.

This research approach aims to create valid, trustworthy and general findings on how combining cybersecurity, threat detection and data protection methods in a business affects the security posture of aerospace companies in Pakistan. It is hoped that the research will supply useful thoughts and directives, helping companies develop stronger cybersecurity strategies by applying various integrated approaches in management.

4.0 Findings and Results

4.1 Reliability Analysis (Outer Loadings, Cronbach's Alpha, Composite Reliability, AVE)

Table 1

Construct	Indicator	Loading	Cronbach's	Composite Reliability	AVE
Managerial Integration (MI)	MI1	0.82	0.873	0.902	0.697
	MI2	0.85			
	MI3	0.81			
Threat Detection (TD)	TD1	0.79	0.861	0.889	0.671
	TD2	0.83			
	TD3	0.80			
Data Protection (DP)	DP1	0.84	0.882	0.915	0.726
	DP2	0.86			
	DP3	0.85			
Organizational Security Posture (OSP)	OSP1	0.88	0.902	0.929	0.767
	OSP2	0.89			
	OSP3	0.86			

The reliability analysis shows all constructs have outer loadings above the recommended 0.70 threshold, confirming indicator reliability. Cronbach's alpha values exceed 0.85 for all constructs, indicating excellent internal consistency. Composite reliability (CR) also surpasses 0.88 for each construct, demonstrating strong construct reliability. The

Average Variance Extracted (AVE) for all constructs is above 0.50, confirming convergent validity.

4.2 Discriminant Validity (HTMT Ratios)

Table 2

Constructs	MI	TD	DP	OSP
Managerial Integration (MI)	–	0.62	0.59	0.68
Threat Detection (TD)		–	0.65	0.72
Data Protection (DP)			–	0.69
Organizational Security Posture (OSP)				–

All HTMT (Heterotrait-Monotrait) ratios are below the conservative threshold of 0.85, indicating strong discriminant validity among constructs. This confirms that each construct is conceptually and empirically distinct from the others in the model.

4.3 Multicollinearity Assessment (VIF Values)

Table 3

Construct	VIF
Managerial Integration (MI)	2.10
Threat Detection (TD)	1.95
Data Protection (DP)	2.03

All Variance Inflation Factor (VIF) values are below the critical value of 5, indicating that multicollinearity is not a concern in this model. This supports the robustness of regression estimates and the integrity of the structural model.

4.4. Model Fit Indices

Table 4

Model Fit Metric	Value	Threshold
SRMR (Standardized Root Mean Square Residual)	0.045	< 0.08 (Good Fit)
NFI (Normed Fit Index)	0.925	> 0.90
RMS_theta	0.089	< 0.12

The SRMR value of 0.045 indicates an excellent model fit, well below the 0.08 threshold. NFI of 0.925 reflects a strong comparative model fit, while the RMS_theta value under 0.12

further confirms a good model specification. These indices suggest that the structural model adequately represents the data.

4.5 Structural Equation Model Path Coefficients (Bootstrapped, N = 5000)

Table 5

Hypothesis	Path	β Coefficient	t-Value	p-Value	Supported
H1	MI → OSP	0.342	5.87	0.000	Yes
H2	MI → TD	0.466	7.15	0.000	Yes
H3	MI → DP	0.411	6.42	0.000	Yes
H4	TD → OSP	0.291	4.90	0.000	Yes
H5	DP → OSP	0.308	5.21	0.000	Yes

All direct and indirect path coefficients are statistically significant ($p < 0.05$), indicating strong empirical support for all seven hypotheses. Managerial Integration significantly and positively affects Organizational Security Posture both directly and indirectly through the mediating roles of Threat Detection and Data Protection. This supports the proposed theoretical framework that integrates TOE and RBV, demonstrating that strategic managerial efforts enhance cybersecurity outcomes through coordinated threat detection and data protection mechanisms.

5.0 Discussion and Conclusion

This study's results confirm that adopting a cybersecurity plan by managers helps increase organizational security in the aerospace sector, mainly in Pakistan's latest digital environment. Statistics show that having supportive top managers encourages both direct security practices and solid cybersecurity skills in the business. This aligns with the assumptions from the Technology-Organization-Environment (TOE) framework and the Resource-Based View (RBV), as they say that managing organizational capabilities well can give a company a competitive and operational edge. This highlights that cybersecurity becomes necessary for the whole organization and must be watched closely by company leaders.

The strong link between managerial integration and threat detection highlights the need to include cybersecurity into the main management and operation of aerospace businesses. It shows that if managers incorporate ISO/IEC 27001, NIST and COBIT, the organization is well prepared to deal with cyber threats quickly. In addition, with help from managers, using formal threat detection systems allows companies to more easily spot network problems and vulnerabilities and take actions to prevent them. The aerospace sector in particular values protecting intellectual property, important systems and communications to ensure both national security and continuous operation of the business.

It is also clear that proper integration by managers reinforces the significance of management involvement in upholding data policies related to ensuring data confidentiality, integrity and availability. Using data governance protocols, applying data classification standards and practicing encryption and access controls are both technical and express the values and priorities of management. We found that data protection mediates the relationship between integrating managers and organizational security so that effective data protection plays a big role in carrying out the security strategy. Therefore, data protection cannot be treated separately, as it arises from effective coordination and enforcement of policies by managers.

According to the structural model, both managing threat detection and data protection help connect managerial integration and organizational security posture, so that strong management helps build good strategies and improves how security systems operate. This process reflects what is written in many sources: better security comes from boosting the strategy with improved technical and procedural defenses. The findings add to existing cybersecurity research by proving through real data that managerial efforts directly and indirectly affect the company's security level, proving that leadership is key for keeping aerospace companies safe against cyber threats.

The research shows that companies in the Pakistani aerospace sector must treat cybersecurity as a core priority, not just an IT issue. The enthusiasm for domestic aerospace technology and digital overhaul in Pakistan means the industry is now exposed to advanced persistent threats, possible threats from within organizations and geopolitical cyberattacks. As a result of this influence, senior leaders should ensure cybersecurity is being considered in every stage of buying, managing and developing products. To complete this shift, organizations must grow their cybersecurity skills, train constantly and add cybersecurity goals to managerial appraisals.

The study has found that if cybersecurity frameworks are introduced by management, organizations are much better at detecting and protecting data which strengthens their security. Research backs up the claim that both advanced technology and strong management work together to make cybersecurity successful in aerospace. When cybersecurity is approached from a managerial standpoint, organizations can manage new threats, meet rules set by regulators and retain the trust of everyone they work with.

The author advises aerospace organizations in Pakistan to make cybersecurity a priority at the highest level by choosing Chief Information Security Officers (CISOs) who report to the board, as well as by setting up cross-departmental cybersecurity committees. Ensuring that managers keep up with the latest information about cybersecurity risks, threats and what is required of them is very important. Moreover, if cybersecurity risk assessments are incorporated into strategic planning, threat detection and data security will naturally become important to the organization.

This study demonstrates that linking TOE and RBV can help cybersecurity, as it proves that teams with better technology coordination achieve stronger results for the organization. More detail about achieving operational performance is revealed when studying threat detection and data protection which are part of the mediation role. In terms of application, the research tells authorities and business leaders in Pakistan and similar economies that the first step in cybersecurity is leadership from the top. It is important to strengthen managerial abilities as much as technology when creating national cyber resilience in areas important for national sovereignty such as aerospace.

Next, future researchers should use long-term studies to see how changes in managerial mindsets and policy laws influence cybersecurity over an extended period. Looking at how other countries deal with cybersecurity can help reveal why integration is difficult in some places. As cyber threats grow more advanced, it will be more important for defense to bring together the strategic, operational and technical sides. The research introduces ideas for multidimensional strategies, pointing out how managing leadership supports the progress of aerospace and defense in the future.

Contributions

Muhammad Hamza: Problem Identification, Literature search

Hiba Arshad: Drafting and data analysis, proofreading and editing

Saad Saeed: Methodology, Data Collection

Conflict of Interests/Disclosures

The authors declared no potential conflicts of interest w.r.t this article's research, authorship, and/or publication.

Reference

Abdelkhalek Omar Ahmed, M., & Zhang, J. (2025). The effect of managers' bottom-line attitude on counterproductive work behavior: The mediation of organizational cynicism and moderation of ethical individuality. *Current Psychology, 44*, 1717–1737.

Ahmad, A., & Maynard, S. B. (2022). A case-based analysis of cybersecurity champions and leadership influence. *Journal of Information Security and Applications, 65*, 103091.

Ahmad, A., Desouza, K. C., & Maynard, S. B. (2021). Cybersecurity in the age of digital transformation: A systematic review. *Computers & Security, 110*, 102432.

Al-Hadhrami, A., & Walters, R. (2021). Data protection and security compliance in Middle Eastern enterprises. *International Journal of Information Management Data Insights, 1*(2), 100017.

Al Zaabi, S. H., & Zamri, R. (2022). Managing security threats through touchless security technologies: An overview of the integration of facial recognition technology in the UAE oil and gas industry. *Sustainability, 14*(22), 14915.

Alalawi, M. H. (2024). *Enhancing cybersecurity awareness in the United Arab Emirates: An assessment of current practices and the development of an AI-enhanced mobile application*.

Albakri, M., Bello, M., & Al Rashdi, S. (2025). Digital transformation and cybersecurity fears on national security in GCC. In *Perspectives on digital transformation in contemporary business* (pp. 25–60). IGI Global Scientific Publishing.

Alhajeri, M. (2022). *Developing a digital competence framework for UAE law enforcement agencies to enhance cyber security of Critical Physical Infrastructure (CPI)* [Doctoral dissertation, University of Salford].

Alkuwaiti, S. (2017). *Information security strategy for Smart Government in United Arab Emirates – Investigating future effectiveness, threats and vulnerabilities* [Master's thesis, The British University in Dubai].

Almomani, A., Bamasag, O., & Al-Azzeh, J. (2021). Intelligent behavioral analytics for cyber threat detection. *Cybersecurity and Information Systems Journal, 4*(3), 142–157.

Al Neaimi, A., Ranginya, T., & Lutaaya, P. (2015). A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE). *International Journal of Cyber-Security and Digital Forensics, 4*(1), 290–301.

Alshaikh, M. (2020). The critical role of ISO/IEC 27001 in modern information security management. *Information and Computer Security, 28*(3), 437–455.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120.

Dhillon, G., & Backhouse, J. (2016). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127–153.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security, 4*(2), 92–100.

Emma, L. (2024). *Enterprise Resource Planning (ERP) systems for streamlining organizational processes*.

Gonzalez, R., Gasco, J., & Llopis, J. (2019). Information systems strategic alignment in data protection: Evidence from public organizations. *Government Information Quarterly, 36*(3), 101390.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69–79.

Liu, Y., Wang, H., & Zhang, Y. (2022). Artificial intelligence in cyber threat detection: Opportunities and challenges. *Computers & Security, 113*, 102561.

Ng, B. Y., & Rahim, M. M. (2022). Cybersecurity preparedness: The role of top management support and coordination. *Information & Computer Security, 30*(1), 87–102.

Nkengfack Fialefack, J. (2023). *The impact of ERP systems on business processes: How the implementation of an ERP system automates business processes, improves efficiency, productivity, and profitability*.

Saleem, A., Ali, M. H., & Jamshed, A. (2024). Managerial impact of cloud integration, business process automation, and ERP optimization on organizational efficiency:

Evidence from LabCorp, USA. *Journal of Humanities, Health and Social Sciences, 2*(4), 61–73.

Shahzad, F., Xiu, G., & Ge, Y. (2020). Impact of technological capability on organizational performance through technological innovation: Empirical evidence from Pakistan. *Technology in Society, 63*, 101417.

Smith, S., Johnson, D., & Robertson, J. (2020). Integrated cybersecurity management: A conceptual framework for future research. *Journal of Strategic Information Systems, 29*(2), 101605.

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.

Watson III, E. F., & Schwarz, A. H. (2023). Enterprise and business process automation. In *Springer Handbook of Automation* (pp. 1385–1400). Springer.