


The Influence of Governmental Support on Cyber-Security Adoption and Performance: The Mediation of Cyber Security and Technological Readiness


Aleyah Al-Sharhan, College of Technological Studies, PAAET, Kuwait City, Kuwait

Ahmad Alsaber, American University of Kuwait, Kuwait*


 <https://orcid.org/0000-0001-9478-0404>

Yousef Al Khasham, American University of Kuwait, Kuwait

Anwaar Al Kandari, Kuwait Technical College, Kuwait

 <https://orcid.org/0000-0003-1996-0768>

Rania Nafea, University of Technology, Bahrain

 <https://orcid.org/0000-0001-8114-4775>

Parul Setiya, Govind Ballabh Pant University of Agriculture and Technology, Pantnagar, India

ABSTRACT

The accelerated cyberattacks presents a severe challenge to the companies, as they seem unprepared to confront the threat of cyberattacks, they will suffer enormous losses and have their performance suffer as a result. To better serve its population and communities, Kuwait will have improved and updated its national infrastructure by 2035. This study examines how the governmental top management support, cyber security readiness, and technology readiness affect employee's organizational security adoption intentions in Kuwait governmental organizations and realization of its benefits. The quantitative method was employed in this work. The study found that top management support influencing organizational security performance mediating by cyber security readiness and technology, which affects the tangible and intangible benefits. This study can help policy makers in governmental organizations to improve cyber security adoption. The findings of this study may be utilized for enhancing the sustainability of cyber security in governmental organizations in Kuwait.

KEYWORDS

Cyber Security Readiness, Cyberattacks, Organizational Security, Technology Readiness

INTRODUCTION

The rapid advancement of technology has led to increased concerns about information security and the safety of digital assets and individuals connected to these technologies. Cyber-attacks are becoming more sophisticated and frequent, heightening these security concerns (Dinev & Hart, 2005). These

DOI: 10.4018/IJBDCN.341264

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

concerns have significant economic implications, as organizations face substantial costs in securing data and potential financial repercussions from security breaches (Kruse et al., 2017). Studies have shown that organizations unprepared to respond to accelerated cybersecurity and information security concerns have suffered significant performance and financial losses (Hasan et al., 2021; Hasani et al., 2023). Therefore, understanding cybersecurity and the factors influencing it is crucial for developing effective strategies to safeguard digital assets and ensure the safety of individuals and organizations in the digital era.

The importance of cybersecurity has grown as government, business, and day-to-day activities have shifted online (Taddicken, 2013). The economic implications of these security concerns extend to the substantial costs involved in securing data and the potential financial repercussions of security breaches, where information is exploited (Gordon and Loeb, 2002; Dinev & Hart, 2005). Organizations unprepared for the rapid evolution in cybersecurity and information security not only face operational challenges but also significant financial losses (Hasani et al., 2023). Therefore, it is essential to comprehend the essence of both cyber and technological security and the factors affecting them (Hasani et al., 2023). In conclusion, the digital transformation has brought about unprecedented opportunities for organizations and companies to improve their products and services through digital technology. However, it has also introduced new vulnerabilities and security threats, emphasizing the critical importance of understanding cybersecurity and its implications for organizations and individuals.

Overall Background

The rapid advancement of technology has led to increased concerns about information security and the safety of digital assets and individuals connected to these technologies. Cyber-attacks are becoming more sophisticated and frequent, heightening these security concerns (Dinev & Hart, 2005). These concerns have significant economic implications, as organizations face substantial costs in securing data and potential financial repercussions from security breaches (Kruse et al., 2017). It requires a holistic approach to manage the adoption of technology and its associated risks (Soomro et al., 2016). Studies have shown that organizations unprepared to respond to accelerated cybersecurity and information security concerns have suffered significant performance and financial losses (Hasani et al., 2023). Therefore, understanding cybersecurity and the factors influencing it is crucial for developing effective strategies to safeguard digital assets and ensure the safety of individuals and organizations in the digital era. The importance of cybersecurity has grown as government, business, and day-to-day activities have shifted online (Taddicken, 2013). The economic implications of these security concerns extend to the substantial costs involved in securing data and the potential financial repercussions of security breaches, where information is exploited (Dinev & Hart, 2005). Organizations unprepared for the rapid evolution in cybersecurity and information security not only face operational challenges but also significant financial losses (Hasani et al., 2023). Therefore, it is essential to comprehend the essence of both cyber and technological security and the factors affecting them (Hasani et al., 2023). Basing upon these and other earlier efforts, this study examines how top management support influence the employee's organizational security adoption intentions in Kuwait governmental organization. The study will take into consideration the mediation role both technological as well as cyber security readiness as mediators. This holistic approach is important because with the penetration of technology in to the business, social, and governmental contexts, the technological perspective alone cannot generate a full understanding of the technology usage, adoption, and its ultimate convergence to the performance.

The Importance of the Study

Most of the current studies approach to the cyber security issue is primarily focused on the information technology aspect to evaluated whetehr the information available online are sufficaintly secured (Blakley et al., 2001). However, this approach often overlooks the broader implications of technology adoption by organizations and governments. The risks incurred in this digital era extend beyond

mere information security; they encompass the exposure of valuable economic resources and, more critically, the safety and well-being of humans involved in these processes. As such, the escalating risks necessitate the adoption of comprehensive security technologies, underpinned by a multi-perspective analysis that goes beyond traditional IT security frameworks.

This research aims to address the role of government top-level management in the adoption of security measures. The study will explore how leadership and decision-making at the top echelons of government can influence the holistic adoption of cybersecurity measures. By addressing these aspects, this research intends to provide a more comprehensive understanding of cybersecurity adoption in governmental contexts. It will offer practical insights for policymakers and government leaders in formulating effective cybersecurity strategies.

New Kuwait 2035 Strategic Plan and Cyber Security Adoption

More holistically, the information security and its technology must be a strategic concern of a country to attract more attention and resources for its adoption. The new Kuwait 2035 strategic plan is very much cyber based and naturally sensitive to the security technologies, which will be needed to support such technology driven future governance and operations in the country. As studies have suggested that when security technologies becomes a strategic concern can then guide the associated policy and can further provide guidance and even standards (Höne & Eloff, 2002), so to achieve technological transformation more smoothly and securely.

Aim and Objective of the Study

The aim of this study is to elucidate how support from top-level government management can boost the adoption of sustainable security measures. This investigation will focus on the mediating roles of cybersecurity and technological readiness. The propose model will, therefore, offer a more holistic approach to the security adoption in the government sector in Kuwait.

Literature Review

In recent years, the increasing frequency and sophistication of cyber-attacks have underscored the critical importance of cyber-security readiness for organizations and governments. Technology readiness theory, as proposed by Ahmad et al. (2020), emphasizes the significance of evaluating the contemporary technologies available to organizations and governments to safeguard their digital resources and people in the face of continuous threats. This theory posits that the readiness of an organization to adopt and utilize technology is influenced by various factors, including top-level management support. Bahuguna et al. (2019) have highlighted the pivotal role of top-level management in achieving cyber-security readiness within organizations. Their study suggests that the support and involvement of top management is a crucial resource for enhancing an organization's cyber-security readiness.

Furthermore, Berlilana et al. (2021) have emphasized the importance of top-level management support in transforming readiness into action and channeling security adoption towards organizational benefits. Study done by Smith et al. (2018) also provided empirical evidence of the positive impact of top-level management support on cyber-security readiness within government organizations. In light of the aforementioned literature, the following hypotheses have been formulated:

- H1:** *There is relationship between Governmental Top-Level Management Support to combat cyber-attacks with the organization's cyber-security readiness.*
- H2:** *There is relationship between Governmental Top-Level Management Support to combat cyber-attacks with the organization's technological readiness.*
- H3:** *There is relationship between Governmental Top-Level Management Support with organizational security adoption.*

The relationship between an organization's readiness to combat cyber-attacks and its security performance/adoption (H4), as well as the relationship between the technological readiness of an organization to adopt new technology and its security performance/adoption (H5), are crucial aspects in the context of cybersecurity. Rawindaran et al. (2021) emphasize the significance of cyber security readiness and technology readiness in improving organizational performance. The study highlighted the need for continuous learning strategies within organizations, especially with the rapid evolution in cybersecurity adoption driven by tools such as artificial intelligence and machine learning. Furthermore, Blut and Wang (2019) discuss the concept of technology readiness and its impact on technology usage, emphasizing the importance of understanding people's propensity to embrace and use cutting-edge technologies. This aligns with the need to assess an organization's technological readiness in relation to the adoption of new security technologies.

Moreover, Kilani (2020) provides insights into the indirect effects of cyber-security motivators on internal processes within an organization, emphasizing the importance of cyber-security readiness in shaping organizational processes. This supports the evaluation of the relationship between an organization's readiness to combat cyber-attacks and its security performance/adoption. The synthesis of these references underscores the critical need to assess both cyber security readiness and technological readiness in organizations to understand their impact on security performance and adoption. This comprehensive evaluation is essential for addressing the evolving landscape of cybersecurity threats and the rapid advancements in security technologies. Thus, the following hypotheses has been formed

H4: There is relationship between organization's readiness to combat cyber-attacks with the organization's security performance/adoption.

H5: There is relationship between technological readiness of an organization to adopt new technology and with the security performance/adoption.

The pragmatics of security adoption are important to rationalize the very technology and cyber security adoption. H6 and H7, therefore test whether, security performance results in any tangible and intangible benefits. Both these tangible and intangible goods are the overall outcomes of the path impacts starting with technological readiness, cyber-security readiness, security performance, and ultimate. The study by Berlilana et al. (2021) is particularly relevant as it explores the tangible and intangible benefits arising from good security performance. Additionally, Li and Wang (2014) provide insights into the impact of intangible assets on profitability, which can be correlated with the intangible benefits resulting from good security performance. Furthermore, Rasmussen et al. (2017) extend a risk-benefit framework in donor selection, which can be valuable in understanding the tangible benefits associated with security performance. This research therefore, evaluate the followign two hypotheses to validated if the tangible and in tangible emerge from the good security performance.

H6: Good security performance of an organization results in high tangible benefits for the organization.

H7: Good security performance of an organization results in high intangible benefits for the organization.

The study goes further to evaluate whether both cyber security readiness and technological readiness have any mediation role to enhance the relationship between governmental top-level management support and tangible and intangible benefits post-adoption of organization security. For this purpose, H8 and H9 are designed to be tested. Both cyber-security readiness and technological readiness have been advocated as having stronger mediation roles in transforming the security performance into actual benefits (Berlilana et al., 2021). Additionally, the study done by Nifakos et al. (2021) emphasizes the importance of cybersecurity risk assessment in organizations, recommending the use of European and

international standards to counter social engineering attacks, which underscores the significance of cyber-security readiness in organizational security (Nifakos et al., 2021). Furthermore, the study by Lai et al. (2018) classifies potential factors affecting big data analytics (BDA) adoption into technological, organizational, environmental factors, and supply chain characteristics, highlighting the relevance of technological readiness in the adoption of advanced technologies within organizational contexts (Lai et al., 2018). This supports the argument that technological readiness plays a crucial role in the adoption and implementation of technological solutions.

H8: Cyber-security readiness mediate the relationship between Governmental Top-Level Management Support and Tangible and Intangible Benefits Post-Adoption of Organization Security

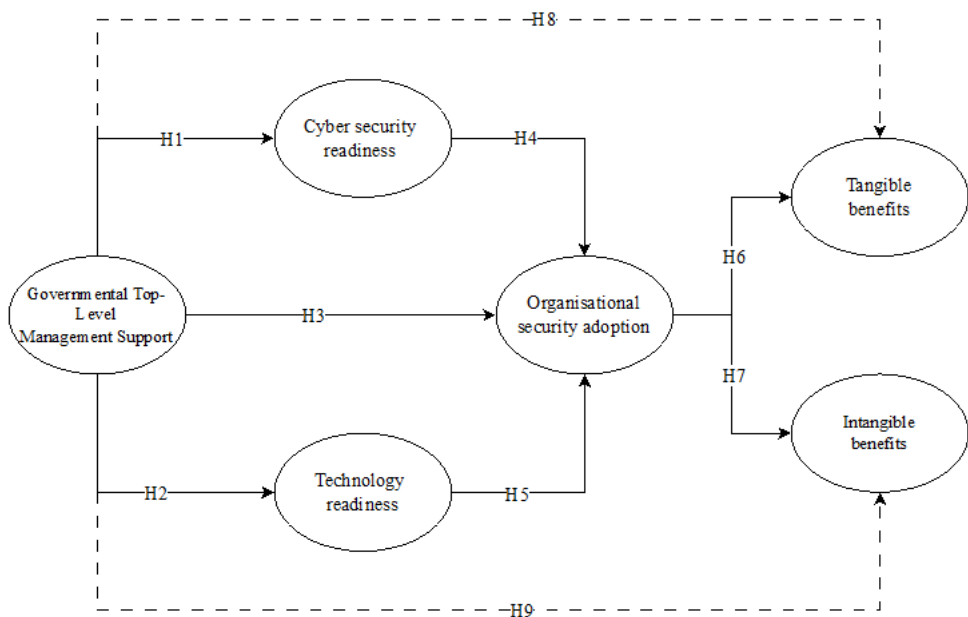
H9: Technological readiness mediation the relationship between Governmental Top-Level Management Support and Tangible and Intangible Benefits Post-Adoption of Organization Security

RESEARCH METHODOLOGY

Data and Variables

This research was conducted to examine the cyber security readiness and organizational technology readiness with the mediation of top-level management support to determine the impact this has on cyber-attacks and the results of tangible and intangible benefits of its appliance. A survey with questionnaires that were distributed online and to governmental sectors to collect samples to solidify the proposed hypothesis. Each construct item is measured with a 5-scale Likert scale and the measurement starts from a scale of 1 represent strongly disagree to a scale of 5 which means strongly agree. Table 6 (Appendix A) demonstrates the model constructs and the corresponding items. Figure 1 shows all 9 hypotheses collectively as model of this study.

Figure 1. Research model conceptual framework



Methodology and Model Specifications

Partial Least Squares Structural Equation Modelling (PLS-SEM) is the best method for assessing complex models with a number of independent and dependent variables (Hair et al., 2014; Henseler et al., 2009). The examination of the measurement model was done first in the SEM research, which was then followed by the assessment of the structural model. The evaluation of a measurement model focuses on the assessment of constructs' reliability, convergent validity, and discriminant validity, in contrast to the structural model assessment, which focuses on the analysis of the connection between latent constructs and measured variables. The SmartPLS software was utilised for conducting PLS-SEM analysis. SmartPLS encompasses a range of metrics, including measurement model analysis, path analysis, and multigroup analysis, for the purpose of conducting model testing.

RESULTS

Table 1 summarizes the demographic characteristics of the participants. The study sample consists 413 participants, among which 52% were male and 48% were female participants. Majority of the participants were from age- group 31-40 (33.7%) and had experience of 16-20 years (27.6%). Majority of the participants had bachelor degree (47.9%) and worked as supervisor (44.8%).

SEM for the Conceptual Proposed Frame Work

Structure Equation Modelling (SEM) is a method that examines numerous connections simultaneously. PLS is advantageous over regression-based approaches because it can assess numerous latent constructs using a wide range of manifest variables. It is a two-step process that begins with the evaluation of the outer measurement model and concludes with the evaluation of the inner measurement model, which is also referred to as the structural model (Henseler et al., 2009). Figure 2 depicts the fundamental node diagram with loadings.

Measurement Model Assessment

Measurement models describe how constructs are assessed using indicators. The validity and reliability of the indicators employed in multivariate analysis must be confirmed by researchers in order to increase the measure's accuracy.

The assessment of measurement models involved the evaluation of construct reliability, convergent validity, and discriminant validity, as per the recommendations outlined by Hair et al., 2017. The value of Cronbach's alpha and composite reliability exceeded the minimum acceptable value of 0.7 (Hair et al., 2017) (Table 2). Therefore, the construct reliability is established. In addition, convergent validity was tested by examining factor loading and average variance extracted (AVE), as suggested by Hair et al., 2017). The present investigation had factor loadings above the threshold value (0.60) and AVEs above the threshold value (0.50), respectively. The convergent validity of the study's constructs was thus verified.

Discriminant validity was examined to ensure that one construct's measures do not correlate with those of another (Ringle et al., 2010). For the assessment of discriminant valid Fornell and Larker's (1981) criteria has been utilized. To have the discriminant validity, the square root of each construct's AVE should exceed its bivariate correlations with other constructs (Ringle et al., 2010). Results of the Fornell and Larcker criterion is shown in Table 3, confirms the discriminant validity condition.

Structural Model Assessment

Path Analysis

According to Hair et al., (2014), path coefficients are estimates of the relationships between the model's constructs. The outcomes of the direct relationship and hypothesis tests are presented in Table 4. It is evident that TopM as a significant effect on EC ($\beta = 0.550$, $T = 13.385$, $p = 0.000$),

Table 1. Demographics

Variable	Overall (N=413)	%
Gender		
Male	214	51.8%
Female	199	48.2%
Age		
Less than 20 y.o.	65	15.7%
20 to 30	101	24.5%
31 to 40	139	33.7%
41 to 50	103	24.9%
51 to 60	5	1.2%
Experience		
Less than one year	34	8.2%
1 to 5	57	13.8%
6 to 10	95	23.0%
11 to 15	102	24.7%
16 to 20	114	27.6%
More than 20 y.o.	11	2.7%
Education		
Secondary or less	24	5.8%
Diploma	68	16.5%
Bachelors	198	47.9%
Master	114	27.6%
Ph.D.	9	2.2%
Employment		
Other	2	0.5%
Employee	106	25.7%
Supervisor	185	44.8%
Controller	73	17.7%
Manager	47	11.4%

OC ($\beta = 0.460$, $T = 9.674$, $p = 0.000$), TC ($\beta = 0.454$, $T = 10.043$, $p = 0.000$), DCT ($\beta = 0.460$, $T = 10.184$, $p = 0.000$), INV ($\beta = 0.522$, $T = 13.057$, $p = 0.000$), INC ($\beta = 0.549$, $T = 14.721$, $p = 0.000$) and OPT ($\beta = 0.557$, $T = 16.459$, $p = 0.000$). Additionally, the findings confirmed that the Organizational Security Adoption (OSA) is significantly influenced by EC ($\beta = 0.211$, $T = 3.801$, $p = 0.000$), OC ($\beta = 0.131$, $T = 2.451$, $p = 0.014$), TC ($\beta = 0.149$, $T = 2.841$, $p = 0.005$), DCT ($\beta = 0.164$, $T = 2.823$, $p = 0.005$), INV ($\beta = 0.178$, $T = 3.335$, $p = 0.001$) and OPT ($\beta = 0.143$, $T = 3.055$, $p = 0.002$). Moreover, the effect of Organizational Security Adoption (OSA) on the output variables IB ($\beta = 0.399$, $T = 8.687$, $p = 0.000$) and TB ($\beta = 0.515$, $T = 12.376$, $p = 0.000$) were also significant.

This study provides a comprehensive analysis of explaining the impact of Government Top-Level Management Support on the security technology adoption and how the same leads to tangible and intangible benefits. The study has confirmed that there is relationship between governmental top-

Figure 2. Node diagram for the PLS-PM model with loading and path estimates

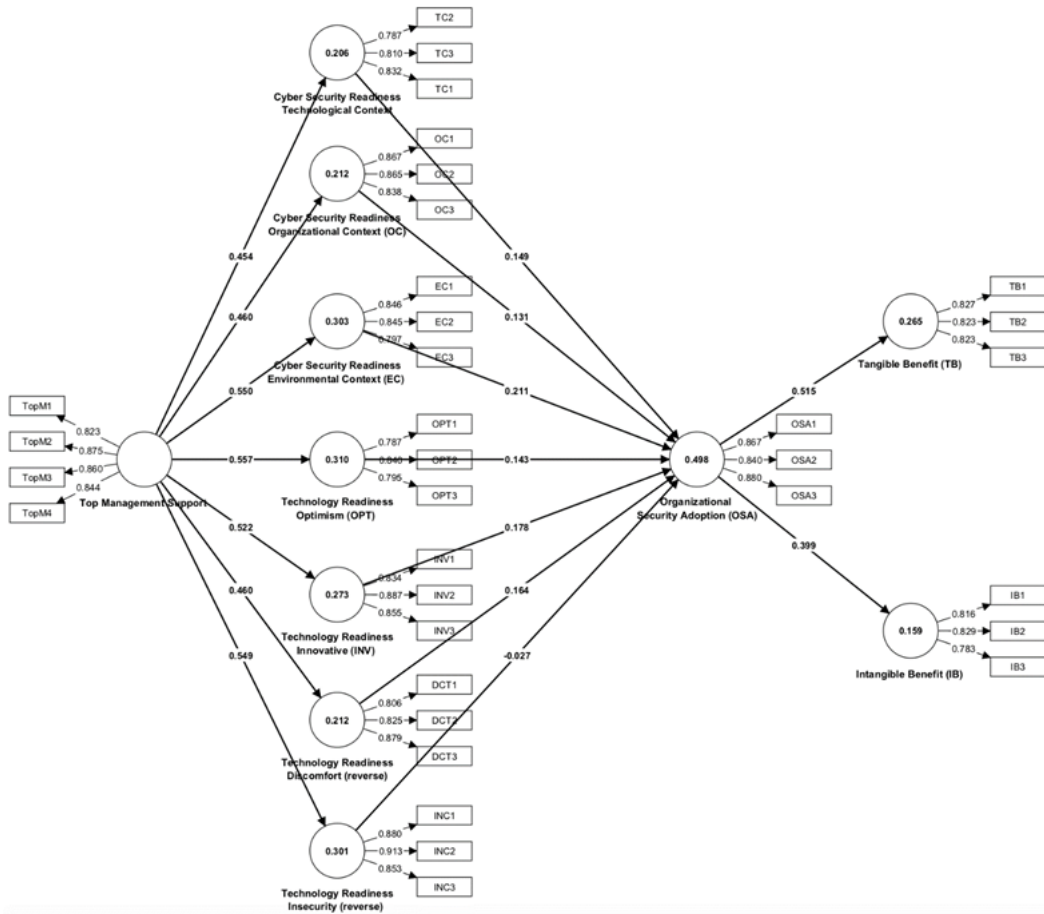


Table 2. Outer model summary table for the PLS-PM Model

Construct	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
EC	0.773	0.773	0.869	0.688
OC	0.819	0.820	0.892	0.734
TC	0.738	0.741	0.851	0.656
IB	0.748	0.780	0.851	0.656
OSA	0.828	0.831	0.897	0.744
TB	0.766	0.771	0.864	0.680
DCT	0.785	0.788	0.875	0.701
INV	0.822	0.825	0.894	0.738
INC	0.857	0.858	0.913	0.778
OPT	0.733	0.734	0.849	0.652
TopM	0.873	0.873	0.913	0.724

EC: Environmental Context, OC: Organizational Context, TC: Technological Context, IB: Intangible Benefit, OSA: Organizational Security Adoption, TB: Tangible Benefit, DCT: Discomfort, INV: Innovative, INC: Insecurity, OPT: Optimism, Top: Top Management Support

Table 3. Fornell-Larcker criterion results

	EC	OC	TC	IB	OSA	TB	DCT	INV	INC	OPT	TopM
EC	0.83										
OC	0.56	0.85									
TC	0.44	0.57	0.81								
IB	0.22	0.13	0.21	0.81							
OSA	0.57	0.54	0.48	0.39	0.86						
TB	0.54	0.49	0.38	0.23	0.515	0.82					
DCT	0.40	0.39	0.31	0.23	0.47	0.51	0.83				
INV	0.51	0.46	0.32	0.26	0.52	0.54	0.48	0.85			
INC	0.54	0.54	0.37	0.14	0.48	0.61	0.50	0.62	0.88		
OPT	0.56	0.51	0.44	0.21	0.52	0.52	0.37	0.44	0.47	0.80	
TopM	0.55	0.46	0.45	0.27	0.57	0.59	0.46	0.52	0.54	0.55	0.85

level management support to combat cyber-attacks with the organization's cyber-security readiness. This finding is in line with other studies in the discipline and particularly true in the context when there are hierarchical cultures. The study by Georgiadou et al. (2022) provides a comprehensive analysis of the impact of governmental top-level management support on security technology adoption and its subsequent influence on tangible and intangible benefits within organizations. The findings confirm the relationship between governmental top-level management support and an organization's cyber-security readiness, where top-management support is considered, an emergent culture prioritizing cyber-security readiness, leading to the development of an overall security culture. This aligns with the argument that top-management support enables a holistic security support environment, fostering experiential learning and perpetually advancing technology preparedness and performance.

Moreover, the study affirms the relationship between governmental top-level management support and an organization's readiness to combat cyber-attacks, which stimulates the use of preparedness towards security performance and adoption, as evidenced in other studies (Tomaschek et al., 2016). Additionally, the study accepts the relationship between technological readiness and security performance, acknowledging the theoretical and empirical evidence supporting the influence of technology readiness on organizational performance.

Going further on the web of relationships, the study also partially accept that there is a relationship between technological readiness of an organization to adopt new technology and with the security performance of the organization. As technology readiness though found leading to the performance and the phenomenon is well establish both theoretically as well empirically (Olechowski et al., 2015). New technology, however, brings new challenges and doubts may therefore make organizations to remain hesitant while switching to new technology. This is usual as new constraints emerge while making the required changes in the preparedness (Olechowski et al., 2020).

The study proceeds further and confirm that a good security performance of an organization also results in high tangible benefits for the organization. This results further strengthen the path of impacts towards the outcomes of technology adoption. These tangible benefits can be in the form of more improved operation results and profitability and reduction of losses that can be measured as it is believed that "finance and technology meet at the crossroads of technology readiness" (Clausing and Holmes, 2010). Additionally, it establishes that good security performance leads to high intangible benefits for organizations and stakeholders, contributing to perceived safety and corporate social responsibility (Ying et al., 2016).

Further, it has also been confirmed that a good security performance of an organization results in high intangible benefits for the organization. As and when the organization demonstrate a good security performance, results in intangible benefits to not just the organization and the stakeholders around it but to the society at large as perceived safety is established through corporate social responsibly of maintaining a safe working place (Berlilana et al., 2021).

Mediation Analysis

The impact of the mediating variable between the independent and dependent variables was examined using mediation analysis. The results of the mediation analysis are depicted in Table 5.

The analysis of the mediating effects in the study provides crucial insights into the dynamics of cybersecurity implementation and its outcomes. It reveals that the mediating role of Organizational Security Adoption (OSA) is significant across most constructs, with the notable exceptions being the relationships between INC and TB, and INC and IB, where OSA does not exhibit a significant mediating effect. This suggests that while OSA generally plays a key role in bridging various elements of cybersecurity readiness and performance, its influence is not universal across all variables.

Furthermore, the mediating effect of INC (Investment in Cybersecurity) is not significant when linking Top-Level Management (TopM) support to Organizational Digital Adoption (ODA), nor in the combined effect of INC and OSA between TopM and Tangible Benefits (TB). This implies that the investment in cybersecurity, while crucial, does not always directly translate to digital adoption or tangible benefits, especially when considered in tandem with OSA. The study underscores the pivotal role of governmental top-level management support in mediating the relationship between cybersecurity readiness and both tangible and intangible benefits post-adoption. This highlights that effective cybersecurity implementation is not solely a matter of technical readiness but also significantly depends on the strategic and administrative support provided by top management. When this support is aligned with enhanced security performance, the likelihood of realizing both tangible

Table 4. Bootstrap results for the inner model regression paths

Path	Original sample (O)	Standard deviation (STDEV)	T statistics (IO/STDEV)	P values	Decision
EC -> OSA	0.211	0.056	3.801	0.000	Supported
OC -> OSA	0.131	0.054	2.451	0.014	Supported
TC -> OSA	0.149	0.052	2.841	0.005	Supported
OSA -> IB	0.399	0.046	8.687	0.000	Supported
OSA -> TB	0.515	0.040	12.736	0.000	Supported
DCT -> OSA	0.164	0.058	2.823	0.005	Supported
INV -> OSA	0.178	0.053	3.335	0.001	Supported
INC -> OSA	-0.027	0.055	0.485	0.627	Not Supported
OPT -> OSA	0.143	0.047	3.055	0.002	Supported
TopM -> EC	0.550	0.041	13.385	0.000	Supported
TopM -> OC	0.460	0.048	9.674	0.000	Supported
TopM -> TC	0.454	0.045	10.043	0.000	Supported
TopM -> DCT	0.460	0.045	10.184	0.000	Supported
TopM -> INV	0.522	0.040	13.057	0.000	Supported
TopM -> INC	0.549	0.037	14.721	0.000	Supported
TopM -> OPT	0.557	0.034	16.459	0.000	Supported

(such as reduced cyber incidents and enhanced operational efficiency) and intangible benefits (like improved stakeholder trust and reputation) increases. Moreover, these benefits extend beyond the internal workings of an organization. They impact external stakeholders, suggesting a broader societal benefit. However, this raises further questions about the preparedness of external users and their ability to adapt to and benefit from enhanced cybersecurity measures, as indicated by Parasuraman (2000).

The study partially confirms the mediating role of technological readiness in the relationship between governmental top-level management support and the tangible and intangible benefits post-adoption. This suggests that while technological preparedness is essential, its effectiveness in translating top-level support into concrete cybersecurity benefits is only partially realized. The reasons for this could range from the pace of technological change outstripping organizational adaptation abilities, to potential gaps in aligning technological capabilities with strategic objectives. In conclusion, this comprehensive analysis indicates that while the interplay between top-level management support, investment in cybersecurity, and technological readiness is complex, they are crucial factors in determining the successful adoption and benefits realization of cybersecurity measures within organizations.

Table 5. Bootstrap results for the inner model regression paths (Mediation analysis)

Path	Original sample (O)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values	Decision
OPT -> OSA -> TB	0.073	0.026	2.881	0.004	Supported
TopM-> EC-> OSA -> IB	0.046	0.014	3.314	0.001	Supported
EC -> OSA -> IB	0.084	0.023	3.673	0.000	Supported
TopM -> INC -> OSA	-0.015	0.031	0.484	0.629	Not Supported
TopM -> OPT -> OSA -> TB	0.041	0.015	2.690	0.007	Supported
TC -> OSA -> TB	0.077	0.027	2.855	0.004	Supported
TopM-> TC -> OSA -> TB	0.035	0.014	2.522	0.012	Supported
TC -> OSA -> IB	0.059	0.022	2.686	0.007	Supported
TopM-> INC -> OSA -> IB	-0.006	0.013	0.471	0.638	Not Supported
OC -> OSA -> IB	0.052	0.022	2.380	0.017	Supported
TopM -> INC -> OSA -> TB	-0.008	0.016	0.483	0.629	Not Supported
TopM-> INV -> OSA -> IB	0.037	0.014	2.648	0.008	Supported
TopM-> TC -> OSA -> IB	0.027	0.011	2.434	0.015	Supported
EC -> OSA -> TB	0.109	0.032	3.439	0.001	Supported
DCT -> OSA -> IB	0.066	0.026	2.526	0.012	Supported
TopM-> OC -> OSA	0.060	0.027	2.282	0.023	Supported
INC -> OSA -> IB	-0.011	0.023	0.472	0.637	Not Supported
TopM-> EC -> OSA -> TB	0.060	0.019	3.109	0.002	Supported
INC -> OSA -> TB	-0.014	0.029	0.486	0.627	Not Supported
TopM-> EC -> OSA	0.116	0.033	3.479	0.001	Supported
TopM-> DCT -> OSA -> IB	0.030	0.013	2.303	0.021	Supported
Top -> INV -> OSA	0.093	0.030	3.110	0.002	Supported
TopM-> OPT -> OSA	0.079	0.028	2.878	0.004	Supported

continued on following page

Table 5. Continued

Path	Original sample (O)	Standard deviation (STDEV)	T statistics (O /STDEV)	P values	Decision
TopM-> DCT -> OSA -> TB	0.039	0.016	2.507	0.012	Supported
TopM-> DCT -> OSA	0.076	0.030	2.537	0.011	Supported
DCT -> OSA -> TB	0.085	0.030	2.802	0.005	Supported
TopM-> INV -> OSA -> TB	0.048	0.016	2.999	0.003	Supported
TopM-> TC -> OSA	0.067	0.026	2.559	0.011	Supported
INV -> OSA -> TB	0.092	0.028	3.287	0.001	Supported
OC -> OSA -> TB	0.068	0.029	2.354	0.019	Supported
TopM-> OC -> OSA -> IB	0.024	0.011	2.214	0.027	Supported
OPT -> OSA -> IB	0.057	0.020	2.838	0.005	Supported
INV -> OSA -> IB	0.071	0.025	2.812	0.005	Supported
TopM-> OPT-> OSA -> IB	0.032	0.012	2.682	0.007	Supported
TopM-> OC -> OSA -> TB	0.031	0.014	2.151	0.032	Supported

CONCLUSION

This paper explains a web of relationships showing the influence of governmental support on the security adoption and performance with the mediation of security and technological readiness. The paths evaluated in this study are establishing relationships starting with showing how the government top-level management support impacts the security adoption and then the same support transforms into both tangible and intangible benefits. More importantly, the study suggests that the technological readiness and cyber-security readiness both mediate relationship of government support and the security performance. More interestingly, the study reveals some doubts in the form of partial acceptances of few hypothesis where the public sector employees have shown to remain hesitant to adopt new technology, in spite of them being having sufficient technological and security preparedness. These new insights from the paths analysis are import and provide holistic understanding of how government support leads to both tangible and intangible benefits, while going through the complex web of variables such as technology preparedness and security performance using the government employees' perspective in Kuwaiti government. The findings are well-timed as governments in various parts of the world are struggling to routinely make decisions for acquiring and implementing security technology and consider, whether the same will be sufficiently beneficial at times when rapid development of cyberspace is disrupting the social and economic locales.

ACKNOWLEDGEMENT

This publication was made possible by the support of the AUK Open Access Publishing Fund.

REFERENCES

- Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, 71(8), 939–953. doi:10.1002/asi.24311
- Bahuguna, A., Bisht, R. K., & Pande, J. (2019). Assessing cybersecurity maturity of organizations: An empirical investigation in the Indian context. *Information Security Journal: A Global Perspective*, 28(6), 164–177.
- Berlilana, N., Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini, . (2021). Organization benefit as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness. *Sustainability (Basel)*, 13(24), 13761. doi:10.3390/su132413761
- Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 97–104). ACM. doi:10.1145/508171.508187
- Blut, M., & Wang, C. (2019). Technology readiness: A meta-analysis of conceptualizations of the construct and its impact on technology usage. *Journal of the Academy of Marketing Science*, 48(4), 649–669. doi:10.1007/s11747-019-00680-8
- Clausing, D., & Holmes, M. (2010). Technology readiness. *Research Technology Management*, 53(4), 52–59. doi:10.1080/08956308.2010.11657640
- Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2), 7–29. doi:10.2753/JEC1086-4415100201
- Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Working from home during COVID-19 crisis: A cyber security culture assessment survey. *Security Journal*, 35(2), 486–505. doi:10.1057/s41284-021-00286-2
- Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. [TISSEC]. *ACM Transactions on Information and System Security*, 5(4), 438–457. doi:10.1145/581271.581274
- Hair, J. F., Hult, G. T., Ringle, C. M., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (2nd ed.). SAGE.
- Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial Least Squares Structural Equation Modeling (PLS-SEM): An Emerging Tool in Business Research. *European Business Review*, 26(2), 106–121. doi:10.1108/EBR-10-2013-0128
- Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58, 102726. doi:10.1016/j.jisa.2020.102726
- Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, 3(5), 97. doi:10.1007/s43546-023-00477-6 PMID:37131522
- Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The Use of Partial Least Squares Path Modeling in International Marketing. *Advances in International Marketing*, 20, 277–319. doi:10.1108/S1474-7979(2009)0000020014
- Höne, K., & Eloff, J. H. P. (2002). Information security policy—What do international information security standards say? *Computers & Security*, 21(5), 402–409. doi:10.1016/S0167-4048(02)00504-7
- Kilani, Y. (2020). Cyber-security effect on organizational internal process: Mediating role of technological infrastructure. *Problems and Perspectives in Management*, 18(1), 449–460. doi:10.21511/ppm.18(1).2020.39
- Kruse, C., Frederick, B., Jacobson, T., & Monticone, D. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1), 1–10. doi:10.3233/THC-161263 PMID:27689562
- Lai, Y., Sun, H., & Ren, J. (2018). Understanding the determinants of big data analytics (bda) adoption in logistics and supply chain management. *International Journal of Logistics Management*, 29(2), 676–703. doi:10.1108/IJLM-06-2017-0153

- Li, H., & Wang, W. (2014). Impact of intangible assets on profitability of hong kong listed information technology companies. *Business and Economic Review*, 4(2), 98. doi:10.5296/ber.v4i2.6009
- Nifakos, S., Chandramouli, K., Nikolaou, C., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors (Basel)*, 21(15), 5119. doi:10.3390/s21155119 PMID:34372354
- Olechowski, A., Eppinger, S. D., & Joglekar, N. (2015, August). Technology readiness levels at 40: A study of state-of-the-art use, challenges, and opportunities. In *2015 Portland international conference on management of engineering and technology (PICMET)* (pp. 2084-2094). IEEE.
- Olechowski, A. L., Eppinger, S. D., Joglekar, N., & Tomaschek, K. (2020). Technology readiness levels: Shortcomings and improvement opportunities. *Systems Engineering*, 23(4), 395–408. doi:10.1002/sys.21533
- Parasuraman, A. (2000). Technology Readiness Index (TRI) a multiple-item scale to measure readiness to embrace new technologies. *Journal of Service Research*, 2(4), 307–320. doi:10.1177/109467050024001
- Rasmussen, S., Henderson, M., Kahn, J., & Segev, D. (2017). Considering tangible benefit for interdependent donors: Extending a risk–benefit framework in donor selection. *American Journal of Transplantation*, 17(10), 2567–2571. doi:10.1111/ajt.14319 PMID:28425206
- Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers*, 10(11), 150. doi:10.3390/computers10110150
- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215–225. doi:10.1016/j.ijinfomgt.2015.11.009
- Taddicken, M. (2013). The ‘privacy paradox’ in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, 19(2), 248–273. doi:10.1111/jcc4.12052
- Tomaschek, K., Olechowski, A., Eppinger, S., & Joglekar, N. (2016, July). A survey of technology readiness level users. *INCOSE International Symposium*, 26(1), 2101–2117. doi:10.1002/j.2334-5837.2016.00283.x
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38, 97-102.
- Ying, W., So, K., & Sparks, B. (2016). Technology readiness and customer satisfaction with travel technologies: A cross-country investigation. *Journal of Travel Research*, 56(5), 563–577.

APPENDIX- APPENDIX A

Table 6. Model constructs and items (questionnaire items), measurement scale from “Strongly Disagree” to “Strongly Agree” on a five-point scale

<i>Cyber Security Readiness—Technological Context (TC)</i>
TC1: In my organization, there are sufficient experts in the field of information technology in quantity and quality in managing cyber security, TC2: In my organization, there is sufficient infrastructure in quantity to manage cyber security, TC3: The resources owned by the organization from the technological aspect to ensure cyber security in quantity and quality are better.
<i>Cyber Security Readiness—Organizational Context (OC)</i>
OC1: Availability of skilled qualified personnel to manage cyber security, OC2: In my organization, there are workshops, training, and activities that support quality improvement for personnel who manage cyber security, OC3: Availability of resources from the personnel aspect to manage cyber security in the organization
<i>Cyber Security Readiness—Environmental Context (EC)</i>
EC1: In my organization, the managers always seek to establish communication with the environment involved to ensure cyber security activities run smoothly, EC2: In my organization, the managers always enhance cyber security together with the organizational environment involved on an ongoing basis, EC3: In my organization, manages knowledge derived from experience to ensure it can solve problems in the environment involved, quickly and accurately
<i>Organizational Security Adoption (OSA)</i>
OSA1: In my organization, aspects of cyber security are always considered, OSA2: In my organization, software and hardware to support cyber security are always used and managed properly, OSA3: From the operational and strategic aspects, my organization always prioritizes cyber security
<i>Technology Readiness—Optimism (OPT)</i>
OPT1: The security of the new technology makes me believe it is more effective and efficient at work, OPT2: The security of the new technology makes me feel more freedom in my activities in my work, OPT3: In trying to learn about security in new technologies I have found the benefits of those technologies
<i>Technology Readiness—Innovative (INV)</i>
INV1: From the service and security aspect, the new technology in my organization is easy to use, INV2: From the aspect of security, it is very helpful in activities in the work environment, INV3: With cyber security technology that is always updated, I feel a lot of interest
<i>Technology Readiness—Discomfort (DCT; reverse scored)</i>
DCT1: Guidelines that provided in my organization for using cyber security services are rarely read and paid attention to, DCT2: The manual book provided by my organization for cyber security is difficult to understand, DCT3: The assistance provided in my organization to handling security incidents made me uncomfortable
<i>Technology Readiness—Insecurity (INC; reverse scored)</i>
INC1: I am worried that confidential data and information may be widely publicized in my organization, INC2: I'm worried about the security of the online activity in my organization, INC3: I am concerned about confidential data and information to external providers
<i>Tangible Benefit (TB)</i>
TB1: In recent years, the employee performance in my organization have increased, TB2: In recent years my organization goals have been met, TB3: In recent years my organization security against cyber-attacks were controlled
<i>Intangible Benefit (IB)</i>
IB1: In my organization, Customer loyalty has increased in recent years, IB2: The number of new customers has increased in recent years, IB3: In recent years, my organization have had a significant competitive advantage among other organizations
<i>Top Management Support (Top)</i>
TopM1: Top management help to provide resources for adopting cyber security, TopM2: Top management help to understand the benefits of cyber security, TopM3: Top management help to encourage the development of cyber security, TopM4: Top management intends to issue supporting regulations for cyber security in my organization

Ahmad R. Alsaber, Ph.D. from University of Strathclyde, in 2022. His specialty is related to data-science, artificial intelligence and multivariate time-series analysis with focus on random forest, neural network and missing imputation analysis. In his research, he targeted materials with environmental, rheumatology studies, and multivariate time series analysis.

Parul Setiya is a dedicated and accomplished data scientist, specializing in biostatistics, with a rich academic and professional background rooted in India. After receiving her Ph.D. in Biostatistics, Dr. Setiya has accumulated over a decade of experience in leveraging the power of data to solve complex problems in the healthcare industry.