International Journal of Business Data Communications and Networking
Volume 19 • Issue 1

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

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