International Journal of Scientific Research and Management (IJSRM)
||Volume||12||Issue||06||Pages||1266-1273||2024||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v12i06.ec03

A Review of the Literature on an Examination of the Effects of Cyber Security in Improved Public Sector Institution Performance in Jordan

Alanoud Amer Saleem Alrkeebat

Abstract
One of the study's intended results was gaining a more precise knowledge of the present level of cyber security adoption by public sector institutions—particularly in Jordan. In order to improve the effectiveness of these institutions, the research reviewed various literature reviews on the current state of cyber security adoption. It also identified the obstacles these institutions faced in embracing and executing these technologies and the tactics required to improve cybersecurity applications. The assessment also highlighted cyber security initiatives that can boost operational effectiveness, enhance service delivery, and give the populace of the nation access to a safer digital environment. Therefore, by highlighting the difficulties and obstacles these organizations encounter, the research may contribute to formulating policy and decision-making frameworks that will direct future expenditures on cyber security and associated technology. Additionally, the results of this study may help improve cyber security protocols and implement them in Jordan's public sector organizations. This might thus result in better service delivery, more operational efficiency, and a safer online environment for the nation's people. The study may also contribute to policy and decision-making processes by highlighting the obstacles and difficulties these organizations confront, which might direct subsequent investments in cybersecurity innovations and technology.

Keywords: Artificial Intelligence, Cyber Security, Security Measures, Security Challenges, Digital Environment

Introduction

Ensuring the security of information systems requires corporations to emphasize security and implement risk-reduction measures. A crucial initial step is establishing robust access control procedures involving authorization and authentication. Authentication confirms a user's identity, whereas authorization establishes their degree of resource access. This assists in avoiding unauthorized access to private information by restricting access to authorized people. An essential extra safety measure is encrypting critical data in transit and with rest (Nwankwo & Ukaoha, 2019).

Data is encrypted or changed into code to prevent unauthorized access. This ensures that hackers cannot decipher the data even if they manage to obtain it. Regular security audits and evaluations are required to identify and address system vulnerabilities. This ensures that the system is safe and impervious to outside attacks. Employee education on cybersecurity and the risks associated with accessing or disclosing sensitive data is also essential. This comprises guidance on creating secure passwords, using safe online conduct, and spotting phishing scams (Atoum et al., 2017)

To sum up, the safety of information systems is essential, particularly for e-government and web-based banking operations. Businesses should stress cyber security and implement the necessary precautions to minimize risks and guarantee critical information integrity, safety, and availability.

Cyber Security

Cybersecurity refers to the methods and plans utilized to protect cyberspace from a wide range of known and unknown dangers. The International Telecommunications Union describes cybersecurity as a collection of measures, including engagement, standard procedures, security plans, training, threat executives, and expertise to safeguard enterprises, information systems, and their property. When malicious actors undertake

cyberattacks, information and communication technology (ICT) can be used as a weapon or target. Cybersecurity is crucial to stop attacks like these on the Internet, electrical systems, computer networks, and other equipment (Nwankwo & Ukaoha, 2019).

In the digital era, businesses depend increasingly on internet connectivity, which emphasizes the need for cybersecurity. Confidential information may be made public through hacking and information breaches, making a business less competitive. (Ewurah, 2017). The accessibility, privacy, and reliability of a company's information and communication technologies and data are all at risk from successful cyberattacks (Ali et al., 2021). Cyber theft, sometimes called cyber espionage, gives the invader an advantage by exposing financial, confidential, or private data while incurring the legitimate organization's money or intellectual property.

Jordan Public Sector Institutions

Cybersecurity has become a significant concern since public sector organizations increasingly depend on information and communication technology (ICTs) to provide residents with essential services. Since the consolidated budget or resources allotted by the legislature support public offices and services in Jordan, cybersecurity is crucial to guarantee these institutions' effective and safe functioning. The importance of this subject was demonstrated by the literature on how cybersecurity affects Jordanian public sector institution performance. Amer & Al-Omar (2023) examined how cybersecurity affected the operational efficiency of Jordanian government organizations. The study's findings indicate that cybersecurity breaches have the potential to seriously impair public sector organizations' performance and efficiency by causing significant financial losses, harm to their reputation, and interruption of vital services.

Al-Mariah (2022) investigated cybersecurity's potential to improve Jordan's e-government service delivery in different research. Strong cybersecurity measures are crucial, according to the authors, in order to safeguard private information and guarantee the privacy, accuracy, and accessibility of online services. They contended that strong cybersecurity policies may boost public confidence in e-government programs, boosting adoption rates and enhancing service provision. The literature also emphasizes the cybersecurity difficulties that Jordanian public sector Institutions confront.

Numerous studies have suggested frameworks and tactics for enhancing cybersecurity in the public sector to solve these issues. For example, Saleh, Obeidat, and Khamayseh (2013) created a thorough cybersecurity architecture specifically suited to the requirements of Jordanian government institutions. The framework emphasizes adopting a risk-based approach, implementing substantial access restrictions, and creating incident response and catastrophe recovery strategies. Moreover, the research emphasizes how international standards and best practices may improve government cybersecurity. Itradat et al.'s (2014) study examined how Jordanian government institutions implemented the ISO/IEC 27001 standard for information security management systems. The authors discovered that following this guideline may significantly strengthen public sector firms' overall security posture and increase their resistance to cyberattacks.

The literature highlights the significance of cybersecurity awareness, training for public sector workers, and technological solutions. Atom, Otoom, and Ali (2017) studied the Jordanian government employees' understanding of cybersecurity. The findings showed that extensive training programs were required to teach staff members about cybersecurity threats, best practices, and their roles in safeguarding sensitive data and vital systems.

The body of research on the impact of cybersecurity on Jordanian public sector institution performance emphasizes how crucial this problem is. In addition to safeguarding sensitive information and vital infrastructure, effective cybersecurity measures also increase public confidence, boost service delivery, and guarantee the smooth running of governmental institutions. However, tackling cybersecurity issues calls for a diversified strategy that includes establishing strong technological controls, adopting international standards, and encouraging a cybersecurity-aware culture among workers and residents.

Statement of the Research Problem

The performance and effectiveness of Jordan's public sector, which includes government ministries and related parastatals, are seriously threatened by severe cybersecurity risks. Cyber risks have become more prevalent due to deploying e-government solutions to enable the smooth delivery of public services across digital networks (Al-ma'aitah, 2022; Atoum et al., 2017). Several Jordanian-specific socio-cultural elements,

such as organizational procedures, technology infrastructure, human competencies, and socio-cultural dynamics, affect how well e-government systems are adopted (Al-Jaghoub et al., 2010).

The hacks on official websites in 2014 that exposed private, sensitive financial, and classified data highlighted the need for cybersecurity in Jordan's public sector. According to Amer & Al-Omar (2023) and Werlinger, Hawkey, & Beznosov (2009), these assaults caused significant financial losses estimated at over JOD 18 million (about USD 25 million), damaged public confidence in e-government projects and impeded the efficient provision of services. Therefore, research examining the variables impacting cybersecurity practices inside Jordan's public sector organizations is desperately needed.

The relationship between organizational management, security concerns, and the implementation of e-government has been highlighted in previous studies (Saleh et al., 2013). However, most research has been primarily technical, using quantitative methods to analyze information system security (Itradat et al., 2014; Siponen et al., 2006). The literature is still lacking in its exploration of the specific socio-cultural dynamics and their impact on traditional cybersecurity approaches within the Jordanian context, even though an extensive assessment of information system security emphasizes the significance of non-technical factors, such as organizational culture, employee awareness, and governance structures, in protecting sensitive information (Itradat et al., 2014; Werlinger et al., 2009; Siponen et al., 2006).

Understanding that public and private companies function differently and require different management approaches is essential (Siponen et al., 2009). Unlike private companies, public institutions in Jordan are subject to strategic planning and open deliberations over resource allocation by the legislative and executive branches, which can have political ramifications. Furthermore, rather than focusing on achieving financial sustainability, public organizations must uphold a physical presence and offer products and services for the benefit of the public (Siponen et al., 2009). As such, unique protocols and security frameworks suited to their particular operating environment must be followed by Jordanian public entity managers (Saleh et al., 2013).

Due to their intrinsic needs for openness, diffusion, and availability of information and services, e-government systems in Jordan pose unique privacy and security concerns. The literature suggests that, despite the topic's significance, there needs to be more empirical study on the relationship between cybersecurity and information and communication technologies (ICTs), specifically e-government in the Jordanian setting. Itradat et al. (2014) examined how Jordanian government institutions adopted the ISO/IEC 27001 standard for information security management systems, emphasizing how it may strengthen security posture and cyber threat resistance. Although this study offers insightful information, organizational and human aspects impacting cybersecurity procedures in Jordan's public sector should be more covered.

Similar to this, Saleh, Obeidat, and Khamayseh (2013) created a thorough cybersecurity architecture specifically suited to the requirements of Jordanian government institutions, stressing the significance of an incident response and disaster recovery plans, as well as a risk-based strategy and substantial access restrictions. Nevertheless, this study needs to explore the leadership and interpersonal factors that influence the successful use of these frameworks. In their study on cybersecurity awareness among Jordanian government workers, Atoum, Otoom, and Ali (2017) found that extensive training programs are necessary to inform staff members about cybersecurity risks, best practices, and their roles in safeguarding sensitive data and vital systems. Although the significance of human factors in cybersecurity is emphasized in this study, organizational and cultural elements that impact cybersecurity practices within Jordan's National Government Ministries are not particularly examined.

In conclusion, most of the material already written has concentrated on specific cybersecurity issues facing Jordan's public sector or cybersecurity concerns in various circumstances. A comprehensive study on how cybersecurity affects Jordan's public sector organizations—including government ministries and related parastatals—is needed. Such studies ought to examine the organizational, cultural, and psychological elements that impact cybersecurity procedures and the establishment of successful security frameworks in these establishments. This study vacuum may be filled to provide essential insights on how to strengthen cybersecurity measures specific to the operational reality and distinct socio-cultural setting of Jordan's public institutions, hence improving the performance and efficiency of these institutions.

Research Objectives

This research determined how cybersecurity improvements affected Jordanian public sector entities' performance. The study aimed to ascertain the extent of cyber security adoption in Jordanian public sector

institutions, assess the impact of enhancing cyber security on public sector performance, assess the obstacles public sector institutions in Jordan encounter while integrating and executing cybersecurity and AI, and suggest tactics for enhancing the integration and application of these technologies in public sector entities in Jordan.

Literature Review

Empirical Literature Review

The organizational and psychological elements that affect computer and information security (CIS) have been the subject of several studies. These investigations have covered a wide range of topics, such as employee acceptance and adherence to security rules, management support for CIS adoption and implementation, and the adoption and implementation of security strategies and policies (Ali, 2019). These studies have also shown several cultural elements of security systems, including reliable security protocols, top management support, governance, coordination and control, employee engagement and training, and workers' satisfaction with security. Other studies have studied information system security in terms of organizational and human aspects (Stewart & Jürjens, 2017).

Osho & Onoja (2015) identified several cybersecurity goals for Nigeria, including addressing ICT system and network vulnerabilities, developing a cybersecurity awareness culture among institutions and individuals, encouraging successful cybersecurity collaboration between private and public organizations, keeping up with emerging trends in cybercrime and their solutions, and guaranteeing the accessibility, integrity, confidentiality, and authenticity of systems.

Akbar et al. (2024) developed a three-layered model focusing on cloud computing security. The first layer included suitable user identification authentication techniques; the second layer included data identification and encryption for security; and the third layer involved using cryptography techniques to secure data transmission. In their research on current cybersecurity issues in India, Friedman & Hoffman (2008) discovered that although people prioritize security for their personal computers, they frequently ignore protection for their mobile devices, even though there is a chance that these devices would be the target of cyberattacks. According to their findings, personal firewalls can protect specific devices against dangers that come via wireless networks or the Internet.

In examining the literature, Hiller and Russell, 2013) concluded that most commercial and public organizations are working to protect data and information from hackers and cybercriminals. The authors pointed out that several tactics are being developed to safeguard data from hackers and that data sharing is difficult for public and commercial companies. Upadhyaya et al. (2012) identified several crucial factors that affect the security of e-government systems in developing nations. These factors include top management support, management and employee security awareness, information system security infrastructure, security culture, management change and security, style of management, and privacy regulations.

According to Panneerselvam's (2016) research, information security is hampered by technological advancements and social norms related to politics, culture, the law, and morality. This has implications for the development of e-government structures in certain African countries. The study found that e-government activities include many persons and are subject to several legal frameworks and laws, which adds complexity and subtlety to security challenges. Njoroge, Ogalo, and Ratemo (2021) studied the limiting factors impacting the cybersecurity assessment framework in Kenyan government ministries by looking at strategy, priority, baseline assessment, and behavior management in administration. The current study, which also considers human aspects and leadership in applying cybersecurity frameworks, is connected to this research.

In order to address system vulnerabilities and ensuing cyber-attacks, technology solutions have taken precedence over human and organizational aspects of information systems security (Werlinger et al., 2009). Critical systems must be protected because human and organizational components constantly interact with technology and systems. Management support, a security policy, employee education, and awareness all impact how successful ICT security is in a company (Yeh & Chang, 2007). Government organizations are increasingly using information systems (IS) more and more. A government needs an efficient, confidential, and trustworthy information system to preserve social and economic stability and compete globally. Public sector information systems that lack security can negatively affect public confidence and desire to use government agencies, thus jeopardizing social and economic stability (Ewurah, 2017).

In order to achieve successful cybersecurity, Ani, He, and Tiwari (2019)identified several essential elements, such as determining the ICT assets and exposure involved, putting cybersecurity standards and strategy into practice and following them, enhancing responsiveness to frequent technological changes and the threats they pose, addressing human factors in awareness and emerging vulnerabilities, and highlighting the importance of leadership in promoting positive change in cybersecurity strategy, human factors, and leadership.

It is crucial to remember that this study will be carried out worldwide, emphasizing rich countries, which can restrict its applicability to the public sector and developing country initiatives. Insiders who occasionally conduct cyberattacks can be broadly classified into three groups: (i) employees seeking retaliation for what they understand to be "disproportionate" treatment within the company as a whole; (ii) those within using the assets of the organization for their gain; and (iii) insiders who unintentionally assist outside attacks, although they are not the actual attackers (Wall, 2013).

Investigating psychological and organizational aspects Several factors, such as management support, worker acceptance and commitment, security policy implementation, and cultural elements like trust, management, collaboration, oversight, and worker engagement and training, have been found to have an impact on computer and information security (Ali, 2019). Various contexts have specified cybersecurity objectives, including fixing vulnerabilities, raising awareness, encouraging collaboration, and guaranteeing system integrity (Osho & Onoja, 2015).

Multi-layered models that include data encryption, user authentication, and cryptographic techniques for safe transmission have been presented in the context of cloud computing (Akbar et al., 2024). Research has also indicated that, despite the possible hazards, people prioritize security for their desktop computers over protecting their mobile devices (Friedman & Hoffman, 2008). The public and private sectors have acknowledged the difficulties associated with data sharing and the requirement for cybersecurity measures (Hiller & Russell, 2013).

Top management backing, security awareness, culture, infrastructure, and privacy rules are just a few of the factors that have been shown to influence e-government security (Upadhyaya et al., 2012). Beyond technological innovations, information security restrictions also include social norms and political, legal, cultural, and moral behaviors, especially regarding e-government activities involving several individuals and legal frameworks (Panneerselvam, 2016).

Research has examined the constraints found in cybersecurity assessment frameworks, including strategy, prioritization, behavior management, and baseline assessment (Njoroge et al., 2021). Additionally, Werlinger, Hawkey, and Beznosov (2009) highlighted the necessity of addressing organizational and human factors in addition to technological solutions. According to Yeh & Chang (2007), security policies, management commitment, employee training, and awareness are all related to the effectiveness of information and communication technology. Ewurah (2017) has also highlighted the significance of dependable information systems for the stability and competitiveness of government.

The identification of assets and exposures, the application of strategies and standards, the ability to adapt to threats and changes in technology, the consideration of human factors in vulnerability and awareness, and the importance of leadership in bringing about positive change are all considered critical components of successful cybersecurity (Ani et al., 2019). However, in the context of emerging countries and the public sector, the application of global research centered on rich countries may be restricted. Furthermore, it has been acknowledged that insider threats might originate from workers seeking personal benefit, retaliation, or inadvertently aiding external assaults (Wall, 2013).

Summary of Empirical Literature Review

The current corpus of research on public sector cyber security emphasizes how crucial it is for decision-makers to understand the ramifications of e-governments and how they work with existing systems. Organizations need to inventory their critical infrastructure assets to build a solid cyber security plan. If an organization does not know what it has, it cannot protect it. Comprehending the IT infrastructure of a business's assets may also help identify the sources and features of cyber hazards, enabling adequate preparedness.

Managers must analyze human factors and organizational issues that might lead to cyber security vulnerabilities because the structure is only as resilient as its most vulnerable component (Bougaardt & Kyobe, 2011). Worker's awareness, leadership dedication to strategies and policies, the structure of the

organization (especially information systems architecture), implementers' technology along with cyber security skills and training, and ethical conduct on the part of employees are among the components that prior research has identified. The challenges of safeguarding information in e-government have received little attention, especially in developing and Middle Eastern countries. Previous studies on e-government have primarily focused on the stages of development, adoption, and design. This study aims to close the knowledge discrepancy on the factors influencing cyber safety in public sector businesses in Jordan.

Review Observations

The public sector, which comprises the government and related parastatals, is most vulnerable to cyberattacks (Wirtz & Weyerer, 2017). A cyber security breach could lead to a variety of outcomes, such as the loss of intellectual property, financial loss, exposure of private customer information, disruption of business operations, increased expenses for rebuilding the organization's infrastructure, dwindling stakeholder confidence, loss of competitive advantage, distribution of operational strategies, and potentially even the dissolution of an organization or the loss of jobs. Cyberattacks cost Jordan's government agencies an estimated JOD five million in damages, whereas the financial services industry lost JOD 4 million. Wealthy nations invest large sums of money in e-government, yet unstable systems can negatively impact stakeholder trust and confidence.

Encouraging dependability and confidence in the provision of services requires e-government cybersecurity. E-government services may have different efficient cyber safety characteristics than those provided by the private sector because of their diverse operating settings and constraints. Cybersecurity issues fall into two groups: external attacker motivations and internal system defects or weaknesses that intruders can exploit.

The Internet's wide accessibility has made it easier for authorized people to utilize. However, it has also made vital infrastructure more vulnerable to hacking attempts by those who are not authorized. State departments and agencies have recently been using the Internet as an instrument of warfare against their enemies, particularly foreign governments (Joyner & Lotrionte, 2017). Cyberattacks may be classified into four main groups based on the underlying causes of the attackers: government-backed cyber aggression, severe and coordinated crime, philosophical and geopolitical extremism, and hacker exploitation. These assaults are motivated by various goals, including political, economic, and national security (Rahman et al., 2023). The underlying objectives behind these assaults are often hidden or obscured, even when the attacker poses as having a cause.

These days, extremist groups utilize the Internet to spread propaganda, locate funds, organize in-person attacks, and enlist new members. Financial gain is the primary motivation for non-political system assaults. For effective planning and execution of cyber security. Rahman, Wuest, and Shafae (2023) emphasize the need to classify and rank the many cyberattack sources. Analyzing the main motivations of cyber attackers concerning the company's systems is essential for successful cyber security strategy and execution.

Conclusion

Policymakers would discover great value in the study's conclusions as they would guide the development of policies and laws that affect specific internet users. Information security professionals may utilize the study's findings to choose the best action for dealing with cyber threats. Those employed in essential infrastructure and safety organizations responsible for safeguarding vital assets may find value in the study's examination of the model's shortcomings and recommendations for improvements against malevolent insiders and outsiders. The study's findings would broaden our understanding of cybercrime in Jordan's government sector. The study can also help identify possible research topics for internet safety in the general public sector for upcoming academics and researchers. The study's findings would also be an essential resource for other investigations.

References

1. Akbar, M., Waseem, M. M., Mehanoor, S. H., & Barmavatu, P. (2024). Blockchain-based cyber-security trust model with multi-risk protection scheme for secure data transmission in cloud computing. *Cluster Computing*, 1-15.

2. Ali, L. (2019). Cyber crimes-A constant threat for the business sectors and its growth (A study of the online banking sectors in GCC). *The Journal of Developing Areas*, *53*(1), 267-279.
3. Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, *11*(8), 3383.
4. Al-Jaghoub, S., Al-Yaseen, H., & Al-Hourani, M. (2010). Evaluation of Awareness and Acceptability of Using e-Government Services in Developing Countries: The Case of Jordan. *Electronic Journal of Information Systems Evaluation*, *13*(1), pp1-8.
5. Al-ma'aitah, M. A. (2022). Investigating the drivers of cybersecurity enhancement in public organizations: The case of Jordan. *The Electronic Journal of Information Systems in Developing Countries*, *88*(5), e12223.
6. Amer, T. B., & Al-Omar, M. I. A. (2023). The Impact of Cyber Security on Preventing and Mitigating Electronic Crimes in the Jordanian Banking Sector. *International Journal of Advanced Computer Science and Applications*, *14*(8).
7. Amer, T. B., & Al-Omar, M. I. A. (2023). The Impact of Cyber Security on Preventing and Mitigating Electronic Crimes in the Jordanian Banking Sector. *International Journal of Advanced Computer Science and Applications*, *14*(8).
8. Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2-35.
9. Atoum, I., Otoom, A., & Ali, A. A. (2017). Holistic cyber security implementation frameworks: A case study of jordan. *International Journal of Information, Business and Management*, *9*(1), 108.
10. Atoum, I., Otoom, A., & Ali, A. A. (2017). Holistic cyber security implementation frameworks: A case study of jordan. *International Journal of Information, Business and Management*, *9*(1), 108.
11. Bougaardt, G., & Kyobe, M. (2011, April). Investigating the factors inhibiting SMEs from recognizing and measuring losses from cybercrime in South Africa. In *ICIME 2011-Proceedings of the 2nd International Conference on Information Management and Evaluation: ICIME* (p. 62).
12. Ewurah, S. M. (2017). The concept of eGovernment: ICT policy guidelines for the policy makers of Ghana. *Journal of Information Security*, *8*(2), 106-124.
13. Friedman, J., & Hoffman, D. V. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management*, *7*(1-2), 159-180.
14. Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review*, *29*(3), 236-245.
15. Itradat, A., Sultan, S., Al-Junaidi, M., Qaffaf, R., Mashal, F., & Daas, F. (2014). Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study. *Jordan Journal of Mechanical & Industrial Engineering*, *8*(2).
16. Joyner, C. C., & Lotrionte, C. (2017). Information warfare as international coercion: Elements of a legal framework. In *The Use of Force in International Law* (pp. 433-473). Routledge.
17. Njoroge, P. M., Ogalo, J. O., & Ratemo, C. M. (2021). Information System Security Practices and Implementation Issues and Challenges in Public Universities. *European Journal of Information Technologies and Computer Science*, *1*(5), 11-15.
18. Nwankwo, W., & Ukaoha, K. C. (2019). Socio-technical perspectives on cybersecurity: Nigeria's cybercrime legislation in review. *International Journal of Scientific and Technology Research*, *8*(9), 47-58.
19. Osho, O., & Onoja, A. D. (2015). National cyber security policy and strategy of Nigeria: a qualitative analysis. *International Journal of Cyber Criminology*, *9*(1), 120.
20. Panneerselvam, R. (2016). Managing E-Commerce Adoption Challenges for SMEs in Developing Countries. In *Encyclopedia of E-Commerce Development, Implementation, and Management* (pp. 1241-1249). IGI Global.
21. Rahman, M. H., Wuest, T., & Shafae, M. (2023). Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use cases of cyberattack taxonomies. *Journal of Manufacturing Systems*, *68*, 196-208.

22. Saleh, Z. I., Obeidat, R. A., & Khamayseh, Y. (2013). A Framework for an E-government Based on Service Oriented Architecture for Jordan. *International Journal of Information Engineering and Electronic Business*, *5*(3), 1.
23. Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Technical opinion Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, *52*(12), 145-147.
24. Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information & Computer Security*, *25*(5), 494-534.
25. Upadhyaya, P., Shakya, S., & Pokharel, M. (2012). Information security framework for e-government implementation in Nepal. *Journal of Emerging Trends in Computing and Information Sciences*, *3*(7).
26. Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security journal*, *26*, 107-124.
27. Wirtz, B. W., & Weyerer, J. C. (2017). Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats. *International Journal of Public Administration*, *40*(13), 1085-1100.
28. Yeh, Q. J., & Chang, A. J. T. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management*, *44*(5), 480-491.