Remittances Review
September 2024,
Volume: 9, No: S 4, pp. 979-990
ISSN: 2059-6588(Print) | ISSN 2059-6596(Online)
Received : 25 July 2024, Accepted: 18 September 2024
DOI: https://doi.org/10.33282/rr.vx9i2.56

The Impact of IT Systems Support, Cybersecurity Implementation, and Network Security and Infrastructure Optimization on Organizational Efficiency: A Study of Financial and Energy Sectors

[1st] Izza Fatima, [2nd] Mohaiminul Alam, [3rd] Owais Ali, [4th] Muhammad Azhar Mushtaq, [5th] Muhammad Kaleem, [6th] Dr. Sadaqat Ali Ramay, [7th] Zaid Sarfraz

1. MS- Scholar, Computer Science, Department of Physical and Numerical Sciences
Qurtuba University of Science & Information Technology, Dera Ismail Khan, Khyber Pakhtunkhwa, Pakistan izzafatimaqu@gmail.com
2. Application Support Analyst L2/L3 Morgan Stanley Montreal, Quebec
3. Specialist as Cybersecurity ADNOC (Abu Dhabi National Oil Company)
Abu Dhabi , UAE
4. Department of Information Technology, Faculty of Computing & IT
University of Sargodha, Sargodha, 40100, Pakistan.
5. Department of Information Technology, Faculty of Computing & IT
University of Sargodha, Sargodha, 40100, Pakistan.
6. Department of Computer Science, TIMES Institute, Multan, Pakistan.
7. Department of Computer Science, MNS University of Engineering and Technology, Multan, Punjab, Pakistan.

Abstract

This study investigates the impact of IT systems support, cybersecurity implementation, and network security optimization on organizational efficiency within Pakistan's financial and energy sectors. The research aims to understand how these technological and security factors collectively contribute to enhanced operational outcomes. A quantitative research design was employed, utilizing a survey-based questionnaire distributed to professionals in the targeted sectors. A sample of 300 respondents was selected using purposive sampling, and the data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). The findings reveal that all three factors significantly and positively influence organizational efficiency, with cybersecurity implementation emerging as the strongest predictor ($\beta = 0.45$). IT systems support ($\beta = 0.30$) and network security optimization ($\beta = 0.25$) also exhibited significant effects, highlighting their role in streamlining processes and ensuring secure operational frameworks. The model demonstrated strong explanatory power ($R^2 = 0.68$), underscoring the substantial contribution of these variables to organizational efficiency. This study provides actionable insights for industry leaders and policymakers, emphasizing the importance of adopting advanced IT systems, robust cybersecurity measures, and optimized network infrastructures. The findings contribute to the literature on organizational efficiency, particularly in technology-intensive industries, offering theoretical and practical implications for sustainable growth.

Remittances Review
September 2024,
Volume: 9, No: S 4, pp. 979-990
ISSN: 2059-6588(Print) | ISSN 2059-6596(Online)
Keywords: IT systems support, cybersecurity implementation, network security optimization and organizational efficiency

1.0 Introduction

In today's world of digital time economy, the financial and energy sector has become more and more dependent on information technology (IT) systems to run their operations, establish customer relationships, and interchange data effectively. As these industries keep growing and changing, they have many challenges when it comes to the way that their IT infrastructure is operated and secured. Higher the robustness of IT systems support, better the cybersecurity measures and the optimization of network security and infrastructure, organizational efficiency often goes hand in hand with it. In order to perform operations smoothly, overcome cyber threats as well as maintain the performance of organization, these are the factors crucial. Both financial and energy sectors are high stakes as inefficiencies or security breaches can have enormous financial loss, regulatory penalties, and compromise of reputation. Consequently, organizations within these sectors spend significantly on sophisticated IT solutions as well as cybersecurity protocols to minimize risks and improve operational efficiency. Like everything else in IT infrastructure, continuous improvement needs are dynamic and organizations are seeking new strategies for optimizing their systems, securing their networks and working more efficiently.

The support for IT systems, cybersecurity implementation, network security, and infrastructure optimization in the realm of information technology is a complex and multifaceted relationship. ITS Support is the management and maintenance of hardware, software and networks which are necessary for an organization to function. There are technologies, processes & practices that are deployed to protect systems and data from cybersecurity threats like hacking, phishing & malware guaranteed cybersecurity implementation. Cybersecurity is a subset of network security, dedicated to ensuring that network and its data are secure and available. Infrastructure optimization is designing, operating and scaling IT systems to current and future operational requirements. In the first place, these variables are interrelated such that one variable influences the other variables and eventually affect organization efficiency. Effective IT systems support, for example, can assure that systems are properly configured to effect cybersecurity measures; a network infrastructure that is secure may halt cyberattacks from derailing operations. A number of theoretical frameworks, including the Resource-Based View (RBV) and the Technology-Organization-Environment (TOE) are utilized to identify how these variables interact to support an organizations overall performance. As per the RBV, IT systems are important resources, which can provide firm with a competitive advantage, and the TOE framework posits that organizational and environmental factors influence firms' adoption and implementation of technological innovations.

Although the relationship between IT systems support, cybersecurity, and network security, infrastructure optimization, and organizational efficiency have been extensively researched, there have also been gaps. Until now, most studies have focused on individual components of IT

infrastructure alone without any consideration to the holistic impact of all these factors at play at the same time. For example, although the significance of cybersecurity in protecting financial transactions and sensitive data has been repeatedly emphasized in the literature, there is a gap in the literature with regards to addressing the matter on whether cybersecurity measures embedded within a highly optimized network infrastructure can directly increase the efficiency of the organization. In addition, the specific dynamics of how these variables interact within the specific contexts of the financial and energy sector are under researched. The studies of the IT systems support in these sectors separately have not considered effect of cybersecurity and network optimization on organizational performance in combination. It is also another gap in the existing literature for the limited focus on the financial and energy sectors as separate case studies. Like it or not, both sectors rely very heavily on IT systems, but each has its own operational requirements and different security threats. The money businesses and their confidential data, therefore, warrant more care by the financial institutions, while energy companies are overly concerned with the physical and digital protection of their infrastructure (that is, power grids and energy management system). However, to develop suitable strategies to improve their organization's efficiency through IT systems, it is important to understand such sector specific nuance.

This study addresses the research problem of the need to research the combined effect of IT systems support, cybersecurity implementation, and network security and infrastructure optimization on organizational efficiency of the financial and energy sectors. Although several studies have measured these factors alone, no single comprehensive analysis has been made of how all of these things work together to improve efficiency. In this study, the interrelationships among these variables and their effects on organizational performance will be addressed in an effort to close this gap. Through an analysis of the financial and energy sectors, the study will provide a comparative point of view on how these sectors leverage IT infrastructure to optimize operations, secure their assets and operations, and improve efficiency overall. The investigation is critical since more and more companies in both industries depend on complex IT systems for the sake of continued competitive advantage in an increasingly complex technological field. Focusing on these sectors, the study will provide useful insights into the challenges and opportunities organizations face in utilizing IT to help increase their organizational performance.

The importance of this work is in the possibility of the collective influence of IT systems, cybersecurity, and network optimization in enhancing organizational efficiency that can enhance the understanding of such phenomena in high stakes domains such as finance and energy. The results can provide practical guidance for managers and decision makers in these professions who seek to strengthen their IT infrastructure, reduce threats to information security and improve operational performance. This research will help organizations tackle modern IT challenges by raising the awareness for how to approach IT systems management, cybersecurity and infrastructure optimization with an integrated approach. The study also makes important theoretical contributions to the literature by elucidating how these factors work together in the

context of the financial and energy sectors. These insights are critically important to organizations in these industries who continue to be challenged by changing security threats and operational realities and will enable them to make informed IT investment and long-term strategy decisions. Through addressing the gaps in the extant literature, and providing new perspectives on these issues, the study will contribute to the ongoing discourse on the role of technology in supporting organizational performance.

2.0 Literature Review

The Resource-Based View (RBV) and Technology-Organization-Environment (TOE) framework are the two main theoretical backbones for understanding the IT systems support, cybersecurity implementation and network security impact for achieving organizational efficiency. The RBV states that firms may achieve sustainable competitive advantage from resources, such as technological capabilities, if they possess those resources, they are valuable, (r)are, inimitable, and non(substitutable). In this case, IT infrastructure, such as systems support, network security and other information systems support, can be used as a critical resource to enable higher organizational efficiency. IT systems support, cybersecurity, and network optimization are considered as strategic asset that has to protect and optimize the flow of information, optimize operational efficiency, reduce the associated disruptions. However, the TOE framework shows that IT technologies adoption rely on technological, organizational, and environment factors. Network security protocols as well as optimized infrastructure, utilized for easing technological development, are considered as one of the areas that will improve the efficiency of organization, the same way they will improve the efficiency of financial business sectors and the energy sector since these two are suffering from huge operational and security risks. Successful implementation of these technologies depends very much on the organizational context (such as management support and resource allocation). Further environmental factors, such as market pressures, regulatory requirements and the competitive landscape determine how these technologies are adopted and used to improve efficiency. Combined, these are theoretical perspectives providing a thorough lens on how IT systems, cybersecurity and network infrastructure are connected and how they all contribute to organizational success.

Specifically, existing empirical studies have focused on IT systems support, cybersecurity, network security, and infrastructure optimization, and examined their individual and collective effect on organizational performance. By studying the role IT systems support can play in increasing the operational efficiency in the financial sector, Ali, et al., (2023) established that robust IT systems support makes decision making and operational agility better. According to their study, in addition to the integration of cybersecurity measures into IT systems support, this can reduce the possibility of risk and increase the firm's ability to react quickly to the threats and, at the same time, improve the overall efficiency of the firm. In the energy sector, too, Lee and Kim (2022) showed that improved network infrastructure and strong cybersecurity protocols made operations more resilient, including from rising cyber-attacks on critical energy infrastructure.

Instead, their findings showed that, when energy companies invested in detailed network security measures, they were able to reduce downtime and service interruptions thereby improving efficiency in their operations. There is a substantial body of literature emphasizing the criticality of such cybersecurity in the cases of the financial and energy sectors, with research pointing out the rising complexity of cyber-attacks and the related outcome for organizational performance. For instance, Zhang and Zhao (2021) study found that an organization that neglects to develop an efficient cybersecurity program will likely experience operational disruptions, financial losses, and damage to reputation, all of which are negative on organizational efficiency. Many studies have demonstrated how network optimization has made a similar significant impact on efficiency with network speed and reliability being pivotal toward enabling organizations to undertake transactions and maintain continuous operations. A unique study conducted by Rajasekaran et al. (2020) concluded that firms that invested in the infrastructure optimization via advanced networking technologies would benefit from increases in firm productivity, cost savings, smoother internal and external communication, and more streamlined operation, leading to an enhanced organizational efficiency.

Along with the sector specific studies, there have been broader investigations to understand the confluence of IT system, cybersecurity, and network optimization with the organization's performance. For example, according to Aydin et al. (2022), the study investigates the correlation of cybersecurity maturity with organization efficiency, which suggests that the high cybersecurity mature organizations can manage risk, prevent data breach incidents, and continue the operational processes better than others. The overall efficiency in their operations was further increased. A study by Nguyen, et al (2023) on financial sector identified the need for a well optimized IT infrastructure to optimise business operations, cut down on operational costs and offer better customer services. Focusing on the requirements of organizations in maintaining competitive advantages and economic advantages, the authors conclude that a strategic combination of support of IT systems, cyber security, as well as a network optimization must be in place. In contrast, an International Energy Agency (2021) report noted that energy companies were using more sophisticated IT systems and cybersecurity program frameworks to operate such global organizations and respond to increased threats from cyberattacks. It pointed out that energy companies should strengthen the network infrastructure and improve cybersecurity to keep a balance between business efficiency and the security of critical assets. Much of the existing literature has emphasized the importance of these technologies in enhancing organizational efficiency but few studies provide a holistic view of how all these elements are connected together, especially in the financial and energy sectors, where these technology investments bear higher risk and rewards.

The results of this study leverage the empirical findings to conclude IT system support, cybersecurity, and network security optimization have a critical effect on an organization’s efficiency. Other areas for further exploration include how these factors interact to influence the

combined effect on elements of performance in the financial and energy sectors, as well as the need to expand such research into areas outside of the financial and energy sectors. Additionally, the current literature does not provide a clear understanding of how organizational characteristics, in terms of size, management support and internal capabilities may shape adoption and effectiveness of these technologies. In addition, although it is known from prior studies that individual investments in IT support or cybersecurity can lead to increased efficiency, there is a lack of research to suggest how these elements as a whole contribute to organizational success.

Methodology

In this study, a Quantitative Research design was used to explore the impact of IT systems support, cybersecurity implementation, and network security and infrastructure optimization on organisational efficiency in the financial and energy sectors of Pakistan. The quantitative approach was appropriate for this study because it enabled the collection and analysis of numerical data with which relationships between the independent and dependent variables could be identified. The research design was based on structured data collection and analysis for the development, testing, and hypothesis formulation that the results can be generalized to a broader population identified in the given sectors. The study adopted a positivist philosophy, which matched with the quantitative research approach and was based on the need of objectivity and empirical measurement of the variables to be studied. Positivism was fit for this research in that the research aimed at building up causal connections and researching theories applying observable and quantifiable information.

For this study, we considered the population as organizations standing in the financial and energy sectors in Pakistan with their special focus on those which had implemented advanced IT systems and cybersecurity measures. They were selected for their critical dependence on secure and efficient IT infrastructure. Banks, insurance companies and other financial institutions comprised the financial sector, while electric power companies, energy distribution firms and oil and gas companies comprised the energy sector. These two sectors constitute the target population from which the study was drawn, because both of them encountered substantial challenge of keeping the IT systems secure and efficient, hence they were suitable contexts in which to explore the relationships between the study variables.

For this study, a sample of 300 employees was possible, of which 150 were from the financial sector and 150 from the energy sector. Respondents were selected from managerial and technical positions to directly participate in decision making processes, and to possess knowledge relevant to the implementation of IT systems, cybersecurity measures and network optimization strategies. For this study, stratified random sampling proved to be an excellent sampling strategy because it assured that the sample was representative of the population, and captured the variability in both sectors. The sample was stratified random sampling by subdividing the population into subgroups (strata) according to relevant characteristics, e.g., sector type (financial or energy) and

job position (managerial or technical). By using this approach, I was able to ensure that the sample was more likely to accurately mirror the different views that existed among the whole population and provide more exact comparison among the two sectors.

This study collected data through a survey questionnaire that drew on the respondents' perceptions of support for IT systems, cybersecurity implementation, network protection, and infrastructure optimization in the organizations. The questionnaire was made of a blend of Likert-scale items, multiple choice questions, and open-ended questions to catch both quantitative data and qualitative conclusions. Likert scale items were used to assess the respondents' views of the effectiveness of various IT and cybersecurity practices in improving organizational efficiency, and multiple-choice questions were employed to collect demographic data and organizational context. In order to get the widest possible range of respondents, the survey was done both online and in person. Before the full-scale data collection, the questionnaire was pre tested with small sample to detect reduction of ambiguities or problems.

Partial Least Squares Structural Equation Modeling (PLS-SEM) was used for data analysis. Whenever the research under consideration requires multiple variables investigation and if both reflective and formative constructs were involved, PLS-SEM is a powerful statistical method to use. This was an appropriate choice for this study as it enabled the usage of IT systems support, cybersecurity implementation, network security, infrastructure optimization, and organizational efficiency in the modeling of relationships between these different variables. Hypotheses were tested using PLS-SEM and an examination of the direct and indirect effect of the independent variables on organizational efficiency. Software like SmartPLS were used for carrying out the analysis by providing necessary tools for model estimation, path analysis and significance testing. Following that, the reliability and validity of measurement model was tested and subsequently structural model was conducted to test for the strength and the significance of the relationship between the constructs.

In this study, ethical consideration was a fundamental component that went into the research process to safeguard the benchmark of ethical conducts in research. All participants gave informed consent, i.e., knew the aim of study, that their participation was voluntary, and their right to withdraw at any stage without consequence. The responses were anonymized to protect respondent privacy and stored securely. To ensure that no sensitive or personal information was collected other than necessary, the survey did not ask for any details. The study also complied with ethical guideline relating to use of data, and reported findings honestly without manipulation. This also entailed transparency in the process of data analysis and responsible presentation of the results, so that the users were able to distinguish observed patterns from speculative interpretations.

4.0 Data Analysis

4.1 Reliability Analysis

The reliability analysis showed that all constructs had good internal consistency, with Cronbach's Alpha values higher than the set acceptable threshold value of 0.70. The reliability of measurement model was further reinforced by the composite Reliability (CR) values for IT Systems Support (0.91), Cybersecurity Implementation (0.92), Network Security Optimization (0.91) and Organizational Efficiency (0.93). Furthermore, all the constructs had above 0.50 Average Variance Extracted (AVE) values indicating that the constructs explain a sufficient proportion of variance from their indicators. This made sure the measures employed were alike for assessing the constructs in the model.

Table 4.1: Reliability Analysis

Construct	Cronbach's Alpha	Composite Reliability (CR)	Average Variance Extracted (AVE)
IT Systems Support	0.89	0.91	0.65
Cybersecurity Implementation	0.88	0.92	0.67
Network Security Optimization	0.87	0.91	0.66
Organizational Efficiency	0.90	0.93	0.68

4.2 Discriminant Validity Analysis (HTMT)

Discriminant validity among the constructs was evidenced in the HTMT analysis. No HTMT values were over the threshold of 0.90, and the highest value was 0.85 between IT Systems Support and Cybersecurity Implementation. The results suggest that each construct is empirically distinct and does not share substantial overlap with other constructs in the model. Results verify the theory behind separating IT Systems Support, Cybersecurity Implementation, Network Security Optimization, and Organizational Efficiency for the purpose of meaningful interpretation of the relationships between them.

Table 4.2 Discriminant Validity Analysis (HTMT)

Constructs	IT Systems Support	Cybersecurity Implementation	Network Security Optimization	Organizational Efficiency
IT Systems Support	-	0.85	0.78	0.80
Cybersecurity Implementation	0.85	-	0.82	0.79
Network Security Optimization	0.78	0.82	-	0.81

Constructs	IT Systems Support	Cybersecurity Implementation	Network Security Optimization	Organizational Efficiency
Organizational Efficiency	0.80	0.79	0.81	-

4.3 Model Fitness

Structural model fit indices indicated that the model was well specified and in keeping with acceptable standards. The SRMR value of 0.065 was less than 0.08, which is very good fit. The value of Normed Fit Index (NFI), 0.91, which is higher than benchmark value of 0.90, is an additional confirmation of the adequacy of the model. Furthermore, R^2 value for Organizational Efficiency (0.68) indicates that the predictors collectively explained a considerable amount of variance in the dependent variable thereby strengthening the stated model.

Table 4.3 Model Fitness

Fitness Index	Value	Threshold
SRMR (Standardized Root Mean Square Residual)	0.065	<0.08
NFI (Normed Fit Index)	0.91	>0.90
R^2 (Organizational Efficiency)	0.68	High (>0.26)

4.4 Structural Model Results

Results of the structural model showed significant and positive relationships between the independent variables with Organizational Efficiency. The standardized path coefficient (β) was moderate at 0.30 for IT Systems Support and 0.45 for Cybersecurity Implementation was the strongest influence. Network security optimization also affected significantly with a β of 0.25. The proposed hypotheses were supported by all relationships with p-values < 0.001. The findings suggest that IT systems and security related factors are important in facilitating organizational efficiency in the financial and energy sector.

Table 4.4 Structural Model Results

Path	β	Standard Error	t-value	p-value	Decision
IT Systems Support → Organizational Efficiency	0.30	0.05	6.00	<0.001	Supported

Path	β	Standard Error	t-value	p-value	Decision
Cybersecurity Implementation → Organizational Efficiency	0.45	0.06	7.50	<0.001	Supported
Network Security Optimization → Organizational Efficiency	0.25	0.04	6.25	<0.001	Supported

Discussion and Conclusion

This study found that IT systems support, cybersecurity, and network security optimization played a very crucial role to enhance the organizational efficiency of financial and energy sectors in Pakistan. Support demonstrated for IT systems having a positive and strong relationship with organizational efficiency was consistent with previous studies that have shown that technology is a significant factor in streamlining business operations, enhancing decision making and facilitating innovation (Alkhatib et al., 2023). The moderate 0.30 β coefficient shows that robust IT systems are foundational tools that boost overall efficiency through processes integration and efficiency improvement from redundant effort.

The strongest predictor was cybersecurity implementation, with β of 0.45, as the importance of cybersecurity in the digital economy grows. This finding shows that the connection to secure digital infrastructures to protect sensitive organizational data and build trust among the stakeholders is growing. This is line with recent literature, effective cybersecurity measures do not only mitigate risk, but also increase operational continuity and efficiency (Khan et al., 2022). The need here is to focus more in cybersecurity investments in sectors such as finance and energy that can suffer disastrous consequences from data breaches.

Network security and infrastructure efficiency had a similarly large impact (β = 0.25), reinforcing the need to maintain robust and efficient communication networks (β=0.25). Infrastructure that is efficient supports real time data flow, creates operational resilience, and allows organizations to respond quickly to market changes. Our findings are consistent with Rahman et al. (2021) which emphasize that optimal network infrastructure is a strategic enabler of increased productivity and service delivery in dynamic industries. Collectively, the results suggest that the integration of IT systems, well designed security measures and an optimized network infrastructure have a synergistic effect on organizational efficiency. As a validation of the substantial explanatory power of the proposed model, this is further supported by the high R^2 value (0.68), which shows that these factors altogether explain a considerable proportion of variance in organizational efficiency.

Conclusion

IT systems support; Cybersecurity implementation; Network security optimization are the major push factors for organizational efficiency in both the financial and energy sectors, as found in this study. There are several reasons for that, and each of them affect uniquely, with cybersecurity proving to be the most important one. The results suggest that companies must move toward the management of complex IT systems and proactive security measures as a means of staying ahead of the curve in a quickly changing environment.

Recommendations

Then based on the findings, organizations in the financial and energy industries are recommended to invest in whole framework of cybersecurity to protect their digital assets and operational processes. Furthermore, organizations should be able to enhance their IT systems by integrating the use of technologies that can both scale and be used easily to handle dynamic operational needs. It is also recommended that network infrastructure is regularly assessed and upgraded for optimal performance and security. With staff training programs to increase staff technological literacy and cybersecurity awareness, these measures are encouraged.

Implications

This study also offers theoretical implications for the growing literature on the efforts to improve organizational efficiency, evidencing the interconnected roles of IT systems and security measures. This study integrates these factors into an understanding of organizational efficiency with the aim of providing a more nuanced view of the joint impact that technological and security advancements can have on performance outcomes. The findings also provide practical direction to policymakers and industry leaders in Pakistan's financial and energy sectors. Therefore, policymakers should subsidize or offer tax breaks for adoption of technologies that enhance security and industry leaders need to incorporate these learnings into their strategic planning in order to improve competitiveness. In the end, this study also stresses on building a security conscious environment because it is a key to sustainable efficiency in a digitized economy. This integration of these findings into theoretical, practical, and policy frameworks illustrates the relevance of the study to tackling the issues that contemporary firms operating in technology sectors are facing.

References

Aydin, M., Kara, E., & Demir, H. (2022). Correlation between cybersecurity maturity and organizational efficiency in dynamic industries. *Journal of Cybersecurity and Risk Management, 12*(4), 67-89.

Ali, H., Hussain, M., & Khan, A. (2023). The role of IT systems support in enhancing decision-making agility and operational efficiency. *Journal of Business Technology and Management, 18*(2), 45-60.

International Energy Agency. (2021). Strengthening cybersecurity and IT infrastructure for operational resilience in the energy sector. *IEA Annual Report on Energy Systems*, 120-135.

Khan, R., Ali, Z., & Tariq, M. (2022). Cybersecurity practices and organizational performance in emerging economies: Evidence from the energy sector. *International Journal of Cybersecurity and Resilience, 18*(2), 67-89.

Lee, S., & Kim, J. (2022). Cybersecurity protocols for critical infrastructure resilience: A case study of the energy sector. *Asia-Pacific Journal of Information Systems, 14*(4), 89-102.

Nguyen, T. H., Tran, L. M., & Hoang, D. N. (2023). Optimized IT infrastructure for cost reduction and customer service enhancement in the financial sector. *Global Journal of Information Systems Research, 20*(3), 34-48.

Rajasekaran, K., Verma, S., & Singh, R. (2020). Network optimization as a strategic enabler of organizational productivity. *Journal of Information Systems Engineering, 9*(1), 23-35.

Rahman, H., Zafar, M., & Qureshi, K. (2021). Optimizing network infrastructure for improved organizational efficiency: A case study approach. *Journal of Information Systems and Infrastructure, 10*(3), 45-60.

Zhang, L., & Zhao, Y. (2021). The impact of cybersecurity deficiencies on organizational performance: A review. *Journal of Business Risk and Technology, 15*(5), 89-101.