Impact of Critical Infrastructure Protection as a Distributed Security System in Computer Networks in the Banking Sector

Abstract

Aims: Over the past few decades, technological advancements have significantly contributed to computer systems, becoming even more apparent in organisations and institutions. Therefore, the main aim of the current study was to analyse the impact of critical infrastructure protection as a distributed security system in computer networks in the context of the banking sector.

Method/Design: In the current study primary quantitative research method was used in which information was gathered from 200 participants using a survey questionnaire based on the 5-point Likert scale. For data analysis, descriptive and inferential analysis were used using the statistical software SPSS.

Findings: Findings in the regression analysis revealed that assistance in information and security and risk management has a positive and significant influence, whereas risk to control system has a negative and significant influence on the performance of security system in the computer network of the banking sector. Further, the moderating analysis also revealed that assistance in information and security and risk management moderating with the adoption of standardised technologies has a positive effect, and risk to control system moderating with the adoption of standardised technologies has a negative impact on computer networks of the banking sector.

Keywords: *critical infrastructure, banking sector, computer network, security, control system, risk management, cyber security.*

Introduction

Critical infrastructure includes the basic components essential for the normal and general working of society. Critical infrastructure is defined by Ouyang (2014) as the body of networks, assets, and systems that are critical for the continuation of the operation to ensure the safety and security of society, nation, or the health of the public. The demolition of critical infrastructure can significantly impact every aspect of life due to the failure to maintain functions (Walker-Roberts, Hammoudeh & Dehghantanha, 2018). Critical infrastructure can be viewed only as the nervous system of the economy of a nation that can make the nation difficult to function properly. However,

Ani et al. (2019) argued that critical infrastructure includes energy, industrial control, dams, and defence.

The debate and distress about the protection and safety of critical infrastructure are increasing. The real concern of the researcher is to protect the critical infrastructure of banking, economic development, and social development by emphasising the efficiency, production, and performance of critical infrastructure (Vugrin, 2016; Ani et al., 2019). In the modern world, all the systems and networks are coupled with critical infrastructure, receiving and transmitting crucial information. The coupling of all the systems creates the complex system known as the system of systems. The interconnectedness of the systems raises many questions about the security of the banking systems. Emerging new technologies like the internet of things are starting to be used in the banking system's critical infrastructure, creating new threats, cyber-attacks and vulnerabilities (Bairagi, Khondoker & Islam, 2016). Critical infrastructure offers many benefits if the system works properly and does not weaken. For this purpose, the critical infrastructure must not be harmed by any means and must be protected from all compromises that can potentially lead to destruction (CYBERSECURITY, 2013). Understanding the potential risks of security and the way to manage the protection software and tools has become crucial in the banking system.

The research was conducted to determine the importance of critical infrastructure as a dispersed system in the banking industry. Challenges faced by the banking industry's critical infrastructure were identified. The critical improvements infrastructure is making in the banking sector and the effect of critical infrastructure on computer networking in banking was identified in the research. Following are the aims and objectives of the research:

- To explore the significance of critical infrastructure projection as a distributed system in the banking sector
- To determine the challenges and opportunities in critical infrastructure projects faced by the banking sector.
- To identify the impact of the critical infrastructure projection in computer networks of the banking sector.

Literature Review and Hypothesis Development

CIP network protection is costly to run for corporations since it incorporates security technologies like Identification and Access Managing (IAM), Distributed Disruption of Systems (DDoS) prevention, Intrusion Detecting Systems (IDS), encrypting, and risks and accountability monitoring (Miloslavskaya, 2021). CIP refers to any resource, framework, or component or such which is extremely crucial for the servicing of crucially important socioeconomic operations, including the wellbeing, protection, stability, financial, or socioeconomic well-being of individuals and whose interruption or damage had a very significant influence as a result of the malfunction to preserve those processes. CIP incorporates factors crucial to standard business operations (Besenyő & Fehér, 2020).

Each banking institution can access copies of the most recent customer information due to a distributed databases monitoring system (DBMS) (Andrew, 2020). Furthermore, because the bank copies of the consumer's banking information, every transaction could be recorded and handled directly instead of being forwarded to a centralised server (Thach & Vu, 2021). Irrespective of the uptime of a centralised server, the distributed system enables banks to get the material they require when needed. Moreover, Besenyő (2020) argue that a distributed databases monitoring system enables banks can avoid unreliable site by redirecting their informational inquiries to another one. In order to ensure that the banking industry operates effectively, appropriate and comprehensive CIP with DBMS is essential. This is because it performs a significant role in defining the areas of operational processes and the different kinds of practises that could emerge within such a given industry.

Moreover, a DBMS with CIP is important for avoiding harm to technical data and resources due to a cyberattack or other disasters in the banking industry. Furthermore, it is essential to reduce the amount of damages in the case of an effective attack or a disaster (Zio, 2016). The following hypothesis has been developed based on the literature analysis to evaluate the impact of critical infrastructure protection on the Performance of Security systems in Computer Networks in the Banking Sector.

H1= Critical infrastructure protection has a significant effect on the Performance of Security systems in Computer Networks of the Banking Sector

The absence of security experts is the leading challenge to CIP in the banking industry. Security risks might result from a skill gap in public and private domains. Industry control structures (ICS), which enable CIP, are computerised structures that qualified cybersecurity experts must protect. Cybersecurity Ventures predicts that there will be 3.5 million jobs for security experts of CIP by 2023 (Shen, 2019). The ICS's interdependence has made the staffing problem worse. Economies like the UK and Japan are having trouble recruiting qualified cybersecurity specialists. One of the studies by Wu & Wang (2020) states that CIP operators lack operating technology (OT) cybersecurity expertise and seem incapable of managing CIP events in the banking industry. With the emergence of virtual markets, cybersecurity experts have a growing shortfall to control CIP in the banking industry. Security experts must be informed and qualified for CIP systems to be used properly.

Furthermore, the banking industry has opportunities in CIP due to the growing use of cloud computing and IoT technologies. The Internet of Things (IoT) and the clouds significantly contribute to the growth in demand for CIP services. CIP sectors like communications, IT, energy, and financial institutions have chosen cloud-based technologies to preserve private and sensitive information since the cloud technologies deliver dependable, affordable, and accessible alternatives. The Internet of Things Securities Institution (IoTSI) has published an IoT security paradigm with regulations to defend, manage, and monitor IoT security throughout banking institutions to protect IoT computer networks over these systems (Karagiannis & Polyviou, 2019).

An information and communication system (ICT) is a layout made up of devices, programming, content, and the users who have used these. Communication technologies, such as the internet, are frequently included. ICT is not similar to computer systems. To protect classified data from being misused, manipulated, deleted, or revealed, ICT security procedures are required (Mbilla & Ayimpoya, 2020). ICT facilitates business operations, management decisions, and workforce cooperation. Banking institutions increase the efficacy and productivity of their operations to consumers and enhance their competing positioning in rapidly evolving and rising

industries. Today, it is crucial for ICT to improve cybersecurity by preserving sensitive data and putting security procedures in place to avoid cybercriminals' activities, such as spamming and malware efforts (Peace & Abomeh, 2018). The following hypothesis has been developed based on the above literature review analysis for evaluating the relation between assistance in information and communication systems and the performance of security systems in computer networks of the banking sector

H2= Assistance in Information and Communication System has a significant effect on the Performance of Security System in Computer Networks of Banking Sector

Risk to control System is a collection of approaches the banking industry uses to assess prospective damages and take measures to lessen or remove them. It is a strategy that makes use of the results of risk evaluation, which entails evaluating possible risk elements in a firm's processes, including such technological and non-technical corporate characteristics, monetary policies, and some other concerns that might have an impact on the company's operations (Muhunyo & Jagongo, 2018). Moreover, the Risk to Control System makes proactive adjustments to mitigate risk within those domains. Thus, risk management facilitates businesses in minimising wasted resources and revenue. A crucial part of a bank's enterprise risks monitoring (ERM) procedure is the risk to management framework.

Furthermore, risk management is crucial for the banking industry's security network effectiveness. It safeguards from financial problems that could hurt the bottom lines while assisting banks in achieving their objectives and maximising earnings (Rahim & Faeeq, 2018). Based on the literature analysis, the following hypothesis has been formulated to determine the relationship between the Risk to Control Systems and the Performance of Security systems in Computer Networks of the Banking Sector.

H3= Risk to control System has a significant effect on the Performance of Security System in Computer Networks of Banking Sector

Security risk management is the dynamic procedure of determining such potential risks and implementing procedures to overcome these. The possibility that well-known threats might take advantage of flaws and their effects on costly assets are factors that help evaluate the risk. A

strong data security risk management approach in the banking industry is necessary for the sustainable implementation of security administration. One of the main objectives financial institutions evaluate their risk is to guard against expensive and disrupting disruptions. Risk management techniques can help secure personal details and defend businesses against cybercrime. The following hypothesis has been created to evaluate the relationship between Security and Risk Management and the Performance of Security systems in Computer Networks in the Banking Sector.

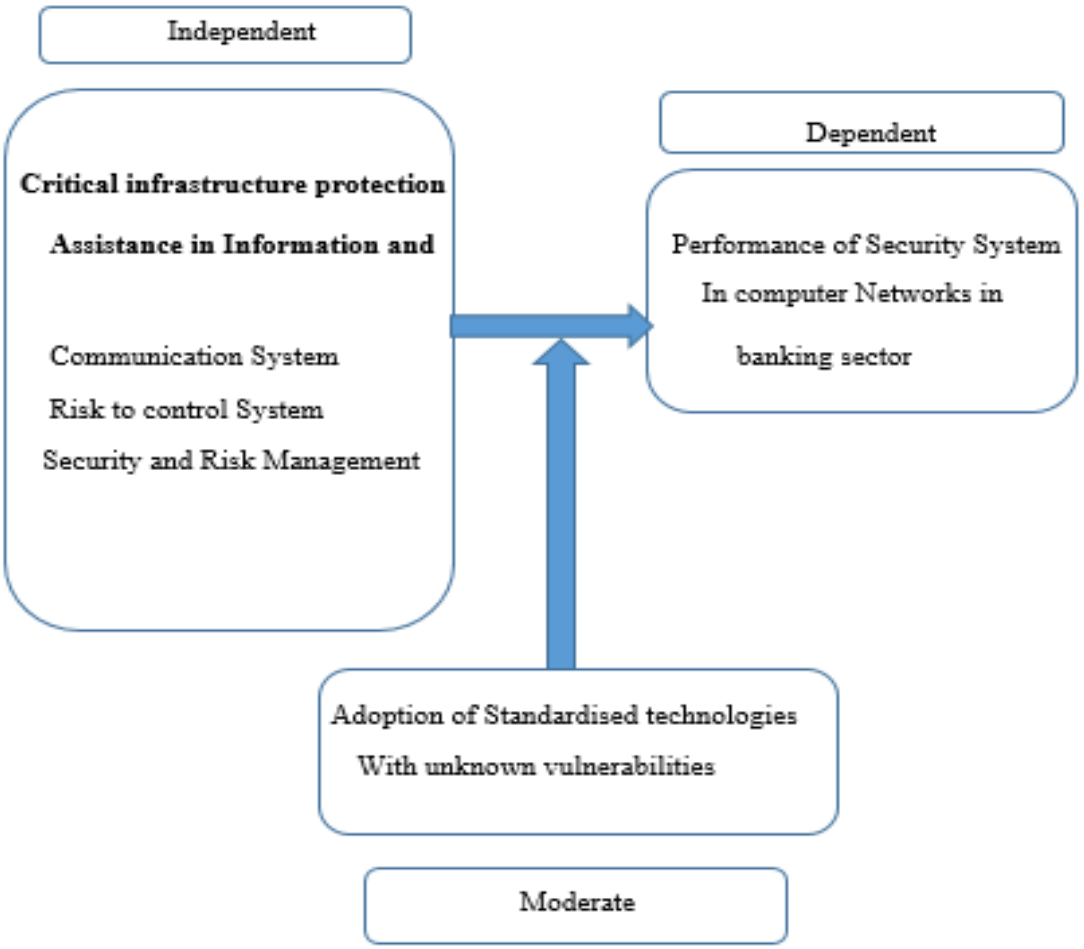
H4= Security and Risk Management has a significant effect on the Performance of Security System in Computer Networks of Banking Sector

Technology standardisation is the procedure of aligning software and IT infrastructures to a fundamental set of criteria that match the strategic plan, security guidelines, and objectives (Saleem & Ande, 2018). Furthermore, the Known Vulnerabilities are openly documented security flaws that are frequently discovered and documented by banking customers or security professionals in banking institutions. These problems are highly critical to fix since they are easily discovered and exploited by cybercriminals due to their critical nature (Brass & Blackstock, 2018). By adopting technology standardisation, banks can deliver services that nobody else does, increase revenue sources of banks, and give the banking sector CIP of their security systems. Furthermore, for the moderator, the following hypothesis has been created.

H5= There is a moderating effect of the Adoption of Standardised technologies with Known Vulnerabilities over the relationship between critical infrastructure protection and performance of security systems in the computer network of the banking sector.

Conceptual Framework

Figure 1 Conceptual Framework


Independent
Critical infrastructure protection
Assistance in Information and
Communication System
Risk to control System
Security and Risk Management
Dependent
Performance of Security System
In computer Networks in
banking sector
Adoption of Standardised technologies
With unknown vulnerabilities
Moderate

Methodology

Research philosophy refers to the fundamental assumptions that the investigator can use to lead their overall investigation project (Park & Artino, 2020). In the current analysis, the researcher employed the positivist philosophy. Positivist philosophy facilitates the investigator in distinguishing between observable and subjective material found in literature. Only those components were employed to build the literature assessment element that quantitative data might support. Furthermore, the positivist approach facilitated the analyst in overcoming biases from material gathered by emphasising objective information that was double-checked for validity and reliability.

The investigator in the present investigation used a quantitative research design, depending on numerical information to discover the facts (Bloomfield & Fisher, 2019). The quantitative methodology utilised literature to initially lay the groundwork for the data, which can then be applied to create the research questionnaire. The quantitative approach also facilitated using analytical techniques from mathematics and statistics that were crucial in assuring maximum reliability of the information and results. Systemic and psychological biases can be lessened through quantitative research. The research approach describes the methodology used to conduct an analysis (Pearse, 2019). The present analysis depended on a quantitative researcher design; hence, the investigator adopted a deductive method. Hypotheses have been constructed using a deductive methodology in the context of recent previous studies and the objectives and goals of this investigation.

Regarding the data collection, there are two main types of methods; primary and secondary data collection. Hence, in the current primary research, the quantitative research method has been used through a survey questionnaire. The primary reason for using this method as it enables the researcher to collect up-to-date information related to the research topic, and it assists in reducing the inherent biases. For data collection, the survey questionnaire was chosen based on the 5-point Likert scale, which assisted the researcher in determining the appropriate relationship between dependent and independent variables. Moreover, referring to the data sampling and size,

convenience sampling was employed to extract the information in which 200 participants were selected based on the convenience of participants' availability and accessibility. Furthermore, for data analysis, descriptive statistics were used to analyse the variables' features (i.e. mean and standard deviation). Correlation and regression analysis has also been used to determine the relationship between dependent and independent variables.

Results and Analysis

Descriptive Statistics Analysis

Table 1 - Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Risk to control System	200	.000	3.333	1.3117	.760
Assistance in Information and Communication System	200	.000	4.000	1.320	.948
Security and Risk Management	200	.000	4.0000	1.6234	.995
Performance of Security System in Computer Networks of Banking Sector	200	.000	4.000	1.478	.993
Adoption of Standardised technologies with Known Vulnerabilities	200	.0000	3.000	.9483	.914
Valid N (listwise)	200				

Descriptive statistics have been used as a first step to analyse the characteristics of the variables involved in the current study. From table 1, it can be seen that a total of 200 respondents have participated in the study, which is denoted by "N". Referring to the mean value, a risk to control system, assistance in information system, security and risk management, the performance of security system, and adoption of standardised technologies with known vulnerabilities are determined to be 1.31, 1.32, 1.62, 1.47, and 0.94 respectively. Thus, it implies that an average

number of respondents are inclined to agree. On the contrary, standard values of these variables are estimated to be 0.76, 0.94, 0.99, 0.99, and 0.91, respectively, which depicts that mean values are expected to remain towards agreeing.

Correlation Analysis

Table 2 - Correlation Analysis

		Risk to control System	Assistance in Information and Communication System	Security and Risk Management	Adoption of Standardised technologies with Known Vulnerabilities	Performance of Security System in Computer Networks of Banking Sector
Risk to control System	Pearson Correlation	1	.830**	.812**	.143*	.782**
	Sig. (2-tailed)		.000	.000	.044	.000
Assistance in Information and Communication System	Pearson Correlation	.830**	1	.961**	.123	.966**
	Sig. (2-tailed)	.000		.000	.083	.000
Security and Risk Management	Pearson Correlation	.812**	.961**	1	.112	.981**
	Sig. (2-tailed)	.000	.000		.116	.000
Adoption of Standardised technologies with Known Vulnerabilities	Pearson Correlation	.143*	.123	.112	1	.091
	Sig. (2-tailed)	.044	.083	.116		.199

Performance of Security System in Computer Networks of Banking Sector	Pearson Correlation	.782**	.966**	.981**	.091	1
	Sig. (2-tailed)	.000	.000	.000	.199	
	N	200	200	200	200	200

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 2 indicates the association between variables involved in the research. From the table, it can be seen that the performance of security systems in computer networks of the banking sector has a positive and strong association with all variables except the adoption of standardised technologies with known vulnerabilities. As it can be seen that the coefficient value of risk to control system is determined to be 0.782, assistance in an information system is 0.966, and security and risk management is 0.716. These values demonstrate that the performance of security systems in computer networks of the banking sector (dependent variable) has a strong and positive relationship with risk to control system, assistance in an information system, and security and risk management (Independent variables). On the contrary, the performance of security systems in computer networks of banking sectors has a positive but weak association with standardised technologies (Moderating variable).

Regression Analysis

Table 3 - Regression Analysis

a. Dependent Variable: Performance of Security System in Computer Networks of Banking Sector

Model		Unstandardised Coefficients B	Unstandardised Coefficients Std. Error	Standardised Coefficients Beta	t	Sig.
1	(Constant)	-0.007	0.026		-0.283	0.777
	Risk to control System	***-0.128	0.028	-0.098	-4.621	0.000

	Assistance in Information and Communication System	***0.387	0.047	0.370	8.251	0.000
	Security and Risk Management	***0.704	0.043	0.706	16.471	0.000
R-squared	0.986		Adjusted R-squared		0.973	

*Significant at 10%; **Significant at 5%; ***Significant at 1%

The above regression analysis table indicates the influence of independent variables on dependent variables. From the table, it can be seen that risk to control system has a negative and significant influence on the performance of security system in the computer network of banking sector, as coefficient value is determined to be -0.128, and P = 0.000 < 0.01. On contrary, assistance in information and security and risk management has a positive and significant influence on the performance of security system in computer network of banking sector, as coefficient values are found to be 0.387 and 0.704, and P-value = 0.000 < 0.01. Further, referring to the above table, the value of R-squared is found to be 0.986 which implies that 98.6% changes in the performance of security system in computer network of banking sector is due to the changes in the risk to control system, assistance in information, and security and risk management. The value of adjusted R-squared is found to be 0.973 which depicts that 97.3% model is fit for the analysis.

Interactive Regression Model

Table 4 - Interactive Regression Model

a. Dependent Variable: Performance of Security System in Computer Networks of Banking Sector

Model		Unstandardised Coefficients B	Unstandardised Coefficients Std. Error	Standardised Coefficients Beta	t	Sig.
2	(Constant)	1.166	0.075		15.493	0.000
	Risk to Control System * Adoption of Standardised technologies with Known Vulnerabilities	***-0.370	0.096	-0.639	-3.845	0.000

Assistance in Information and Communication System * Adoption of Standardised technologies with Known Vulnerabilities	***0.591	0.181	1.099	3.260	0.001
Security and Risk Management * Adoption of Standardised technologies with Known Vulnerabilities	0.004	0.153	0.010	0.029	0.977
R-squared	0.316		Adjusted R-squared	0.305	

*Significant at 10%; **Significant at 5%; ***Significant at 1%

The interactive regression model has also been used to analyse the moderating effect of adoption of standardised technologies with known vulnerabilities on the security system performance in the banking sector's computer network. From the above table, it can be observed that risk to control system moderating with adoption of standardised technologies has a negative and significant influence on security system performance. On the contrary, assistance in information and security and risk management moderating with adoption of standardised technologies has a positive effect on security system performance, as coefficient values of these variables are found to be 0.591, and 0.004 respectively. In addition to this, it is also important to note that only risk to control system and assistance in information has a significant influence on the performance of security system, as sig values are found to be less than 0.01.

Discussion and Hypothesis Assessment Summary

The main emphasis of the research was to analyse the influence of critical infrastructure protection as a distributed security system in computer networks in the context of the banking sector. For the purpose of this three main variables of critical infrastructure protection were identified i.e. risk to control system, assistance in information and communication system, and security and risk management, and how it influence on the computer networks of banking sector. Although, findings in the previous studies pointed out that critical infrastructure protection facilitates the business

organisation in its operation of computer network and enhance the performance of security system of computer network (Peace & Abomeh). Similarly, findings in the current study has also revealed that critical infrastructure protection enhance the security and risk management which in turn positively contributed in the performance of the security system in computer network of banking sector. More so, it has also been evidenced from the previous studies that risk to control system is one of the major barriers in implementing the critical infrastructure protection (Mbilla & Ayimpoya, 2020), and it has also been linked with the findings in the current research. However, following table provide a summary of hypothesis that has been accepted or rejected based on the findings in the current study.

Table 5 Hypothesis assessment summary

S. No.	Developed and tested hypothesis	Status
H1	The assistance in information and communication system has a significant effect on the performance of security system in computer network of banking sector.	Accepted
H2	Risk to control system has a significant effect on the performance of security system in computer network of banking sector.	Accepted
H3	Security and risk management has a significant effect on the performance of security system in computer network of banking sector.	Accepted
H4	There is a moderating effect of adoption of standardised technologies with known vulnerabilities between critical infrastructure protection and performance of security system in computer network of banking sector.	Accepted

Conclusion

The main emphasis of this research journal was to analyse the impact of critical infrastructure protection as a distributed security system in computer networks in the context of the banking sector. Hence, to address this aim primary quantitative research method was used through using a survey questionnaires, and information was collected from 200 participants (employees and

managers) in the banking sector. After gathering an information, descriptive, correlation, regression, and moderating analysis were used to determine the relationship between variables. However, findings revealed that assistance in information and security and risk management is considered as an opportunity from critical infrastructure protection, and it positively contributed in the performance of security system in computer network of banking sector. On contrary, risk to control system is one of the major challenge in critical infrastructure protection, and it negatively influence on the performance of security system in computer network of banking sector. Similarly, findings in the previous studies have also revealed that critical infrastructure assist in information, communication, and risk management which in turn positively contributed in the performance of the computer networks in the context of banking sector. Furthermore, adoption of standardised technologies was also used as a moderating variable. Findings revealed that assistance in information and security and risk management moderating with adoption of standardised technologies has a positive effect, and risk to control system has a negative impact on computer networks of the banking sector. Thus, based on the findings it can be said that critical infrastructure protection can help in enhancing the performance of security system in computer network of banking sector.

References

Andrew, L. (2020). The vulnerability of vital systems: how'critical infrastructure'became a security problem. In Securing 'the Homeland' (pp. 17-39). Routledge.

Ani, U. D., Watson, J. M., Nurse, J. R., Cook, A., & Maples, C. (2019). A review of critical infrastructure protection approaches: improving security through responsiveness to the dynamic modelling landscape.

Bairagi, A. K., Khondoker, R., & Islam, R. (2016). An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures. *Information Security Journal: A Global Perspective*, *25*(4-6), 197-212.

Besenyő, J., & Fehér, A. (2020). CRITICAL INFRASTRUCTURE PROTECTION (CIP) AS NEW SOFT TARGETS: PRIVATE SECURITY VS. COMMON SECURITY. Journal of Security & Sustainability Issues, 10(1).

Besenyő, J., & Fehér, A. (2020). CRITICAL INFRASTRUCTURE PROTECTION (CIP) AS NEW SOFT TARGETS: PRIVATE SECURITY VS. COMMON SECURITY. Journal of Security & Sustainability Issues, 10(1).

Bloomfield, J., & Fisher, M. J. (2019). Quantitative research design. Journal of the Australasian Rehabilitation Nurses Association, 22(2), 27-30.

Brass, I., Tanczer, L., Carr, M., Elsden, M., & Blackstock, J. (2018). Standardising a moving target: The development and evolution of IoT security standards.

Karagiannis, I., Mavrogiannis, K., Soldatos, J., Drakoulis, D., Troiano, E., & Polyviou, A. (2019). Blockchain-Based Sharing of Security Information for Critical Infrastructures of the Finance Sector. In Computer Security (pp. 226-241). Springer, Cham.

Mbilla, S., Nyeadi, J. D., Gbegble, M. K., & Ayimpoya, R. N. (2020). Assessing the impact of monitoring, information and communication on banks performance in Ghana. Asian Journal of Economics, Business and Accounting, 14(3), 58-71.

Miloslavskaya, N. (2021). Network protection tools for network security intelligence centers. *Procedia Computer Science*, *190*, 597-603.

Muhunyo, B. M., & Jagongo, A. O. (2018). Effect of internal control systems on financial performance of public institutions of higher learning in Nairobi City County, Kenya. International Academic Journal of Human Resource and Business Administration, 3 (2): 273, 87.

Order, E., & Cybersecurity, I. C. I. (2015). President Barak OBAMA decree 12 February 2013. *URL: https://www. Whitehouse. gov/the-press office/2013/02/12/executive-order-improving-critical-infrastructure cybersecurity, Consult at May*.

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & system safety*, *121*, 43-60.

Park, Y. S., Konge, L., & Artino, A. R. (2020). The positivism paradigm of research. Academic Medicine, 95(5), 690-694.

Peace, N. N., Sidi, C. P., & Abomeh, O. S. (2018). Impact of information and communication technology on the performance of deposit money banks in Nigeria. International Journal of Management and Sustainability, 7(4), 225-239.

Pearse, N. (2019, June). An illustration of deductive analysis in qualitative research. In 18th European conference on research methodology for business and management studies (p. 264).

Rahim, N. F. A., Ahmed, E. R., & Faeeq, M. K. (2018). Internal Control System and Perceived Operational Risk Management in Malaysian Conventional Banking Industry. Global Business & Management Research, 10(1).

Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. (2018, June). IoT standardisation: Challenges, perspectives and solution. In Proceedings of the 2nd international conference on future networks and distributed systems (pp. 1-9).

Shen, S. (2019). Critical infrastructure and climate change. In The Routledge Handbook of Urban Resilience (pp. 117-129). Routledge.

Thach, N. N., Hanh, H. T., Huy, D. T. N., & Vu, Q. N. (2021). technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in

emerging markets-the case in Vietnam. International Journal for Quality Research, 15(3), 845.

Vugrin, E. D. (2016). Critical infrastructure resilience. *An edited collection of authored pieces comparing, contrasting, and integrating risk and resilience with an emphasis on ways to measure resilience*, *236*.

Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A. (2018). A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access*, *6*, 25167-25177.

Wu, Y., Dai, H. N., & Wang, H. (2020). Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. IEEE Internet of Things Journal, 8(4), 2300-2317.

Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering & System Safety, 152, 137-150.

Appendix

Demographic Characteristics

Gender

0 = Male

1 = Female

Age

0 = 20 - 25

1 = 26 - 35

2 = 36 – 49

3 = 50 and Above

Occupation

0 = Employee

1 = Manager

ajbmss.org

Survey Questionnaire

Variable/ Codes	**0**	**1**	**2**	**3**	**4**
Independent Variables	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
Risk to control System					
To what extent do you agree that risk to control system negatively impact on the computer network system of banking sector.					
Mitigation of risk to control system can help in enhancing the performance of security system in computer network of banking sector.					
Risk to control system is essential to control for the effectiveness of critical infrastructure protection					
Assistance in Information and Communication System					
To what extent do you think information and communication systems improve the performance of security systems in computer network of the banking sector.					
Critical infrastructure protection helps in information and communication system					
Information and communication system has a significant influence on the performance of security system in computer network of banking sector.					

Security and Risk Management					
Critical infrastructure protection ensure the security of their customers in the banking sector.					
It also assist in the management of risk and vulnerabilities.					
To what extent do you agree that critical infrastructure protection enhances the capabilities of the banking sector in management of risk?					
Moderating Variable					
Adoption of Standardised technologies with Known Vulnerabilities					
Adoption of Standardised technologies can help in reducing the risk to the control system.					
Adoption of Standardised technologies in banking sector enhance the information and communication system.					
It also help in reducing the risk of security which leads to improvement in the performance of security system in computer network of banking sector.					
Dependent Variable					
Performance of Security System in Computer Networks of Banking Sector					
To what extent do you prefer critical infrastructure protection in the banking sector?					

Performance of security system in computer network of banking sector can be enhance through adoption of Standardised technologies.					
There is a strong association of critical infrastructure protection and performance of security system in computer network of banking sector.					