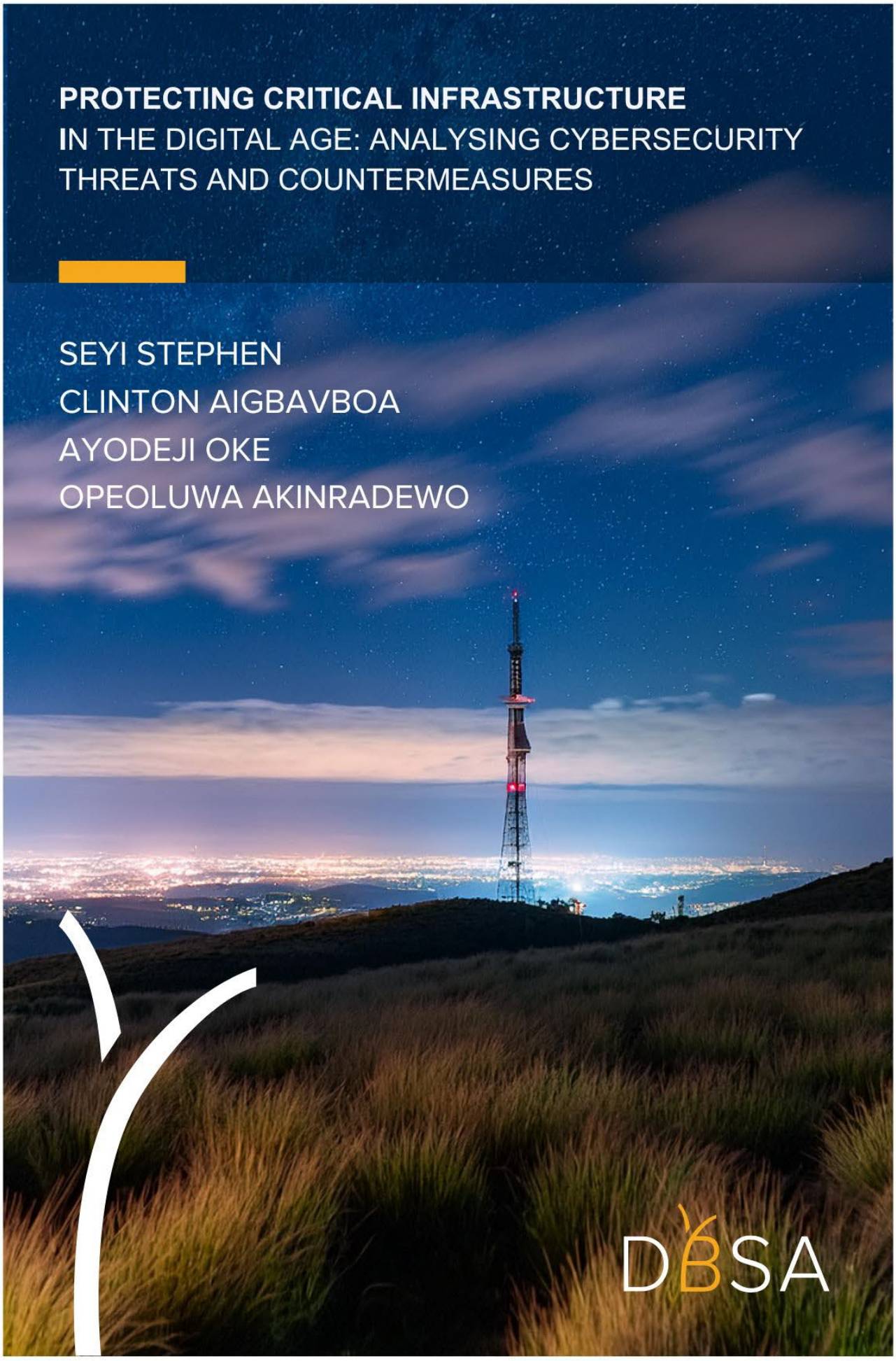
PROTECTING CRITICAL INFRASTRUCTURE IN THE DIGITAL AGE: ANALYSING CYBERSECURITY THREATS AND COUNTERMEASURES

SEYI STEPHEN
CLINTON AIGBAVBOA
AYODEJI OKE
OPEOLUWA AKINRADEWO



DBSA

PROTECTING CRITICAL INFRASTRUCTURE IN THE DIGITAL AGE: ANALYSING CYBERSECURITY THREATS AND COUNTERMEASURES

Seyi STEPHEN[1], Clinton AIGBAVBOA[1], Ayodeji OKE[1], and Opeoluwa AKINRADEWO[1]

[1]Department of Construction Management & Quantity Surveying, University of Johannesburg, South Africa.

Email: seyistephen.ss@gmail.com; caigbavboa@uj.ac.za; emayok@gmail.com; opeakinradewo@gmail.com*

ABSTRACT

This study explored the concerns surrounding infrastructure and cybersecurity in the South African construction industry (SACI), revealing significant apprehension regarding the impact of cybersecurity threats on infrastructure resilience. A quantitative research approach was employed, involving the distribution of 86 structured questionnaires to key construction stakeholders, including architects, engineers, builders, and quantity surveyors, alongside cybersecurity experts. The data collection process spanned four months and utilized random sampling techniques to ensure diverse participation. Data analysis incorporated descriptive statistics, exploratory factor analysis (EFA), and non-parametric tests such as the Kaiser-Meyer-Olkin (KMO) measure and Bartlett's test of sphericity to validate the results. The findings revealed that two-factor authentication emerged as the most effective cybersecurity practice, followed by one-time passwords, firewalls, and encryption techniques. Other important practices included utilizing threat intelligence, adopting a comprehensive and strategic cybersecurity approach, and implementing incident preparedness plans. The study highlighted the dynamic, evolving, and sophisticated nature of cybersecurity threats, necessitating adaptive and responsive countermeasures. Ongoing research, continuous innovation, and proactive strategies are essential to maintaining infrastructure resilience in the face of emerging digital threats. Additionally, continuous cybersecurity training, education, and awareness programs tailored for construction stakeholders are crucial for mitigating potential risks. Furthermore, the study emphasised the importance of fostering collaboration between government agencies, infrastructure operators, construction professionals, and cybersecurity experts to develop and implement effective, adaptive cybersecurity strategies. The contribution of the study lies in its focus on protecting critical infrastructure by addressing cybersecurity challenges, thereby ensuring that the systems supporting modern society continue to function efficiently, safely, and without disruption.

Keywords: Adaptive strategies, Countermeasures, Critical infrastructure, Cybersecurity, Digital Age

INTRODUCTION

As the world is connected, safeguarding critical infrastructure has become paramount as we navigate the complexities of the digital age (Argyroudis et al., 2022). The threat landscape has evolved dramatically with the increasing integration of technology into essential systems like energy grids, transportation networks, and financial institutions (Lukasik, 2020). Humayun et al., (2020) stated that cybersecurity threats loom large, ranging from sophisticated nation-state attacks to opportunistic cybercriminal activities. Understanding these threats and implementing effective countermeasures is essential to ensure the resilience and reliability of our critical infrastructure.

According to Lehto (2022), background research reveals a concerning trend, namely that the frequency and sophistication of cyber-attacks targeting critical infrastructure are rising. Incidents such as the 2015 Ukrainian power grid attack and the 2020 SolarWinds supply chain breach underscore the vulnerability of essential systems to malicious actors (Rees and Rees, 2023). These attacks disrupt operations and pose significant security, public safety, and economic stability risks. Addressing cybersecurity vulnerabilities becomes an urgent priority as our reliance on digital systems grows.

Despite increased awareness and investment in cybersecurity, a notable knowledge gap persists regarding the most effective strategies for protecting critical infrastructure in the digital age, especially in developing countries (Schmitt, 2023). While various frameworks and technologies exist, determining the optimal approach remains challenging. Additionally, the evolving nature of cyber threats requires continuous adaptation and innovation in defensive measures. Bridging this gap requires comprehensive research that analyses emerging threats, evaluates existing countermeasures, and identifies areas for improvement. By addressing these gaps in knowledge, the study aims to evaluate strategies to mitigate cyber risks and safeguard our critical infrastructure effectively.

LITERATURE REVIEW

Cybersecurity Threats in Critical Infrastructure

Critical infrastructure refers to the essential systems, services, and assets for society, economy, and national security (Argyroudis et al., 2022). It cuts across energy, transportation, water, communications, healthcare, financial services, emergency services, etc. (Schmitt, 2023). Protecting critical infrastructure in the digital age is increasingly challenged by cybersecurity threats, necessitating robust countermeasures to mitigate risks and ensure resilience (González-Granadillo, González-Zarzosa and Diaz, 2021). Dhirani, Armstrong and Newe (2021) and Djenna, Harous and Saidouni (2021) have extensively explored the evolving landscape of cyber threats targeting critical infrastructure sectors such as energy, transportation, healthcare, and finance. Ervural and Ervural (2018) and Coburn et al. (2019) have highlighted the vulnerability of these sectors to cyber-attacks, pandemics, extreme weather, acts of terrorism, accidents, or technical failures, emphasising the potential for widespread disruption and economic loss, as shown in Figure 1. Vulnerabilities peculiar to cybersecurity are data exfiltration, contagious malware, financial theft, cloud outages, and distributed Denial of Service (DDoS) attacks, as illustrated in Figure 2 below.

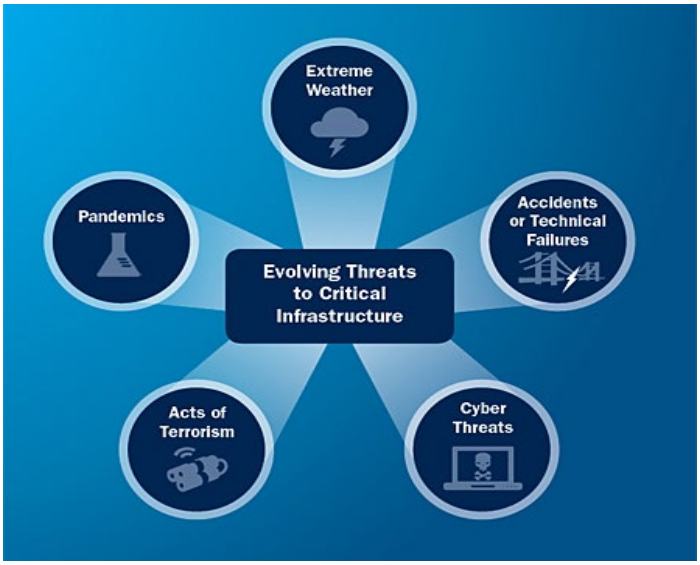


Figure 1: Evolving threats to critical infrastructure (IT-Online, 2023)

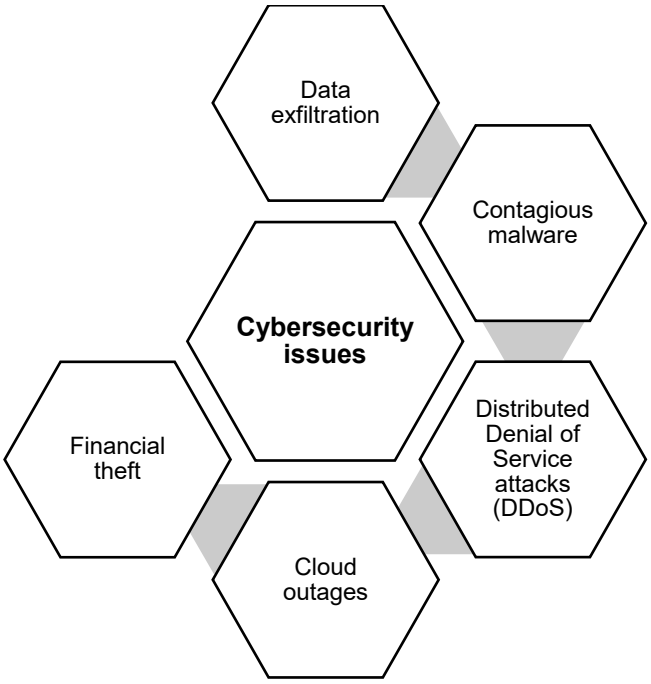


Figure 2: Issues associated with cybersecurity (Ervural and Ervural, 2018; Coburn et al., 2019)

Analysing cybersecurity threats to critical infrastructure reveals various attack vectors, including malware, ransomware, denial-of-service attacks, and insider threats. Eunice et al., (2021), Mallik et al., (2019) have investigated threat actors' tactics, techniques, and procedures to infiltrate and compromise critical systems, emphasising the need for initiative-taking defence mechanisms. As illustrated in Figure 3, the researchers summarised firewalls, intrusion detection systems (IDS), digital certificates, one-time passwords (OTP), two-factor

authentication, security tokens, digital signatures, vulnerability scanning tools, and biometrics as security tools to counter cyber-attacks.

Figure 3: Security tools for cybersecurity (Eunice et al., 2021; Mallik et al., 2019)

In response to these challenges, countermeasures and best practices have been proposed to enhance the cybersecurity posture of critical infrastructure (Shokry et al., 2022). These include implementing robust access controls, deploying intrusion detection and prevention systems, conducting regular vulnerability assessments, and fostering information sharing and collaboration among stakeholders (Di Pietro et al., 2020). Additionally, Telo (2023) stated that integrating advanced technologies such as artificial intelligence and blockchain holds promise for improving the detection and mitigation of cyber threats in critical infrastructure environments.

This section underscores the urgency of addressing cybersecurity threats to safeguard critical infrastructure in the digital age. By analysing emerging threats and deploying effective countermeasures, stakeholders can mitigate risks, enhance resilience, and ensure the continued operation of essential services vital to society and the economy, as reiterated by Vähäkainu, Lehto and Kariluoto (2022). However, ongoing research and collaboration are essential to stay ahead of evolving cyber threats and adapt to the dynamic nature of the cybersecurity landscape.

Need For Cybersecurity in Critical Infrastructure

As critical infrastructures become increasingly interconnected, a pressing need arises to defend against targeted cyber threats to disrupt or damage vital systems (Argyroudis et al., 2022). Ensuring the uninterrupted operation of essential services is imperative, as it safeguards public safety and preserves economic stability. Moreover, these infrastructures must possess interoperability capabilities with other digital technologies and practices, such

as digital twins (DT), building information modelling (BIM), artificial intelligence (AI), and smart building systems. This integration enhances overall efficiency and effectiveness, facilitating better management and response to evolving challenges in the digital age.

The transition towards real-time access to data and intelligence marks a notable change in thinking in protecting critical infrastructures, driven by the dynamic interplay between the physical and digital realms known as the Physical-to-Digital-to-Physical (PDP) loop (Kaivo-oja et al., 2020). This evolution is underpinned by eleven pillars of technological advancement encompassing big data analytics, autonomous robots, simulation and augmented reality, horizontal and vertical integration, supply chain optimisation, additive manufacturing, cloud cybersecurity, the industrial internet of things, artificial intelligence, and novel business models shown in Figure 4 (Tortorella et al., 2021). In embracing the digital era of Industry 4.0, these pillars revolutionise production processes and redefine the infrastructure necessary for future endeavours. Collaboration across government entities, individuals, organisations, and consumers facilitates realising goals within existing resources and personnel capabilities.

Figure 4: Pillars of technological advancement of Industry 4.0 (Haiston, 2023)

RESEARCH METHODOLOGY

The study employed a quantitative methodology through questionnaires to gather information about the study. This method was obtained for the study as it allows for the systematic measurement and analysis of data, providing empirical insights into the prevalence, patterns, and effectiveness of different security measures, thereby enhancing the precision and objectivity of the research findings (Zyphur and Pierides, 2017). Out of the 150 questionnaires distributed over four (4) months, 86 respondents were obtained. A random sampling was employed to select respondents from different South African construction industry professionals. It was adopted because it provides an unbiased representation of the study's population, ensuring that each member has an equal chance of being selected, which enhances the generalisability and validity of the results. The respondents were construction stakeholders (architects, builders, engineers, quantity surveyors) and cybersecurity experts in the South African construction industry (SACI). Demographic results revealed from the study regarding the background information showed that 33.8% of the SACI construction professionals had spent 6 to 10 years in the sector the responses gathered. Also, there was no bias as construction managers, civil engineers, and quantity surveyors comprise over 50% of the respondents' professions and other professions in the study's sample population.

While most respondents worked in consultancy, government and contracting firms duly represented others. Furthermore, the respondents have an average of nineteen (19) years of experience in the industry with a minimum average qualification of a bachelor's degree in relevant fields. With the respondents handling an average of ten (10) projects in construction (with relevance to modern buildings erected now), it is viable to deduce that they are more than capable of doing justice to cybersecurity-related topics in the SACI, owing to their vast academic and professional experiences in the industry. Their opinions (perceptive) are thus validated and can be relied upon now or for further studies.

RESEARCH RESULTS

Table 1 presents the mean scores, standard deviations (SD), commonalities extraction values, Kruskal-Walli's statistics, and ranks for various practices to improve cybersecurity. Two-factor authentication emerges as the top-ranked practice with the highest mean score of 4.55, followed closely by one-time passwords (4.51) and firewalls (4.48). These practices also exhibit low standard deviations, indicating an elevated level of agreement among respondents regarding their effectiveness. Other notable practices with high mean scores include utilising threat intelligence, adopting a strategic approach, and being prepared for cybersecurity incidents. On the other hand, practices like picking the right plan and personal data protection have lower mean scores, suggesting a perceived lower effectiveness. The communalities extraction values indicate the proportion of variance explained by each practice, and higher values suggest better explanatory power. The Kruskal-Wallis statistics and ranks provide insights into the variability and significance of differences among the practices. The table comprehensively overviews perceived effectiveness and variance in cybersecurity practices.

Table 1: Practices for improving cybersecurity

Practices for improving cybersecurity	Mean	SD	Communalities extraction		Kruskal-Wallis	Rank
Two-factor authentication	4.55	0.597	0.758		11.00	1
One-time password	4.51	0.737	0.573		4.40	2
Firewalls	4.48	0.598	0.609		3.00	3
Biometrics	4.47	0.661	0.680		7.61	4
Utilise threat intelligence	4.47	0.680	0.661		4.81	5
Digital signature	4.43	0.594	0.638		2.52	6
Strategic approach	4.43	0.733	0.693		3.34	7
Digital certificate	4.40	0.654	0.522		6.22	8
Be prepared for when, not if	4.40	0.799	0.819		5.50	9
Cyber liability insurance	4.40	0.712	0.710		3.71	10
Security tokens	4.39	0.610	0.621		6.36	11
Vulnerability scanning tool	4.39	0.691	0.766		10.20	12
Focus on compliance	4.39	0.652	0.799		8.45	13
Collaborate and report	4.39	0.746	0.752		5.59	14
Intrusion detection system	4.38	0.586	0.633		10.40	15
Personal data protection (PDP)	4.38	0.726	0.734		5.74	16
Private sector-initiated cybersecurity implementation frameworks	4.36	0.724	0.688		3.19	17
Evaluating risks so it is properly allocated through contract	4.36	0.724	0.611		4.76	18
Capacity building and awareness	4.36	0.647	0.593		2.66	19
Adopt a defence-in-depth approach	4.35	0.703	0.661		4.93	20
Promote a security-focused cyberculture	4.35	0.644	0.547		5.19	21
International information security standards	4.34	0.736	0.758		7.76	22
Developing national cybersecurity strategies/agendas	4.32	0.768	0.618		2.81	23
Picking the plan that is right for you	4.31	0.674	0.463		5.02	24
The role of the private sector in cybersecurity	4.31	0.693	0.725		5.49	25
Country-initiated cybersecurity implementation frameworks	4.30	0.745	0.744		6.29	26
National cybersecurity framework	4.30	0.689	0.625		6.03	27
Strengthening regional and international cooperation	4.29	0.776	0.594		9.03	28
Building a team of trusted advisors	4.23	0.759	0.519		4.80	29
Frameworks for implementing national cybersecurity initiatives	4.17	0.768	0.670		5.68	30

Source: Authors' Work

Table 2 presents the Structure Matrix and provides insights into the relationship between different cybersecurity practices and the underlying components identified through Principal Component Analysis. By examining the pattern of high loadings, or correlations, within each component, the study identifies clusters of practices that tend to be associated with each other.

Table 2: Structure Matrix

Structure Matrix					
	Component				
	1	2	3	4	5
International information security standards	0.852				
Country-initiated cybersecurity implementation frameworks	0.829				
Private sector-initiated cybersecurity implementation frameworks	0.800				
Frameworks for implementing national cybersecurity initiatives	0.783				
Cyber liability insurance	0.766				
Developing national cybersecurity strategies/agendas	0.734				
Digital certificate	0.686				
Be prepared for when, not if	0.670				
Picking the plan that is right for you	0.642				
Utilise threat intelligence	0.627				
Evaluating risks so it is properly allocated through contract	0.604				
One-time password	0.590				
Promote a security-focused cyberculture	0.541				
Two-factor authentication		0.862			
Vulnerability scanning tool		0.855			
Security tokens		0.752			
Digital signature		0.747			
Biometrics		0.701			
Focus on compliance		0.688			
The Role of the Private Sector in Cybersecurity		0.648			
Intrusion detection system			0.402		
Personal data protection (PDP)			0.825		
Strategic approach			0.819		
National cybersecurity framework			0.753		
Firewalls				0.517	
Capacity building and awareness				0.520	
Strengthening regional and international cooperation				0.441	
Building a team of trusted advisors					0.477
Collaborate and report					0.308
Adopt a defence-in-depth approach					0.672
Extraction Method: Principal Component Analysis. Rotation Method: Oblimin with Kaiser Normalization.					

Source: Authors' Work

Cluster 1: Cybersecurity Frameworks

The first component, as identified through the table above, emphasises adherence to "International information security standards (85.20%)", "Country-initiated cybersecurity implementation frameworks (82.90%)", "Private sector-initiated cybersecurity implementation frameworks (80.00%)", "Frameworks for implementing national cybersecurity initiatives (78.30%)", "Cyber liability insurance (76.60%)", "Developing national cybersecurity strategies/agendas (73.40%)", "Digital certificate (68.60%)", "Be prepared for when, not if (67.00%)", "Picking the plan that is right for you (64.20%)", "Utilize threat intelligence

(62.70%)", "Evaluating risks so it is properly allocated through contract (60.40%)", "One-time password (59.00%)", and "Promote a security-focused cyberculture (54.10%)". This cluster underscores the significance of global and national frameworks in guiding cybersecurity efforts. Compliance with established standards and frameworks is crucial for ensuring consistency and interoperability in cybersecurity practices (Maglaras et al., 2019). These standards often originate from international bodies like ISO (International Organisation for Standardisation) or regional organisations such as the European Union Agency for Cybersecurity (ENISA). On the other hand, national frameworks such as National Cybersecurity Policy Framework (NCPF) and NIST Cybersecurity Framework (CSF) 2.0 provide standardised guidelines to enhance critical infrastructure resilience against cyber threats through comprehensive risk management and regulatory compliance (NIST, 2018). By aligning with these standards and frameworks, organisations can enhance their cybersecurity posture and establish a common language for collaboration and information sharing on a global scale.

Cluster 2: Technological Security Measures

The second component highlights the importance of technological security measures such as "Two-factor authentication (86.20%)", "Vulnerability scanning tool (85.50%)", "Security tokens (75.20%)", "Digital signature (74.70%)", "Biometrics (70.10%)", "Focus on compliance (68.80%)", and "The role of the private sector in cybersecurity (64.80%)". These practices emphasise the implementation of advanced authentication protocols and tools to safeguard digital assets and sensitive information. Two-factor authentication, for instance, adds an extra layer of security by requiring users to provide two forms of identification before accessing a system (Di Pietro et al., 2020). Similarly, vulnerability scanning tools help identify and mitigate potential security weaknesses within an organisation's information technology (IT) infrastructure (Chadwick et al., 2020). Biometrics, using unique biological characteristics for authentication, offers a robust method for verifying user identities (Telo, 2023). Incorporating these technological measures is essential for mitigating cyber threats and protecting against unauthorised access to systems and data.

Cluster 3: Risk Management and Preparedness

The third component focuses on practices related to risk management, preparedness, and strategic planning for cybersecurity incidents. Concepts such as "Intrusion detection system (40.20%)," "Personal data protection (PDP) (82.50%)," "Strategic approach (81.90%)," and "National cybersecurity framework (75.30%)" underscore the initiative-taking approach needed to address evolving cyber threats (NIST, 2021). Effective risk management involves identifying, assessing, and prioritising potential risks to an organisation's assets and implementing appropriate controls to mitigate these risks (ISO/IEC, 2018). By utilising threat intelligence and evaluating risks, organisations can allocate resources efficiently and respond effectively to cybersecurity incidents (NCSC, 2020). This cluster highlights the importance of adopting a comprehensive risk management framework to enhance resilience and minimise cyber-attacks' impact on operations and reputation.

Cluster 4: Organisational and Cultural Practices

The fourth component emphasises organisational and cultural aspects of cybersecurity, including practices like “Firewalls (51.70%),” “Capacity building and awareness (52.00%),” and “Strengthening regional and international cooperation (44.10%)”. Building a strong cyber culture within an organisation involves fostering awareness, accountability, and shared responsibility for cybersecurity (Uchendu et al., 2021). Compliance with regulations and industry standards is also critical for demonstrating due diligence and minimising legal and financial risks associated with data breaches (Meglio, 2020). Additionally, recognising the role of the private sector in cybersecurity collaboration and information sharing is essential for addressing cyber threats effectively (Trim and Lee, 2021). This cluster underscores the significance of integrating cybersecurity into organisational culture and operations to establish a resilient security posture.

Cluster 5: Privacy and Regulatory Compliance

The fifth component highlights practices related to privacy protection and regulatory compliance in cybersecurity. Concepts such as “Building a team of trusted advisors (47.70%),” “Collaborate and report (30.80%),” and “Adopt a defence-in-depth approach (67.20%)” underscore the importance of safeguarding sensitive information and adhering to legal requirements (Wallis, Johnson and Khamis, 2021). As mentioned in this cluster, firewalls are essential network security components that regulate incoming and outgoing traffic based on predefined security rules (Nife and Kotulski, 2020). A strategic approach to privacy and compliance involves understanding regulatory obligations, implementing appropriate controls, and continuously monitoring and adapting to changes in the regulatory landscape (NIST, 2017). By prioritising privacy protection and regulatory compliance, organisations can build trust with stakeholders and mitigate the risk of regulatory penalties and reputational damage associated with data breaches.

Table 3 below presents the results of two key statistical tests for factor analysis and data reduction: Kaiser-Meyer-Olkin (KMO) and Bartlett's test of sphericity. The KMO value is high at 0.885, close to 1, indicating that the dataset is highly suitable for factor analysis. A KMO above 0.6 is acceptable, and above 0.8 is particularly good. The "Approx. chi-square" value is 1630.827, with 435 degrees of freedom and a significant p-value of 0.000 from Bartlett's test, supporting the rejection of the null hypothesis. This implies compelling evidence of correlation among variables, justifying factor analysis.

Table 3: KMO and Bartlett's test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin measure of sampling adequacy.		0.885
Bartlett's test of sphericity	Approx. Chi-Square	1630.827
	df	435
	Sig	0.000

Source: Authors’ Work

DISCUSSION

In this study, the efficacy of various cybersecurity practices is evaluated systematically. Two-factor authentication is the most effective practice, closely followed by one-time passwords and firewalls. Notable practices include utilising threat intelligence, adopting a strategic approach, and being prepared for cybersecurity incidents. Conversely, picking the right plan and personal data protection receive lower perceived effectiveness scores. The study emphasises the importance of practices aligning with international cybersecurity standards and technological security measures for a comprehensive overview of perceived effectiveness and variance in cybersecurity practices, especially in a developing nation like South Africa.

The outlined measures above play a crucial role in safeguarding critical infrastructure by implementing a series of robust security layers and protocols. These strategies are designed to mitigate cyber threats effectively, incorporating advanced authentication methods like two-factor authentication and biometrics. Additionally, initiative-taking measures such as intrusion detection systems and the utilisation of threat intelligence further enhance security measures. Collaborative efforts, alongside adherence to national cybersecurity frameworks and private sector standards, bolster resilience and ensure a unified approach to defending critical infrastructure against cyber-attacks.

It can be inferred that the study provides a comprehensive assessment of cybersecurity practices, revealing insights into their perceived effectiveness and variance. The clusters highlight the importance of cybersecurity frameworks, technological security measures, risk management, organisational culture, and privacy protection in building a robust cybersecurity posture. Organisations are encouraged to prioritise these practices to enhance their resilience against evolving cyber threats and potential breaches.

CONCLUSION

The findings of this research underscore the multifaceted nature of cybersecurity, and the diverse array of practices organisations must employ to mitigate cyber threats effectively. Evaluating mean scores, standard deviations, and other statistical measures provides valuable insights into these practices' perceived effectiveness and variability. Two-factor authentication emerges as a top-performing practice, closely followed by technological security measures and initiative-taking risk management strategies. Additionally, adherence to international standards, integration of cybersecurity into organisational culture, and emphasis on privacy protection and regulatory compliance are crucial components of a comprehensive cybersecurity framework. By understanding the strengths and weaknesses of different practices, organisations can tailor their cybersecurity strategies to address specific vulnerabilities and enhance overall resilience against cyber-attacks.

Recognising critical infrastructure's indispensable role as the foundation of modern society, it becomes imperative to delve deeper into its intricacies through further studies. Critical infrastructure sustains essential services and economic activities and drives the achievement of the Sustainable Development Goals (SDGs) and the Africa Agenda 2063. By focusing on cybersecurity, this study contributes to SDG 9, which emphasises building resilient infrastructure and fostering innovation, and SDG 16, which promotes peace, justice, and strong institutions. Strengthening cybersecurity ensures the integrity and reliability of critical

infrastructure, which is vital for sustainable economic growth and societal stability. Additionally, the research aligns with Africa Agenda 2063's goals of fostering a secure and interconnected continent, promoting technological advancements, and ensuring robust and resilient infrastructure to support Africa's transformation and inclusive growth. Through proactive cybersecurity strategies, we can safeguard essential services, protect economic assets, and enhance the overall development framework across the continent.

Amidst the rapid integration of digital technologies into these vital systems, a pressing need arises to comprehend their digital vulnerabilities. The heightened reliance on digital infrastructure consequently amplifies the susceptibility of these systems to cyber threats. Thus, prioritising cybersecurity measures is paramount in safeguarding critical infrastructure. By doing so, we ensure the resilience of these foundational systems, mitigate potential disruptions to society, and uphold national security imperatives. Moreover, the clustering of practices highlights distinct thematic areas within cybersecurity, emphasising the importance of a functional approach encompassing technological, organisational, and regulatory dimensions. From adhering to international standards to fostering a culture of security within organisations, each cluster offers valuable insights into the multifaceted nature of cybersecurity challenges. Moving forward, organisations must prioritise adopting effective cybersecurity practices identified in this research to strengthen their defences against an increasingly sophisticated threat landscape. By continuously evaluating and refining their cybersecurity strategies, organisations can adapt to evolving threats and safeguard their digital assets, mitigating cyber incidents' potential financial, reputational, and operational impacts.

RECOMMENDATIONS

Based on the findings of this research, several recommendations can be made for further exploration and action. Firstly, future research endeavours could delve deeper into understanding the underlying factors contributing to the perceived effectiveness of cybersecurity practices. This could involve qualitative studies to gain insights from stakeholders regarding their experiences and perceptions of various practices. Additionally, longitudinal studies could track the evolution of cybersecurity practices over time to assess their long-term efficacy and adaptability to emerging threats. Furthermore, interdisciplinary research collaborations between cybersecurity experts, behavioural scientists, and policymakers could facilitate a better understanding of the human factors influencing cybersecurity practices and organisational decision-making.

In addition, investing in resilience emerges as a pivotal strategy in addressing the imperative of fortifying critical infrastructure against cyber threats. Allocating resources towards developing resilient infrastructure bolsters its capacity to withstand future cyber incidents. It facilitates swift recovery, thus safeguarding the continuity of essential services and upholding national security imperatives. Moreover, continuous monitoring is another crucial measure in the defence arsenal. Organisations can detect and swiftly mitigate real-time cybersecurity risks by establishing mechanisms for ongoing surveillance and gathering threat intelligence. This initiative-taking approach enhances the defensive posture of critical infrastructure

systems, ensuring their readiness to counter emerging threats effectively, which aids disaster management.

Regarding stakeholders, organisations are encouraged to prioritise investments in cybersecurity practices that have demonstrated effectiveness and resilience. This involves adopting technological solutions and fostering a culture of security within the organisation. Stakeholders should collaborate with industry partners, government agencies, and regulatory bodies to share best practices, exchange threat intelligence, and advocate for cybersecurity resilience policies. Furthermore, ongoing education and training programs should be implemented to enhance cybersecurity awareness and skills among employees at all levels of the organisation. By engaging stakeholders and fostering a collective commitment to cybersecurity, organisations can effectively navigate the complex cybersecurity landscape and mitigate the risks posed by cyber threats.

REFERENCES

Argyroudis, S.A., Mitoulis, S.A., Chatzi, E., Baker, J.W., Brilakis, I., Gkoumas, K., Vousdoukas, M., Hynes, W., Carluccio, S., Keou, O., Frangopol, D.M. and Linkov, I. (2022). Digital technologies can enhance climate resilience of critical infrastructure. Climate Risk Management, 35, (100387) pp. 1-9). doi: https://doi.org/10.1016/j.crm.2021.100387

Chadwick, D.W., Fan, W., Costantino, G., de Lemos, R., Di Cerbo, F., Herwono, I., Manea, M., Mori, P., Sajjad, A. and Wang, X.-S. (2020). A cloud-edge based data security architecture for sharing and analysing cyber threat information. Future Generation Computer Systems, 102(2020)) pp.710–722. doi: https://doi.org/10.1016/j.future.2019.06.026

Coburn, A.W., Daffron, J., Quantrill, K., Leverett, E., Bordeau, J., Smith, A. and Harvey, T. (2019). Cyber risk outlook: Centre for risk studies, university of Cambridge, in collaboration with risk management solutions, inc. Available at: https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/cyber-riskoutlook/cyber-risk-outlook-2019 (Accessed 20 September 2024)

Dhirani, L.L., Armstrong, E. and Newe, T. (2021). Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. Sensors, 21(11), pp. 1-30. doi: https://doi.org/10.3390/s21113901

Di Pietro, R., Raponi, S., Caprolu, M., Cresci, S. (2021). Critical infrastructure. In New dimensions of information warfare. *Advances in information security* (vol 84, pp.157–196), Springer, Cham. doi: https://doi.org/10.1007/978-3-030-60618-3_5

Ervural, B.C., Ervural, B. (2018). Overview of cyber security in the industry 4.0 era. In Ustundag, A., Cevikcan, E., Industry 4.0: Managing the digital transformation. *Springer Series in Advanced Manufacturing (pp. 267-284).* Springer, Cham. doi: https://doi.org/10.1007/978-3-319-57870-5_16

Eunice, A. D., Gao, Q., Zhu, M. Y., Chen, Z. & Na, L. V. (2021). Network anomaly detection technology based on deep learning in IEEE 3rd international conference on frontiers technology of information and computer (ICFTIC), 12-14 November, pp. 6-9, Greenville, USA

González-Granadillo, G., González-Zarzosa, S. and Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, trends, and usage in critical infrastructures. Sensors, 21(14), pp. 1-28. doi: https://doi.org/10.3390/s21144759. Haiston, J. (2023). What are the 11 pillars of industry 4.0? Available at: https://www.symmetryelectronics.com/blog/11-pillars-of-industry-4-0/ [Accessed 01 June 2024]

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M. and Mahmood, S. (2020). Cyber security threats and vulnerabilities: A systematic mapping study. Arabian Journal for Science and Engineering, 45(1), pp.3171-3189. doi: https://doi.org/10.1007/s13369-019-04319-2. IT-Online. (2023). Threats to critical infrastructure on the rise. Available at: https://it-online.co.za/2023/10/09/threats-to-critical-infrastructure-on-the-rise/ [Accessed 14 April 2024]

Kaivo-oja, J., Knudsen, M.S., Lauraeus, T. and Kuusi, O., (2020). Future knowledge management challenges: Digital twins' approach and synergy measurements. Management, 8(2), pp.99-109

Lukasik, S. (2020). Protecting critical infrastructures against cyber-attack. Available at: https://books.google.co.za/books?hl=en&lr=&id=hhUHEAAAQBAJ&oi=fnd&pg=PP1&dq=safe guarding+critical+infrastructure+in+digital+age&ots=WHzWamx_gQ&sig=sRTRGHwo45juxnX DfFWU3qGQtjA&redir_esc=y#v=onepage&q&f=false [Accessed 14 Feb. 2024]

Maglaras, L., Ferrag, M. A., Derhab, A., Mukherjee, M., & Janicke, H. (2019). Cyber security: From regulations and policies to practice. In *Strategic Innovative Marketing and Tourism: 7th ICSIMAT, Athenian Riviera, Greece, 2018* (pp. 763-770). Springer International Publishing. doi: https://doi.org/10.1007/978-3-030-12453-3_88

Mallik, A., Ahsan, A., Shahadat, M. & Tsou, J. (2019). Man-in-the-middle-attack: Understanding in simple words. International Journal of Data and Network Science, 3(2), pp. 77-92

Meglio, M. (2020). Embracing insecurity: Harm reduction through a no-fault approach to consumer data breach litigation. Available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/bclr61&div=31&id=&page= [Accessed 14 Feb. 2024]

National Institute of Standards and Technology (NIST). (2017). Framework for improving critical infrastructure cybersecurity. Retrieved from: ://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v11_without-markup.pdf (Accessed 19 September 2024)

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity: National institute of standards and technology. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Accessed 20 September 2024)

Nife, F.N. and Kotulski, Z. (2020). Application-aware firewall mechanism for software defined networks. Journal of Network and Systems Management, 28(3), pp.605–626. doi: https://doi.org/10.1007/s10922-020-09518-z

Rees, J. and Rees, C.J. (2023). Cyber-security and the changing landscape of critical national infrastructure: State and non-state cyber-attacks on organisations, systems and services. In: Montasari, R. (eds) *Applications for artificial intelligence and digital forensics in national security (pp. 67-89).* Advanced Sciences and Technologies for Security Applications. Springer, Cham. doi: https://doi.org/10.1007/978-3-031-40118-3_5

Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection, Journal of Industrial Integration, 36 (100520), pp. 1-12. doi: https://doi.org/10.1016/j.jii.2023.100520

Shokry, M., Awad, A.I., Abd-Ellah, M.K. and Khalaf, A.A.M. (2022). Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision. Future Generation Computer Systems, 136(2022), pp.358–377. doi: https://doi.org/10.1016/j.future.2022.06.013

Telo, J. (2023). Smart City Security Threats and Countermeasures in the Context of Emerging Technologies. International Journal of Intelligent Automation and Computing, 6(1), pp.31–45. Tortorella, G.L., Fogliatto, F.S., Cauchick-Miguel, P.A., Kurnia, S. and Jurburg, D., (2021). Integration of industry 4.0 technologies into total productive maintenance practices. International Journal of Production Economics, 240(108224), pp. 1-14. doi: https://doi.org/10.1016/j.ijpe.2021.108224

Trim, P.R.J. and Lee, Y.-I. (2021). The global cyber security model: Counteracting cyber-attacks through a resilient partnership arrangement. Big Data and Cognitive Computing, 5(3), pp. 1-16

Uchendu, B., Nurse, J.R.C., Bada, M. and Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109(102387), pp. 1-23

Vähäkainu, P., Lehto, M., and Kariluoto, A. (2022). Cyberattacks against critical infrastructure facilities and corresponding countermeasures. In: Lehto, M., Neittaanmäki, P. (eds) Cyber Security. *Computational methods in applied sciences* (vol 56, pp. 255-292). Springer, Cham. doi: https://doi.org/10.1007/978-3- 030-91293-2_11

Wallis, T., Johnston, C., and Khamis, M. (2021). Interorganizational cooperation in supply chain cybersecurity: A cross-industry study of the effectiveness of the UK implementation of the NIS directive. Information and Security: An International Journal, *48(2)*, pp. 36-68. doi: https://doi.org/10.11610/isij.4812

Zyphur, M.J. and Pierides, D.C. (2017). Is quantitative research ethical? Tools for ethically practicing, evaluating, and using quantitative research. Journal of Business Ethics, 143(1), pp.1–16