

Bringing Change in Construction: Analysing Strategies for Managing Cybersecurity Disasters in the South African Construction Industry

Seyi Segun Stephen¹, Clinton Ohis Aigbavboa², Jummai Okikiola Bello³, and Ayodeji Emmanuel Oke⁴

¹⁻⁴Construction Management and Quantity Surveying / Faculty of Engineering and the Built Environment, University of Johannesburg, South Africa

Abstract

This study explored strategies for managing cybersecurity risks in the South African construction industry. Using a quantitative research methodology, the study targeted construction professionals and cybersecurity experts in Gauteng province through structured questionnaires, of which 150 were distributed and 90 were retrieved. The data was analysed using descriptive statistics, exploratory factor analysis (EFA), and correlation techniques to identify key cybersecurity risks and evaluate the effectiveness of existing strategies using Statistical Package for the Social Sciences (SPSS) software. The findings showed that companies prioritise adopting new technology and responding to cyber threats, but struggle to integrate cybersecurity into overall business strategies. Many firms focus on either strategic planning or cybersecurity, rarely balancing both due to resource limitations. The study concludes that bringing change requires a combined approach where cybersecurity measures align with strategic goals. Practical implications suggest that construction firms must invest in cybersecurity training, adopt stronger security policies, and use advanced technologies like AI and encryption. Companies should also improve stakeholder involvement to ensure that cybersecurity is a key consideration in project management. Future research should explore specific challenges preventing firms from fully implementing security measures and how government policies can support better cybersecurity practices. This study highlights the urgent need for a balanced approach to cybersecurity and strategic planning in the construction industry.

Keywords: Construction security, Technology adoption, Cyber threats, Risk management, Strategic planning

1. Introduction

The South African construction industry is undergoing significant transformation as it embraces digital technologies to improve efficiency and competitiveness (Jeza & Lekhanya, 2022). The industry is shifting from traditional methods to more innovative solutions with the growing adoption of Building Information Modelling (BIM), cloud-based systems, and advanced project management tools. These changes offer immense potential for cost savings, better collaboration, and faster project delivery. However, Jimmy (2021) noted that this change to digital integration also brings new challenges, particularly the risk of cybersecurity threats, which can disrupt operations and compromise sensitive data. To fully realise the benefits of digital tools, the industry must prioritise robust strategies to manage these emerging risks.

According to Stephen *et al.* (2024), cybersecurity has become a critical concern in construction, as the reliance on digital platforms increases the exposure to cyber risks. The study continued that construction companies now store valuable project data, financial records, and intellectual property on digital systems, making them attractive cyberattack targets. Möller (2023) and Stephen *et al.* (2024) noted that some cybersecurity disasters or threats, like data breaches, ransomware, and phishing attacks, can lead to financial

losses, reputational damage, and project delays. Additionally, the studies explained further that weak cybersecurity measures can affect the entire supply chain, putting clients, contractors, and other stakeholders at risk. Addressing these vulnerabilities is essential to ensure the successful and secure adoption of digital technologies in construction.

Mantha and García de Soto (2021) and Mantha *et al.* (2021) stated that the lack of awareness about cybersecurity threats and the absence of comprehensive strategies to manage these risks are some of the challenges experienced in the digital construction industry. Many firms are unprepared for potential cyberattacks, which leaves their digital systems vulnerable. Pieterse (2021) gave examples of 74 cyber incidents, such as Johannesburg facing major cyberattacks in 2019, including a ransomware attack on City Power and a breach by Shadow Kill hackers, disrupting essential services. In 2020 and 2021, cyber incidents surged, impacting industries like finance, healthcare, and construction, highlighting vulnerabilities in South Africa's infrastructure. Therefore, the rationale for this research is to address this gap by providing insights into how construction companies can better prepare for and respond to cybersecurity disasters. The study's objectives are to examine the current state of cybersecurity in the construction industry, identify common vulnerabilities, and propose practical strategies for risk management.

¹ Corresponding Author

Email address: seyistephen.ss@gmail.com

This research will benefit construction firms, project managers, Information Technology (IT) professionals, and policymakers by equipping them with tools and knowledge to safeguard digital systems. Ultimately, the study aims to analyse strategies for managing cybersecurity disasters in the construction industry, focusing on South Africa.

2. Cybersecurity Threats in the Construction Industry

Like many other sectors, the construction industry has embraced digital tools to enhance efficiency, collaboration, and project management (Jeza & Lekhanya, 2022). However, a growing risk of cybersecurity threats comes with increased reliance on digital systems (Mantha & García de Soto, 2021). Rane (2023) explained that construction companies often manage vast amounts of sensitive data, including project designs, financial records, and client information. This data, stored on cloud platforms or shared across digital networks, becomes a prime target for cybercriminals. According to McKane (2020) and Tanga *et al.* (2022), the South African construction industry has experienced several real-life cyberattacks, highlighting the industry's cyber risks. In 2019, a major construction company, Stefanutti Stocks, suffered a ransomware attack that disrupted its operations and delayed projects. The hackers tried to steal login details to access sensitive project data. In another case, malware infected a construction software system used by a subcontractor, causing delays in a large housing project in Gauteng. These examples show how cyberattacks can lead to financial loss, project delays, and damage to company reputations, highlighting the need for stronger cybersecurity.

One of the significant cybersecurity threats in construction is ransomware attacks, where hackers encrypt a company's data and demand payment for its release (Connolly & Wall, 2019). Such incidents can paralyse operations, delay projects, and result in financial losses. Phishing schemes are another common threat, where attackers trick employees into revealing sensitive information or downloading malicious software (Alkhalil *et al.*, 2021). Additionally, the construction industry is vulnerable to insider threats, as disgruntled employees or contractors with access to sensitive systems may misuse their privileges (Saxena *et al.*, 2020). These risks are compounded by the industry's complex supply chains, where third-party vendors or subcontractors may inadvertently introduce vulnerabilities.

Furthermore, the impact of cybersecurity threats extends beyond financial losses (Lee, 2021). A successful cyberattack can lead to reputational damage as clients lose trust in a company's ability to protect their data. For instance, a confidential project design breach can result in legal liabilities or competitive

disadvantages. Moreover, Kure *et al.* (2022) stated that attacks targeting critical infrastructure projects pose national security risks, and Pieterse (2021) stated that 74 cyber incidents were identified occurring between 2010 and 2020. This emphasises the need for stringent cybersecurity measures. Kure *et al.* (2022) continued that despite these risks, many construction companies underestimate the importance of cybersecurity, focusing more on operational priorities like cost and deadlines. This lack of awareness leaves them unprepared for potential threats, making them easy targets for cybercriminals, as Mantha *et al.* (2021) explained.

2.1. Cybersecurity Frameworks and Standards

This section reviews key cybersecurity frameworks and standards developed by governments and international organisations, focusing on their relevance to the construction industry. These frameworks address the unique challenges of protecting operational technology (OT) systems on construction sites, which are crucial for on-site operations, as Sonkor and García de Soto (2021) explain. Shackelford *et al.* (2015) highlighted the role of organisations like the National Institute of Standards and Technology (NIST) and the International Organisation for Standardisation (ISO) in creating guidelines that help industries, including construction, strengthen cybersecurity. Examples include the UK's Minimum Cyber Security Standard (MCSS) of 2018, which sets baseline cybersecurity requirements (Srinivas *et al.*, 2019), and ISO/IEC 27001:2013, which provides universal guidelines for managing information security systems (Koza, 2022). In South Africa, the National Cybersecurity Policy Framework (NCPF) was influenced by global policies from the EU, NATO, and the US. Still, it raised concerns about its adaptation to local needs (Sutherland, 2017). Its goals include reducing threats, promoting cooperation, and building cybersecurity capacity (Djebbar & Nordström, 2023). In the construction sector, ISO 19650-5:2020 is an industry-specific standard focused on securing sensitive information in projects that use Building Information Modelling (BIM) and cybersecurity (Abbasnejad *et al.*, 2024). This standard addresses cybersecurity throughout the entire lifecycle of built environments, from design to operation. Unlike ISO/IEC 27001, which applies broadly across industries, ISO 19650-5 is tailored to the collaborative data-sharing processes in construction, making it a valuable resource for stakeholders.

According to Snail ka Mtuze and Musoni (2023), South Africa has a cyber framework called the Cybercrimes Act, which was signed into law in 2021. This law helps fight cyber threats by defining cybercrimes, setting punishments, and improving cybersecurity measures. It makes hacking, identity theft, and data breaches illegal while also giving authorities more power to investigate cyberattacks. For example, after the Experian data breach in 2020, where the personal data of 24 million

South Africans was exposed, the Cybercrimes Act now ensures stricter penalties for companies that fail to protect sensitive information. This framework helps protect industries like construction, which aim to fully rely on secure digital systems for project management and financial transactions.

2.2. Mitigating Cybersecurity Disasters in the Construction Industry

Mitigating cybersecurity disasters in the construction industry begins with building awareness and prioritising cybersecurity as a critical part of operations. Many construction firms underestimate the risks posed by cyber threats, often focusing more on traditional physical security. To begin with, Chagadama and Luamba (2022) stated that educating employees, contractors, and stakeholders about the potential dangers of cyberattacks and how to identify suspicious activities is essential. The authors continued that regular training sessions on safe online practices, such as recognising phishing emails and securely handling sensitive data, can significantly reduce human errors, which are a leading cause of cybersecurity breaches. Mantha and García de Soto (2021) concluded that construction companies can strengthen their first line of defence against cyber threats by creating an awareness culture.

Isakov *et al.* (2024) noted that another crucial step is the implementation of advanced technological measures to protect digital systems. The study explains that robust firewalls, up-to-date antivirus software, and data encryption should be standard practices. Additionally, companies should adopt multi-factor authentication (MFA) to add an extra layer of security when accessing systems and sensitive information (Cahyaningrum, 2024). The study explained that regular vulnerability assessments and cybersecurity audits can help identify and address weaknesses in existing systems. Ohueri *et al.* (2024) opined that investing in secure cloud-based platforms and adhering to internationally recognised standards, such as ISO/IEC 27001 and ISO 19650-5, can further enhance the security of critical systems and data, especially in projects relying on Building Information Modelling (BIM) and other digital tools.

Furthermore, collaboration and partnerships also play an important role in mitigating cybersecurity disasters (Bradshaw, 2015). The study explained that construction companies often work with multiple subcontractors, vendors, and external partners, making it vital to establish clear cybersecurity policies and protocols across the supply chain. It continued that these companies could collaborate with cybersecurity experts to develop tailored risk management strategies and incident response plans. In addition, Markopoulou and Papakonstantinou (2021) suggested that governments and industry bodies can support these efforts by providing resources, guidelines, and frameworks that address sector-specific risks. By

integrating these efforts, the construction industry can build a united front against cyber threats, ensuring the protection of assets, data, and critical infrastructure. However, from the literature reviewed, a notable gap lies in the practical implementation and evaluation of cybersecurity frameworks specifically tailored to the construction industry's unique challenges. While existing standards like ISO/IEC 27001:2013 and ISO 19650-5:2020 provide comprehensive guidelines, limited evidence or case studies demonstrate their effective adoption within real-world construction environments, particularly in regions like South Africa.

Moreover, the literature highlights the industry's increasing digital integration but underscores a lack of widespread awareness and preparedness among construction firms.

3. Research Methodology

This study used a quantitative approach to examine how construction companies in South Africa are managing cybersecurity risks, following a descriptive research design to identify key issues and explore relationships. It focused on construction professionals and cybersecurity experts in Gauteng province, including architects, quantity surveyors, construction managers, engineers, and cybersecurity specialists. Cybersecurity experts were selected based on their qualifications and experience, while construction professionals were chosen from registered industry bodies such as the South African Council for the Quantity Surveying Profession (SACQSP). Aghimien *et al.* (2020) highlighted the role of professional bodies, with updates from the researcher showing that SACAP (2025) had 11,551 registered members, ECSA (2022) had 53,000 members, including 35,333 professional engineers, SACPCMP (2018) recorded 7,785 construction and project managers, and SACQSP (2018) had 4,339 members, rising to 4,539 by December 2018, totalling 59,208 professionals. According to Darling (2022), sample size depends on margins of error, where a $\pm 10\%$ margin at a 90% confidence level resulted in a sample size of 380 when Cochran's (1963) formula was used for the study. However, due to response challenges, 150 questionnaires were distributed via Google Forms, with 90 responses received, achieving a 60% response rate, which Sue and Ritter (2007) considered good. Bihu (2021) noted that questionnaires were chosen for most studies due to their cost-effectiveness, convenience, and the ability to overcome geographic barriers.

The data for the study were analysed using descriptive statistics, such as mean and standard deviation, using the Statistical Package for the Social Sciences (SPSS) software. This analysis helped understand construction companies' cybersecurity threats, as Grancharova and Aleksandrova (2023) noted. Exploratory Factor Analysis (EFA) was conducted to identify key

cybersecurity strategies further using the Kaiser-Meyer-Olkin (KMO) test and Bartlett's test, yielding a KMO value of 0.905, indicating the adequacy of the data. EFA was helpful in uncovering patterns, grouping related variables, and simplifying complex data.

4. Findings and Discussion

Stephen *et al.* (2024) illustrated that the cybersecurity adoption in South African construction is low despite Pieterse (2021) and Snail ka Mtuze and Musoni (2023) stating that numerous cyber incidents were identified

occurring over time. To mitigate this, Table 1 shows measures to address cybersecurity risks in South African construction based on their mean scores and standard deviations (SD). "Readiness to incorporate technological innovations" ranks highest (Mean = 4.35, SD = 0.684), showing strong agreement and low variability among respondents. Close behind are "Response to data theft" (Mean = 4.31, SD = 0.693) and "Implementing strategic direction" (Mean = 4.30, SD = 0.727), both seen as highly important. Measures like "The validity of the strategy," "Usage of strategy control," and "Adopting zero-trust (ZTA)" also score

Table 1: Strategies to Address Cybersecurity Risk in Construction

Strategies	Mean	SD	Rank
Readiness to incorporate technological innovations	4.35	0.684	1
Response to data theft	4.31	0.693	2
The validity of the strategy	4.30	0.779	4
Implementing strategic direction	4.30	0.727	3
Usage of strategy control	4.30	0.689	5
Adopting zero-trust (ZTA)	4.26	0.865	6
Stakeholders' involvement in strategy implementation	4.26	0.750	7
Improving security software development	4.25	0.728	8
Availability of behavioural analytics	4.23	0.944	9
Adopting strategic formulation	4.23	0.742	10
Defensive AI and machine learning for cybersecurity	4.22	0.837	12
Infrastructure and security as code	4.22	0.719	11
Risk-based automation	4.18	0.839	13
Engaging usage of homomorphic encryption	4.17	0.849	14
Availability of elastic log monitoring for large data sets	4.17	0.801	15
Proper environmental assessment	4.16	0.796	16

(Source: Authors')

Table 2: Communalities

Pattern Matrix ^a		
	Component	
	1	2
Stakeholders' involvement in strategy implementation	0.811	
Usage of strategy control	0.809	
Proper environmental assessment	0.807	
Implementing strategic direction	0.793	
Readiness to incorporate technological innovations	0.791	
Adopting strategic formulation	0.762	
The validity of the strategy	0.747	
Response to data theft	0.571	
Infrastructure and security as code		-0.925
Defensive AI and machine learning for cybersecurity		-0.799
Availability of elastic log monitoring for large data sets		-0.769
Adopting zero-trust architecture (ZTA)		-0.750
Risk-based automation		-0.748
Improving security software development		-0.540
Engaging usage of homomorphic encryption		-0.536
Availability of behavioural analytics		-0.457

(Source: Authors')

high but with slightly more variation. Lower-ranked measures, such as "Proper environmental assessment" (Mean = 4.16, SD = 0.796) and "Availability of elastic log monitoring for large data sets" (Mean = 4.17, SD = 0.801), still have strong mean scores but less priority. Some measures, like "Engaging usage of homomorphic encryption" and "Defensive AI and machine learning," show higher variability, reflecting mixed opinions. Overall, the high mean scores indicate that all measures are important, with differences in ranking showing varying levels of emphasis.

The findings highlight the construction industry's prioritisation of technological innovations and strategic responses to cybersecurity risks, aligning with existing literature emphasising the growing need for advanced measures in this sector. For instance, Shopina *et al.* (2020) stress the importance of readiness for technological innovation to counter emerging threats, which supports the top-ranked measure in this study. Similarly, the focus on responses to data theft and strategic direction corroborates Oke *et al.* (2023)'s observation that organisations must integrate targeted strategies to manage risks effectively. However, the lower rankings of measures like "Proper environmental assessment" and "Elastic log monitoring for large data sets" contrast with recommendations by Upadhyay and

achieving organisational goals. This can help mitigate cyber-attacks in the South African construction industry. Conversely, cybersecurity measures, such as infrastructure security and defensive AI, align with studies indicating that security concerns often compete with strategic priorities for resources and focus (Rane, 2023; Abbasnejad *et al.*, 2024). Putting in place simple cyber measures when planning construction can go a long way in addressing disasters over time. South African firms can prioritise strategic and cybersecurity measures to help combat further cyber incidents, as Pieterse (2021) noted.

Table 3 provides the results of the KMO and Bartlett's test of sphericity, which are essential assessments in factor analysis. The KMO is a value between 0 and 1, with higher values indicating better suitability for factor analysis. In this case, the KMO value is 0.905, which is close to 1. This high KMO value suggests that the dataset is highly suitable for factor analysis. In this specific analysis, Bartlett's test of sphericity yields an approximate chi-square value of 881.872 with 120 degrees of freedom. This suggests that the variables in the dataset exhibit significant intercorrelations, supporting the use of factor analysis to explore these relationships further, as Sharma *et al.* (2023) suggested.

Table 3: KMO and Bartlett Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin measure of sampling adequacy.		0.905
Bartlett's test of sphericity	Approx. Chi-Square	881.872
	df	120
	Sig.	0.000

(Source: Authors')

Sampalli (2020), who argue that monitoring and environmental assessments are crucial for detecting vulnerabilities. This contrast may reflect practical limitations in implementing such measures in construction settings.

Table 2 shows the two main components influencing strategy and security measures. The first component, grouped as **strategic measures**, has high positive values for factors related to strategic implementation, such as stakeholder involvement (0.811), strategy control (0.809), and environmental assessment (0.807), among others. This suggests that these elements work together in effective strategy execution. The second component, grouped as **cybersecurity measures**, has high negative values for cybersecurity measures like infrastructure security (-0.925) and defensive AI (-0.799), indicating that these factors are separate from or even inversely related to strategy implementation. This means organisations may focus on either strategic execution or cybersecurity, but not both simultaneously. According to Koza (2022), strategic implementation relies heavily on stakeholder involvement, structured control, and environmental assessment, which are crucial for

5. Discussion and Conclusion

The current state of cybersecurity in the South African construction industry reveals a mixed level of preparedness, with companies recognising the risks but often struggling to implement effective measures. Key issues include low awareness of critical security steps, such as proper environmental assessments and elastic log monitoring for large data sets, which are often overlooked. Challenges such as high costs, limited technical knowledge, and resistance to adopting new systems hinder progress. Research by Shopina *et al.* (2020), Oke *et al.* (2023), Rane (2023), and Abbasnejad *et al.* (2024) show that firms tend to focus either on strategic planning or cybersecurity improvements, rarely balancing both. This disconnect limits their ability to integrate security into their operations fully. Factors like stakeholder involvement and resource allocation are crucial, as firms often face tough decisions between investing in strategic growth or enhancing security. Furthermore, effective strategies for improving cybersecurity should include better integration of security measures into everyday operations and prioritising innovations like

infrastructure security and defensive artificial intelligence (AI) while addressing resource challenges by aligning cybersecurity initiatives with overall business strategies. South African construction firms can build resilience against cyber threats and achieve sustainable growth.

The study's scope is limited to Gauteng. A broader geographic scope beyond the province and including qualitative insights from industry leaders could offer a more comprehensive understanding of the required strategies. Furthermore, future research should explore practical ways to help construction companies implement both cybersecurity and strategic planning together. Studies could also examine the specific

barriers preventing companies from fully adopting advanced security measures and how government policies or industry guidelines can support better cybersecurity practices.

References

- Abbasnejad, B., Soltani, S., Karamoozian, A. & Gu, N. (2024). 'A systematic literature review on the integration of Industry 4.0 technologies in sustainability improvement of transportation construction projects: state-of-the-art and future directions', *Smart and Sustainable Built Environment*. Vol. ahead-of-print No. ahead-of-print. <https://doi.org/10.1108/SASBE-11-2023-0335>
- Aghimien, D.O., Aigbavboa, C.O. and Oke, A.E., (2020). 'Critical success factors for digital partnering of construction organisations—a Delphi study', *Engineering, Construction and Architectural Management*, 27(10), pp. 3171-3188.
- Alkhalil, Z., Hewage, C., Nawaf, L. & Khan, I. (2021). 'Phishing attacks: A recent comprehensive study and a new anatomy', *Frontiers in Computer Science*, 3, pp. 1–23.
- Bihu, R. (2021). 'Questionnaire survey methodology in educational and social science studies', *International Journal of Quantitative and Qualitative Research Methods*, 9(3), pp. 40-60.
- Bradshaw, S. (2015). 'Combating cyber threats: CSIRTs and fostering international cooperation on cybersecurity', *Global Commission on Internet Governance Paper Series, Paper, 1*(23), 1–24.
- Cahyaningrum, Y. (2024). 'Evaluation of system access security in the implementation of MultiFactor Authentication (MFA) in educational institutions', *Journal of Practical Computer Science*, 4(1), pp. 11-19.
- Chagadama, D.B.A. & Luamba, D.S. (2022). 'Cyberattacks: A huge concern for small business sustainability', *Global Scientific and Academic Research Journal of Economics, Business and Management*, 1(2), pp. 60–75.
- Connolly, L.Y. & Wall, D.S. (2019). 'The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures', *Computers and Security*, 87, pp. 1–18.
- Darling, H.S. (2022). 'Are you confident about your confidence in confidence intervals?' *Cancer Research, Statistics, and Treatment*, 5(1), pp. 139–144.
- Djebbar, F. & Nordström, K., (2023). 'A comparative analysis of industrial cybersecurity standards', *IEEE Access*, 11, pp. 85315-85332.
- Grancharova, G. & Aleksandrova, S. (2023). 'Measures of central tendency and dispersion', *Health Investigation: Analysis-Planning-Evaluation*, pp. 73–92.
- Isakov, A., Urozov, F., Abduzhapporov, S. & Isokova, M. (2024). 'Enhancing cybersecurity: Protecting data in the digital age', *Innovations in Science and Technologies*, 1(1), pp. 40–49.
- Jeza, S. & Lekhanya, L.M., (2022). 'The influence of digital transformation on the growth of small and medium enterprises in South Africa', *Problems and Perspectives in Management*, 20(3), pp. 1–14.
- Jimmy, F. (2021). 'Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defences', *Valley International Journal Digital Library*, 1, pp. 564–574.
- Koza, E. (2022). 'Semantic analysis of ISO/IEC 27000 standard series and NIST cybersecurity framework to outline differences and consistencies in the context of operational and strategic information security', *Medical Engineering Themes*, 2, pp. 26–39.

- Kure, H.I., Islam, S. & Mouratidis, H., (2022). 'An integrated cyber security risk management framework and risk prediction for the critical infrastructure protection', *Neural Computing and Applications*, 34(18), pp. 15241–15271.
- Lee, I. (2021). 'Cybersecurity: Risk management framework and investment cost analysis', *Business Horizons*, 64(5), pp. 659–671.
- Mantha, B., de Soto, B.G., & Karri, R. (2021). 'Cyber security threat modelling in the AEC industry: An example for the commissioning of the built environment', *Sustainable Cities and Society*, 66, pp. 1–15.
- Mantha, B.R. & García de Soto, B., (2021). 'Cybersecurity in construction: Where do we stand and how do we get better prepared', *Frontiers in Built Environment*, 7, pp. 1–13.
- Markopoulou, D. & Papakonstantinou, V., (2021). 'The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular', *Computer Law and Security Review*, 41, pp. 1–12.
- McKane, J. (2020). 'South African construction company hit by cyberattack', Retrieved at <https://mybroadband.co.za/news/security/365908-south-african-construction-company-hit-by-cyberattack.html>
- Möller, D.P. (2023). 'Ransomware attacks and scenarios: Cost factors and loss of reputation', In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*, Switzerland, Springer Nature, pp. 273–303.
- Ohueri, C.C., Masrom, M.A.N. & Seghier, T.E., (2024). 'Digital twin for decarbonising operating buildings: A systematic review and implementation framework development', *Energy and Buildings*, 320, pp. 1–18.
- Oke, A.E., Adetoro, P.E., Stephen, S.S., Aigbavboa, C.O., Oyewobi, L.O. & Aghimien, D.O., (2023). 'Risk Management Practices in Australia', In *Risk Management Practices in Construction: A Global View*, Switzerland, Springer Nature, pp. 107–117.
- Opoku, A., Ahmed, V. & Akotia, J., (2016). 'Choosing an appropriate research methodology and method', in *Research Methodology in the Built Environment*, London, Routledge, pp. 32–49.
- Pieterse, H. (2021). 'The cyber threat landscape in South Africa: A 10-year review', *The African Journal of Information and Communication*, 28, pp. 1–21. <https://doi.org/10.23962/10539/32213>
- Rane, N. (2023). 'Integrating Building Information Modelling (BIM) and Artificial Intelligence (AI) for smart construction schedule, cost, quality, and safety management: Challenges and opportunities', *Cost, Quality, and Safety Management: Challenges and Opportunities (September 16, 2023)*, pp. 1–20. <http://dx.doi.org/10.2139/ssrn.4616055>
- Roopa, S. & Rani, M.S., (2012). 'Questionnaire designing for a survey', *Journal of Indian Orthodontic Society*, 46(4), pp. 273–277.
- Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.K.R. & Burnap, P., (2020). 'Impact and key challenges of insider threats on organisations and critical businesses', *Electronics*, 9(9), pp. 1–29.
- Shackelford, S.J., Proia, A.A., Martell, B., & Craig, A.N. (2015). 'Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices', *Texas International Law Journal*, 50, pp. 305–315.
- Sharma, V., Manocha, T., Garg, S., Luthra, A., Dixit, S., & Sharma, M. (2023, February). Factors affecting awareness and practices of green technology. In *2023, the 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM)*, Uttar Pradesh, India, 2023, pp. 1–5.
- Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S. & Shpenov, D. (2020). 'Cybersecurity: Legal and organisational support in leading countries, NATO and EU standards', *Journal of Security and Sustainability Issues*, 9(3), 977–992
- Snail ka Mtuze, S. and Musoni, M., (2023), 'An overview of cybercrime law in South Africa.' *International Cybersecurity Law Review*, 4(3), pp. 299–323.
- Sonkor, M.S. & García de Soto, B., (2021). 'Operational technology on construction sites: A review from the cybersecurity perspective', *Journal of Construction Engineering and Management*, 147(12), pp. 1–22.
- Srinivas, J., Das, A.K. & Kumar, N., (2019). 'Government regulations in cyber security: Framework, standards and recommendations', *Future Generation Computer Systems*, 92, pp. 178–188.

- Stephen, S., Aigbavboa, C., Oke, A., Akinradewo, O. & Idowu, A. (2024). 'Constructing cyber resilience: A focus on cybersecurity measures in the South African construction sector', *Engineering Proceedings*, 76(1), pp. 1–8.
- Sue, V. M., & Ritter, L. A. (2007). '*Conducting online surveys*', Sage Publishing, USA. Pages 1–9.
- Sutherland, E. (2017). 'Governance of cybersecurity-the case of South Africa', *The African Journal of Information and Communication*, 20, pp. 83–112.
- Tanga, O., Akinradewo, O., Aigbavboa, C., & Thwala, D. (2022). 'Cyber attack risks to construction data management in the fourth industrial revolution era: A case of Gauteng province, South Africa', *Journal of Information Technology in Construction*, 27, pp. 1–19.
- Upadhyay, D. & Sampalli, S. (2020). 'SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations', *Computers and Security*, 89, pp. 1–18.