Environment and Social Psychology (2024) Volume 9 Issue 8
doi: 10.59429/esp.v9i8.2551

RESEARCH ARTICLE

Developing a framework for managing cybercrime in the Nigerian built environment industry: An explorative approach

Andrew Ebekozien[1,2,3,4,*], Mohamed Ahmed Hafez Ahmed[2], Clinton Aigbavboa[1], Wellington Didibhuku Thwala[5], Mohamad Shaharudin Samsurijan[4], Nor Malina Malek[4], Maslina Mohmed Shaed[4], Faith Osaremen Emuchay[6]

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

[2] *Department of Engineering, INTI International University, Nilai, Malaysia.*

[3] *Department of Quantity Surveying, Auchi Polytechnic, Auchi, Nigeria.*

[4] *Development Planning and Management, School of Social Sciences, Universiti Sains Malaysia, Gelugor, Malaysia.*

[5] *Faculty of Engineering, Built Environment and Information Technology, Walter Sisulu University, South Africa.*

[6] *Department of Telecoms Engineering, Middlesex University, London, United Kingdom.*

*** Corresponding author:** Andrew Ebekozien, ebekoandy45@yahoo.com

ABSTRACT

Cybercrime activities are fast-growing and threatening critical sectors, including the built environment industry (BEI). This may threaten achieving Sustainable Development Goal 9 (industry, innovation and infrastructure). Cyber attackers may attack the industry more if measures are not taken to manage cybercrime activities in industrial innovation and infrastructure development. Developing a framework to manage cybercrime may improve BEI's cybersecurity and, by extension, improve achieving Goal 9 is pertinent. Thus, the study explores the root causes and identifies the information necessary to develop a Nigerian BEI cybersecurity framework for managing cybercrime to improve achieving Goal 9. Given the unexplored issues in Nigeria, twenty-eight experts were selected from Abuja and Lagos. The study achieved saturation. The interviewees were experts in cybercrime in the BEI. The study's data were coded and analysed using a thematic method. Findings show that human-related sources are the major root cause of the Nigerian BEI's cyberattack. Five key variables emerged as the information required to develop a BEI cybersecurity framework for managing cybercrime. The rapid construction digitalisation and administrative operations into cyberspaces have enhanced cyberattacks. This study raises awareness about cybersecurity implications and promotes cybersecurity framework management adaption, especially in Nigeria's built environment industry, to improve achieving Goal 9.

Keywords: Built Environment Industry (BEI); construction digitalisation; cyberattacks; framework; Nigeria; sustainable development Goal 9

1. Introduction

The Built Environment Industry (BEI) is among the largest sectors and offers facilities for economic advancement[1]. The industry forms an element of our lives. This is because it generates economic wealth and

ARTICLE INFO
Received: 13 February 2024 | Accepted: 8 April 2024 | Available online: 20 August 2024

CITATION
Ebekozien A, Ahmed MAH, Aigbavboa C, et al. Developing a framework for managing cybercrime in the Nigerian built environment industry: An explorative approach. *Environment and Social Psychology* 2024; 9(8): 2551. doi: 10.59429/esp.v9i8.2551

provides physical infrastructure. Bogue[2] claimed that the industry is worth over $10 trillion annually. Mantha and de Soto [3] opined that the industry might adopt construction digitalisation technologies slowly. This includes three-dimensional printing, digital twin, robots, cyber-physical systems, blockchain, augmented reality, and big data. They avowed that these digital advancements belong to the fourth industrial revolution (4IR). It is pertinent to embrace construction digitalisation. Ebekozien and Aigbavboa[4] acknowledged using recycled waste materials, mass customisation of designs, and decreasing waste from precise material placement as benefits of digital construction. Dwivedi et al. [5] asserted that many 4IR technologies usage over the years has increased, but implementation challenges remain. Embracing construction digitalisation may have increased cyberattacks on the sector. This may be a threat to achieving Goal 9. Goal 9 (Industry, Innovation and Infrastructure) is all about building resilient infrastructure, promote inclusive and sustainable industrialisation and foster innovation. A cybercrime is a criminal motive enhanced via a computer or electronic devices to harm victims. This may hinder construction digitalisation and innovation in the industry if not mitigated. It may cause severe damage to the hardware of delicate infrastructure [6] and, by extension, hindering achieving Goal 9. Hence the need for BEI's cybersecurity framework.

International Telecommunication Union[7] described cybersecurity as a collection of policies, tools, approaches, mechanisms, best practices, and models that protect firms' assets. Mantha and de Soto [3] discovered that cybersecurity research started receiving attention in the 1990s. The cybersecurity industry is growing. Holst [8] projected that the global cybersecurity market would hit 250 billion US dollars by 2023. The cybersecurity market growth is a plus to the economic impact to mitigate the damages caused by cyberattacks. The Identity Theft Resource Center [9] stated that the data records and breaches exposed from 2005 to 2018 had increased drastically from 67 to 447 million and 157 to 1,244 million, respectively. Ponemon Institute and Accenture Securuty[10] reported that this increase had affected cybercrime costs by 30% for the UK, Japan, and the USA from 2017 to 2018. They affirmed that different industries, such as healthcare, insurance, and banking, insurance account for almost $12, $16, and $19 million, respectively. Mantha and de Soto[3] opined that the BEI needs more attention as statistics are unavailable for the sector. They reported that BEI's record might have been merged with other sectors, including infrastructure projects and government facilities.

There are few studies in this area, for example, Alshammari et al. [11], Tezel et al. [12], and Mantha et al. [13]. Alshammari et al. [11] affirmed that to achieve a cyber-physical system, IoT concept must be used. The IoT interconnects the building construction lifecycle and extracts data from the project's processes. Tezel et al. [12] studied the challenges and opportunities of blockchain's influence on transparency, trust, and cybersecurity. They contributed to cyber-physical convergence in construction digitalisation. Mantha et al. [13] developed a proposed cybersecurity threat framework for the construction sector. Others are Brooks et al.[14], who emphasised how to understand and reduce cybersecurity vulnerabilities. Mutis and Paramashivam[15] suggested cloud-BIM applications overwhelm the restrictions and BIM models' security vulnerabilities. None of these studies investigated the root cause of the Nigerian built environment industry (BEI) cyberattacks and how to develop a framework that might mitigate the attacks to improve achieving Goal 9 via the field participants' perception. Goal 9 is critical to construction digitalisation. No sector is excused from cybercrime attacks, including the BEI. Cyber attackers may attack the industry if measures are not taken to manage cybercrime activities. Developing a framework to manage cybercrime may improve BEI's cybersecurity. Nigeria's framework for managing cybercrime linked with BEI is still being determined. Thus, the study explores the root causes and identifies the information necessary to develop a Nigerian BEI cybersecurity framework for managing cybercrime to improve achieving Goal 9 via the following objectives.

i. To explore the root cause of cybercrime in the Nigerian built environment industry.

ii. To identify the information required to develop a built environment industry cybersecurity framework.

iii. To develop a cybersecurity framework for the built environment and improve achieving Goal 9.

2. Literature review

2.1. Cybercrime's background

Studies such as Soomro and Hussain[16] and Badamasi and Utulu [17] affirmed that cybercrime is ranked among the largest man-made risk. The word cybercrime is a combination of cyber (a derivative of cybernetics employed to explain interactions that concern or involve networks or computers) and crime (defined inactions or actions that is legally prohibited and could cause injurious to the public). Cybercrime encompasses all illegal tasks executed by internet fraudsters, hackers, and scammers [17]. Keshta and Odeh [18] affirmed that human tasks might include executing to gain illegitimate reception to information or sending malware and spam into electronic devices and linking to make them malfunction. Adesina and Ingirige [19] asserted that cybercrimes have devastatingly influenced public and private enterprises, including individuals. Billions of the US dollars' worth of damages, website defacement, and data loss went down the drain [17]. The outcome has sent many individuals, corporate companies, and government ministries/departments/agencies into insolvency [20]. Cybercrime is a menace to all sectors, including the built environment industry. It is estimated to cost the world economy US$6 trillion per annum from 2021 from $3 trillion in 2015 [17]. They found that the eruption of COVID-19 in early 2020 contributed to the high projection because of the movement restriction. From 2025, cybercrime may cost US$10.5 trillion per annum. Chapman[21] and Morgan[22] projected that losses to ransomware might cost the world US$20 billion by 2021. Badamasi and Utulu [17] identified ransomware as among the fastest-growing cybercrime. The BEI is not exempted. A few examples of past reported cyberattacks are the hacking of building management systems of the Google office in Australia and illegal access to the target's network via the mechanical contractor, which led to millions of credit and debit card accounts in the USA [23]. Greenwood [24] reported the Australian Secret Intelligence Services stole construction plans and specifications. Similarly, the USA-based construction companies' (Turner and Whiting-Turner) data breach of staffers information. Konecranes and Marous Brothers Construction lost 1.7 million United States dollars and 17.2 million euros because of unwarranted payments and wire fraud. Also, Bouygues Construction suffered ransomware, leading to the firm's closed-off systems. Similarly, Bam Construct closed its website because of the cyberattack [3].

However, most cyberattacks on individuals, private, and public organisations are executed via spearphishing emails, including the organisations in the BEI. The need for a cybersecurity management framework to curb the menace of cybercrime through providing knowledge to firms (private and public), especially BEI, has become pertinent. Badamasi and Utulu [17] asserted that cybercrime frameworks offer a diversity of principles and plans targeted at preventing or mitigating cyberattacks. In Nigeria, all sectors may be prone to cyberattacks. The 2023 Presidential and National Assembly elections suffered 12,988,978 attacks, as reported by the Nigerian Minister of Communications and Digital Economy [25]. It was reported that threats to portals and public websites daily was 1,550,000 and skyrocketed to 6,997,277 on Presidential Election Day. This calls for concern and shows that every sector is only free if there is a mechanism to check the menace. Cybercrime or cyberattack is clustered into password sniffing, hacking, logic bombs, spam, spyware, viruses, trojan horse, cyberstalking, worm, fake copy-cat websites, wiretapping, malware, phishing, bad rabbit ransomware, cyber fraud, ransomware, and cyber terrorism [26,27,28]. Ibrahim [29] identified the quest for wealth, urbanisation, inadequately equipped law enforcement agencies, joblessness, lax implementation of cybercrime laws, negative role models, corruption, gullibility/greed, poverty, and the porous nature of the internet as the causes of cybercrime in Nigeria. Osho and Onoja [30] re-emphasised the need for implementing a consolidated cybersecurity framework. This aligns with the mission of the National Information and Technology

Development Agency and the Office of the National Security Adviser, in collaboration, shares similar opinions with the National Institutes of Standards and Technology and Microsoft to address the threats from these cyberattacks. It is for sectors, like manufacturing, financial sector, and oil and gas. These continues threats motivated this study. Thus, the study attempts to develop cybersecurity framework for Nigerian BEI because of the sector's relevance to the economy.

Regarding the digital components of the built environment industry. This includes design and planning innovations and material, equipment, and machinery innovations. The design and planning innovations is sub-clustered into three groups. This includes virtual building design and information modelling (3D modelling, construction programming [4D], baseline quantities and costs [5D], direct fabrication, and asset management), off-site manufacture (just-in-time, lean production, concurrent engineering and design, IT-enabled planning, and time- and space-based scheduling), and green urbanism (sustainable communities, slim city, and urban informatics). Also, material, equipment and machinery innovations are sub-clustered into four groups. This includes passive building technologies (passive lighting systems, advanced insulation technology, spectrally sensitive glazing, dynamic façade systems, and passive efficiency modelling), sustainable products (energy innovations and material innovations), extreme weather-proofing technology (fire-retardant construction materials, flooding and cyclone resistance, and disaster mitigation modelling), and control and monitoring systems (building management systems, automated project performance control, and machine guidance technology) [12]. Also, AlBalkhy et al. [31] identified digital twin as increasing noticeably in the built environment. There are challenges despites potential advantages. Cyberattack may not be exempted. This can hinder Goal 9 if not checked.

2.2. Cybersecurity issues in the built environment industry

Construction digitalisation is making the BEI more exposed to cybercrimes and cyberattacks. This is because the industry progressively depends on cyber-physical systems that may be prone to new risks linked with cyberattacks [13]. Alshammari et al. [11] affirmed that IoT could be employed to achieve a cyber-physical system in a building construction lifecycle. Digitalisation and control systems assist in making buildings smarter. This is because of novelties in HVAC, health and safety, utilities, telecommunications, and building management systems. Howell et al. [32] opined that frequent innovation in artificial intelligence and IoT realms result in mature products and services. Alshammari et al. [11] emphasised how data cybersecurity is set-up, the common data environments, and shared repositories and supply chain. They avowed that construction is unaccustomed to accommodating cybersecurity considerations.

Cybersecurity aligns with standards to function. This includes Advanced Encryption Standard (AES), Federal Information Processing Standard (FIPS) 201, and ISO 27002:2013, as identified by Technology [33]. These systems offer fair costs and ensure high levels of security and performance. Applying suitable hazard assessments has become pertinent to enhance reliance on the asset [32]. Boyes [34] claimed that the United Kingdom Government encourages relevant stakeholders to consider cyberspace security. This includes the certification by contractors of ISO 27001. Generation and Storage [35] discovered that BIM's future that can communicate with IoT devices might present critical cybersecurity concerns. Similarly, Alshammari et al. [11] found that cybersecurity implementation in smart grids used in energy systems concerns stakeholders. Howell et al. [32] suggested three ways to enhance performance and security. First, the study should identify and quantify the risk of a security and privacy breach to the quality of service and systemic reliability caused by insecure authentication. Second, the study should identify and quantify the loss of data, breach of vulnerability, and privacy because of mixed communication infrastructure. Third, the study should develop guidelines or a framework for information security management. This is part of the study's motivation to develop a framework for managing cybercrime in the built environment industry. Mantha et al. [13] identified cybersecurity risk

model relevant to the BEI. They showed how robotic systems collect data as a possible countermeasure to proffer answers to the cybersecurity encumbrances hindering the building certification and commissioning phase.

2.3. Cybersecurity framework for the built environment industry to improve achieving Goal 9

Cybersecurity framework has to do with reducing cybersecurity menaces. This has become pertinent because the world embraces digitalisation, including the BEI, to mitigate growing risks associated with digitalisation. Organisations in the BEI face several digital risks. These risks may hinder improving achieving Sustainable Development Goal 9 if not mitigated. Goal 9 comprises of eight targets and twelve indicators[37,38]. The industry needs innovation and digitalisation through industrialisation to foster sustainable growth. Any slight threat through cyber-attack may hinder Goal 9. The risks include human-related, nature-related, and third party-related, such as contractors [13]. Cybersecurity may mitigate the risk associated with cyberattacks. Mikkola et al. [36] affirmed that risk is an impulsive incidence or situation in firms with a harmful influence. The influence includes quality, cost, or time. Purohit et al. [39] emphasised that the mechanisms involve hazard preparation, evaluation, explanation, responses, and management. Every sector, including the BEI, that wants to excel should develop competencies to handle menaces, especially from digital-related components. A proactive cybersecurity framework is advisable to stem the underpinning issues. Pattinson et al. [40] acknowledged many cybersecurity frameworks. Smith [41] identified Cybersecurity Risk Framework, Global Cybersecurity Index, Specified Frameworks, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework as the major framework. NIST [42] identified five core roles that firms should proffer solutions to proactively mitigate cyberattacks to commercial dealings: identification, discovery, defence, response, and recovery in formulating NIST Cyber Security Framework.

Also, Global Cybersecurity Index Framework generated by the International Telecommunication Union (ITU) is widely used by global firms [43]. The framework examines the firm's development in cybersecurity systematically. Maarten et al. [44] and ITU [43] identified five key variables that influence the dimension of cybersecurity within firms. This includes legal measures, cooperation, technical measures, capacity building, and organisational measures. The frameworks are mostly used in developed countries, besides Badamasi and Utulu [17], which developed cybersecurity frameworks for Nigerian universities based on reviewed literature. Thus, justifying the study's motivation to fill the theoretical (empirical) gap. The study adapts Badamasi and Utulu [17] five constructs used in the developed universities' cybersecurity framework. The BEI should understand its technical contexts, operations, and security problems to mitigate cybersecurity threats. To achieve this goal, the BEI should offer solutions to the issues raised: what threats face Nigerian BEI cybersecurity? What should be the objectives of Nigerian BEI cybersecurity programmes? What techniques are used for managing cyberattacks by Nigerian BEI? How can the Nigerian BEI cybersecurity programmes be tested and evaluated? How can the Nigerian BEI cybersecurity programmes be communicated to key stakeholders?

3. Research method

This study adopted an inductive method. This implies inducting real-life issues as the motivation for the research [45,46,47]. Also, a phenomenology method was employed via virtual interviews with selected participants in Lagos and Abuja, Nigeria. Lagos and Abuja are the major construction and commercial hubs in Nigeria [48]. It was utilised because this aspect of the research is scarce in Nigeria's BEI cybersecurity framework and used in a similar method by Alshabib and Martins[49] and Ebekozien et al. [48]. Alshabib and Martins [49] used interviews to engage Gulf Cooperation Council members who were cybersecurity experts to counter the complex encumbrances posed by cybercrime. Ebekozien et al. [48] explored the qualitative approach

to investigate blockchain relevance in the Nigerian construction industry. Qualitative research has the advantage of locating insights and meanings that engage participants placed [47,50]. This motivated the approach adopted and contributed to the theoretical implications. The study engaged 28 interviewees and achieved saturation at the 25th participant. This includes contracting organisations, consulting firms, academicians in construction and cybersecurity, government ministries/departments/agencies in IT matters, and cybersecurity experts. The position of the interviewees, as presented in **Table 1**, indicates that they are the most qualified. They are experts in the subject. The researchers adopted virtual interviews for the collected data via semi-structured questions, as presented in Appendix A. A semi-structured approach offers the investigator to seek flexible questions from the general to the specific [51]. The collected data were validated via secondary sources in line with Ebekozien [52], who employed empirical published papers as sources of validation.

Table 1. Interviewees' background.

ID	Participant	Location	Years of experience	Rank/Firm
P1	Quantity Surveyor	Lagos	34 years	Principal Partner/QS consultancy firm
P2	Quantity Surveyor/Academician		23 years	Senior Quantity Surveyor/QS firm
P3	Architect		28 years	Director/Architectural consultancy firm
P4	Architect/Academician		22 years	Senior Architect/Consultancy firm
P5	Engineer		26 years	Operational Director/Engineering consultancy firm
P6	Engineer/Academician		20 years	Senior Engineer 1/Consultancy firm
P7	Cybersecurity expert		26 years	MD, IT Consultant
P8			20 years	PM /Consultancy firm
P9	Construction Contractor		30 years	Director/Medium contracting firm
P10			25 years	CEO/small contracting firm
P11			22 years	Operation Manager contracting firm
P12			20 years	Deputy Manager contracting firm
P13	Govt dept/agency		20 years	Senior staff
P14			20 years	
P15	Quantity Surveyor	Abuja	30 years	Senior Partner/QS consultancy firm
P16	Quantity Surveyor/Academician		26 years	Senior Quantity Surveyor/QS firm
P17	Architect		25 years	Senior Director/Architectural consultancy firm
P18	Architect/Academician		19 years	Senior Architect/Consultancy firm
P19	Engineer		25 years	Director/Engineering consultancy firm
P20	Engineer/Academician		20 years	Senior Engineer/Consultancy firm
P21	Cybersecurity expert		22 years	Partner, IT Consultant
P22			24 years	MD, IT firm
P23	Construction Contractor		37 years	Director/Medium contracting firm
P24			25 years	CEO/small contracting firm
P25			20 years	Project Manager contracting firm
P26			24 years	Site Manager contracting firm
P27	Govt dept/agency		21 years	Senior staff
P28			22 years	Deputy Director

Source: Authors work

The researchers conducted the study's data collection from November 2022 to late February 2023 and took 45 minutes average per interviewee. Purposive sampling method was employed for the selection of competent participants. The research collected data were analysed manually and presented in themes. The technique identified and engaged the interviewees willing to participate [1]. The researchers sent invitation letters to intending participants regarding the participants' selections, as presented in Appendix A. The study adopted open coding and allotted labels to develop constructs. The researchers adopted emotion, invivo, themeing, and narrative coding techniques [53]. The researchers generated 95 codes and re-clustered based on occurrence, reference, and frequency. Fifteen sub-themes emerged from the 95 codes and were mapped into three themes.

4. Results and discussion

The reviewed literature revealed that a viable framework has the potential to prevent or mitigate cyberattacks in the BEI. This section presents the main study's findings and is followed by discussions. This includes findings associated with the root cause of cyberattacks, information necessary to develop a cybersecurity framework to manage cybercrime in the BEI, and the developed framework as follows:

4.1. Theme one: Root cause of cybercrime in the BEI

In this sub-section, the interviewees opine that the BEI's cyberattacks are majorly caused by human beings with negative intentions to harm their victims. Results align with Soomro and Hussain[16], and van Schaik et al. [54]. They opined that cybercrime is among the top list of the largest man-made risk. The root causes of cybercrimes, especially in the finance sector, are not new but none regarding the BEI in Nigeria. This study clustered the 15 causes into primary and secondary sources. The primary root causes are unemployment, the quest for wealth, negative role models, corruption, gullibility/greed, lax implementation of cybercrime laws, inadequately equipped law enforcement agencies, poverty, the porous nature of the internet, and urbanisation. The secondary sources are increased construction digitalisation, reliance on cyber-physical systems, lax preparation and management processes, inadequate centralised management systems, and construction project life cycle vulnerabilities. Findings agree that cyber fraud (identity theft), hacking, password sniffing, and copy-cat websites are the most frequent cybercrimes in the Nigerian BEI (majority). Identity theft or cyber fraud is the act of dishonest intention to benefit or gain illegitimately (P3, P7, P13 & P24). Participant P12 says, "…. *cybercrime has developed unethical skills lazy youths in many developing countries, Nigeria inclusive, want to learn. The intention is to defraud people via illegal means. The value system has not helped matter. How can parents and guardians encourage young adults under 20 years old who ought to be in a higher institution or learning a trade/skill via apprenticeship to go into fake website design learning to commit fraud? One of my clients was a victim. Thank God, the financial transaction to buy the property was unsuccessful due to bank network problems, the story would have become something else* ……" Findings agree with Ibrahim [55], who affirmed that fraudsters create fake 'copy-cat' websites to take advantage of victims not vast with internet procedures or the genuine website address of the organisation.

The quest for wealth, negative role models, corruption, and gullibility/greed have pushed many young adults to phish and password sniffing. Phishing is a digital identity theft that snips the personal data and identity of gullible victims and commits acts of fraud against a genuine individual or firm. Participant P2 says, "…. *I was almost a victim of phishing but thank God for the follow-up via phone conversation before the final transaction. The fraudster sent a false email to me but with a similar pattern to the previous trail of emails. Please, the government needs to do something drastically.*…" Results align with Hassan et al. [26] and Ibrahim [55]. Hassan et al. [26] identified the quest for wealth, negative role models, corruption, and gullibility/greed as root causes of cybercrime. Ibrahim[29] and Sibe and Kaunert [55] identified lax implementation of cybercrime

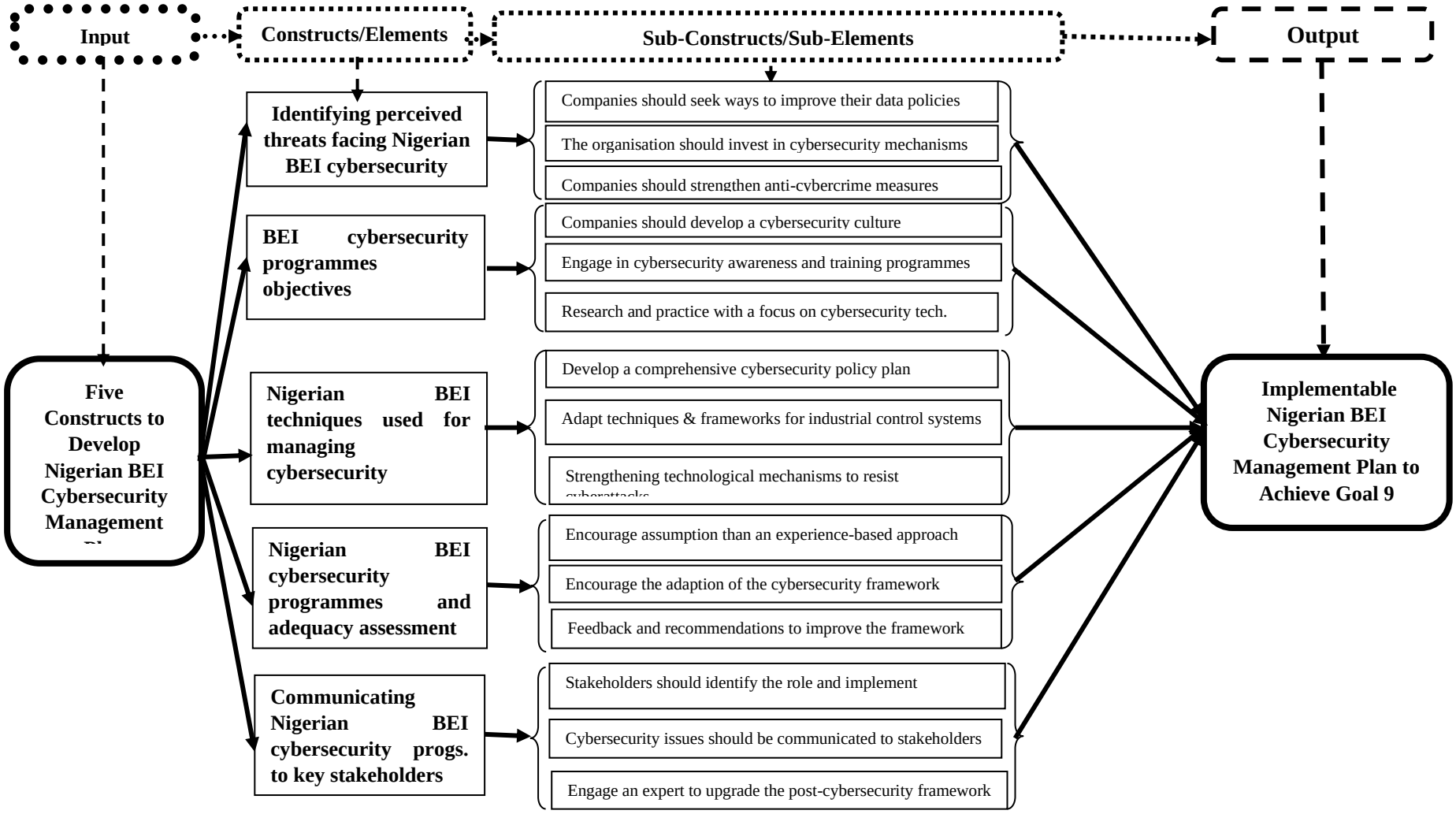
laws, the quest for wealth, urbanisation, joblessness, inadequately equipped law enforcement agencies, negative role models, corruption, gullibility/greed, poverty, and the porous nature of the internet as the causes of cybercrime in Nigeria. Regarding increased construction digitalisation and cyber-physical systems, findings agree with Mantha et al. [13] and Tezel et al. [12]. They found that rapid construction digitalisation, including smart cities, increases vulnerability to cyberattacks because they depend on cyber-physical systems for effective practices. Cyber-physical systems are prone to new risks and vulnerable to cyberattacks (P7, P8, P21, & P22). Also, findings agree with Mantha and de Soto [3]. They found that cyberattacks occur because of vulnerabilities of construction projects during the life cycle. Participant P18 says, "…. *inconsistencies and vulnerabilities attacks can occur in other phases. Hence, understanding the different construction project phases and their interdependencies is needed to develop an effective cybersecurity risk management plan. It will enhance developing countermeasures for the root cause of the cyberattacks….*"

4.2. Theme two: information necessary to develop BEI cybersecurity framework

This sub-section offers the participants the platform to identify constructs required to develop BEI cybersecurity framework in Nigeria. Cybersecurity is a multifaceted socio-technical phenomenon linking many facets (P1, P7, P20, P22, & P28). Thus, key stakeholders should give digital security attention in the BEI to mitigate criminals and hackers using sophisticated mechanisms to gain access to sensitive information, including the financial transaction of multinational construction companies. One novelty is the emerged five constructs (identifying perceived threats facing Nigerian BEI cybersecurity, BEI cybersecurity programmes objectives, Nigerian BEI techniques used for managing cybersecurity, Nigerian BEI cybersecurity programmes and adequacy assessment, and communicating Nigerian BEI cubersecurity programmes to key stakeholders) in the Nigerian BEI context as the established independent variables and implementable Nigerian BEI cybersecurity management plan to mitigate threats and breaches as the dependent variable, as revealed in **Figure 1**. This modification from Badamasi and Utulu [7] developed a cybersecurity framework for universities based on reviewed literature. Besides this current study exploring a different sector (BEI), the developed framework is based on empirical findings.

4.2.1. Identifying perceived threats facing Nigerian BEI cybersecurity

The BEI's primary activities are producing goods and service delivery. Globally, the industry is not exempted from attack, thus, is vulnerable to various cybersecurity issues, especially construction companies. This includes data protection, adapting new technologies, compromising employee salary records, and hacking company portals (P3, P9, P12, P23, P25, & P27). Refusal to mitigate may hinder achieving Goal 9. Goal 9 is critical to foster sustainable infrastructure and enhance construction digitalisation. Findings reveal overtime falsification clearance, viruses, website defacement, spyware, fake websites, phishing, password sniffing, worm, illegal interception of telecommunication, spam, malware, distributed denial of service, and identity theft as the cybersecurity issues facing the Nigerian BEI. Findings agree with Tanga et al. [28]. Besides their study in South Africa, they still need to develop a framework to manage cyberattacks facing the BEI. Participant P21 says, "…. *these issues are causing more damages to the built environment sub-sectors than imaged and more in the future if drastic actions are not taken to curb them, such as seeking ways to improve data protection policies, invest in cybersecurity mechanisms, including skilled manpower, and strengthen anti-cybercrime measures with strict and enforceable laws* …." Findings agree with Tsado et al. [56], who reported that in 2017, Nigeria lost US$649 million to cybercrimes. Also, Participants P3, P7, P13, P21, & P26 identify 'will scam' and computer/internet service time theft as new emerging issues faced by some indigenous construction companies and consultancy firms embracing digitalisation for administration operations. Evaluating and understanding cyberattack damages and the attackers are key to cyberattack management. There is a possibility



Source: Authors' work.

Figure 1. Developed framework for the Nigerian Built Environment Industry (BEI) cybersecurity management plan.

of halting cyberattack as quickly as possible if the attacks and attackers are understood (P6, P12, P21, P22, & P28). Participant P22 opines that this is part of cyberattack management and is key to influencing the cybersecurity framework for upgrading. Participant P3 says, "…. *we were a victim of a will scam. The scammer told us that one of our late partners had an investment, and several attempts to reach us failed until recently via our Facebook contact. We knew that investment was from the organisation profits but was dealing with impostor. We made the 1% payment as requested to process the claim, and the scammer immediately blocked all the communication channels*…." Results aligned with Bian et al. [57] and discovered that the fraudster sends electronic messages to claim that the prey is the recipient in the will and needs to make some payment for processing.

4.2.2. Nigerian BEI cybersecurity programmes' objectives

The modern organisations are driven by digital technology and innovation. Foster innovation and resilient infrastructure are component of Goal 9. Hence, cybersecurity programmes are pertinent to mitigate the vulnerability of networks and information systems of the BEI in cyberspace. Participants P10, P14, P22, & P27 affirm that setting goals for cybersecurity programmes for sub-sectors and firms in the BEI might be complex because of the nature of the industry. Participant P27 says, "…. *the set objectives would guide stakeholders and promote cybersecurity in the Nigerian BEI, especially the small- and medium-sized enterprises (SMEs) that dominate the industry*…." Findings agree with Bada and Nurse [58]. They found that cyberattacks on SMEs are higher and continue to increase. Findings attribute inadequate expertise, weak corporate cybersecurity, inadequate resources, and lack of awareness as the root causes (major). Findings agree with Paulsen [59], who found that SMEs struggle with cybersecurity because of the absence of awareness and expertise to manage the operation. To improve cybersecurity programmes in the BEI and achieve the key objectives, Participants P4, P6, P8, P16, P20, & P22 suggest cybersecurity awareness and training programmes for stakeholders, especially those in the SMEs category, cannot be over-emphasised. This is germane to achieving the objectives. Findings agree with Sonkor and de Soto [60]. They found a lack of cybersecurity awareness in the built environment as one of the challenges to overcoming the cybersecurity problems and suggested that stakeholders should be trained in cybersecurity modules to raise awareness and establish the needed competencies. Also, stakeholders should develop a strong cybersecurity culture to mitigate behavioural problems reinforcing cybersecurity lax (majority). Findings suggest reviewing programme resources via research and practice to proffer answers to the deficiencies of resources and expertise (P6, P17, & P26).

4.2.3. Nigerian BEI techniques used for managing cyberattacks

Cybersecurity management framework is pertinent for managing cyberattacks and threats from cybercrime. Findings show that most organisations in the BEI still need a comprehensive cybersecurity policy management plan. Policies tailored towards encouraging cybersecurity policy management plan will improve achieving Goal 9. Goal 9 is centred on upgrading infrastructure and retrofitting industries to make them sustainable, with increased resource-use efficiency and greater adoption of clean and environmentally sound technologies. These attributes cannot happen in the presence of cyberattacks. Participant P21 says, "…. *we should expect more cyberattacks, especially from SMEs, as more firms in the BEI embraces digitalisation. The absence of techniques to manage attacks from these digital technologies would enhance more issues for them to manage*…." Providing an integrated framework to manage attacks is pertinent to avert cybersecurity attacks (majority). Findings suggest that stakeholders, especially medium and small contractors embracing digitalisation in their daily operations, should strengthen their technological defense mechanism to resist cyberattacks. Also, Participants P1, P11, P16, P24, & P27 suggest modifying the techniques and models proposed for industrial control systems in critical infrastructure into the building phase considering its distinct

features. These techniques and frameworks have been tested and used in oil and gas, manufacturing, and power sectors regarding operational technology cybersecurity [60].

4.2.4. Nigerian BEI cybersecurity programmes appropriateness and adequacy assessment

Assessment and adequacy are key components of cybersecurity framework management. This key component allows the participants to evaluate the adequacy of the cybersecurity framework. The sub-theme evaluation was clustered into two: based on experience and assumptions in line with Badamasi and Utulu [17]. The two methods to evaluate the adequacy of the BEI's cybersecurity frameworks can assist stakeholders in adapting existing cybersecurity models. They promote a platform for constructive feedback and improve the framework for better efficiency (majority). Participants P7, P10, P14, & P24 assert that stakeholders' feedback and suggestions were made feasible because of cybersecurity appropriateness and adequacy evaluation mechanism. Findings reveal that the assumption-based cluster occurs where adequacy is influenced before the cyberattack [61]. The experience-based cluster occurs where adequacy is based on experience after the cyberattack [62]. The outcome of the damage might be minor and allows for improving the appropriateness and adequacy evaluation of the cybersecurity management framework.

4.2.5. Communicating Nigerian BEI cybersecurity programmes to key stakeholders

Findings show a lacuna in communicating cybersecurity issues to the stakeholders, especially the non-technical ones. Participants P2, P7, P12, P17, & P21 identify the complexity of problems and concerns as a possible reason for the non-communication. Results aligned with Culot et al. [63]. They discovered that cybersecurity professionals fail to make the matter important and accessible to non-technical partners. The study suggests two communication approaches (pre- and post-cyberattack phases) aligned with Badamasi and Utulu [7]. Participants P4, P9, P19, & P25 opine that the pre-cyberattack should comprise expectations from each stakeholder and how the cybersecurity framework plan operates. Also, for the post-cyberattack, Participants P4, P12, P18, & P22 affirm that organisations in the BEI are expected to communicate the gaps in the cybersecurity framework that enhanced the cyberattacks experienced and how the reviewed cybersecurity framework addresses the issues from the lacunas. Participant P21 says, "…*if not for these lacunas, the system would not have experienced these attacks. Thus, communication is key, might be tedious sometimes, and enhances knowledge sharing to mitigate future attacks…*." Findings agree with Smith [41], who affirmed that communicating thoughts to large firms may be a multifaceted duty. Findings agree that cybersecurity complex nature and the trouble in identifying the culprits and their intentions makes the communication act a complex endeavour (majority). But the need to communicate weak cybersecurity plan links with appropriate stakeholders should not be taken with laxity (P7, P15, P21, & P22.

4.3. Theme three: develop a framework implementing the BEI's cybersecurity

This sub-section develops a framework implementing BEI's cybersecurity in Nigeria. The necessary information required to develop the framework is the five constructs identified in the previous sub-sections, as presented in **Figure 1**. **Figure 1** presents the developed framework for implementing BEI's cybersecurity management in Nigeria to improve achieving Goal 9. Results aligned with Mantha et al. [13] and suggested that a framework can assist in proffering an answer to the safety and cyber security of the BEI's stakeholders during critical stages of construction projects. The framework will foster innovation and promote construction digitalisation through sustainable industrialisation. **Figure 1** articulates the five key constructs and 15 sub-constructs required to develop a BEI's cybersecurity framework to manage cyberattacks in Nigeria. The study's findings reveal the key measurement and operationalisation of the constructs (five) and sub-constructs (fifteen). The study adopted an implementable Nigerian BEI cybersecurity management plan as the dependent variable. Also, findings reveal identifying perceived threats facing Nigerian BEI cybersecurity, BEI

cybersecurity programmes objectives, Nigerian BEI techniques used for managing cybersecurity, Nigerian BEI cybersecurity programmes and adequacy assessment, and communicating Nigerian BEI cubersecurity programmes to key stakeholders as the independent variables. These threats may hinder Goal 9 if not mitigated. Referring to **Figure 1**, results show that the sub-constructs were identified. Each of the constructs comprises three main sub-constructs. The study suggests the developed cybersecurity framework can mitigate cyberattacks in the built environment industry if key stakeholders play their role responsibly. This gap needed to be included in previous works regarding the construction cybersecurity framework. Results align with Mantha et al. [13]. They stated that the proposed framework could assist in proffering answers to the safety and cyber security of the BEI's during construction projects and improve achieving Goal 9.

5. The study's implications

The study's developed cybersecurity framework could be used by the Nigerian BEI stakeholders, especially the construction consultants embracing digitalisation administration practices and emerging construction contractors, as a guideline to enhance BEI cybersecurity implementation in the sector. This is a component of the study's implications. Construction practitioners could employ the cybersecurity framework to assess construction and consultant firms' compliance levels concerning implementing the main sub-constructs in the future and improve achieving Goal 9. One benefit of this cybersecurity framework is the integrated independent constructs that promote BEI cybersecurity framework management implementation across the sector, as illustrated in **Figure 1**. Hence, the developed BEI cybersecurity framework would act as a roadmap for ease of implementation in Nigeria. Besides a theoretical search found no evidence of a study concerning exploring the information needed to develop a Nigerian BEI cybersecurity framework for managing cybercrime, the study's formulation of a BEI cybersecurity management plan in the form of a framework and ensuring that key stakeholders comply with a pertinent dimension that sought to emphasise as a practical consideration for the Nigerian Government. Finally, suggested findings from the 15 sub-constructs in **Figure 1** would support drivers of BEI cybersecurity framework implementation and enhance BEI's cybersecurity academic literature in developing countries. In practice, the developed BEI's cybersecurity framework could be employed to expand the knowledge of the BEI concerning compliance level and to stir up the advancement of the BEI cybersecurity framework for the sector regarding improve achieving Goal 9.

6. Limitations and areas for future study

The study has limitations and should be borne in mind. First, the empirical data that developed the BEI's cybersecurity framework were from Abuja and Lagos via a qualitative approach. Future studies should consider wider coverage via a quantitative approach. This will enhance the findings' generalisation and validate the present study's findings.

7. Conclusion

Construction digitalisation has come to stay and will continue to grow across the globe. The attacks from cyberspace on firms in the BEIs call for concern. Thus, cyberattacks may continue to expand, except there are scientific mechanisms to check the menace. This is a threat to Goal 9 and may hinder construction innovation and industrialisation. This research investigated the root cause of cybercrime in the Nigerian BEI and identified the variables required to develop a cybersecurity framework to manage cyberattacks in the Nigerian BEI via a qualitative approach. The developed framework would increase the level of cybersecurity awareness among stakeholders and how it can contribute to improve achieving Goal 9. Also, findings will promote cybersecurity implementation in the BEI, especially in developing countries with lax cybersecurity, such as Nigeria. This shows the need for organisations to make intensive efforts towards formalising and detailing cybersecurity

management plans into implementable frameworks as a component of the company's policies. This study presents a developed framework to resuscitate stakeholders in the Nigerian BEI and government regulators to set off integrated, all-inclusive actions toward developing an implementable cybersecurity framework.

Acknowledgements

Special thanks to the participants for providing scholarly contributions to enhance the findings of this study. The authors appreciate the comments, suggestions, and recommendations provided by the anonymous reviewers, which honed and strengthened the quality of this manuscript during the blind peer-review process.

Funding

This research was funded by School of Social Sciences, Universiti Sains Malaysia, George Town, Malaysia and Faculty of Engineering and the Built Environment and CIDB Centre of Excellence, University of Johannesburg.

Johannesburg, South Africa, grant number 05-35-061890. The APC was funded by INTI International University, Nilai, Malaysia.

Conflict of interest

The authors declare no conflict of interest.

References

1. Ebekozien A (2020a). Corrupt acts in the Nigerian construction industry: is the ruling party fighting corruption? Journal of Contemporary African Studies, 38(3): 348-365. doi: 10.1080/02589001.2020.1758304
2. Bogue R (2018). What are the prospects for robots in the construction industry? Industrial Robot: An International Journal, 45(1): 1-6. doi.10.1108/IR-11-2017-0194
3. Mantha BR, de Soto BG (2021). Cybersecurity in construction: Where do we stand and how do we get better prepared. Frontiers in Built Environment, 7, 612668.
4. Ebekozien A. Aigbavboa C (2021). Covid-19 recovery for the Nigerian construction sites: The role of the fourth industrial revolution technologies. Sustainable Cities and Society, 69: 1-10. doi.org/10.1016/j.scs.2021.102803
5. Dwivedi KY, Hughes DL, Coombs C, Constantiou I, Duan Y, Edwards JS, Upadhyay N (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. International Journal of Information Management, 55. https://doi.org/10.1016/j.ijinfomgt.2020.102211.
6. Theohary CA, Finklea K (2015). Cybercrime: conceptual issues for congress and U.S Law Enforcement. Congressional Research Service Report.
7. International Telecommunication Union (ITU) (2008). Definition of Cybersecurity, Geneva: ITU.
8. Holst A (2020). Global Cybersecurity Market Forecast 2017-2023, Hamburg: Statista.
9. Identity Theft Resource Center. (2018). 2018 End of Year Data Breach Report. Los Angeles, CA: Identity Theft Resource Center.
10. Ponemon Institute and Accenture Securuty. (2019). Ninth annual cost of cybercrime study unlocking the value of improved cybersecurity protection the cost of cybercrime contents. New York, NY: Accenture Securuty.
11. Alshammari K, Beach T, Rezgui Y (2021). Cybersecurity for digital twins in the built environment: current research and future directions. Journal of Information Technology in Construction, 26: 159-173. doi.10.36680/j.itcon.2021.010
12. Tezel A, Papadonikolaki E, Yitmen I, Bolpagni M (2021). Blockchain opportunities and issues in the built environment: Perspectives on trust, transparency and cybersecurity. In Industry 4.0 for the Built Environment: Methodologies, Technologies and Skills (pp. 569-588). Cham: Springer International Publishing.
13. Mantha B, de Soto BG, Karri R (2021). Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment. Sustainable Cities and Society, 66, 102682.
14. Brooks DJ, Coole M, Haskell-Dowland P (2020). Intelligent building systems: security and facility professionals' understanding of system threats, vulnerabilities and mitigation practice. Secur. J. 33: 244–265. doi: 10.1057/s41284-019-00183-9

15. Mutis I, Paramashivam A (2019). Cybersecurity management framework for a cloud-based BIM model," in Advances in Informatics and Computing in Civil and Construction Engineering, (Berlin: Springer International Publishing), 325–333. doi: 10.1007/978-3-030-00220-6_39
16. Soomro TR, Hussain M (2019). Social media-related cybercrimes and techniques for their prevention. Applied Computer Systems, 24(1): 9-17.
17. Badamasi B, Utulu SCA (2021). Framework for managing cybercrime risks in Nigerian universities. Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development.
18. Keshta I, Odeh A (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2): 177-183.
19. Adesina R, Ingirige B (2019). Dismantling barriers to effective disaster management in Nigeria. 14th International Postgraduate research conference 2019: Contemporary and Future Directions in the Built Environment.
20. De Paoli S, Johnstone J, Coull N, Ferguson I, Sinclair G, Tomkins P, Brown M, Martin R (2020). A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. Policing: A Journal of Policy and Practice, 3: 12-18.
21. Chapman J (2019). How safe is your data? Cyber-security in higher education. Higher Education Policy Institute Policy, 23: 12-23.
22. Morgan S (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine, 12: 1-9.
23. Shu, K., Sliva, A., Wang, S., Tang, J., Liu, H. (2017). Fake news detection on social media: A data mining perspective. ACM SIGKDD explorations newsletter, 19(1), 22-36.
24. Greenwood, J. W. (2020). Intelligence agencies in cyberspace: Adapting the intelligence cycle to cyber threats and opportunities (Doctoral dissertation, The University of Waikato).
25. Faminu G (2023). Nigeria suffered over 12.9m cyber-attacks during presidential, NASS elections – Pantami. Business Day, Retrieved from https://businessday.ng/news/article/nigeria-suffered-over-12-9m-cyber-attacks-during-presidential-nass-elections-pantami/
26. Hassan AB, Lass FD, Makinde J (2012). Cybercrime in Nigeria: causes, effects and the way out. Journal of Science and Technology, 2(7): 626 –631.
27. Wada F Odulaja GO (2012). Assessing cybercrime and its impact on e-banking in Nigeria using Social Theories. African Journal of Computing & ICTs. 5(1): 69-82.
28. 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 (ITcon), 27: 845-863.
29. Ibrahim UMARU (2019). The Impact of Cybercrime on the Nigerian Economy and banking system. NDIC Quarterly, 34(12): 1-20.
30. Osho O, Onoja AD (2015). National cyber security policy and strategy of Nigeria: A qualitative analysis. International Journal of Cyber Criminology, 9(1): 22-28.
31. AlBalkhy W, Karmaoui D, Ducoulombier L, Lafhaj Z, Linner T (2024). Digital twins in the built environment: Definition, applications, and challenges. Automation in Construction, 162, 105368.
32. Howell S, Rezgui Y, Beach T (2018). Water utility decision support through the semantic web of things. Environmental Modelling & Software, 102: 94-114.
33. Technology NIS (2017), "FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors.
34. Boyes H (2014). Building Information Modelling (BIM): Addressing the Cyber Security Issues. Iet: 1–12. doi: 10.1049/etr.2014.9001.
35. Generation D, Storage E (2011). IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads IEEE Standards Coordinating Committee 21 Sponsored by the.
36. Mikkola M, Oksanen A, Kaakinen M, Miller BL, Savolainen I, Sirola A, Zych I, Paek H.-J (2020). Situational and Individual Risk Factors for Cybercrime Victimisation in a Cross-national Context. International Journal of Offender Therapy and Comparative Criminology, 0306624X20981041.
37. United Nations (2020). The Sustainable Development Goals Report 2020. New York: United Nations. https://unstats .un .org/ sdgs/ report/ 2020/ The -Sustainable-Development- Goals -Report -2020 .pdf.
38. United Nations (2022). Secretary General outlines priorities for 2022. Retrieved from https://www.un.org/ press/ en/ 2022/ sgsm21113 .doc .htm
39. Purohit DP, Siddiqui N, Nandan A, Yadav BP (2018). Hazard identification and risk assessment in construction industry. International Journal of Applied Engineering Research, 13(10): 7639-7667.
40. Pattinson MR, Butavicius MA, Ciccarello B, Lillie M, Parsons K, Calic D, McCormac A (2018). Adapting cyber-security training to your employees. HAISA.
41. Smith W (2019). A comprehensive cybersecurity defense framework for large organisations.

42. NIST. (2020) Cybersecurity framework. https://www.tenable.com/lp/campaigns/20/whitepapers/adhering-to-the-nist-framework-with-tenable-ot/?utm_campaign=gs-{9662775243}-{100779850978}{426501511627}_00021238_fy21q1&utm_promoter=tenable-indegy-nb 00021238&utm_source=google&utm_term=%2Bnist%20%2Bframework&utm_medium=cpc&utm_geo=emea&gclid=EAIaIQobChMIjbXbsunm7wIVAtWyCh2j7g6IEA AYASAAEgIu0PD_BwE
43. ITU. (2015). Global cybersecurity index & cyberwellness profiles report (Cybersecurity, Issue. I.T. Union. https://www.itu.int/pub/D-STR-SECU-2015
44. Maarten G, Artur U, Erik F, Michel R (2015). A meta-analysis of threats, trends, and responses to cyber-attacks (Assessing Cyber Security, Issue. T. H. C. f. S. Studies. https://hoffmannbv.nl/sites/default/files/Report%20Assessing%20Cyber%20Security%2016%20april%202015.pdf
45. Fellows R, Liu MMA (2015). Research methods for construction (4th ed.). West Sussex, United Kingdom: John Wiley & Sons.
46. Jaafar M, Ebekozien A, Mohamad D (2021a). Community participation in environmental sustainability: A case study of proposed Penang Hill Biosphere Reserve, Malaysia. Journal of Facilities Management. doi.10.1108/JEM-03-2021-0033.
47. Jaafar M, Salim AAN, Salleh MN, Sulieman BZ, Ulang MN, Ebekozien A (2021b). Developing a framework for fire safety management plan: the case of Malaysia's public hospital buildings. International Journal of Building Pathology and Adaptation. doi.10.1108/IJBPA-04-2021-0060.
48. Ebekozien A, Aigbavboa C, Samsurijan SM (2023). An appraisal of blockchain technology relevance in the 21st century Nigerian construction industry: perspective from the built environment professionals. Journal of Global Operations and Strategic Sourcing, 16(1): 141-160 doi. 10.1108/JGOSS-01-2022-0005.
49. Alshabib HN, Martins JT (2022). Cybersecurity: perceived threats and policy responses in the Gulf Cooperation Council. in IEEE Transactions on Engineering Management, 69(6): 3664-3675 doi: 10.1109/TEM.2021.3083330.
50. Ibrahim FS, Ebekozien A, Khan P, Aigbedion M, Ogbaini IF, Amadi G (2022). Appraising fourth industrial revolution technologies' role in the construction sector: How prepared is the construction consultants? Facilities. doi.10.1108/F-09-2021-0086.
51. Creswell JW (2014). Research design: qualitative, quantitative, and mixed methods approach (4th ed.). Thousand Oaks, Califonia, USA: Sage.
52. Ebekozien A (2020b). A qualitative approach to investigate low-cost housing policy provision in Edo State, Nigeria. International Planning Studies, 1-18. doi:10.1080/13563475.2020.1779671
53. Corbin J, Strauss A (2015). Basics of qualitative research: Techniques and procedures for developing grounded theory (4th ed.). Thousand Oaks, California, USA: Sage.
54. Van Schaik P, Jeske D, Onibokun J, Coventry L, Jansen J, Kusev P (2017). Risk perceptions of cyber-security and precautionary behaviour. Computers in Human Behaviour, 75: 547-559. doi.1016/j.chb.2017.05.038
55. Sibe, R. T. Kaunert, C. (2024). Cyber Crime in Nigeria—Reviewing the Problems. In Cybercrime, Digital Forensic Readiness, and Financial Crime Investigation in Nigeria (pp. 19-55). Cham: Springer Nature Switzerland.
56. Tsado, L., Raufu, A., Ben-Edet, E. Krakrafaa-Bestman, D. (2023). Combatting the Threat of Cybercrime in Nigeria: Examining Current Laws and Policies. Journal of Applied And Theoretical Social Sciences, 5(4), 413-430.
57. Bian S, Deng Z, Li F, Monroe W, Shi P, Sun Z, Wu W, Wang S, Wang WY, Yuan A (2018). Icorating: A deep-learning system for scam ico identification arXiv preprint arXiv:1803.03670
58. Bada M, Nurse JRC (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)", Information and Computer Security, 27(3): 393-410. https://doi.org/10.1108/ICS-07-2018-0080
59. Paulsen C (2016). Cybersecuring small businesses. Computer, 49(8): 92-97.
60. Sonkor MS, de Soto BG (2021). Operational technology on construction sites: A review from the cybersecurity perspective. Journal of Construction Engineering and Management, 147(12) 04021172
61. Armenia S, Angelini M, Nonino F, Palombi G, Schlitzer MF (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems, 113580.
62. Glantz C, Somasundaram S, Mylrea M, Underhill R, Nicholls A (2016). Evaluating the maturity of cybersecurity programs for building control systems. US Department of Energy Office of Scientific and Technical Information.
63. Culot G, Fattori F, Podrecca M, Sartor M (2019). Addressing industry 4.0 cybersecurity challenges. in IEEE Engineering Management Review, 47(3): 79-86, doi: 10.1109/EMR.2019.2927559.

Appendix A: Virtual interview questions

Dear Participant,

Request for Virtual Interview

Cybercrime activities are fast-growing and threatening critical sectors, especially in developing countries. No sector is exempted, including the built environment industry (BEI). Cyber attackers may attack the industry more if measures are not taken to manage cybercrime activities. Developing a framework to manage cybercrime may improve BEI's cybersecurity. Nigeria's framework for managing cybercrime linked with BEI is still being determined. Therefore, this research is titled: Developing a Framework for Managing Cybercrime in the Nigerian Built Environment Industry: An Explorative Approach. Specifically, the researchers will achieve this research through the following objectives:

i. To explore the root cause of cybercrime in the Nigerian built environment industry.

ii. To identify the information required to develop a built environment industry cybersecurity framework.

iii. To develop a cybersecurity framework for the built environment and improve achieving Goal 9.

Note the interview questions are going to be within the stated objectives. Responses provided by you will be collated and analysed with those of other engaged participants. It will make up the value and contribution to achieving the success of this research. We will treat information provided with confidentiality.

Thanks for the anticipated participation.

Regards.

Yours faithfully,

(Researchers)

Basic questions for the participants

1. Please, for record purposes, what is the name of your organisation?
2. Please, what is your position in the organisation?
3. Please, how long have you been working?
4. Are you knowledgeable about cybercrime, Goal 9, and the Nigerian built environment industry (BEI)?
5. If yes to question 4, in general terms, from your perception, how can you describe the influence of cybercrime on the built environment in Nigeria?
6. Please, can you identify the root cause of cybercrime in the Nigerian built environment industry?
7. As a stakeholder in the construction sector, which of the cyberattacks are frequent?
8. Can a BEI cybersecurity framework mitigate cyberattacks?

9. If yes, how?
10. If not, why?
11. Can you identify the information required to develop a BEI cybersecurity framework for managing cybercrime?
12. From your perspective, what role can the framework perform in mitigating cyberattacks and, by extension, improve achieving Goal 9?
13. Please, what role can the key stakeholders play in mitigating cyberattacks in the Nigerian built environment to improve achieving Goal 9?