Received 7 December 2022
Revised 14 March 2023
Accepted 11 April 2023

Cybersecurity effectiveness in UK construction firms: an extended McKinsey 7S model approach

Sulafa Badi
Faculty of Business, British University in Dubai, Dubai, United Arab Emirates, and
Mohamed Nasaj
Abu Dhabi University, Abu Dhabi, United Arab Emirates

Abstract

Purpose – This study aims to assess the essential elements of internal organisational capability that influence the cybersecurity effectiveness of a construction firm. An extended McKinsey 7S model is used to analyse the relationship between a construction firm's cybersecurity effectiveness and nine internal capability elements: shared values, strategy, structure, systems, staff, style, skills, relationships with third parties and regulatory compliance.

Design/methodology/approach – Based on a quantitative research strategy, this study collected data through a cross-sectional survey of professionals working in the construction sector in the United Kingdom (UK). The collected data was analysed using descriptive and inferential statistical methods.

Findings – The findings underlined systems, regulatory compliance, staff and third-party relationships as the most significant elements of internal organisational capability influencing a construction firm's cybersecurity effectiveness, organised in order of importance.

Research limitations/implications – Future research possibilities are proposed including the extension of the proposed diagnostic model to consider additional external factors, examining it under varying industrial relationship conditions and developing a dynamic framework that helps improve cybersecurity capability levels while overseeing execution outcomes to ensure success.

Practical implications – The extended McKinsey 7S model can be used as a diagnostic tool to assess the organisation's internal capabilities and evaluate the effectiveness of implemented changes. This can provide specific ways for construction firms to enhance their cybersecurity effectiveness.

Originality/value – This study contributes to the field of cybersecurity in the construction industry by empirically assessing the effectiveness of cybersecurity in UK construction firms using an extended McKinsey 7S model. The study highlights the importance of two additional elements, third-party relationships and construction firm regulatory compliance, which were overlooked in the original McKinsey 7S model. By utilising this model, the study develops a concise research model of essential elements of internal organisational capability that influence cybersecurity effectiveness in construction firms.

Keywords Cybersecurity, Effectiveness, McKinsey's 7S model, Construction firms, United Kingdom

Paper type Research paper

1. Introduction

The 21st-century construction industry is currently undergoing a digital transformation known as Construction 4.0 (Forcael *et al.*, 2020; Osunsanmi *et al.*, 2020). This transformation is driven by rapid advancements in information and operational technologies such as the Internet of things (IoT), big data, building information modelling (BIM), building automation and control systems (BACSs) and industrial automation and control systems (IACS). These technologies are changing the way construction projects are designed, planned, built, operated and maintained, resulting in reduced project time and cost, increased quality and improved productivity (Osunsanmi *et al.*, 2018; García de Soto *et al.*, 2022). However, with increased digital interconnectivity, cybersecurity is becoming increasingly crucial in the construction industry (Patel and Patel, 2020; Alshammari *et al.*, 2021; Demirkesen and Tezel, 2022). Cybersecurity refers to the practice of protecting computers, networks and stored data from unauthorised access by digital criminals and other threats (Craigen *et al.*, 2014).

Engineering, Construction and Architectural Management
Vol. 31 No. 11, 2024
pp. 4482-4515

0969-9988
DOI 10.1108/ECAM-12-2022-1131

Cybersecurity vulnerabilities can originate from two main sources: system weaknesses or flaws and user behavior that can lead to security breaches (Kabanda *et al.*, 2018). Most cyberattacks are not reported (Amir *et al.*, 2018). Firstly, cyberattacks can cause irreversible damage to a company's reputation (Kejwang, 2022). Secondly, attackers often use advanced methods to conceal their identities while executing their operations clandestinely (NCSC, 2022).

The construction industry is increasingly vulnerable to cyberattacks (Turk *et al.*, 2022a, b; NCSC, 2022). Construction firms may face various cybersecurity threats, including cybercriminals seeking financial gain, malicious insiders using company data or networks for harmful activities and hacktivists attempting to disrupt or cause damage to security systems (NCSC, 2022). According to Hiscox's (2021) cyber readiness report, which surveyed global organisations, there has been a rise in cyberattacks against firms, with construction being one of the top five targeted sectors (Hiscox, 2021). In fact, a 2022 survey revealed that 44% of United Kingdom (UK) construction firms had experienced a ransomware attack in the past two years, with 25% encountering two to four incidents and 5% experiencing five or more (Gayne, 2022). Among the infamous incidences of cyberattacks on UK construction firms include.

(1) Interserve suffered a cyberattack in May 2020 that resulted in the theft of 113,000 sensitive employee data. The hackers used a phishing email to gain access to the company's network and infiltrated data such as employees' names, addresses and bank account details (ICO, 2022)

(2) Bouygues Construction suffered a ransomware attack in January 2020, with personal data of its employees being published online by a cybercrime group, who demanded ransom to unlock encrypted data (Kelly, 2020)

(3) Bam Construct suffered a ransomware attack in May 2020 after hackers exploited a vulnerability on their website and encrypted the firm's files, demanding payment for access to them (Weinfass, 2020)

In fact, a report published by the UK National Cyber Security Centre (2022) in collaboration with the Chartered Institute of Building (CIOB) highlighted that cybercriminals view construction businesses as easy targets. Construction firms often have high cash flows and transact in high-value payments due to the sector's extensive use of suppliers and subcontracting (NCSC, 2022). Construction businesses are also a prime target for spear phishing, a scam in which attackers send a targeted email pretending to represent a reliable organisation to deceive the recipient into depositing money into a fake account (NCSC, 2022). To gain an unfair advantage, criminals also target valuable information such as bidding and building design information (Watson, 2018; Pash, 2018; Rogers, 2022). Cybercriminals also look for sensitive employee data such as bank account numbers, social security numbers and payroll information to commit identity theft or create realistic authentic-looking emails for phishing attacks (NCSC, 2022). Data breaches, regulatory fines and business disruption can all result from inadequate cybersecurity (Lloyd, 2020).

The construction industry has several cybersecurity effectiveness frameworks, regulations and guidelines. Cybersecurity guidelines developed by regional and global organisations include the National Institute of Standards and Technology (NIST) framework for improving critical infrastructure cybersecurity (NIST, 2018), the European Union Network and Information Systems (NIS) Directive (European Parliament, 2016), the Code of Practice for Cyber Security in the Built Environment by the Institution of Engineering and Technology (IET, 2014) and ISO 19650–5:2020 (ISO, 2020) by the International Organization

for Standardization (ISO). However, as detailed in Table 1, these guidelines may have limitations in assisting a company in determining its internal organisational capability for protecting its technology. For instance, Turk *et al.* (2022a) highlighted the restricted focus of NIST, the high-level requirements of NIS and IET's poorly defined attributes and lack of internal logic and construction peculiarities. Finally, the ISO 19650–5:2020 regulation is seen to be limited to information management within the built environment and does not provide comprehensive guidance on cybersecurity (Turk *et al.*, 2022a). In addition, most of these guidelines are geared toward cybersecurity risk management (Turk *et al.*, 2022a), making them unsuitable for assessing a company's overall cybersecurity effectiveness across the

Policy/Standard	Location	Description	Potential limitations
NIST framework for improving critical infrastructure cybersecurity - National Institute of Standards and Technology (NIST) (NIST, 2018)	United States	The NIST framework for improving critical infrastructure cybersecurity (NIST, 2018) is a set of guidelines developed by the National Institute of Standards and Technology to help organisations improve their cybersecurity posture. The framework is designed to be flexible, scalable, and adaptable to different types of organisations and industries, and consists of five core functions: identify, protect, detect, respond, and recover (NIST, 2018)	The potential limitations of NIST include its focus on critical infrastructure, limited scope to operations, reliance on existing cybersecurity protocols, and inability to identify cybersecurity risks (Turk *et al.*, 2022a)
European Union Network and Information Systems (NIS) Directive (European Parliament, 2016)	European Union	The European Union Network and Information Systems (NIS) Directive (European Parliament, 2016) is a legislative act of the European Union that aims to increase the overall level of cybersecurity across the EU. The directive sets out requirements for the security of network and information systems used by operators of essential services and digital service providers, and establishes a cooperation framework between EU member states to ensure effective response to cybersecurity incidents. The directive also establishes national competent authorities and sets out penalties for non-compliance (European Parliament, 2016)	The limitations of NIS include, its focus on protecting critical and high-value asset. Another weakness is that the directive provides high-level requirements without specific guidance on how to implement them, which may lead to confusion and inconsistent implementation (Turk *et al.*, 2022a)

Table 1.
Several cybersecurity regulations and guidelines

(*continued*)

Policy/Standard	Location	Description	Potential limitations
The Code of Practice for Cyber Security in the Built Environment by the Institution of Engineering and Technology (IET, 2014)	United Kingdom	The Code of Practice for Cyber Security in the Built Environment (IET, 2014) is a set of guidelines developed by the Institution of Engineering and Technology (IET) to help those involved in the design, construction, and operation of buildings and infrastructure to improve cybersecurity. The code provides guidance on cybersecurity considerations throughout the entire lifecycle of a building or infrastructure project, from design to operation, and covers areas such as access control, network security, and incident response (IET, 2014)	The limitations of the IET include poorly defined attributes and elements, lack of internal logic, and a borrowed process from ISO that lacks construction peculiarities, leading to ambiguities and differences in understandings of risk and threat from construction risk management (Turk *et al.*, 2022a)
ISO 19650–5:2020 Organization and digitisation of information about buildings and civil engineering works - International Organization for Standardization (ISO) (ISO, 2020)	Worldwide	ISO 19650–5:2020 (ISO, 2020) is a standard that provides guidelines for managing information related to the built environment, with a specific focus on information security. The standard covers topics such as risk management, asset management, and access control, and is intended to be used by organisations involved in the design, construction, and operation of buildings and infrastructure	One weakness of ISO 19650–5:2020 is that it is focused on information management within the built environment and does not provide comprehensive guidance on cybersecurity (Turk *et al.*, 2022a)

Source(s): IET (2014), European Parliament (2016), NIST (2018), ISO (2020), Turk *et al.* (2022a)

Table 1.

levels of individual employees, strategy and operations. In summary, the limitations of these regulations highlight the need for organisations to supplement these regulations with other frameworks to ensure comprehensive cybersecurity measures.

Despite its increasing significance, the empirical study of cybersecurity effectiveness in construction firms is still in its early stages. Mantha and de Soto (2020) evaluated the cybersecurity of participants in a construction project network using a Common Vulnerability Scoring System. From a cybersecurity standpoint, Sonkor and García de Soto (2021) analysed the use of operational technology in the building industry. Turk *et al.* (2022a) have also created a cybersecurity framework for the construction industry that views the process from a holistic perspective. The framework highlights the four crucial elements – material, information, people and systems – that require protection to ensure cybersecurity. While several studies (Mantha and de Soto, 2020; Sonkor and Garcia de Soto, 2021; Turk *et al.*, 2022a) have focused on the project level, there is a paucity of research at the organisational level. However, studies at the organisational level is essential because, as noted by the Mantha and de Soto (2020) study, insider threats are the primary cause of cybersecurity

breaches in construction networks. An internal agent attack can occur when an employee blunders unintentionally, such as acquiring unauthorised data or misusing the system. Internal attacks can also involve agents discovering system weaknesses or vulnerabilities to expose flaws or cause intentional damage out of greed, betrayal, or other wicked motives (Prabhu and Thompson, 2022). Infamous internal agent attacks include the 2011 incident when a former employee at a water treatment facility in Australia sought to persuade his former employer to re-employ him after he had intentionally destroyed the facility's computer systems (Henrie, 2013). The young US soldier who leaked 750,000 classified documents to WikiLeaks in 2010 is also notoriously publicised (Roberts, 2012). Hence, a practical cybersecurity framework for construction firms must address issues within the boundaries of the construction organisation and their personnel, strategy and operations. However, very scarce research attention has hitherto been paid to the elements of internal organisational capability that influence a construction firm's cybersecurity. In view of this shortcoming, this research aims to assess the internal organisational capability elements that influence the cybersecurity effectiveness of a construction firm by posing two main research questions, which are:

RQ1. What are the essential elements of internal organisational capability that influence the cybersecurity effectiveness of a construction firm?

RQ2. Which elements are the most important for cybersecurity?

The study endeavored to answer these two questions by adopting an extended McKinsey 7S model; an organisational diagnosis and development model proposed by Waterman and Peters (1982). The McKinsey 7S model has been adapted to numerous settings and industries due to its usefulness in diagnosing firms of all sizes and its emphasis on interdependence. A recent literature review reveals that the 7S model has been used in several studies to investigate the security culture of businesses – see, for example, commercial banks (Chen and Liu, 2010) and airports (Gechkova and Kaleeva, 2020). However, a lack of studies systematically applies the 7S model to diagnose a construction organisation's cybersecurity capabilities. In addition, the study extends the McKinsey 7S model by arguing for the importance of two additional elements for the cybersecurity effectiveness of a construction firm: (1) third-party relationships and (2) regulatory compliance by the construction firm. Introducing these two elements brings to the fore interactions between the company and its environment, two critical internal capability elements not considered in the original McKinsey 7S model. First, because of the intricate relationships within the supply chain and the interconnectedness of construction projects, cybersecurity is critical when selecting third-party suppliers and contractors (Turk *et al.*, 2022a). Construction projects that use BIM, for example, have complex supply chain relationships, making cybersecurity a problem involving multiple companies and stakeholders (Parn and Edwards, 2019; Mutis and Paramashivam, 2019; Turk *et al.*, 2022b). Because these systems are linked, there may be flaws that attackers can exploit (Ghadiminia *et al.*, 2021; Turk *et al.*, 2022b). Cybercriminals have the ability to gain access to vital services and steal trade secrets, affecting not only the targeted company but also its customers and suppliers. The infamous incident at the Maroochy water treatment works in Australia exemplifies the difficulty of managing supply chain relationships: a former contractor gained unauthorised access to the plant controls, remotely changed valves and subsequently released a large amount of raw sewage into the surrounding area (Abrams and Weiss, 2008). As a result, evaluating how third-party relationships are managed can provide important insights into a construction firm's cybersecurity effectiveness (Karadsheh, 2012; Vitunskaite *et al.*, 2019). Furthermore, due to the numerous regulations and requirements relating to data privacy and security, construction firms must prioritise regulatory compliance, which should be evaluated as

part of overall cybersecurity effectiveness. Noncompliance with cybersecurity regulations can result in significant fines and reputational harm (ICO, 2022). For example, the UK Information Commissioner's Office (ICO) fined Interserve £4,4 million in 2022 for violating the General Data Protection Regulation (GDPR) by failing to prevent unauthorised access to its employees' information. Adherence to regulations, on the other hand, reduces the likelihood of data security lawsuits, lowers cyber risks and improves the efficiency of thwarting attacks (Kosseff, 2016, 2020; Shackelford, 2016).

This study contributes to the body of knowledge by assessing the effectiveness of cybersecurity in UK construction firms using the extended McKinsey 7S model. Unlike previous construction research that focused on the project-level (e.g. Mantha and de Soto, 2020; Sonkor and Garcia de Soto, 2021; Turk *et al.*, 2022a), this study considers the organisation-level of analysis and identifies the specific elements of internal organisational capability that are essential for effective cybersecurity in construction firms. The study highlights the importance of a comprehensive strategy for cybersecurity that includes both technical and non-technical factors and provides practical implications for construction companies and policymakers.

The paper begins by outlining the theoretical parameters of the study and then builds the conceptual model and hypotheses based on an extended version of the McKinsey 7S model. In the fourth section, we detail our quantitative method, including questionnaire design, data collection and analysis. The findings of our investigation are discussed in section five. The paper concludes by summarising the results and discussing implications and future research directions.

2. The McKinsey 7S model

The 7S model, created by Waterman and Peters for McKinsey, is a diagnostic tool that adopts a resource-based perspective to analyse the fundamental capabilities of a company (Waterman and Peters, 1982). Essentially, organisational diagnosis is the process of assessing an organisation's current state " i.e. health" to improve its effectiveness (Van Tonder and Dietrichsen, 2008). It involves gathering data, analyzing it and drawing conclusions to provide recommendations for improvement (Cummings and Worley, 2014). Emphasising the multidimensionality of an organisation, the McKinsey 7S model's purpose is to provide a concise overview of the seven primary elements that contribute to its success in achieving its strategic goals. The first three elements are typically considered "hard," more technical, tangible and measurable and thus easier for management to control: strategy, structure and systems. The other four elements are considered "soft" because they are primarily social, less observable and more challenging to exert direct control over; they are style (management style), staff, skills and shared values (culture). As depicted in Figure 1, the model emphasises the interdependence of the seven components to demonstrate how altering one component necessitates changing the others. The model avoids privileging one element over the others, even though shared values are typically placed at the centre of such representations. The model's strength lies in the importance it places on the congruence among the seven drivers of a firm's performance.

Practitioners continue to explore the McKinsey 7S model as a useful diagnostic model for analysing organisations, often during an organisational change (e.g. Singh, 2013; Hanafizadeh and Ravasan, 2011). The model enables the identification of optimal organisational design and managing the change processes by examining the seven elements and searching for misalignments. The McKinsey 7S model has also been widely used in several research contexts since its conception, including in the construction industry. For example, Naipinit *et al.* (2014) used the model to investigate the supply chain management practices of local small and medium-sized enterprises (SMEs) in the construction industry in

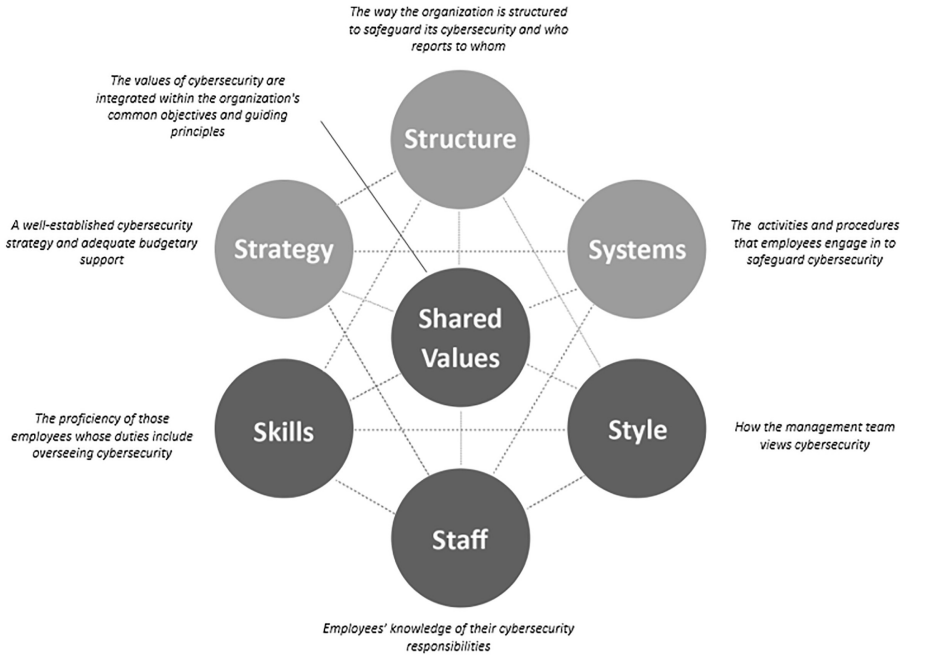


Figure 1.
Mckinsey 7S model

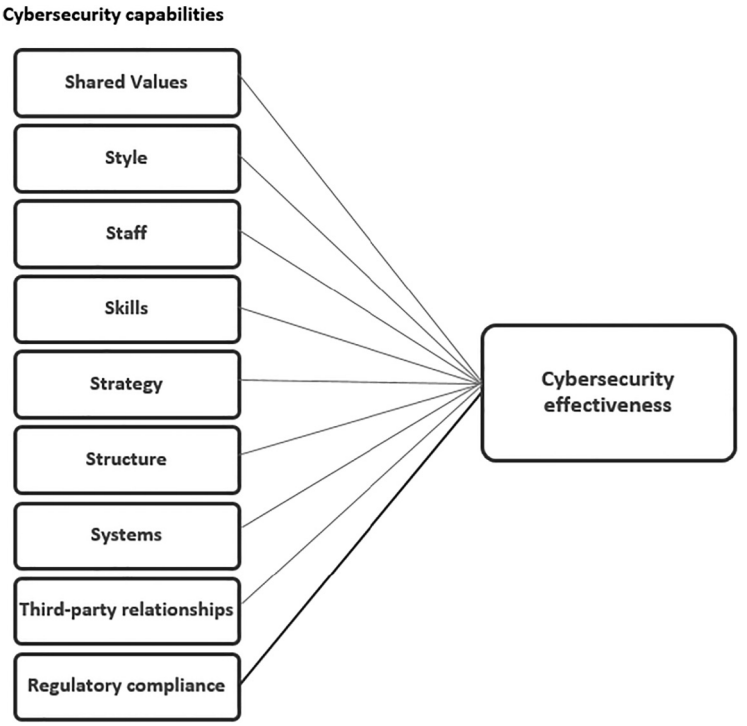
Source(s): Waterman and Peters, 1982 (updated by author to the context of cybersecurity)

Thailand and Rahmat and Ibrahim (2018) examined the factors that influence the successful integration of multiple organisations into a single project in Malaysia. Our study extends the 7S model by arguing for the importance of two additional factors not included in the original model to the cybersecurity effectiveness of a construction firm: third-party relationships and regulatory compliance, as will be elaborated upon in the next section.

3. Conceptual model and hypothesis development

This study developed a research model to examine the internal capability elements that influence a construction organisation's cybersecurity effectiveness based on an extended McKinsey 7S model and to underline which elements have the most significant relationships. It established a set of hypotheses postulating that all seven elements—shared values, strategy, structure, systems, staff, style and skills—affect an organisation's cybersecurity effectiveness. Additionally, third-party relationships and regulatory compliance were added as predictors in the model to extend the model as depicted in Figure 2.

The first element proposed to influence the cybersecurity effectiveness of a construction firm is the "shared values" among employees concerning cybersecurity. Employees' attitudes, beliefs, assumptions and knowledge substantially influence corporate cybersecurity (Da Veiga, 2016). According to Da Veiga (2016), a company's cybersecurity culture is determined by "how things are done when interacting in cyberspace" (p. 1008). A strong cybersecurity culture cultivates cybersecurity as a traditional organisational value and creates an overall environment with security-minded thinking (Knapp *et al.*, 2006). A company's employees must share a commitment to cybersecurity protection and common values. Shared cybersecurity values are essential because cybersecurity breaches may still



Source(s): Author's own creation

Figure 2.
Research model

occur despite implementing an effective cybersecurity strategy, organisational structure and systems (Park *et al.*, 2021). This is due to the possibility of inaccurate and skewed information spreading within the organisation without an organisational culture that values cybersecurity (Huang and Pearlson, 2019). In addition, without internal cooperation and information sharing, employees are more likely to intentionally or unintentionally compromise sensitive information (Argaw *et al.*, 2020). On the other hand, AlHogail (2015) argued that when a company's employees are committed to an information security culture and choose to collaborate, security breaches decrease. Internal information security cooperation increases employees' situational awareness (Argaw *et al.*, 2020) and reduces an organisation's cybersecurity investment (Alshaikh, 2020). As argued by Rajivan and Cooke (2017), teamwork improves an organisation's cybersecurity situational awareness, problem-solving and decision-making. Organisations with employees who value cybersecurity, share cybersecurity norms and engage in effective cybersecurity practices will demonstrate higher cybersecurity effectiveness than those with employees who do not (Knapp *et al.*, 2006). Hence, we advance the following hypothesis:

H1. The shared values element is significantly related to an organisation's cybersecurity effectiveness.

The management "style" of a construction firm's senior leaders is the second element influencing its cybersecurity effectiveness. Leaders are responsible for shaping the organisation's cybersecurity values and attitudes and bringing everyone in line with the

organisation's cybersecurity objectives (Huang and Pearlson, 2019). If a company's leadership is unconcerned about cybersecurity, it could result in a weak security management system and data breaches (Fitzgerald, 2018; Rothrock *et al.*, 2018). On the other hand, top management teams who express a desire to address cybersecurity issues openly and transparently have a significant influence on the effectiveness of cybersecurity (Kumar *et al.*, 2020; Shaikh and Siponen, 2023). A company's cyber defences may evolve depending on its senior management approach to cybersecurity (Ogbanufe *et al.*, 2021). A company that places a high priority on cybersecurity, with active promotion and consideration of cybersecurity during decision-making processes by the senior management team, will outperform a company that does not prioritise cybersecurity. Therefore, the following hypothesis is advanced:

H2. The style (management style) element is significantly related to an organisation's cybersecurity effectiveness.

The third element that may influence the cybersecurity of a construction firm is its "staff", defined as employees' knowledge of their responsibilities concerning cybersecurity. Despite implementing stringent regulations and a systematic strategy, an organisation's cybersecurity efforts may fail if its members are unwilling to cooperate (Daud *et al.*, 2018). Indeed, employee behaviour and skills are strong indicators of a company's security culture (Da Veiga, 2016). In order to ensure effective cybersecurity measures, it is crucial for employees to have a clear understanding of their specific roles and responsibilities related to cybersecurity (Yoon and Kim, 2013). This can be achieved through comprehensive cybersecurity training (He and Zhang, 2019) and strict adherence to all relevant regulations and policies governing cybersecurity (Li *et al.*, 2019). To ensure that a company can protect itself online and maintain good cybersecurity capabilities, it is important to evaluate how well employees adhere to cybersecurity values and codes of conduct during their daily work. This can be incorporated into employee performance evaluations, as suggested by Alshaikh (2020). Additionally, companies must enforce their cybersecurity policies by sanctioning employees who breach them, according to Knapp and Ferrante (2012). Overall, the attitudes of employees toward cybersecurity have a significant impact on a company's ability to maintain cybersecurity, making it critical to ensure that employees are aware of their responsibilities and follow relevant regulations and policies. Thus, the below hypothesis is postulated.

H3. The staff element is significantly related to an organisation's cybersecurity effectiveness.

The "skills" of employees responsible for overseeing cybersecurity is the fourth factor that impacts cybersecurity effectiveness. As argued by Colbert *et al.* (2016), it is essential for these employees to possess the necessary knowledge and skills to defend against cybersecurity attacks. Fisher *et al.* (2021) suggest that employees who have received adequate cybersecurity training and information can serve as the most effective defense against cyber threats. To encourage employees to take preventive and protective measures, practical cybersecurity training should focus on their risk perceptions, according to He and Zhang (2019). Prioritising cybersecurity skills can produce significantly different outcomes for a company's cybersecurity efforts compared to not prioritising them. Therefore, we propose the following hypothesis.

H4. The skills element is significantly related to an organisation's cybersecurity effectiveness.

The effectiveness of a construction firm's cybersecurity is influenced by various factors, including its "strategy", which is the plan or approach used to achieve cybersecurity goals. According to the 2022 Global Digital Trust Insight survey conducted by PWC, senior

management must articulate a clear security and privacy principle as a business imperative and align the cybersecurity strategy with the overall business strategy (PWC, 2022). Despite the apparent risks associated with cybersecurity breaches, many small and medium-sized construction businesses are reluctant to invest in cybersecurity, believing that they are not likely targets due to their size (NCSC, 2022). However, numerous research studies underscore the importance of having a well-designed cybersecurity strategy and sufficient funding to implement it (e.g. Densham, 2015; Soomro *et al.*, 2016; Sullivant, 2016; Rothrock *et al.*, 2018; Xu *et al.*, 2019; Park *et al.*, 2021). These measures can improve businesses' readiness for cybersecurity threats and enable them to respond effectively to any cyberattacks that may occur. Therefore, it is necessary to allocate a budget for cybersecurity to safeguard against cybersecurity breaches and investment allocation strategies and policies are essential to prioritise investments in cybersecurity. Thus, the hypothesis is proposed as follows.

H5. The strategy element is significantly related to an organisation's cybersecurity effectiveness.

An organisation's cybersecurity effectiveness depends largely on its "structure". Modenov and Vlasov (2018) suggest that an organisation's cybersecurity capabilities are influenced by its organisational structure and the existence of a division responsible for protecting technology. Even with a systematic cybersecurity strategy, it would be challenging to execute cybersecurity activities if there is no dedicated department to oversee and implement them. Offner *et al.* (2020) propose that firms should have a department with a manager to supervise cybersecurity operations and ensure that each member understands their roles and responsibilities. The organisation's structure should also facilitate easy movement of information about cybersecurity in all directions, including upwards, downwards, laterally and diagonally, as recommended by Johnson *et al.* (2016). Therefore, we hypothesise the following.

H6. The structure element is significantly related to an organisation's cybersecurity effectiveness.

The seventh element that affects the cybersecurity effectiveness of a construction firm refers to the "systems" that ensure cybersecurity within the organisation. To enhance its cybersecurity, the organisation should implement cybersecurity control frameworks and security control policies, as suggested by Kohnke *et al.* (2016). Additionally, the organisation requires sufficient information and communication technology tools and software to support its cybersecurity efforts. Cybersecurity breaches should be treated seriously, and senior management must be promptly informed (Soomro *et al.*, 2016). Employees should have both formal and informal channels to report cybersecurity incidents, and violations of cybersecurity should be viewed as opportunities for improvement (Ahmad *et al.*, 2012). Systems for capturing and sharing cybersecurity knowledge and learning, such as recording and assessing employee suggestions for enhancing cybersecurity, should also be in place (Zwilling *et al.*, 2022). Alahmari and Duncan (2020) emphasise that effective risk management and cybersecurity awareness among managers and employees are crucial. It is essential to educate staff about cybersecurity risks, involve them in risk management and ensure the implementation of cybersecurity strategies by both managers and staff (Alahmari and Duncan, 2020). Therefore, we propose the following hypothesis:

H7. The systems element is significantly related to an organisation's cybersecurity effectiveness.

The eighth element influencing a construction firm's cybersecurity effectiveness is its "relationships with third parties" such as contractors, subcontractors and consultants. Given the complex supply chain relationships and interconnectedness of construction projects through technologies such as BIM, cybersecurity is never a single firm's issue. For example, Ghadiminia *et al.* (2021) argue that when a building is modelled using BIM software, a digital "golden thread" of information is created, which intruders can use to compromise the building's security during its operational stages. Hence, cybersecurity concerns should be considered when selecting third-party suppliers and contractors (Turk *et al.*, 2022a). Organisations can strengthen their cybersecurity by including service-level agreements in their contracts with outside parties to ensure that all third-party vendors and service providers adhere to the same high levels of cybersecurity protection as the rest of the company (Karadsheh, 2012; Vitunskaite *et al.*, 2019). To strengthen a construction firm's cybersecurity effectiveness, it is important to coordinate with third-party vendors and service providers (Sarder and Haschak, 2019). It's also important to maintain open and honest communication regarding cybersecurity concerns (Pollini *et al.*, 2022). Therefore, the following hypothesis is advanced.

H8. The third-party relationships element is significantly related to an organisation's cybersecurity effectiveness.

Regulatory compliance is our model's ninth and final element that may influence a construction firm's cybersecurity effectiveness. In the UK construction industry, data privacy and security are regulated by several laws and regulations. The GDPR is a significant regulation for cybersecurity that came into effect in May 2018. The regulation was incorporated into UK law through the Data Protection Act 2018. The GDPR sets out the rules for how personal data must be collected, processed and stored and gives individuals greater control over their personal data. UK construction companies are required by law to report specific incidents (such as a data breach) to the ICO (NCSC, 2022). There is evidence that compliance with regulations reduces data security lawsuits (Kosseff, 2016), mitigates cyber risks (Shackelford, 2016) and increases the effectiveness of fighting attacks (Kosseff, 2020). Hence, we make the following final hypothesis.

H9. The regulatory compliance element is significantly related to an organisation's cybersecurity effectiveness.

4. Methods

4.1 Sampling and data collection

This study adopts a positivist and deductive epistemological approach (Turner, 1985; Halfpenny, 1982) to test the proposed linkages between an organisation's internal capabilities and cybersecurity effectiveness. A random sampling approach was adopted, and the demographic from which we drew our sample was made up of professionals working in the construction sector in the UK. In 2022, almost 2.1 million people were employed in the UK construction sector (Statista, 2022). A survey was developed using an online questionnaire administration platform (QuestionPro.com). The data were collected randomly from UK-based construction companies' employees with the help of a professional data collection company (cint.com) at a cost of $3 per completed questionnaire. In June 2022, the questionnaire was distributed to employees in waves of 1,000, resulting in a total of 2,000 surveys being sent out. Out of these, 414 responses were received, which accounts for approximately a 21% response rate. After initial examination, 47 responses were deleted due to the short duration of questionnaire completion (below five minutes) or/and missing data.

In total, 367 responses were deemed complete and useable for the analysis. As shown in Table 2, the sample demographics were fairly distributed in age, education level, years of experience, type of organisation and the number of employees.

4.2 Measurements

As shown in Appendix, the measurement items used to operationalise the research constructs were adapted from previous studies and tailored to the needs of this study. Respondents were asked to rate their level of agreement or disagreement with a series of statements on a 5-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree).

4.3 Data analysis

The IBM SPSS Statistics v.23 program was used to analyse the collected data and verify the study hypotheses.

4.3.1 Reliability and validity tests. The reliability of a construct is defined as the degree to which respondents' responses to one survey question are correlated with their responses to other questions in the same survey (Saunders *et al.*, 2016). On the other hand, construct validity refers to how well the survey questions measure the constructs and variables under investigation (Cooper and Schindler, 2013). We used Cronbach's alpha to assess the constructs' reliability, and the findings are shown in Table 3. Based on George and Mallery (2019), Cronbach's alpha thresholds, our results range between Acceptable and Excellent. The Kaiser–Meyer–Olkin (KMO) test (Kaiser, 1974) which assesses sample adequacy, and the Bartlett Test of Sphericity (Bartlett, 1954), which probes the existence of correlations, were also performed to learn more about the variables' reliability. Table 3 summarises the findings of these two tests, showing that the KMO tests yielded values more than 0.50 and closer to 1, indicating that the scales in question are reliable (Kaiser, 1974). Results from Bartlett's test of sphericity were 0.000, a significant value indicating that the scales are reliable (Hair *et al.*, 2010).

Exploratory factor analysis (EFA) (Fabrigar *et al.*, 1999; Costello and Osborne, 2005) and confirmatory factor analysis (CFA) (Brown, 2006; Kline, 2011) were used to examine the validity of the study constructs. The constructs for EFA were extracted using principal component analysis with the Varimax rotation approach. Overall, the EFA findings for all constructs were satisfactory and appropriate. Figure 3 is a scatter plot showing that ten latent variables in the study had Eigenvalues greater than 1, which aligns with the study's estimated number of constructs. In addition, all CFA indexes are within the range of acceptability: the ratio of the chi-square statistic (χ^2) to the degrees of freedom (df) in a model (χ^2/df) = 1.970 (Schreiber *et al.*, 2006), the Comparative Fit Index (CFI) = 0.908 (Byrne, 2016), the Incremental Fit Index (IFI) = 0.908 (Bentler, 2007), the Tucker-Lewis Index (TLI) = 0.900 (Marsh *et al.*, 2004), the Root Mean Square Error of Approximation (RMSEA) = 0.051 (Steiger, 2007). Figure 4 shows how CFA was used to confirm the factor structure of our observed data set.

Finally, a common method bias (CMB) analysis was performed to check for any potential bias in the data. CMB occurs in survey research when data are collected using the same method, which may lead to flawed conclusions about underlying links (Podsakoff and Organ, 1986). Using the Harman single-factor test for CMB, this investigation reveals that this component accounts for just 42.312% of the observed variation. This percentage is lower than the Podsakoff and Organ (1986) criterion of 50%. Hence the data are deemed bias-free. As a result of passing the tests above, the data may be trusted and used in further analyses.

4.3.2 Descriptive statistics. Table 4 summarises the sample mean, median, range, variance and standard deviation, as well as other descriptive statistics based on the responses provided by the participants.

Characteristics	Respondents (number)	Respondents (percentage of total)
Gender		
Female	145	39.5
Male	222	60.5
Age		
Less than 24	15	4.1
25–30	104	28.3
31–40	130	35.4
41–50	68	18.5
51 or above	50	13.6
Education		
High School	147	40.1
Bachelor	93	25.3
Diploma	65	17.7
Masters	48	13.1
Doctorate	14	3.8
Years of Experience		
Less than 1	8	2.2
2–5	42	11.4
6–10	90	24.5
11–15	89	24.3
15 +	138	37.6
Job Title		
Senior Management	68	18.5
Middle Management	132	36.0
Front Line	60	16.3
IT Department	27	7.4
Others	80	21.8
Size		
1–49	90	24.5
50–250	107	29.2
251–1,000	73	19.9
More than 1,000	97	26.4
Organisation Type		
Client/Owner/Developer	25	6.8
Architecture/Design Consultant	9	2.5
Management Consultant/Project Manager	25	6.8
Engineering Consultant	28	7.6
Quantity surveying	7	1.9
Legal Consultant	9	2.5
Main Contractor	70	19.1
Subcontractor	47	12.8
Supplier	33	9.0
Manufacturer	25	6.8
Facility Manager	7	1.9
Academic Institution	3	0.8
Government	7	1.9
Real estate	16	4.4
Other	56	15.3

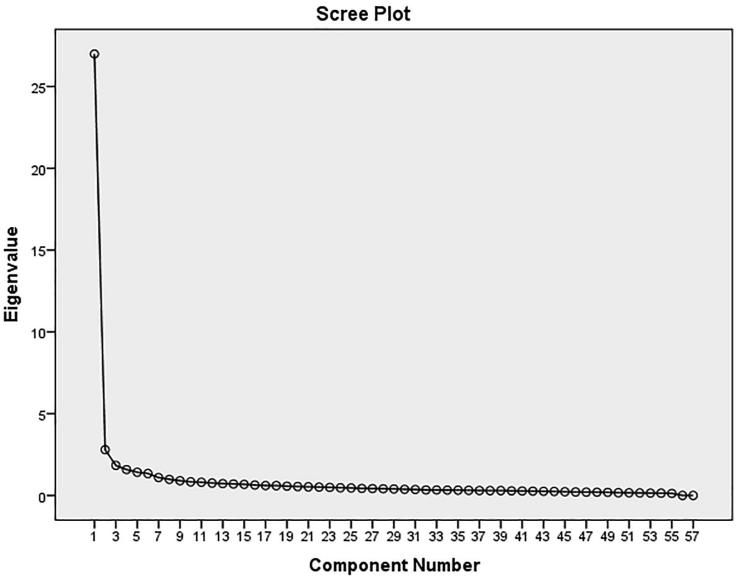
Source(s): Author's own creation

Table 2. Participants' demographics

The variables	Number of items	Cronbach's alpha	Kaiser–Meyer–Olkin (KMO)	Bartlett's test of sphericity
Shared values	6	0.876	0.877	0.000
Style	5	0.881	0.869	0.000
Skills	5	0.846	0.828	0.000
Staff	5	0.825	0.818	0.000
Strategy	5	0.883	0.868	0.000
Structure	4	0.851	0.810	0.000
Systems	12	0.936	0.952	0.000
Third-party relationships	5	0.896	0.888	0.000
Regulatory compliance	4	0.871	0.819	0.000
Cybersecurity effectiveness	4	0.744	0.760	0.000

Source(s): Author's own creation

Table 3.
Reliability and validity tests

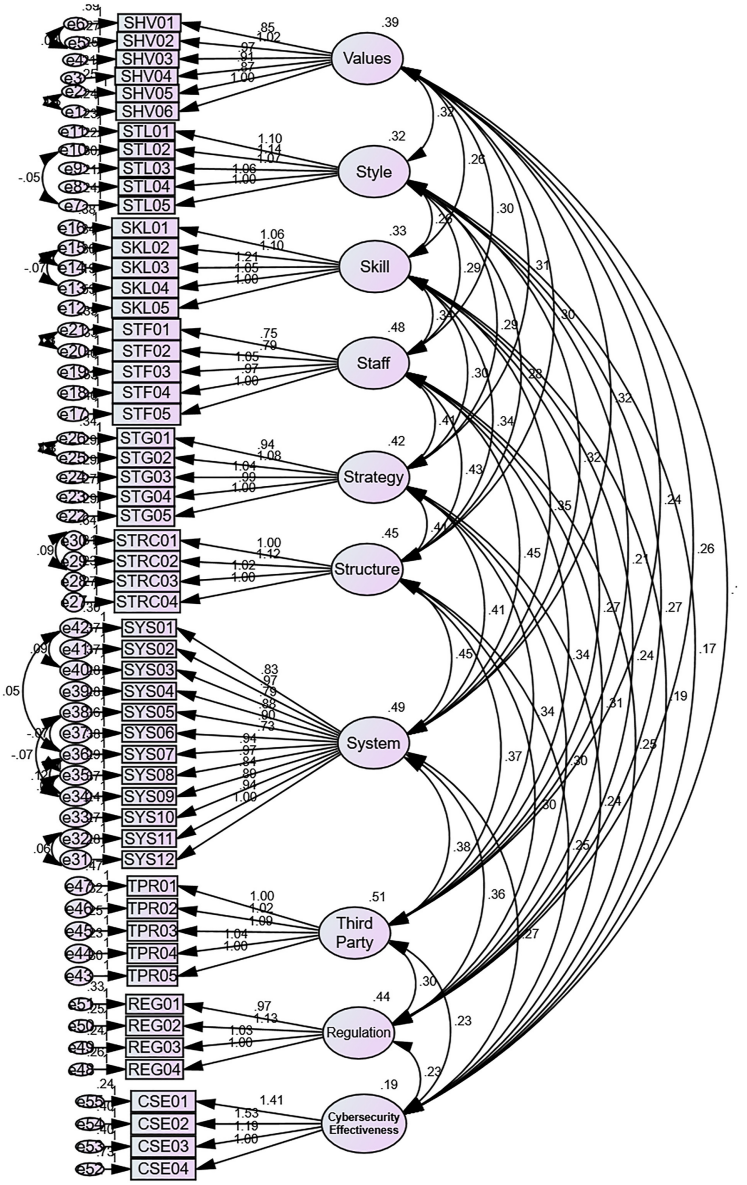


Source(s): Author's own creation

Figure 3.
EFA analysis

4.3.3 Correlation analysis. We conducted a series of correlation analyses between the variables included in the research to understand better their interrelationship (Pallant *et al.*, 2016). Table 5 displays the results of the correlation analysis, which demonstrate a medium to a high degree of correlation between all of the study constructs. The correlation coefficient's value and sign (+ or −) indicates a relationship's strength and direction.

4.3.4 Regression analysis. Multiple regression analysis was utilised to determine the statistical significance between the elements of the extended McKinsey model and



Source(s): Author's own creation

Figure 4.
CFA analysis

cybersecurity effectiveness. The present study employed the following equation to predict the cybersecurity effectiveness of organisations:

Table 4. Descriptive statistics

Construct name	Item number	Item questions	Participants' answers percentage Strongly disagree (%)	Disagree (%)	Neither (%)	Agree (%)	Strongly Agree (%)
Cybersecurity effectiveness	CSE1	My company protects its cyberspace well	0.3	3.3	19.6	51.2	25.6
	CSE2	My company is better at managing cybersecurity than are other companies	0.5	9.5	33.0	37.3	19.6
	CSE3	My company has fewer cybersecurity breaches/incidents compared to other companies	0	5.2	35.1	41.4	18.3
	CSE4	My company never suffered major damage from cybersecurity breaches/incidents	1.1	9.3	23.7	41.1	24.8
Shared values	SHV1	My company has an organisational culture that promotes good cybersecurity practices	3	3	21.8	44.7	27.5
	SHV2	In my company, cybersecurity is traditionally considered an important organisational value	0.8	2.5	20.2	46.9	29.7
	SHV3	In my company, employees value the importance of Cybersecurity	0	3.3	20.2	48.2	28.3
	SHV4	In my company, practising good cybersecurity is the accepted way of doing business	0	1.9	17.2	52	28.9
	SHV5	In my company, the overall environment fosters cybersecurity-minded thinking	0	1.9	24.5	51	22.6
	SHV6	In my company, cybersecurity is a key norm shared by organisational members	0.3	2.7	24.8	47.4	24.8
Style	STL1	The senior management team at my company considers cybersecurity as an important organisational priority	0.5	1.6	16.3	44.4	37.1
	STL2	The senior management team at my company has a high level of interest in cybersecurity	0.3	2.5	19.6	45.2	32.4
	STL3	The senior management team at my company takes cybersecurity issues into account during decision-making processes	0.5	3.3	19.1	46.6	30.5
	STL4	The senior management team at my company actively supports cybersecurity	0.5	1.4	16.3	49.9	31.9
	STL5	The senior management team shows a desire to address cybersecurity issues openly and transparently	0	2.7	19.1	51.2	27

(*continued*)

Table 4.

Construct name	Item number	Item questions	Participants' answers percentage Strongly disagree (%)	Disagree (%)	Neither (%)	Agree (%)	Strongly Agree (%)
Skills	SKL1	At my company, employees responsible for cybersecurity have the competencies and expertise required for the cybersecurity job	0.8	6	23.4	47.1	22.6
	SKL2	At my company, employees responsible for cybersecurity have the relevant professional certifications	0	7.6	25.6	45.5	21.3
	SKL3	At my company, employees responsible for cybersecurity receive the relevant professional training	0.5	6.8	26.7	43.1	22.9
	SKL4	At my company, employees responsible for cybersecurity foster teamwork and an atmosphere of mutual trust regarding Cybersecurity	0	3	24	52.6	20.4
	SKL5	At my company, external cybersecurity specialist consultants are employed	0.5	9.8	25.1	42.2	22.3
Staff	STF1	Employees at my company understand their roles and responsibilities toward protecting their cybersecurity	0	4.4	21.8	51	22.9
	STF2	Employees at my company strictly adhere to the relevant regulations and policies to protect their cybersecurity	0.3	3.5	22.1	49.9	24.3
	STF3	Employees at my company receive cybersecurity training	1.9	10.4	23.4	40.6	23.7
	STF4	Employee performance appraisals at my company include how employees demonstrate the cybersecurity values and codes of conduct in their day to day work	2.5	12.3	29.7	38.1	17.4
	STF5	At my company, cybersecurity rules are enforced by sanctioning the employees who break them	1.1	12	25.9	40.3	20.7
Strategy	STG1	My company has a cybersecurity strategy	0.3	7.4	23.7	49	19.6
	STG2	For my company, cybersecurity is a strategic priority	0	7.9	25.1	43.1	24
	STG3	My company invest a sufficient budget in its Cybersecurity	0.3	7.9	25.6	46.9	19.3
	STG4	My company's cybersecurity strategy is periodically reassessed and re-aligned with cybersecurity events experienced in the company	0.5	5.2	25.9	48.2	20.2
	STG5	My company's cybersecurity strategy is periodically reassessed and re-aligned with emerging cybersecurity technologies and trends	0.8	6.3	22.1	51.2	19.6

(*continued*)

Table 4.

Construct name	Item number	Item questions	Participants' answers percentage Strongly disagree (%)	Disagree (%)	Neither (%)	Agree (%)	Strongly Agree (%)
Structure	STR1	My company has a division (or department or unit) responsible for its Cybersecurity	1.4	16.1	21.8	38.1	22.6
	STR2	At my company, the organisation structure facilitates the flow of information regarding cybersecurity upwards, downwards, and across organisational lines	1.1	8.7	28.3	40.3	21.5
	STR3	At my company, cybersecurity reporting relationships are appropriate	0.5	6.3	22.6	51.2	19.3
	STR4	At my company, cybersecurity responsibilities and accountabilities are clearly defined, communicated and understood	0.5	7.1	19.6	52	20.7
Systems	SYS1	My company has the relevant security control policies to support its Cybersecurity	0	4.1	22.9	47.7	25.3
	SYS2	My company has a response manual for the occurrence of cybersecurity breaches	1.4	7.6	23.4	46	21.5
	SYS3	My company has the relevant technologies (IT resources and software) to support its cybersecurity	0	4.6	17.7	46.6	31.1
	SYS4	The senior management team at my company receives sufficient and timely information about cybersecurity breaches and near-misses	0	5.7	23.2	49.6	21.5
	SYS5	At my company, informal and formal processes exist for employees to report cybersecurity breaches and near-misses	0	6.8	15.3	53.7	24.3
	SYS6	At my company, where cybersecurity breaches have arisen, these are taken seriously	0.3	2.2	16.9	45.5	35.1
	SYS7	At my company, there are mechanisms to capture and evaluate employee ideas on how to improve Cybersecurity	0.8	7.9	25.9	43.9	21.5
	SYS8	At my company, there are arrangements to ensure sharing of cybersecurity skills and knowledge	0.3	6.5	25.9	44.1	23.2
	SYS9	At my company, cybersecurity breaches are treated as an opportunity for improvement	0.8	5.4	25.6	47.7	20.4

(*continued*)

Table 4.

Construct name	Item number	Item questions	Participants' answers percentage Strongly disagree (%)	Disagree (%)	Neither (%)	Agree (%)	Strongly Agree (%)
	SYS10	At my company, managers and employees understand the risks they face in terms of cybersecurity	0	3.5	19.1	48.2	29.2
	SYS11	At my company, employees are encouraged to understand cybersecurity risks and be involved in the cybersecurity risk management process	0	5.4	24.3	45.8	24.5
	SYS12	At my company, the organisation's cybersecurity risk management strategy is understood and applied to objectives and decisions by managers and employees	0.8	6.3	23.4	46.3	23.2
Third-party relationships	TPR1	At my company, the appointment of third-party suppliers and contractors considers cybersecurity risks	1.9	12.3	30	37.1	18.8
	TPR2	My company uses service-level agreements in third-party contracts to protect its cybersecurity	1.4	9	24.3	45.8	19.6
	TPR3	My company contractually requires third-party suppliers and contractors to meet enterprise cybersecurity standards	0.8	9.3	27	41.7	21.3
	TPR4	My company works collaboratively with third-party suppliers and contractors to ensure cybersecurity	0.8	8.4	25.1	46.9	18.8
	TPR5	My company communicates openly and transparently with third-party suppliers and contractors about cybersecurity issues	1.4	6	26.7	43.6	22.3
Regulations	REG1	At my company, compliance with the government's cybersecurity laws and regulations is taken seriously	0.8	3	22.3	40.9	33
	REG2	My company works collaboratively with law enforcement to ensure cybersecurity	0.5	6	21.3	41.7	30.5
	REG3	My company communicates openly and transparently with law enforcement about cybersecurity issues	0.3	3	24.8	40.9	31.1
	REG4	Cyberattacks and cybersecurity breaches are communicated to the appropriate authority and responded to openly and effectively	0.5	3	21.5	43.6	31.3

Source(s): Author's own creation

	Mean	Std. Deviation	1	2	3	4	5	6	7	8	9
Shared values	3.984	0.6308	–								
Style	4.080	0.6471	0.778**	–							
Skills	3.825	0.6759	0.617**	0.685**	–						
Staff	3.768	0.7002	0.600**	0.625**	0.716**	–					
Strategy	3.811	0.7038	0.666**	0.688**	0.706**	0.769**	-				
Structure	3.762	0.7625	0.607**	0.644**	0.753**	0.751**	0.815**	-			
Systems	3.909	0.6440	0.660**	0.738**	0.795**	0.801**	0.823**	0.837**	-		
Third-party relationships	3.718	0.7782	0.480**	0.468**	0.598**	0.584**	0.635**	0.670**	0.685**	-	
Regulatory compliance	3.998	0.7301	0.561**	0.632**	0.565**	0.585**	0.604**	0.580**	0.705**	0.561**	
cybersecurity effectiveness	3.7916	0.6550	0.518**	0.549**	0.607**	0.662**	0.667**	0.674**	0.730**	0.598**	0.621**

Note(s): **. Correlation is significant at the 0.01 level (2-tailed)
*. Correlation is significant at the 0.05 level (2-tailed)
Source(s): Author's own creation

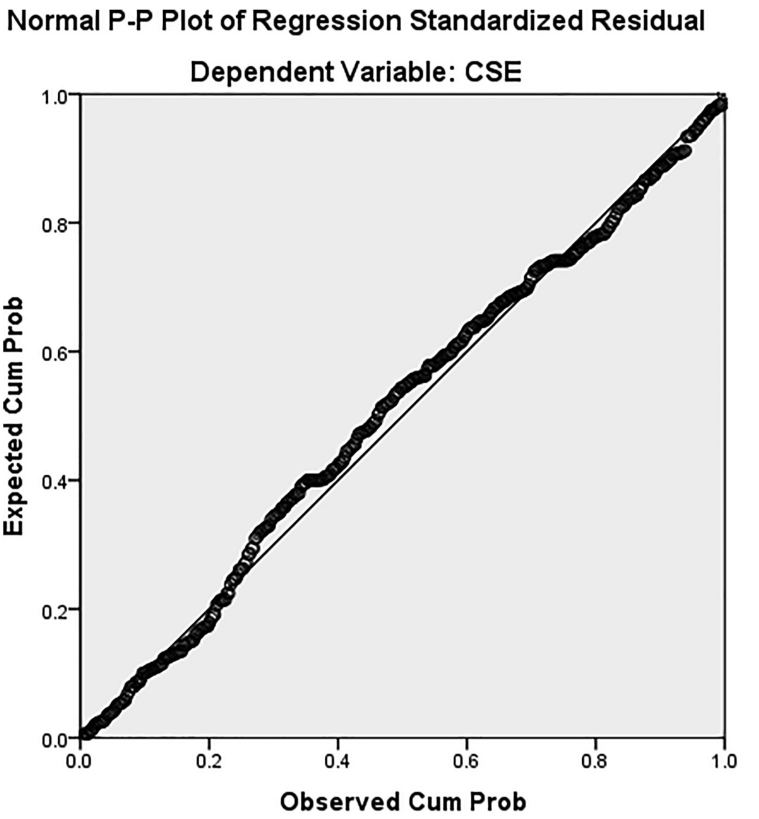
Table 5.
Correlation analysis

$$\begin{aligned} Cybersecurity\ Effectiveness\ = \beta 0\ + \beta 1\,(Shared\ values)\ + \beta 2\,(Style)\ + \beta 3\,(Skills) \\ + \beta 4\,(Staff)\ + \beta 5\,(Strategy) + \beta 6\,(Structure) \\ + \beta 7\,(Systems) + \beta 8\,(Third-Party\ Relationships) \\ + \beta 9\,(Regulatory\ Compliance)\ + \epsilon \end{aligned}$$

$\beta 0$ = constant termϵ = the model's error term (also known as the residuals)

Figure 5 shows that the results were normal when the normality assumption was applied to the dependent variable and the residuals plotted normally. The points in a normal plot of the residuals are near a diagonal line. Therefore, the residual normality is fulfilled. The model was then analysed by regression, with ANOVA results in Table 6 displaying the overall model significance. Table 7 lists the overall relationship significance of the variables.

First, we may infer no obvious multicollinearity issues in the model since none of the predictor variables has a variance inflation factor (VIF) larger than 10, as seen in Table 7.



Source(s): Author's own creation

Figure 5.
CSE normality test

In other words, the model does not include any variables that duplicate the functions of other variables. Second, the results underline two significant relations at a 95% confidence level between staff and third-party Relationships with cybersecurity effectiveness. In addition, two significant relations at a 99% confidence level are identified between Regulation and Systems with cybersecurity effectiveness. Hence, it can be concluded that the research results support H3, H7, H8 and H9. The findings, however, offer no support for H1, H2, H4, H5 and H6. Based on the regression analysis results the research purpose the following regression equation to evaluate the cybersecurity effectiveness of organisations:

$$\begin{aligned} \textit{Cybersecurity Effectiveness} &= (0.681) + (0.274)\,x\,(\textit{System}) \\ &\quad + (0.196)\,x\,(\textit{Regulatory Compliance}) + (0.148)\,x\,(\textit{Staff}) \\ &\quad + (0.110)\,x\,(\textit{Third} - \textit{party Relationships}) + \epsilon \end{aligned}$$

*ϵ = the model's error term (also known as the residuals)

Finally, the coefficient for System indicates the biggest contribution (0.274) out of the four constructs that showed a significant association with the organisation's cybersecurity performance (0.196 for Regulatory Compliance, 0.148 for staff and 0.110 for third-Party Relationship). The implications of these findings will be discussed in the next section.

ANOVA[a]

Model		Sum of squares	df	Mean square	F	Sig
1	Regression	92.425	9	10.269	56.727	0.000[b]
	Residual	64.629	357	0.181		
	Total	157.054	366			

Note(s): [a]Dependent Variable: CSE
[b]Predictors: (Constant), REG, SHV, TPR, STF, SKL, STG, STL, STRC and SYS
Source(s): Author's own creation

Table 6.
ANOVA results

Coefficients[a]

Model		Unstandardised coefficients		Standardised coefficients			Collinearity statistics	
		B	Std. Error	Beta	t	Sig	Tolerance	VIF
1	(Constant)	0.681	0.160		4.270	0.000		
	SHV	0.006	0.059	0.005	0.095	0.924	0.357	2.804
	STL	−0.051	0.065	−0.050	−0.778	0.437	0.278	3.603
	SKL	−0.005	0.059	−0.005	−0.080	0.936	0.312	3.207
	STF	0.139	0.057	0.148	2.416	0.016	0.306	3.271
	STG	0.076	0.065	0.081	1.159	0.247	0.235	4.264
	STRC	0.097	0.061	0.113	1.577	0.116	0.226	4.421
	SYS	0.278	0.089	0.274	3.121	0.002	0.150	6.669
	TPR	0.093	0.042	0.110	2.220	0.027	0.465	2.150
	REG	0.176	0.045	0.196	3.892	0.000	0.453	2.205

Note(s): [a]Dependent variable: CSE
Source(s): Author's own creation

Table 7.
Coefficients

5. Discussion of findings

To investigate the internal capability elements that influence a construction firm's cybersecurity effectiveness, this study utilised an extended McKinsey 7S model. By introducing the two elements of third-party relationships and regulatory compliance, the extended model brings to the fore interactions between the company and its environment, elements not considered in the original McKinsey 7S model.

Our first research question (RQ1) sought to determine the essential elements of internal organisational capability that influence the cybersecurity effectiveness of a construction firm. Multiple regression analysis revealed that a construction firm's cybersecurity effectiveness is primarily affected by four internal capability elements: systems, regulatory compliance, staff and third-party relationships, organised in order of influence. This finding emphasises the significance of a well-rounded cybersecurity approach that encompasses both technical and non-technical elements. By paying attention to these four key internal capability elements, construction firms can enhance their cybersecurity effectiveness and better protect themselves against cyber threats.

In addition, our second research question (RQ2) attempted to ascertain the elements which are most important for cybersecurity. According to our findings, systems were ranked as the most critical factor for managing cybersecurity in UK construction companies ($\beta = 0.274$, $t = 3.121$, $p < 0.01$). This suggests that cybersecurity is primarily managed by the firm's "hard" technological components, with most companies in our dataset relying on cybersecurity control frameworks, security control rules, practical information technology (IT) tools and software and cybersecurity risk management processes. Our findings are consistent with previous research, which has shown that adequate IT tools and software (Soomro *et al.*, 2016), formal and informal incident reporting channels (Ahmad *et al.*, 2012), knowledge management systems (Zwilling *et al.*, 2022) and risk management (Alahmari and Duncan, 2020) are critical for a firm's cybersecurity.

Second, our study findings suggest that regulatory compliance is the second key element to improve cybersecurity effectiveness in construction firms. Specifically, we found a significant positive relationship between regulatory compliance and cybersecurity effectiveness ($\beta = 0.196$, $t = 3.892$, $p < 0.01$). These findings offer empirical evidence in support of prior research that argues that regulatory compliance can reduce data security lawsuits, lower cyber risks and improve the efficiency of thwarting attacks (Kosseff, 2016, 2020; Shackelford, 2016). It's worth noting that some may argue that regulatory compliance is merely a box-ticking exercise that does not necessarily lead to improved cybersecurity outcomes (Marotta and Madnick, 2021). However, we believe that our findings provide compelling evidence to the contrary. Overall, our study highlights the value of extending the 7S model by adding regulatory compliance as a critical element for addressing cybersecurity in construction firms. Construction firms can improve their cybersecurity effectiveness and minimise the risk of cyber incidents by giving precedence to regulatory compliance.

Our study found that the staff element had the third most significant relationship with cybersecurity effectiveness ($\beta = 0.148$, $t = 2.416$, $p < 0.05$), suggesting the critical role that employees play in maintaining a company's cybersecurity posture. These findings align with earlier studies, which has shown that staff knowledge and cooperation are crucial for effective cybersecurity in firms (Daud *et al.*, 2018; Da Veiga, 2016; Yoon and Kim, 2013; He and Zhang, 2019; Li *et al.*, 2019; Alshaikh, 2020; Knapp and Ferrante, 2012). To improve cybersecurity in construction firms, it is important for employees to understand their role in cybersecurity initiatives, undergo cybersecurity training and follow all laws and corporate regulations to protect cybersecurity. By prioritising employee cybersecurity awareness and training, construction firms can enhance their cybersecurity effectiveness and reduce the risk of cyber incidents.

The final significant element for a construction firm's cybersecurity is its relationships with third-party entities ($\beta = 0.110$, $t = 2.220$, $p < 0.05$). Our study found that a construction firm's cybersecurity is significantly influenced by its relationship with contractors, subcontractors and suppliers. Given the interconnected structure of construction supply chains and building projects facilitated by BIM, no single construction company can be solely responsible for cybersecurity. Therefore, it is critical to consider cybersecurity when selecting vendors and service providers to ensure adequate protection. This finding concurs with previous research highlighting the importance of managing third-party relationships to address cybersecurity challenges (Karadsheh, 2012; Vitunskaite *et al.*, 2019; Ghadiminia *et al.*, 2021; Turk *et al.*, 2022a, 2022b). The findings suggest that construction firms can improve their cybersecurity effectiveness and mitigate the risk of cyber incidents by fostering collaboration with third-party subcontractors and suppliers and maintaining transparent and effective communication with them.

Finally, the study's findings indicate that several elements of the McKinsey 7S model, including strategy, structure, style, skills and shared values, did not show a statistically significant relationship with cybersecurity effectiveness in UK construction organisations. This may suggest that these elements are not as critical as other factors, such as effective cybersecurity systems, staff training and awareness, third-party relationships and regulatory compliance, which the study found to be essential for cybersecurity success in the construction sector. Particularly, the research findings suggest that cybersecurity is not a top priority for UK construction CEOs (Chief Executive Officers). The low importance of the Style element reflects the lack of leadership engagement and commitment to cybersecurity, which is a concerning issue given the growing threat landscape and the criticality of construction projects to the UK national infrastructure strategy (HM Treasury, 2020). This finding highlights the need for cybersecurity awareness and education among CEOs, board members and senior executives to understand the risks and impacts of cyber-attacks and to adopt a proactive approach to cybersecurity. Furthermore, the research findings indicate that UK construction firms lack a well-established cybersecurity strategy, adequate budgetary support and effective cybersecurity-protecting organisational structures. The insignificant effects of the strategy, structure and skills elements suggest that UK construction organisations are struggling to develop and implement a comprehensive and aligned cybersecurity strategy that addresses the current and emerging threats. Moreover, the low ranking of shared values indicates a lack of cybersecurity culture and awareness among employees of UK construction organisations. This finding highlights the need for cybersecurity training and education programs that aim to increase employees' awareness and understanding of cybersecurity threats and best practices. Additionally, creating a cybersecurity culture requires a strong commitment from leadership, effective communication and incentives to encourage employees to adopt secure behaviours. In general, the research findings suggest that UK construction firms are still in the early stages of developing comprehensive and aligned internal organisational capability to support their cybersecurity. Future research should focus on identifying the specific challenges and barriers that hinder the development of these capabilities and the strategies and interventions that could help overcome them. It is also worth noting that these findings may be specific to the UK construction industry and may not be generalisable to other sectors, emphasising the need for further research in different industries and geographical regions.

6. Conclusion

The empirical study of cybersecurity effectiveness in construction firms is still in its infancy, despite its growing importance. The objective of this research is to evaluate the essential elements of internal organisational capability that influence the effectiveness of

cybersecurity in construction firms. To achieve this goal, an extended McKinsey 7S model was implemented to explore the relationship between a construction firm's cybersecurity effectiveness and nine internal capability elements. These elements include shared values, strategy, structure, systems, staff, style, skills, relationships with third parties and regulatory compliance. The study utilised a quantitative research strategy and collected data via a cross-sectional survey of professionals working in the construction sector in the UK. The collected data was then analysed using descriptive and inferential statistical methods.

The study brings significant contributions to the field of cybersecurity in the construction industry. Unlike previous research that focused on project-level cybersecurity (e.g. Mantha and de Soto, 2020; Sonkor and Garcia de Soto, 2021; Turk *et al.*, 2022a), this study focuses on the organisation-level of analysis and empirically assesses the effectiveness of cybersecurity in UK construction firms using an extended McKinsey 7S model. The study expands on the McKinsey 7S model by emphasising the importance of two additional elements: third-party relationships and construction firm regulatory compliance. The addition of these two elements highlights interactions between the company and its environment, two critical internal capability elements that were overlooked in the original McKinsey 7S model. By utilising this model, which has not been used before in the context of construction cybersecurity, the study develops a concise yet thorough research model of essential elements of internal organisational capability that influence cybersecurity effectiveness in the construction industry. This model sheds light on how the nine components of the model, including strategy, structure, systems, style, staff, skills, shared values, third-party relationships and regulatory compliance influence the cybersecurity effectiveness in construction firms. Furthermore, by providing empirical data on the variables that impact cybersecurity effectiveness, the study's conclusions demonstrate that effective cybersecurity systems, staff training and awareness, third-party relationships and regulatory compliance are necessary for effective cybersecurity in the construction sector. These findings contribute significantly to the body of knowledge on cybersecurity effectiveness by identifying the essential elements for cybersecurity success in the construction industry.

The study's findings have important implications for practice. To enhance cybersecurity effectiveness, construction firms should use the extended McKinsey 7S model as a diagnostic tool to assess internal capabilities and evaluate implemented changes. Prioritising cybersecurity objectives based on systems, regulatory compliance, staff and third-party relationships can help firms allocate resources more effectively. The study emphasises the importance of educating top-level executives about cybersecurity risks and encouraging a proactive approach to cybersecurity. Implementing cybersecurity systems and training staff on hazard management, incident reporting and risk management are crucial. Firms should also invest in training and awareness programs for employees to adhere to cybersecurity regulations and engage with regulators, policy makers and industry associations to keep updated on evolving threats and best practices. Service-level agreements with third-party vendors can improve cybersecurity. Increasing leadership engagement, developing a comprehensive cybersecurity strategy, creating a cybersecurity culture, and collaborating with industry stakeholders can all contribute to a more resilient construction sector.

The work presented has limitations and provides opportunities for future research in various areas. The proposed diagnostic model can be used to assess cybersecurity effectiveness within a single construction firm and over time, as well as to contextualise specific types of cybersecurity innovation. Future studies can also extend the model by considering external factors that may impact an organisation's performance. The developed model is diagnostic and static, and future research could develop a dynamic cybersecurity effectiveness framework that identifies capability gaps, helps formulate plans for

improvement and oversees execution outcomes to ensure success. More research is needed to explore the relationship between regulatory compliance and cybersecurity effectiveness and specific methods for managing third-party relationships in improving cybersecurity. Additionally, further research could investigate the role of BIM in managing cybersecurity risks in construction supply chains and how different supply chain structures and practices impact cybersecurity outcomes.

References

Abrams, M. and Weiss, J. (2008), "Malicious control system cyber security attack case study-Maroochy Water services", Defense Technical Information Center, Fort Belvoir, VA, available at: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study\report.pdf

Ahmad, A., Hadgkiss, J. and Ruighaver, A.B. (2012), "Incident response teams–challenges in supporting the organisational security function", *Computers and Security*, Vol. 31 No. 5, pp. 643-652.

Alahmari, A. and Duncan, B. (2020), "Cybersecurity risk management in small and medium-sized enterprises: a systematic review of recent evidence", *2020 IEEE international conference on cyber situational awareness, data analytics and assessment (CyberSA)*, Dublin, 15-19 June 2020, pp. 1-5.

AlHogail, A. (2015), "Design and validation of information security culture framework", *Computers in Human Behavior*, Vol. 49, August 2015, pp. 567-575.

Alshaikh, M. (2020), "Developing cybersecurity culture to influence employee behavior: a practice perspective", *Computers and Security*, Vol. 98, 102003.

Alshammari, K., Beach, T. and Rezgui, Y. (2021), "Cybersecurity for digital twins in the built environment: current research and future directions", *Journal of Information Technology in Construction*, Vol. 26, pp. 159-173.

Amir, E., Levi, S. and Livne, T. (2018), "Do firms underreport information on cyber-attacks? Evidence from capital markets", *Review of Accounting Studies*, Vol. 23, pp. 1177-1206.

Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.V., Calcavecchia, F., Anderson, D. and Flahault, A. (2020), "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks", *BMC Medical Informatics and Decision Making*, Vol. 20 No. 1, pp. 1-10.

Bartlett, M.S. (1954), "A note on the multiplying factors for various chi-square approximations", *Journal of the Royal Statistical Society, Series B*, Vol. 16 No. 2, pp. 296-298.

Bentler, P.M. (2007), "On tests and indices for evaluating structural models", *Personality and Individual Differences*, Vol. 42 No. 5, pp. 825-829.

Brown, T.A. (2006), *Confirmatory Factor Analysis for Applied Research*, Guilford Press, New York.

Byrne, B., M. (2016), *Structural Equation Modeling with AMOS: Basic Concepts, Applications and Programming*, Lawrence Erlbaum Associates, NJ.

Chen, J.-X. and Liu (2010), "Research on operational risk management framework for commercial banks in Internet world-based on McKinsey 7S model", *Proceedings of the 2010 International Conference on Internet Technology and Applications*, Wuhan, China, 20-22 August 2010, pp. 1-6.

Colbert, A., Yee, N. and George, G. (2016), "The digital workforce and the workplace of the future", *Academy of Management Journal*, Vol. 59 No. 3, pp. 731-739.

Cooper, D.R. and Schindler, P.S. (2013), *Business Research Methods*, 11th ed., McGraw-Hill, New York.

Costello, A.B. and Osborne, J.W. (2005), "Best practices in exploratory factor analysis: four recommendations for getting the most from your analysis", *Practical Assessment, Research and Evaluation*, Vol. 10 No. 7, pp. 1-9.

Craigen, D., Diakun-Thibault, N. and Purse, R. (2014), "Defining cybersecurity", *Technology Innovation Management Review*, Vol. 4 No. 10, pp. 13-21.

Cummings, T.G. and Worley, C.G. (2014), *Organization Development & Change*, South Western Cengage Learning, Mason, OH.

Da Veiga, A. (2016), "A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument", *2016 SAI Computing Conference (SAI)*, London, 13-15 July 2016, IEEE, pp. 1006-1015.

Daud, M., Rasiah, R., George, M., Asirvatham, D. and Thangiah, G. (2018), "Bridging the gap between organisational practices and cyber security compliance: can cooperation promote compliance in organisations?", *International Journal of Business and Society*, Vol. 19 No. 1, pp. 161-180.

Demirkesen, S. and Tezel, A. (2022), "Investigating major challenges for industry 4.0 adoption among construction companies", *Engineering, Construction and Architectural Management*, Vol. 29 No. 3, pp. 1470-1503.

Densham, B. (2015), "Three cyber-security strategies to mitigate the impact of a data breach", *Network Security*, Vol. 2015 No. 1, pp. 5-8.

European Parliament (2016), "Directive (EU) 2016/1148 of the European parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union", *European Union Law*, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016L1148

Fabrigar, L.R., Wegener, D.T., MacCallum, R.C. and Strahan, E.J. (1999), "Evaluating the use of exploratory factor analysis in psychological research", *Psychological Methods*, Vol. 4 No. 3, pp. 272-299.

Fisher, R., Porod, C. and Peterson, S. (2021), "Motivating employees and organisations to adopt a cybersecurity-focused culture", *Journal of Organizational Psychology*, Vol. 21 No. 1, pp. 114-131.

Fitzgerald, T. (2018), *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers*, Auerbach Publications, New York.

Forcael, E., Ferrari, I., Opazo-Vega, A. and Pulido-Arcas, J.A. (2020), "Construction 4.0: a literature review", *Sustainability*, Vol. 12 No. 22, p. 9755, doi: 10.3390/su12229755.

García de Soto, B., Agustí-Juan, I., Joss, S. and Hunhevicz, J. (2022), "Implications of construction 4.0 to the workforce and organizational structures", *International Journal of Construction Management*, Vol. 22 No. 2, pp. 205-217.

Gayne, D. (2022), "Half of built environment firms hit by ransomware in past two years, survey says", *Buildings*, available at: https://www.building.co.uk/news/half-of-built-environment-firms-hit-by-ransomware-in-past-two-years-survey-says/5117651.article

Gechkova, T. and Kaleeva, T. (2020), "The Mckinsey 7s model in the airport system protection", *Knowledge-International Journal*, Vol. 42 No. 5, pp. 843-848.

George, D. and Mallery, P. (2019), *IBM SPSS Statistics 26 Step by Step: A Simple Guide and Reference*, Routledge, London.

Ghadiminia, N., Mayouf, M., Cox, S. and Krasniewicz, J. (2021), "BIM-enabled facilities management (FM): a scrutiny of risks resulting from cyber attacks", *Journal of Facilities Management*, Vol. 20 No. 3, pp. 326-349.

Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (2010), *Multivariate Data Analysis*, Global edition, Pearson Education, Harlow.

Halfpenny, P. (1982), *Positivism and Sociology: Explaining Social Science*, Allen & Unwin, London.

Hanafizadeh, P. and Ravasan, A.Z. (2011), "A McKinsey 7S model-based framework for ERP readiness assessment", *International Journal of Enterprise Information Systems (IJEIS)*, Vol. 7 No. 4, pp. 23-63.

He, W. and Zhang, Z. (2019), "Enterprise cybersecurity training and awareness programs: recommendations for success", *Journal of Organizational Computing and Electronic Commerce*, Vol. 29 No. 4, pp. 249-257.

Henrie, M. (2013), "Cyber security risk management in the SCADA critical infrastructure environment", *Engineering Management Journal*, Vol. 25 No. 2, pp. 38-45.

Hiscox (2021), "Hiscox cyber readiness report 2021", Hiscox Group, available at: https://www.hiscoxgroup.com/sites/group/files/documents/2021-04/Hiscox%20Cyber%20Readiness%20Report%202021.pdf

HM Treasury (2020), "National infrastructure strategy", available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/938539/NIS_Report_Web_Accessible.pdf

Huang, K. and Pearlson, K. (2019), "For what technology can't fix: building a model of organisational cybersecurity culture", *Proceedings of the 52nd Hawaii International Conference on System Sciences*, Hawaii, January 8-11.

Information Commissioner's Office (ICO) (2022), "'Biggest cyber risk is complacency, not hackers' - UK Information Commissioner issues warning as construction company fined £4.4 million", available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/biggest-cyber-risk-is-complacency-not-hackers/

International Organization for Standardization (ISO) (2020), "ISO 19650-5:2020 Organisation and digitisation of information about buildings and civil engineering works, including building information modelling (BIM) — information management using building information modelling — Part 5. ISO Standard No. ISO 19650-5:2020", Geneva, available at: https://www.iso.org/standard/74206.html

Institution of Engineering and Technology (IET) (2014), "Code of practice for cyber security in the built environment", London, available at: https://electrical.theiet.org/media/2761/code-of-practice-cyber-security-in-the-built-environment-revised-second-edition.pdf

Johnson, C., Badger, L., Waltermire, D., Snyder, J. and Skorupka, C. (2016), "Guide to cyber threat information sharing", *NIST Special Publication*, Vol. 800 No. 150.

Kabanda, S., Tanner, M. and Kent, C. (2018), "Exploring SME cybersecurity practices in developing countries", *Journal of Organizational Computing and Electronic Commerce*, Vol. 28 No. 3, pp. 269-282.

Kaiser, H.F. (1974), "An index of factorial simplicity", *Psychometrika*, Vol. 39 No. 1, pp. 31-36.

Karadsheh, L. (2012), "Applying security policies and service level agreement to IaaS service model to enhance security and transition", *Computers and Security*, Vol. 31 No. 3, pp. 315-326.

Kejwang, B. (2022), "Effect of cybersecurity risk management practices on performance of insurance sector: a review of literature", *International Journal of Research in Business and Social Science (2147-4478)*, Vol. 11 No. 6, pp. 334-340.

Kelly, M. (2020), "Bouygues falls victim to cyber-attack", available at: https://www.constructionnews.co.uk/contractors/bouygues/bouygues-falls-victim-to-cyber-attack-06-02-2020/

Kline, R.B. (2011), *Principles and Practice of Structural Equation Modeling*, 3rd ed., Guilford Press, New York.

Knapp, K.J. and Ferrante, C.J. (2012), "Policy awareness, enforcement and maintenance: critical to information security effectiveness in organisations", *Journal of Management Policy and Practice*, Vol. 13 No. 5, pp. 66-80.

Knapp, K.J., Marshall, T.E., Kelly Rainer, R. and Nelson Ford, F. (2006), "Information security: management's effect on culture and policy", *Information Management and Computer Security*, Vol. 14 No. 1, pp. 24-36.

Kohnke, A., Shoemaker, D. and Sigler, K.E. (2016), *The Complete Guide to Cybersecurity Risks and Controls*, CRC Press, Boca Raton, FL.

Kosseff, J. (2016), "Positive cybersecurity law: creating a consistent and incentive-based system", *Chapman Law Review*, Vol. 19 No. 2, pp. 401-419.

Kosseff, J. (2020), "Hacking cybersecurity law", *University of Illinois Law Review*, Vol. 2020 No. 3, pp. 811-850.

Kumar, S., Biswas, B., Bhatia, M.S. and Dora, M. (2020), "Antecedents for enhanced level of cyber-security in organisations", *Journal of Enterprise Information Management*, Vol. 34 No. 6, pp. 1597-1629.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019), "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behaviour", *International Journal of Information Management*, Vol. 45 No. 2019, pp. 13-24.

Lloyd, G. (2020), "The business benefits of cyber security for SMEs", *Computer Fraud and Security*, Vol. 2020 No. 2, pp. 14-17.

Mantha, B.R. and de Soto, B.G. (2020), "Assessment of the cybersecurity vulnerability of construction networks", *Engineering, Construction and Architectural Management*, Vol. 28 No. 10, pp. 3078-3105.

Marotta, A. and Madnick, S. (2021), "Convergence and divergence of regulatory compliance and cybersecurity", *Issues in Information Systems*, Vol. 22 No. 1, pp. 10-50.

Marsh, H.W., Hau, K.T. and Wen, Z. (2004), "In search of golden rules: comment on hypothesis-testing approaches to setting cutoff values for fit indexes and dangers in overgeneralising Hu and Bentler's (1999) findings", *Structural Equation Modelling*, Vol. 11 No. 3, pp. 320-341.

Modenov, A.K. and Vlasov, M.P. (2018), "Organisational structure and economic security of an enterprise", *Revista Espacios*, Vol. 39 No. 39, p. 22.

Mutis, I. and Paramashivam, A. (2019), "Cybersecurity management framework for a cloud-based BIM model", *Advances in Informatics and Computing in Civil and Construction Engineering: Proceedings of the 35th CIB W78 2018 Conference: IT in Design, Construction, and Management*, Springer International Publishing, pp. 325-333.

Naipinit, T., Kojchavivong, S., Kowittayakorn, V. and Sakolnakorn, T.P.N. (2014), "McKinsey 7S model for supply chain management of local SMEs construction business in upper northeast region of Thailand", *Asian Social Science*, Vol. 10 No. 8, pp. 35-41.

National Cyber Security Centre (NCSC) (2022), "Cyber security for construction businesses", London, available at: https://www.ncsc.gov.uk/files/Construction_Guidance_English_Web_Version.pdf

National Institute of Standards and Technology (NIST) (2018), *Framework for Improving Critical Infrastructure Cybersecurity v1.1*, National Institute of Standards and Technology (NIST), Gaithersburg, MD.

Offner, K.L., Sitnikova, E., Joiner, K. and MacIntyre, C.R. (2020), "Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation", *Intelligence and National Security*, Vol. 35 No. 4, pp. 556-585.

Ogbanufe, O., Kim, D.J. and Jones, M.C. (2021), "Informing cybersecurity strategic commitment through top management perceptions: the role of institutional pressures", *Information and Management*, Vol. 58 No. 7, 103507.

Osunsanmi, T.O., Aigbavboa, C. and Oke, A. (2018), "Construction 4.0: the future of the construction industry in South Africa", *International Journal of Civil and Environmental Engineering*, Vol. 12 No. 3, pp. 206-212.

Osunsanmi, T.O., Aigbavboa, C.O., Emmanuel Oke, A. and Liphadzi, M. (2020), "Appraisal of stakeholders' willingness to adopt construction 4.0 technologies for construction projects", *Built Environment Project and Asset Management*, Vol. 10 No. 4, pp. 547-565.

Pallant, J.F., Haines, H.M., Green, P., Toohill, J., Gamble, J., Creedy, D.K. and Fenwick, J. (2016), "Assessment of the dimensionality of the Wijma delivery expectancy/experience questionnaire

using factor analysis and Rasch analysis", *BMC Pregnancy and Childbirth*, Vol. 16 No. 1, pp. 1-11.

Park, H., Yoo, Y. and Lee, H. (2021), "7S model for technology protection of organizations", *Sustainability*, Vol. 13 No. 13, p. 7020.

Parn, E.A. and Edwards, D. (2019), "Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence", *Engineering, Construction and Architectural Management*, Vol. 26 No. 2, pp. 245-266.

Pash, C. (2018), "How hackers and spies tried to steal the secrets of Australia's one-armed robot Bricklayer", *Business Insider*, available at: https://www.businessinsider.com.au/one-armedbricklaying-robot-security-secrets-2018-11

Patel, T. and Patel, V. (2020), "Data privacy in construction industry by privacy-preserving data mining (PPDM) approach", *Asian Journal of Civil Engineering*, Vol. 21 No. 3, pp. 505205-515225.

Podsakoff, P.M. and Organ, D.W. (1986), "Self-reports in organisational research: problems and prospects", *Journal of Management*, Vol. 12 No. 4, pp. 531-544.

Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F. and Guerri, D. (2022), "Leveraging human factors in cybersecurity: an integrated methodological approach", *Cognition, Technology and Work*, Vol. 24 No. 2, pp. 371-390.

Prabhu, S. and Thompson, N. (2022), "A primer on insider threats in cybersecurity", *Information Security Journal: A Global Perspective*, Vol. 31 No. 5, pp. 602-611.

PWC (2022), "2022 global digital trust insights: the C-Suite guide to simplifying for cyber readiness, today and tomorrow", PricewaterhouseCoopers (PWC), London, available at: https://www.pwc.com/us/en/assets/cyber-global-digital-trust-insights.pdf

Rahmat, A.B. and Ibrahim, C.K.I.C. (2018), "Improving multi-organisational team integration using organisational strategies", *Proceedings of the International Conference on Industrial Engineering and Operations Management*, Paris, July 26-27, 2018.

Rajivan, P. and Cooke, N. (2017), "Impact of team collaboration on cybersecurity situational awareness", *Theory and Models for Cyber Situation Awareness*, pp. 203-226.

Roberts, A. (2012), "WikiLeaks: the illusion of transparency", *International Review of Administrative Sciences*, Vol. 78 No. 1, pp. 116-133.

Rogers, D. (2022), "Caledonian hit by crippling cyber attack just days before it sank into administration", *Building*, available at: https://www.building.co.uk/news/caledonian-hit-by-crippling-cyber-attack-just-days-before-it-sank-into-administration/5117270.article

Rothrock, R.A., Kaplan, J. and Van Der Oord, F. (2018), "The board's role in managing cybersecurity risks", *MIT Sloan Management Review*, Vol. 59 No. 2, pp. 12-15.

Sarder, M.D. and Haschak, M. (2019), *Cyber Security and its Implication on Material Handling and Logistics*, College-Industry Council on Material Handling Education, Charlotte, NC.

Saunders, M., Lewis, P. and Thornhill, A. (2016), *Research Methods for Business Students*, 7th ed., Pearson Education, Abingdon.

Schreiber, J.B., Nora, A., Stage, F.K., Barlow, E.A. and King, J. (2006), "Reporting structural equation modeling and confirmatory factor analysis results: a review", *The Journal of Educational Research*, Vol. 99 No. 6, pp. 323-338.

Shackelford, S.J. (2016), "Protecting intellectual property and privacy in the digital age: the use of national cybersecurity strategies to mitigate cyber risk", *Chapman Law Review*, Vol. 19 No. 2, pp. 445-481.

Shaikh, F.A. and Siponen, M. (2023), "Information security risk assessments following cybersecurity breaches: the mediating role of top management attention to cybersecurity", *Computers and Security*, Vol. 124, 102974.

Singh, A. (2013), "A study of role of McKinsey's 7S framework in achieving organisational excellence", *Organization Development Journal*, Vol. 31 No. 3, pp. 39-50.

Sonkor, M.S. and García de Soto, B. (2021), "Operational technology on construction sites: a review from the cybersecurity perspective", *Journal of Construction Engineering and Management*, Vol. 147 No. 12, pp. 04021172-1-04021172-22.

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: a literature review", *International Journal of Information Management*, Vol. 36 No. 2, pp. 215-225.

Statista (2022), "Number of employees in the construction industry in the UK 2002-2022, by quarters", available at: https://www.statista.com/statistics/432509/number-employees-construction-industry-united-kingdom/

Steiger, J.H. (2007), "Understanding the limitations of global fit assessment in structural equation modeling", *Personality and Individual Differences*, Vol. 42 No. 5, pp. 893-898.

Sullivant, J. (2016), *Building a Corporate Culture of Security: Strategies for Strengthening Organisational Resiliency*, Butterworth-Heinemann, Oxford.

Turk, Ž., de Soto, B.G., Mantha, B.R., Maciel, A. and Georgescu, A. (2022a), "A systemic framework for addressing cybersecurity in construction", *Automation in Construction*, Vol. 133 No. 2022, 103988.

Turk, Ž., Sonkor, M.S. and Klinc, R. (2022b), "Cybersecurity assessment of BIM/CDE design environment using cyber assessment framework", *Journal of Civil Engineering and Management*, Vol. 28 No. 5, pp. 349-364.

Turner, J. (1985), "Defence of positivism", *Sociological Theory*, Vol. 3 No. 2, pp. 24-30.

Van Tonder, C. and Dietrichsen, P. (2008), "The art of diagnosis", in van Tonder, C.L. and Roodt, G. (Eds), *Organisation Development: Theory and Practice*, Van Schaik, Pretoria, pp. 133-166.

Vitunskaite, M., He, Y., Brandstetter, T. and Janicke, H. (2019), "Smart cities and cyber security: are we there yet? A comparative study on the role of standards, third party risk management and security ownership", *Computers and Security*, Vol. 83 June, pp. 313-331.

Waterman, R.H. and Peters, T.J. (1982), *In Search of Excellence: Lessons from America's Best-Run Companies*, Harper & Row, New York, p. 360.

Watson, S. (2018), "Cyber-security: what will it take for construction to act? Construction News", available at: https://www.constructionnews.co.uk/tech/cyber-security-what-will-it-take-forconstruction-to-act-22-01-2018/

Weinfass, I. (2020), "Cyber-attack: the tier ones targeted by hackers – and how to protect your firm", available at: https://www.constructionnews.co.uk/agenda/cyber-attack-how-hackers-are-trying-to-take-down-construction-and-how-to-stop-them-14-10-2020/

Xu, L., Li, Y. and Fu, J. (2019), "Cybersecurity investment allocation for a multi-branch firm: modeling and optimisation", *Mathematics*, Vol. 7 No. 7, p. 587.

Yoon, C. and Kim, H. (2013), "Understanding computer security behavioral intention in the workplace: an empirical study of Korean firms", *Information Technology and People*, Vol. 26 No. 4, pp. 401-419.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N. (2022), "Cyber security awareness, knowledge and behavior: a comparative study", *Journal of Computer Information Systems*, Vol. 62 No. 1, pp. 82-97.

Corresponding author
Sulafa Badi can be contacted at: sulafa.badi@buid.ac.ae

Appendix

Table A1. The measurement instrument

		Source
Shared values		
SHV1	My organisation has an organisational culture that promotes good Cybersecurity practices	Adapted from Knapp *et al.* (2006)
SHV2	In my organisation, cybersecurity is traditionally considered an important organisational value	
SHV3	In my organisation, employees value the importance of cybersecurity	
SHV4	In my organisation, practising good cybersecurity is the accepted way of doing business	
SHV5	In my organisation, the overall environment fosters Cybersecurity-minded thinking	
SHV6	In my organisation, cybersecurity is a key norm shared by organisational members	
Style		
STL1	The senior management team at my organisation considers cybersecurity as an important organisational priority	Adapted from Knapp *et al.* (2006), Park *et al.* (2021)
STL2	The senior management team at my organisation has a high level of interest in cybersecurity	
STL3	The senior management team at my organisation takes Cybersecurity issues into account during decision-making processes	
STL4	The senior management team at my organisation actively supports cybersecurity	
STL5	The senior management team shows a desire to address Cybersecurity issues openly and transparently	
Skills		
SKL1	At my organisation, employees responsible for cybersecurity have the competencies and expertise required for the Cybersecurity job	Adapted from Park *et al.* (2021)
SKL2	At my organisation, employees responsible for cybersecurity have the relevant professional certifications	
SKL3	At my organisation, employees responsible for cybersecurity receive the relevant professional training	
SKL4	At my organisation, employees responsible for Cybersecurity foster teamwork and an atmosphere of mutual trust regarding cybersecurity	
SKL5	At my organisation, external Cybersecurity specialist consultants are employed based on the business security needs	
Staff		
STF1	Employees at my organisation understand their roles and responsibilities toward protecting their cybersecurity	Adapted from Knapp *et al.* (2006), Park *et al.* (2021)
STF2	Employees at my organisation strictly adhere to the relevant regulations and policies to protect their cybersecurity	
STF3	Employees at my organisation receive Cybersecurity training	
STF4	Employee performance appraisals at my organisation include how employees demonstrate the Cybersecurity values and codes of conduct in their day to day work	
STF5	At my organisation, Cybersecurity rules are enforced by sanctioning the employees who break them	

(*continued*)

Table A1.

			Source
Strategy			
STG1	My organisation has a Cybersecurity strategy		Adapted from Park *et al.* (2021)
STG2	For my organisation, cybersecurity is a strategic priority		
STG3	My organisation invests a sufficient budget in its cybersecurity		
STG4	My organisation's Cybersecurity strategy is periodically reassessed and re-aligned with Cybersecurity events experienced in the organisation		
STG5	My organisation's Cybersecurity strategy is periodically reassessed and re-aligned with emerging Cybersecurity technologies and trends		
Structure			
STR1	My organisation has a division (or department or unit) responsible for its cybersecurity		Adapted from Park *et al.* (2021)
STR2	At my organisation, the organisation structure facilitates the flow of information regarding cybersecurity upwards, downwards, and across organisational lines		
STR3	At my organisation, Cybersecurity reporting relationships are appropriate		
STR4	At my organisation, Cybersecurity responsibilities and accountabilities are clearly defined, communicated and understood		
Systems			
SYS1	Cybersecurity control frameworks	My organisation has the relevant security control policies to support its cybersecurity	Adapted from Park *et al.* (2021)
SYS2		My organisation has a response manual for the occurrence of Cybersecurity breaches	
SYS3		My organisation has the relevant technologies (IT resources and software) to support its cybersecurity	
SYS4	Cybersecurity incident reporting	The senior management team at my organisation receives sufficient and timely information about Cybersecurity breaches and near-misses	
SYS5		At my organisation, informal and formal processes exist for employees to report Cybersecurity breaches and near-misses	
SYS6		At my organisation, where Cybersecurity breaches have arisen, these are taken seriously	
SYS7	Cybersecurity knowledge and learning	At my organisation, there are mechanisms to capture and evaluate employee ideas on how to improve cybersecurity	
SYS8		At my organisation, there are arrangements to ensure sharing of Cybersecurity skills and knowledge	
SYS9		At my organisation, Cybersecurity breaches are treated as an opportunity for improvement	

(*continued*)

			Source
SYS10	Cybersecurity risk management Practices	At my organisation, managers and employees understand the risks they face in terms of cybersecurity	
SYS11		At my organisation, employees are encouraged to understand Cybersecurity risks and be involved in the Cybersecurity risk management process	
SYS12		At my organisation, the organisation's Cybersecurity risk management strategy is understood and applied to objectives and decisions by managers and employees	
Third-party relationships			
TPR1	At my organisation, the appointment of third-party suppliers and contractors considers cybersecurity risks		Developed by authors
TPR2	My organisation uses service-level agreements in third-party contracts to protect its cybersecurity		
TPR3	My organisation contractually requires third-party suppliers and contractors to meet enterprise Cybersecurity standards		
TPR4	My organisation works collaboratively with third-party suppliers and contractors to ensure cybersecurity		
TPR5	My organisation communicates openly and transparently with third-party suppliers and contractors about cybersecurity issues		
Regulatory compliance			
REG1	At my organisation, compliance with the government's cybersecurity laws and regulations is taken seriously		Developed by authors
REG2	My organisation works collaboratively with law enforcement to ensure cybersecurity		
REG3	My organisation communicates openly and transparently with law enforcement about Cybersecurity issues		
REG4	Cyberattacks and Cybersecurity breaches are communicated to the appropriate authority and responded to openly and effectively		
Cybersecurity effectiveness			
CSE1	My organisation protects its cyberspace well		Adapted from Park *et al.* (2021)
CSE2	My organisation is better at managing cybersecurity than other companies		
CSE3	My organisation has fewer Cybersecurity breaches/incidents compared to other companies		
CSE4	My organisation never suffered major damage from Cybersecurity breaches/incidents		

Note(s): *Respondents were asked to rate the extent to which they agreed or disagreed with the statements. All responses were measured on a 5-point Likert scale in which 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree or Disagree, 4 = Agree and 5 = Strongly Agree

Table A1.