CHAPTER 9

Cybersecurity Considerations for Deep Renovation

Muammer Semih Sonkor and Borja García de Soto

Abstract Deep renovation efforts to improve the energy performance of buildings are of paramount importance for the overall energy reduction of nations. Like other construction projects, deep renovation ones are affected by the digital transformation of the construction industry. While this transformation involves the increasing utilisation of new technologies to optimise cost, time and quality at every stage, concerns emerge about how to maintain robust cybersecurity. This chapter summarises the cybersecurity research related to each deep renovation phase and provides an overview of relevant cybersecurity frameworks, standards, guidelines and codes of practice. The chapter also discusses the need for a contingency approach in deep renovation cybersecurity due to the varying requirements of each project and organisation.

M. S. Sonkor • B. García de Soto (✉)
S.M.A.R.T. Construction Research Group, Division of Engineering,
New York University Abu Dhabi (NYUAD), Abu Dhabi, United Arab Emirates
e-mail: semih.sonkor@nyu.edu; garcia.de.soto@nyu.edu

T. Lynn et al. (eds.), *Disrupting Buildings*, Palgrave Studies in Digital Business & Enabling Technologies,
https://doi.org/10.1007/978-3-031-32309-6_9

Keywords BIM • Construction 4.0 • Cybersecurity • Cyber-physical systems • Digitalisation • Information technology (IT) • Internet of Things (IoT) • Operational technology (OT)

9.1 Introduction

Sustainable development constitutes one of the highest priority topics on most national agendas, and energy efficiency has a critical role in achieving sustainability targets. Buildings consume a significant amount of energy (Lynn et al., 2021); therefore, reducing the energy consumption of existing buildings can help countries achieve these targets and enhance global energy efficiency. Shnapp et al. (2013, p. 19) define deep renovation as "a renovation that captures the full economic energy efficiency potential of improvement works, with a main focus on the building shell, of existing buildings that leads to a very high-energy performance"[1]. While widely referenced, it is important to note that there is no consensus on the definition of deep renovation and the associated minimum energy reduction required.

Deep renovation can be considered a specialised subcategory of construction. It thus passes through similar stages (e.g., design, construction/retrofitting, operation and maintenance (O&M) and end of life) as with other construction projects, even though its scope involves retrofitting existing buildings rather than building one from the ground up. Therefore, technological advances in the construction industry and the concerns related to these advances are also applicable to deep renovation projects. The digitalisation that the construction industry is going through, often referred to as Construction 4.0 (Klinc & Turk, 2019), affects the information generated and used and the physical tasks performed during the construction and O&M phases (Garcíade Soto et al., 2020). While this transformation improves the cost and time efficiency of processes and construction quality, it also leads to substantial cybersecurity concerns, as with other digitalised industries. The convergence of information technology (IT) and operational technology (OT) (Harp & Gregory-Brown, 2015) further exacerbates the difficulty and complexity of addressing such concerns. Furthermore, safety issues

[1] Chapter 1 in this book provides a more detailed discussion on the definition of deep renovation.

arise due to the increasing use of OT to perform (e.g., autonomous excavators to handle earthworks) and monitor (e.g., autonomous site monitoring devices) site activities (Sonkor & García de Soto, 2021). As a result, the significance of providing robust cybersecurity increases during all phases of construction projects to prevent the exposure of sensitive information and any potential physical damage.

The rest of this chapter is organised as follows. Next, we discuss major types of cybercrimes that affect the construction industry and the related laws and regulations. We then outline some prominent cybersecurity standards, codes of practice and frameworks applicable to the construction industry. Following a review of relevant cybersecurity research organised by the deep renovation phase, we explain the need for a contingency approach to cybersecurity in the construction industry that takes into account the differences in projects, organisations and contexts while highlighting that there cannot be a one-size-fits-all solution for all different sizes of companies and deep renovation projects.

9.2 Cybercrimes and Cybersecurity in Construction

Increased connectivity, remote working and the increasing sophistication of malicious actors are contributing to a rise in cybercrime (FireEye, 2021). The construction sector is not insulated from this trend. As more and more buildings become reliant on remotely operated software systems and the Internet of Things, the attack surface and associated vulnerabilities and risks increase. Construction companies and their employees, specific projects and building systems have been targeted by a wide range of cyberattacks, including phishing, ransomware, denial of service, identity theft and other types of unauthorised access (Nordlocker, 2021; Korman, 2020; Turton & Mehrotra, 2021; Rashid et al., 2019). While financial gain is a common motivation for such attacks, it is not always the case. For example, in 2016, hackers launched a distributed denial of service (DDoS) attack on two residential buildings in Finland by temporarily disabling the computer systems that controlled the heating and hot water distribution systems, resulting in obvious inconvenience and distress for residents (Ashok, 2016). Unsurprisingly, governments worldwide have responded to the threat of cyberattacks. These actions include enacting new laws focusing on cybercrimes and introducing acts and regulations that define criminal offences and the related sanctions. Notwithstanding this, few are

Table 9.1 Common types of cybercrimes, examples from the construction industry and related laws and regulations

Cybercrime	*Description*	*Examples*	*Related laws and regulations*
Phishing	Attempting to convince the victim to reveal sensitive information through e-mail or other means of communication using technical subterfuge and social engineering techniques (Dou et al., 2017)	Turner Construction (Jones, 2016); Central Concrete Supply Co. Inc. (Jones, 2016)	• EU Directive 2019/713 on combating fraud and counterfeiting of non-cash means of payment • 18 U.S. Code § 1343—Fraud by wire, radio or television • UK Fraud Act, 2006
Infection of IT systems with malware (including ransomware and viruses)	Using malicious software such as trojans, spyware, ransomware and botnet malware to perform malicious activities. These activities and their outcomes depend on the type of malware. For example, ransomware can encrypt data, and trojans can steal confidential information (Rashid et al., 2019)	Bouygues Construction (Korman, 2020); Bam Construct (Muncaster, 2020); Grey Energy (Cherepanov, 2018); E.R. Snell Contractor, Inc. (Equipment World, 2022)	• EU Directive 2013/40 on attacks against information systems • US Computer Fraud and Abuse Act (CFAA), 1986 • UK Computer Misuse Act, 1990
Hacking (unauthorised access)	The act of accessing a cyber system without having the right and authorisation (Rashid et al., 2019)	Colonial Pipeline (Turton & Mehrotra, 2021); Oregon Construction Contractors Board (CCB) security breach (Oregon CCB, 2019)	• EU Directive 2013/40 on attacks against information systems • CFAA, 1986 • 18 U.S. Code § 1030—Fraud and related activity in connection with computers • UK Computer Misuse Act, 1990
Denial-of-service attacks	Depleting a system's computing resources (e.g., CPU, memory) to cause unavailability and inaccessibility (Rashid et al., 2019)	Valtia attack (Ashok, 2016); Ukraine power grid attack (Slowik, 2019)	

(*continued*)

Table 9.1 (continued)

Cybercrime	*Description*	*Examples*	*Related laws and regulations*
Identity theft or identity fraud	Stealing an individual's or business's identity information to use it for deception or fraud, usually for financial gain (US DOJ, 2020)	CCB License Fraud (Oregon.gov, 2014); Contractor License Fraud in San Diego (FOX 5 San Diego, 2015); Konecranes (Reuters, 2015)	• EU Directive 2019/713 on combating fraud and counterfeiting of non-cash means of payment • US Identity Theft and Assumption Deterrence Act, 1998 • US Identity Theft Penalty Enhancement Act, 2004 • UK Fraud Act, 2006

specifically focused on the construction industry and buildings per se. Table 9.1 summarises common cybercrimes, examples from the construction industry and related laws and regulations.

9.3 International Standards, Best Practices and Cybersecurity Frameworks

In recent years, national and international institutions have been active in producing standards and guidelines to support companies in assessing their current cybersecurity levels and setting targets for the future. While the overwhelming majority are aimed at the IT sector or firms in general, there are several codes of practice and guidelines aimed at the architecture, engineering, construction and operations (AECO) sector specifically. As modern buildings make widespread use of automation and control systems, for example, for heating, and such systems have been the target

Table 9.2 Summary of the commonly used cybersecurity standards and procedures

Title	*Published by*	*Main purpose and applications*	*Target industry*	*Year*	*Source*
ISO 19650-5:2020—Information management using building information modelling—Part 5: Security-minded approach to information management	ISO	An international standard that introduces a security-minded approach for construction projects and built environments that utilises building information modelling (BIM) in their processes. It targets lowering the risk of loss or unauthorised alteration of sensitive information in built environments	AECO	2020	ISO (2020)
ISO/IEC 27001:2013—Information technology—Security techniques—Information security management systems—Requirements	ISO/IEC	A set of standards that guides companies in implementing and managing information security management systems (ISMS). It can be used either internally or by third parties to evaluate the company's capability to meet the information security requirements. It uses the "Plan-Do-Check-Act" model for structuring ISMS processes	All industries	2013	ISO/IEC (2013)
Service Organization Control (SOC) 2	AICPA	An auditing procedure that defines requirements for organisations to manage their customers' data securely. It is based on five trust principles: confidentiality, processing integrity, availability, security and privacy	All industries	2018	AICPA (2018)

(*continued*)

Table 9.2 (continued)

Title	*Published by*	*Main purpose and applications*	*Target industry*	*Year*	*Source*
ISA/IEC 62443—Security for Industrial Automation and Control Systems (IACSs)	ISA/IEC	A series of standards that provides guidelines to identify and mitigate cybersecurity vulnerabilities in IACSs. It applies to all industries and critical infrastructures (CIs)	Organisations that implement IACSs	2020[a]	ISA (2020)

[a]Indicates the last publication date of an ISA/IEC 62443 Series (in this case, Part 3-2: Security risk assessment for system design)

of cyberattacks, standards and guidelines for the security of such systems are also relevant. While some are industry-specific, others were designed in a generic way to cover a wide range of sectors. Some of the commonly used standards and procedures for cybersecurity are presented in Table 9.2.

In addition to standards and protocols for security and control systems, there are several codes of practice and guidelines. Some are general (for any industry), but others specifically address the construction sector. While codes of practice do not purport to replace standards, they provide guidance and support for achieving standards. Table 9.3 summarises some of the prominent codes of practice, guidelines and frameworks for cybersecurity.

9.4 Related Cybersecurity Research by Renovation Phase

To date, scholarly research has focused primarily on the advantages and potential benefits of increased digitalisation of the construction sector. In comparison, cybersecurity aspects have received less attention. There are notable exceptions. For example, Turk et al. (2022) proposed a systematic framework to address the cybersecurity problems specific to construction projects. Their framework identified cybersecurity as "the absence of the three wrongs across the four kinds of elements" (Turk et al., 2022, p. 1). The three wrongs refer to stealing, harming and lying. The four elements

Table 9.3 Summary of the commonly cite codes of practice, guidelines and frameworks for cybersecurity

Title	*Published by*	*Main purpose and applications*	*Target industry*	*Year*	*Source*
Cyber Security for Construction Businesses	The National Cyber Security Centre (NCSC)/ Chartered Institute of Building (CIOB)/UK Government	Provides cybersecurity guidance to small and medium-sized businesses in the construction industry and provides practical advice for each stage of construction. It helps business owners and managers understand why cybersecurity matters and advises staff responsible for IT equipment and services within construction companies on actions to take	AECO	2022	NCSC (2022)
Code of Practice: Cyber Security in the Built Environment—2nd Edition	The Institution of Engineering and Technology (IET)	Provides guidance to the stakeholders of built environments at every stage of the buildings, from planning to disposal. It identifies the different cybersecurity threats and requirements related to each phase	AECO	2021	IET (2021)

(*continued*)

Table 9.3 (continued)

Title	*Published by*	*Main purpose and applications*	*Target industry*	*Year*	*Source*
Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report	Department for Digital, Culture, Media & Sport/UK Government	A collection of guidelines on consumer Internet of Things (IoT) security that includes a code of practice and several other sections that discuss risks, opportunities and government actions. The code of practice, which is the central part of this report, involves thirteen suggestions prepared by experts to improve IoT cybersecurity	All sectors in the UK using IoT	2021	UK Government (2021)
Cyber Assessment Framework v3.0	NCSC	The framework has four objectives: protection against cyberattacks, management of cybersecurity risks, detection of cybersecurity incidents and minimising the impact of such incidents	All industries	2019	NCSC (2019)

(*continued*)

Table 9.3 (continued)

Title	*Published by*	*Main purpose and applications*	*Target industry*	*Year*	*Source*
Framework for Improving Critical Infrastructure Cybersecurity v1.1	NIST	Provides an extensive guideline for companies to develop their assessment structures using different reference documents (e.g., frameworks and standards)	CI operators; all organisations	2018	NIST (2018)
Network and Information Systems (NIS) Directive	EU	A legislative document that requires EU member states to have national cybersecurity strategies and encourages cooperation among the members to enhance the overall cybersecurity level within the Union	All sectors in the EU	2016	EU (2016)

that might be affected by such wrongful activities are material, information, person and system. After defining cybersecurity, they customised the framework to reflect construction-specific characteristics. These characteristics include the multi-stakeholder settings of projects, overlapping boundaries of different entities involved in different projects and having distinct stages (e.g., design, construction and O&M) with particular challenges.

Several studies in recent years have discussed various aspects of construction cybersecurity and suggested solutions across the construction and deep renovation life cycle. Zheng et al. (2019) stressed the lack of studies concerning the information security aspects of BIM during the design and planning phase. In order to improve confidentiality and reduce the risk of data breaches, a context-aware access control model named

CaACBIM was proposed. Mantha et al. (2021) pointed out that the sensor data collected during the commissioning phase can be altered by malicious actors (e.g., an owner with a malicious intention or a competitor). In order to address this threat, they proposed utilising an autonomous robotic system for randomised check-pointing and illustrated its feasibility with an example.

Modern construction and retrofitting make increasing use of (semi) autonomous and remote-controlled equipment (Sonkor & García de Soto, 2021). This includes the use of complex cyber-physical systems, such as industrial machinery and vehicles (e.g., cranes), exoskeletons, unmanned aerial vehicles (UAV),[2] on-site and off-site automated fabrication and additive manufacturing,[3] to name a few. Notwithstanding the pervasiveness of such equipment, a recent survey of cybersecurity research on such construction equipment by Sonkor and García de Soto (2021) revealed a paucity of studies.

Many of the construction cyberattacks identified in Table 9.1 occur in the O&M phase of construction projects, particularly in smart buildings. Pärn and Edwards (2019) presented the potential cybersecurity issues for CIs during the O&M phase and suggested using blockchain technology for data exchange and storage as a mitigation action. Several studies focused on the cybersecurity aspects of smart buildings. Wendzel et al. (2014) discussed botnets' abilities to control and monitor building automation systems (BASs) and their potential damage to the built environment. On a related topic, Mundt and Wickboldt (2016) undertook a study to identify the cyber risks, possible attackers and attack vectors related to BASs. They presented the security gaps found in two case studies to prove that additional attention is required to ensure robust BAS security. Mirsky et al. (2017) showed how air-gapped building management networks could be attacked using a compromised heating, ventilation and air conditioning (HVAC) system. Lastly, Wendzel et al. (2017) investigated the potential attacks against smart buildings and proposed solutions to protect them.

Interestingly, few studies explore the end-of-life phase of buildings and construction projects from a cybersecurity point of view. As building systems may retain sensitive data that can be exposed due to vulnerabilities, care needs to be taken to ensure suitable cybersecurity safeguards are in place.

[2] See Chap. 8 in this book for a more detailed discussion.
[3] See Chap. 7 in this book for a more detailed discussion.

While it is useful from a research perspective to use a phased approach to identify gaps in the literature, many actors and systems in the construction and renovation process are present across the entire life cycle, particularly as a consequence of digitisation. As such, full life-cycle approaches to cybersecurity assessment and associated research are needed. For example, Mantha and García de Soto (2019) investigated the vulnerability of different project participants and construction entities during the different phases of the life cycle of construction projects as a consequence of Construction 4.0. Their study considered potential risks and provided a basis for assessing the impact of interactions in a digital environment among different project participants. Considering the increasing use of IoT, edge computing and artificial intelligence (AI) and the likelihood that every stage of construction and deep renovation projects is expected to rely on these technologies in the near future, their cybersecurity vulnerabilities and risks require more attention (Ansari et al., 2020).

9.5 The Need for a Contingency Approach

The primary purpose of all the previously mentioned cybersecurity standards, frameworks, guidelines and academic studies is to improve the cybersecurity level of projects and organisations. However, considering the variety in functions, roles and scale differences in construction and deep renovation firms and projects, a one-size-fits-all cybersecurity approach may not be desirable or feasible. For example, public companies will have to meet specific accounting standards to ensure adequate controls are in place, and multinational firms may have to deal with a wide range of cybersecurity and data protection requirements. Similarly, specialist craft renovations are likely to have different cybersecurity requirements and demands than more generic and large-scale construction/renovation projects. Each stakeholder constitutes a different cyber risk, and each one has various cybersecurity concerns. Therefore, care needs to be taken to ensure that an appropriate cybersecurity assessment and associated controls are put in place that can accommodate the range of projects and firms that characterise the sector.

9.6 Conclusion

The integration of construction and digital technologies such as IoT, machine learning and cloud computing disrupts how construction projects are planned, constructed and operated, making the construction

industry and buildings easy targets. At the same time, the sophistication and volume of cyberattacks are increasing. As an inevitable consequence, maintaining robust cybersecurity becomes an everyday challenge. Deep renovation projects face the same hurdles as any other construction project when it comes to protecting sensitive information and maintaining safety. This chapter provides an overview of the cybersecurity efforts in the construction industry and deep renovation and presents relevant frameworks, standards, codes of practice and research. Furthermore, it discusses the need for a contingency approach while considering the cybersecurity requirements of deep renovation projects and the firms that deliver them. There is no silver bullet in cybersecurity. Cybersecurity considerations and related actions should be an indispensable part of deep renovation projects from planning to the end of life, taking into account the needs of all stakeholders.

Acknowledgements The authors would like to thank the Center for Cyber Security at New York University Abu Dhabi (CCS-NYUAD) for the support provided for this study.

References

AICPA. (2018). *SOC 2*. https://www.aicpa.org/cpe-learning/publication/soc-2-reporting-on-an-examination-of-controls-at-a-service-organization-relevant-to-security-availability-processing-integrity-confidentiality-or-privacy

Ansari, M. S., Alsamhi, S. H., Qiao, Y., Ye, Y., & Lee, B. (2020). Security of distributed intelligence in edge computing: Threats and countermeasures. In T. Lynn, J. G. Mooney, B. Lee, & P. T. Endo (Eds.), *The cloud-to-thing continuum* (pp. 95–122). Springer International Publishing. https://doi.org/10.1007/978-3-030-41110-7_6

Ashok, I. (2016). Hackers leave Finnish residents cold after DDoS attack knocks out heating systems. *Yahoo News*. https://sg.news.yahoo.com/hackers-leave-finnish-residents-cold-105147593.html

Cherepanov, A. (2018). *Greyenergy—A successor to Blackenergy*. ESET. https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf

García de Soto, B., Georgescu, A., Mantha, B. R. K., Turk, Ž., & Maciel, A. (2020). Construction cybersecurity and critical infrastructure protection: Significance, overlaps, and proposed action plan. *Preprints 2020*. https://doi.org/10.20944/preprints202005.0213.v1

Dou, Z., Khalil, I., Khreishah, A., Al-Fuqaha, A., & Guizani, M. (2017). Systematisation of Knowledge (SoK): A systematic review of software-based web phishing detection. *IEEE Communication Surveys and Tutorials, 19*(4). https://doi.org/10.1109/COMST.2017.2752087

Equipment World. (2022). Hacked: Construction contractor E.R. Snell shares how to bounce back from a cyberattack. *Equipment World*. https://www.equipmentworld.com/business/article/15290439/how-to-protect-your-construction-business-from-cyberattacks

EU. (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*. Official Journal of the European Union. http://data.europa.eu/eli/dir/2016/1148/oj

FireEye. (2021). *M-Trends 2021*. https://content.fireeye.com/m-trends/rpt-m-trends-2021

FOX 5 San Diego. (2015). Construction contractor accused of fraud, identity theft. *FOX 5 San Diego*. https://fox5sandiego.com/news/construction-contractor-accused-in-identify-theft-scam/

Harp, D. R., & Gregory-Brown, B. (2015). IT / OT convergence bridging the divide. *NexDefense*. https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf

IET. (2021). *Code of Practice: Cyber security in the built environment—2nd edition*. https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-in-the-built-environment-revised-second-edition/

ISA. (2020). *Quick Start Guide: An overview of ISA/IEC 62443 Standards*. Security of Industrial Automation and Control Systems, International Society of Automation (ISA), Global Cybersecurity Alliance. https://gca.isa.org/hubfs/ISAGCA Quick Start Guide FINAL.pdf

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*. https://www.iso.org/standard/74206.html

ISO/IEC. (2013). *ISO/IEC 27001:2013—Information technology—Security techniques -Information security management systems—Requirements*. https://www.iso.org/standard/54534.html

Jones, K. (2016). *Data breaches, cybersecurity, and the construction industry*. Construct Connect (Blog). https://www.constructconnect.com/blog/data-breaches-cyber-security-construction-industry

Klinc, R., & Turk, Ž. (2019). Construction 4.0—Digital transformation of one of the oldest industries. *Economic and Business Review, 21*(3), 393–410. https://doi.org/10.15458/ebr.92

Korman, R. (2020). *Bouygues construction unit gradually recovering after ransomware attack*. Engineering News-Record (ENR). https://www.enr.com/articles/48637-bouygues-construction-unit-gradually-recovering-after-ransomware-attack

Lynn, T., Rosati, P., Egli, A., Krinidis, S., Angelakoglou, K., Sougkakis, V., Tzovaras, D., Kassem, M., Greenwood, D., & Doukari, O. (2021). RINNO: Towards an open renovation platform for integrated design and delivery of deep renovation projects. *Sustainability, 13*(11). https://doi.org/10.3390/su13116018

Mantha, B. R. K., & García de Soto, B. (2019). Cyber security challenges and vulnerability assessment in the construction industry. *Creative Construction Conference*, 29–37. https://doi.org/10.3311/ccc2019-005

Mantha, B. R. K., García de Soto, B., & Karri, R. (2021). Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment. *Sustainable Cities and Society, 66*, 102682. https://doi.org/10.1016/j.scs.2020.102682

Mirsky, Y., Guri, M., & Elovici, Y. (2017). HVACKer: Bridging the air-gap by attacking the air conditioning system. *ArXiv.org*. https://doi.org/10.48550/ARXIV.1703.10454

Muncaster, P. (2020). COVID19 hospital construction firms hit by cyber-Attacks. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/covid19-hospital-construction/

Mundt, T., & Wickboldt, P. (2016). Security in building automation systems—A first analysis. *2016 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2016*. https://doi.org/10.1109/CyberSecPODS.2016.7502336

NCSC. (2019). *Cyber Assessment Framework v3.0*. https://www.ncsc.gov.uk/files/NCSC_CAF_v3.0.pdf

NCSC. (2022). *Cyber security for construction businesses*. NCSC. https://www.ncsc.gov.uk/guidance/cyber-security-for-construction-businesses

NIST. (2018). *Framework for improving critical infrastructure cybersecurity v1.1*. https://doi.org/10.6028/NIST.CSWP.04162018

Nordlocker. (2021). *Top industries hit by ransomware*. Nordlocker. https://nordlocker.com/recent-ransomware-attacks/

Oregon CCB. (2019). *Construction contractors board takes steps to stop data and security breach, inform contractors*. https://www.oregon.gov/CCB/Documents/pdf/JUSTICE-9596167-v1-CCB_-_Data_Disclosure_News_Release.pdf

Oregon.gov. (2014). *Con artist goes to prison for using stolen CCB license number*. Oregon.Gov. https://www.oregon.gov/CCB/news/Pages/stolenCCBlicensenumber.aspx

Pärn, E., & Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain

deterrence. *Engineering Construction and Architectural Management, 26*(2), 245–266. https://doi.org/10.1108/ECAM-03-2018-0101

Rashid, A., Chivers, H., Danezis, G., Lupu, E., & Martin, A. (2019). *The Cyber Security Body of Knowledge (CyBOK) v1.0.* University of Bristol. https://www.cybok.org/

Reuters. (2015). *Finland's Konecranes says subsidiary hit by fraud*. Reuters. https://www.reuters.com/article/konecranes-fraud-idUSFWN10P05K20150814

Shnapp, S., Sitjà, R., & Laustsen, J. (2013). *What is a deep renovation definition?* https://www.gbpn.org/wp-content/uploads/2021/06/08.DR_TechRep.low_pdf

Slowik, J. (2019). *Crashoverride: Reassessing the 2016 Ukraine electric power event as a protection-focused attack*. https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

Sonkor, M. S., & García de Soto, B. (2021). Operational technology on construction sites: A review from the cybersecurity perspective. *Journal of Construction Engineering and Management, 147*(12). https://doi.org/10.1061/(ASCE)CO.1943-7862.0002193

Turk, Ž., García de Soto, B., Mantha, B. R. K., Maciel, A., & Georgescu, A. (2022). A systemic framework for addressing cybersecurity in construction. *Automation in Construction, 133*(January), 103988. https://doi.org/10.1016/j.autcon.2021.103988

Turton, W., & Mehrotra, K. (2021). Hackers breached Colonial Pipeline using compromised password. *Bloomberg*. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

UK Government. (2021). *Secure by design*. UK Government. https://www.gov.uk/government/collections/secure-by-design

US DOJ. (2020). *Identity theft*. Justice.Gov. https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

Wendzel, S., Tonejc, J., Kaur, J., & Kobekova, A. (2017). Cyber security of smart buildings. In H. Song, G. A. Fink, & S. Jeschke (Eds.), *Security and privacy in cyber-physical systems: Foundations, principles, and applications*. John Wiley & Sons Ltd.

Wendzel, S., Zwanger, V., Meier, M., & Szlósarczyk, S. (2014). Envisioning smart building botnets. *Lecture Notes in Informatics (LNI), Proceedings—Series of the Gesellschaft Fur Informatik (GI), P-228* (pp. 319–329).

Zheng, R., Jiang, J., Hao, X., Ren, W., Xiong, F., & Zhu, T. (2019). CaACBIM: A context-aware access control model for BIM. *Information, 10*(2), 47. https://doi.org/10.3390/info10020047