Journal of Civil Engineering and Management
ISSN 1392-3730 / eISSN 1822-3605
2022 Volume 28 Issue 5: 349–364
https://doi.org/10.3846/jcem.2022.16682

CYBERSECURITY ASSESSMENT OF BIM/CDE DESIGN ENVIRONMENT USING CYBER ASSESSMENT FRAMEWORK

Žiga TURK [1*], Muammer Semih SONKOR [2], Robert KLINC [3]

[1, 3]Faculty of Civil and Geodetic Engineering, University of Ljubljana, Ljubljana, Slovenia
[2]S.M.A.R.T. Construction Research Group, Division of Engineering, New York University Abu Dhabi,
Abu Dhabi, United Arab Emirates

Received 22 September 2020, accepted 13 January 2022

Abstract. Digitalisation of the construction industry is exposing it to cybersecurity risks. All phases of construction can be affected. Particularly vulnerable are information-intensive phases such as building design and building operation. Construction is among the last industries that are discovering its cybersecurity risks and can rely on frameworks developed for other contexts. In this paper, we evaluate the cybersecurity risks of the design phase of construction using the Cyber Assessment Framework from the National Cybersecurity Centre (NCSC) of the UK. The goal of this study is twofold. First, to examine cybersecurity risks themselves, and second, to evaluate the applicability of the NCSC framework for construction to see if and how construction is specific. The analysis shows that the cybersecurity risks follow the information impact curve that has been motivating the introduction of Building Information Modelling (BIM). The framework is applicable but is weak in addressing the specifics of the construction industrial ecosystem, which involves a multitude of dynamically connected actors, their overlapping authorities, and conflicting motives. It is suggested that a specialized construction-related framework should be developed.

Keywords: construction, designing, cybersecurity, building information modelling, common data environment, integrated project delivery.

Introduction

The ground-breaking technologies of recent decades have accelerated digital transformation and automation in all industries, including Architecture, Engineering, Construction and Operations (AECO) industry. Key technology for the digitisation of the AECO industry is Building Information Modelling (BIM). It enables a more networked, collaborative, and efficient working environment for the design, construction and operation phases. BIM is often organised around a common data environment (CDE). This is a common repository for all information needed in the project. These advances in digitisation in the construction industry are leading to significant savings in time, cost and quality and support Integrated Project Delivery (IPD).

The collaborative character of BIM requires the use of digital networks to enable communication among the parties involved. Information and communication take place online, connected to public infrastructure. This brings with it the risk of being attacked by external and internal threat agents or of system failures (Nawari & Ravindran, 2019), resulting in a potential interruption of the workflow or disruption of the operation of assets, including but not limited to key infrastructures. Particular risk during the construction and operation phase is related to the Internet of Things technology (IoT) that connects the sensors and the actuators in the built environment to the internet and exposes them to cyberattacks (Humayed et al., 2017). Also, an unauthorised third party accessing the shared repository and BIM data could cause the loss or theft of confidential data (Boyes, 2013).

Cybersecurity aims to defend such systems to minimise the risk of security compromises by implementing technical measures and proposing operational procedures for users. Operational procedures also include non-technical measures such as training, fostering awareness of existing cyber threats, nurturing security culture and preventing risky behaviours in the workplace. To manage cybersecurity, international and national institutions have proposed dozens of security-related frameworks to assess the risks, structure the security planning, and organise the responses to the incidents. These frameworks and models help analyse systems – from a cybersecurity perspective – in an organised and structured way.

*Corresponding author. E-mail: *ziga.turk@fgg.uni-lj.si*

Problem statement

Design is that phase in which the most frequent and influential changes are made to construction information. In the BIM/CDE environment, sharing design documents with the required stakeholders is effortless compared to the conventional systems used in the construction industry, but it also brings additional concerns about data ownership, changes tracking, and unauthorised access to sensitive information. The use of different modelling software across disciplines, the involvement of many designers and other stakeholders, and frequent model changes during the design phase of BIM-enabled construction projects increase the complexity of information security. Especially for large and sensitive projects, good security can be a competitive advantage for design and construction companies and enable them to participate in the international construction market (British Standards Institution [BSI], 2015).

This research addresses the problem of cybersecurity during the design phase of construction projects. It investigates the possible use of existing cybersecurity frameworks for the analysis of security in construction projects. It reviews several international and national guidelines, frameworks and methodologies on information security published by various organisations worldwide. Eighty-six of them are listed in the ENISA's Cybersecurity Guidelines (Publications Office of the European Union, 2018). Although some of the documents listed in the ENISA guidelines are industry-specific, no framework addresses the specific cybersecurity issues that arise in construction projects. Nevertheless, the cybersecurity of a BIM/CDE ecosystem is analysed using one such framework.

Paper structure

This section introduced the topic and states the problem. Section 1 describes the elements of cyberspace in which the construction takes place. It discusses Building Information Modelling (BIM) and Common Data Environments (CDE) in the context of Integrated Project Delivery (IPD). Section 2 introduces the concept of cybersecurity. Ideas about cybersecurity are structured into security frameworks, which are reviewed and compared in Section 3. One such framework is then used in Section 4 to assess security issues in construction design environments. The final section discusses the results and concludes the paper.

1. Cyberspaces of AECO

The life cycle of a construction facility can be divided into three main phases: design, construction, and operation. All three phases are intensively digitised. During the design phase, the vast majority of information is created using computer tools and is available in a digital format. During the construction phase, this information is used to guide and control workers and machinery. In the cyber-physical paradigm of Construction 4.0 (Klinc & Turk, 2019), this machinery uses digital information increasingly autonomously – examples of this are robots and other intelligent devices. In the operating phase, buildings and other facilities are increasingly managed and controlled with electronic systems – for heating and cooling, lighting, access control. Sensors are used to monitor the structural and other performance of the building product.

In short, there are three quite different construction cyber-spaces. This paper deals with the first – the cyberspace of design. The overall goal is to use digital technology to achieve Integrated Project Delivery (IPD). Building Information Modelling is an approach that drives projects towards highly structured information. This and all other information are shared in what is now known as Common Data Environment (CDE). These three elements – IPD, BIM and CDE – are objects of interest for the cybersecurity assessment in Section 4.

1.1. Context – IPD

Integrated Project Delivery (IPD) is a concept that was created to minimise the inefficiency and waste of projects. The American Institute of Architects [AIA] defined IPD as "*a project delivery approach that integrates people, systems, business structures and practices into a process that collaboratively harnesses the talents and insights of all participants to optimise project results, increase value to the owner, reduce waste, and maximise efficiency through all phases of design, fabrication, and construction*" (AIA National, 2007). IPD aims to get the best out of resources (people, materials, systems) by structuring the organisation of the project innovatively.

Successful implementation of the IPD approach in a construction project depends mainly on the collaboration of the project participants (Abdirad & Pishdad-Bozorgi, 2014). Therefore, applying the IPD approach cannot lead directly to increased cooperation. However, the collaborative attitude of the project team supports the success of integrated delivery. Ma et al. (2018) argue that the bulk of IPD collaboration in a construction project takes place during the design phase, as all parties involved need to review and understand the design before construction begins. Also, countless design changes and optimisations increase the complexity of the collaboration (Ma et al., 2018). This argument justifies the explicit focus on the design phase in this research.

In the IPD method, there are three main parties in the project: owners, designers and engineers (AIA National, 2007). This approach requires a careful selection of project participants, as more information is exchanged in all project phases. A large amount of shared information increases confidentiality concerns. Especially in the design phase, where more frequent changes are made, aspects of cybersecurity become very important. One tool that makes the IPD process more robust and efficient is BIM (Ilozor & Kelly, 2012).

1.2. Information – BIM

BIM is an approach to creating, presenting, managing and sharing information that supports architects, engineers and designers in all phases of construction projects, including the design phase (Azhar, 2011). It is generally acknowledged that the benefits of BIM are particularly numerous in the design phase. BIM leads to cost and time savings. Software development companies have contributed greatly to the progress of the BIM-enabled design.

The benefits of BIM in terms of overall design efficiency and quality improvements are shown in Figure 1. It shows the benefits of collaboration in the earlier phases of the project. Collaborators have the opportunity to make better decisions that lead to cost efficiency (Construction Users Roundtable, 2004). On the other hand, Figure 1 also shows where the greatest impacts from cyber-attacks can be expected. These are the phases of most intensive information creation and exchange with the greatest potential impact on the end result.

The traditional challenge of BIM was interoperability (Turk, 2020). Open and international standards, such as IFC, are used to overcome interoperability problems when exchanging data (buildingSMART, n.d.) between different disciplines using various BIM authoring tools.

A recent challenge in the integration of BIM is cybersecurity (Boyes, 2014). The need for security measures is growing, especially as the number of people involved in a collaborative work environment increases (Parn & Edwards, 2019). PAS 1192-5:2015 (BSI, 2015) states: "*The employer or asset owner shall appreciate that in respect of a built asset, a holistic approach needs to address security around the aspects of people and process, as well as physical and technological security*". Data exchanged may be sensitive, either because of the nature of the information – it relates to commercial information, pricing or important negotiating positions – or because the project itself is sensitive- the construction of facilities such as banks, prisons, embassies, or army bases (Boyes, 2013). PAS 1192-5:2015 (BSI, 2015) also points out the need for additional security measures if a sensitive asset is being built near the construction site. Therefore, in cooperative working environments, security procedures are of utmost importance when handling sensitive information either about the project or about the companies involved.

1.3. Environment – cloud computing and CDE

A growing number of digital documents in the BIM workspace require a common repository to share information while avoiding duplication and preserving data ownership. The concept of Common Data Environment (CDE, see Figure 2) was born out of this need. PAS 1192-2:2013 (BSI, 2013) defines CDE as "*single source of information for any*

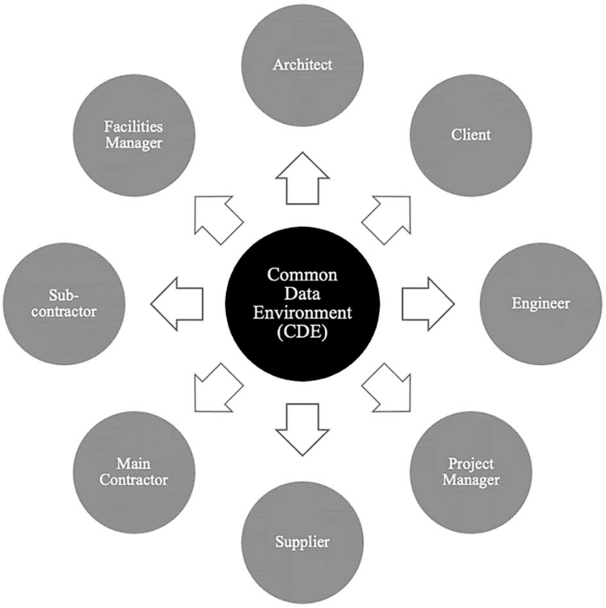

Figure 2. Common Data Environment (CDE)

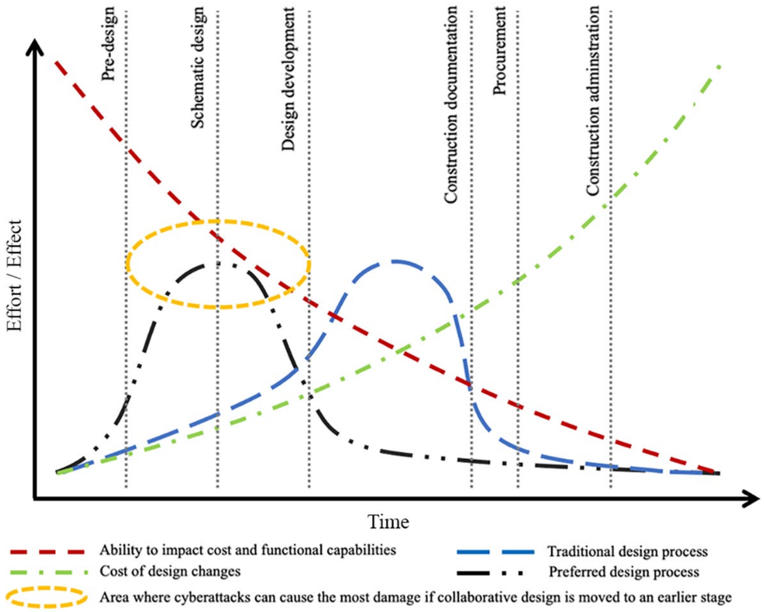

Figure 1. The benefits of BIM in terms of overall design efficiency and quality improvements

given project, used to collect, manage and disseminate all relevant approved project documents for multi-disciplinary teams in a managed process". This definition points out the importance of the CDE for collaboration in a multi-disciplinary working environment. It also shows that a single source of information is needed to manage all stakeholder input more efficiently.

The centralisation of data allows easy access but increases the potential impact of security breaches, which requires additional measures to be applied. According to PAS 1192-2:2013 (BSI, 2013), the originator of the information is the owner of the information. Maintaining the authenticity of the information as well as its integrity is essential to ensure a tamper-proof data flow.

CDE is technically supported by cloud computing architectures which are a security challenge in its own right. There are three models of services that the construction industry is getting from the cloud. Software as a Service (SaaS) means software packages, both complex engineering ones and simple general ones such as email, are run on the cloud. Increasingly construction collaboration is done on platforms (as a service – PaaS), such as Autodesk 360, where information and communication can be exposed. Finally, the infrastructure itself can be presented as a service (IaaS). This includes storage, networking and high performance computing can construction businesses may require. In all three cases, the communication with the service over the internet as well as the remote service itself can be subject to cyber-attacks.

CDEs are recently a particularly popular technology for design collaboration in construction that would be built on top of IaaS, offer or include PaaS and even link to SaaS. But most importantly, they host all the project information and offer an efficient way of exchanging data in BIM-enabled projects, accelerating its integration into the AECO industry (Mahamadu et al., 2013). On the other hand, the use of cloud computing requires the use of a sophisticated security framework that provides the main elements of information security, such as availability, confidentiality, integrity and authenticity of data (Mutis & Paramashivam, 2019).

Allowing different stakeholders to share a common data environment creates uncertainties and vulnerabilities (Eastman et al., 2008). According to Smith et al. (2007), the greatest threats resulting from possible data breaches are the loss of intellectual property and confidentiality, which could potentially lead to strategic actions by competitors. Secure collaboration is still new and only developing in the AECO industry (Mantha & de Soto, 2019).

Structured information using the BIM approach, shared in a CDE as part of an IPD process, are the key elements of the cyberspace that the AECO industry uses in the design phase.

2. Cybersecurity

The progress of information and communication technologies (ICT) in recent years is leading to a digital transformation in most sectors and life in general. However, it may not be possible to achieve the real potential of digitalisation without adequately addressing the challenges of cybersecurity (Thames & Schaefer, 2017).

This section introduces the concept of cybersecurity and explains the characteristics of secure systems. Security is compromised by different threat agents with different motives and using different types of attacks – these elements known from the literature are briefly listed. The process of ensuring cybersecurity, of which evaluation is the key element, is explained. Section 3 then presents some assessment frameworks, which are then used in Section 4 to evaluate AECO's design cyberspace.

2.1. Broader context

Many governments have begun to establish their cybersecurity agencies and centres. In 2004, the EU established The European Union Agency for Cybersecurity [ENISA]. They define cybersecurity as follows (ENISA, 2015): "*Cybersecurity shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace.*" In 2016, the United Kingdom founded National Cybersecurity Centre [NCSC]. They define: "*Cybersecurity is how individuals and organisations reduce the risk of cyber attacks*" (NCSC, n.d.). In 2018, the USA founded Cybersecurity and Infrastructure Security Agency [CISA]. They define cybersecurity as "*the art of protecting networks, devices, and data from unauthorised access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information*" (CISA, 2009).

One of the terms frequently mentioned in the definitions of cybersecurity is "cyber-environment" – sometimes also used as "cyberspace". It refers to the environment in which computer-based electronic devices communicate via interconnected network systems (Boyes, 2013). The cyberspace of construction design was described in Section 1.

2.2. Attributes of cybersecurity

Most definitions of both information security and cybersecurity include three main principles: confidentiality, integrity and availability – also known as the CIA triad (International Organization for Standardization [ISO], 2013). The scope and interpretation of these three principles vary according to industry needs, organisational requirements and applicable laws (Bishop, 2004). Over the years, security experts have developed novel and more comprehensive models by extending these three security principles. Parkerian Hexad (Parker, 2015) adds three more attributes to the CIA triad: possession/control, authenticity and utility. Boyes (2015) points out that two additional facets beyond Parkerian Hexad are required to address security issues in cyber-physical systems (CPS): safety and resilience.

These attributes are discussed in the paragraphs pairs below – the first paragraph of each, from a general perspective, and second, from the construction perspective.

Confidentiality means controlling access to information and preventing unauthorised access to data that could harm the organisation if disclosed (BSI, 2015; Thaseen et al., 2019). From the design perspective and BIM, an insufficient level of confidentiality could lead to (a) disclosure of commercial data, which could result in a disadvantageous position in a tender process; (b) compromising the facility's security information, which could lead to malicious parties breaking into the security system with less effort when the facility is in operation; (c) loss of intellectual property, which could contain valuable information about design calculations, construction techniques and specific know-how (Boyes, 2014).

Confidentiality can be ensured by encrypting data and restricting access to data storage repositories (Thaseen et al., 2019). It is also important to note that some of the data alone may not be sensitive or cause harm if compromised; however, the combination of this data with others may generate sensitive information (Boyes, 2014). Therefore, controlled access should be given to each team member according to their roles and responsibilities.

Integrity can be succinctly defined as preventing unauthorised changes to the information and maintaining consistency (BSI, 2015). Integrity is compromised when an authorised user or an unauthorised third party modifies or deletes some information. As a result, recipients think that the information is as it was created, which is misleading.

As a result, change tracking and configuration management are of paramount importance in BIM-enabled construction projects, where the number of users can rise to thousands. Besides, recovery measures against possible integrity compromises should be taken, such as regular backup procedures, which are already in place (Boyes, 2014).

Availability is the accessibility and usability of information, services and systems by authorised parties at all times (BSI, 2015; Glavach et al., 2017; Thaseen et al., 2019). Systems used for data sharing should have a sufficient level of resilience to achieve the desired availability (BSI, 2015). If a rival party can compromise the availability of information, this can give it a huge competitive advantage (Glavach et al., 2017).

From a BIM perspective, the following critical issues should be addressed, taking into account the importance of time during the design and construction phase: (a) if the project uses a cloud-based CDE, the risks of availability of this particular cloud service should be thoroughly understood; (b) compatibility between different BIM authoring software used by the design teams could be a question of availability during the project life cycle; (c) another concern could be compatibility between different versions of the same modelling software used in different phases of the project. Even if new versions of modelling software support files created with the old versions, there may be losses in embedded comments, diagrams and calculations, resulting in compromised integrity. We see here an overlap between what is seen as an interoperability issue and what are cybersecurity issues.

Possession/control from an information security perspective is defined by Parker (2015) as "*holding, controlling, and having the ability to use information*". It can be achieved by taking preventive measures (BSI, 2015).

From one CPS perspective, it can be seen as a loss of control over the implementation of changes or a loss of the ability to monitor operations (Boyes, 2015). While the loss of confidentiality is caused by the disclosure of confidential and classified information, the loss of possession can occur whether or not the information is confidential. Loss of possession/control can lead to loss of confidentiality, but they must be treated separately to identify protection measures for each individually (Parker, 2015).

Authenticity is the assurance of the authenticity of data and transactions (Thaseen et al., 2019). It is crucial to understand the difference between integrity and authenticity clearly. If there is a transaction between parties A and B, integrity means that there is no unauthorised change or modification of data during the transaction. On the other hand, authenticity means that the data received by B is indeed sent by its alleged sender A.

In ensuring the authenticity of the information during the design phase – which involves many subcontractors – due care is needed to avoid significant differences between the original design and the as-built asset (Boyes, 2015).

Utility can be defined briefly as the usefulness of the data (Parker, 2015).

From a construction perspective, it is about information remaining useful throughout the life cycle of an asset from design to maintenance (BSI, 2015). Considering that the entire life cycle of built assets is much longer than that of modelling software, the usefulness of BIM documents is a high priority (Boyes, 2015). Opening proprietary formats can be a problem, even after a decade of creating the file with earlier versions of modelling software. However, the corresponding data must remain useful during the long maintenance periods of built assets. Therefore, it is advisable to take the necessary measures in the design phase, such as the use of non-proprietary formats.

Safety is one of the attributes that Boyes (2015) has added to Parkerian Hexad to cover the security aspects of built assets comprehensively. Since the failure of CPS can lead to serious safety problems that may even result in physical injury or death, it is reasonable to include them in the safety aspects.

Resilience is the ability of a system to return to its normal state or recover immediately in the event of an adverse action (BSI, 2015). It is of utmost importance to be able to isolate the negatively affected parts of the system from the unaffected parts (Boyes, 2015). Besides, projects and organisations must understand what information is critical and sensitive so that resilience can be created from these points (Davis, 2015).

2.3. Cybersecurity process

The security process is shown in Figure 3. Threats exploit vulnerabilities and lead to exposures that pose risks. Risks can be mitigated by safeguards that protect assets. Assets are endangered by threats (Stewart et al., 2015). This cycle can be used to identify the relationship between risk elements and understand the process of risk mitigation.

Cybersecurity threats include denial of service (DoS) and distributed denial of service (DDoS), insider data theft, email-based fraud, social engineering, trojan attacks, code injection techniques, advanced persistent threats, zero-day attacks, and external software, including malware (Eastman et al., 2015; NCSC, 2016; Kabay, 2015). There are three elements of threats, namely agent, motive and results (Peltier, 2005).

Threat agents are the sources of attacks that intentionally or accidentally cause damage to systems (Humayed et al., 2017). Boyes (2014) divides threat agents into three main groups: external threat agents, internal threat agents, and system/business failures.

Malicious agents can be divided into three main categories according to their intentions (Falk, 2004). White hats are typically hired by organisations to assess the security level of the organisation. Black hats are those who break into systems without authorisation and tamper with the data. Grey hats are used to find security holes in systems without having authorised access. Parker (1998) developed a categorisation into seven groups: pranksters, hacksters, malicious hackers, personal problem solvers, career criminals, extreme advocates and malcontents, addicts and irrational individuals. In 2005 Marcus Rogers developed an eight-level taxonomy: novice, cyber-punks, internals, petty thieves, virus writers, old guard hackers, professional criminals, and information warriors (Rogers, 2005). Parn and Edwards (2019) distinguish between hacktivists, script kiddies, cyber-insiders, cyber-terrorists, malware authors, organised cyber-criminals, patriotic hackers and cyber militias.

According to NCSC (2016), the attack phases are as follows: survey, delivery, breach, and affect. The survey is the phase in which attackers collect information to uncover weaknesses in the target system. The delivery is the process of reaching the exploitation point. The breach is the phase in which a security system is bypassed by attackers. The affect phase includes all activities performed by attackers after the violation phase has occurred.

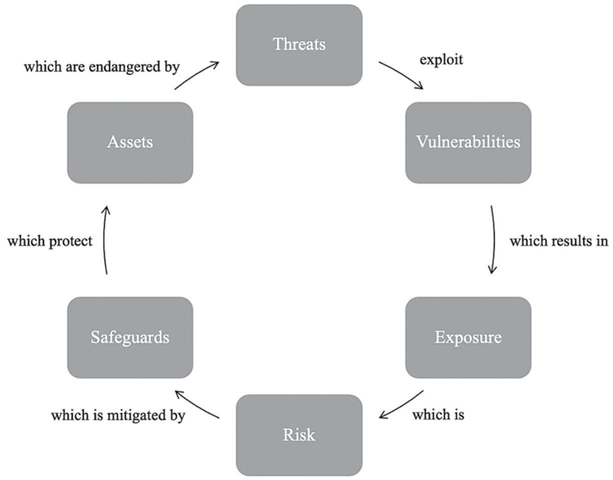

Figure 3. Security process

The effects of cyber-attacks include financial loss (e.g., recovery costs, inspection costs, mitigation costs, contract modification costs), loss or disclosure of the intellectual property or sensitive information (intellectual property for construction projects may include "*trade secrets*, *proprietary processes*, *technical specifications and detailed calculations or methods*" (BSI, 2015)), data corruption, disclosure of personal identity information, damage to reputation, and business interruption (Boyes, 2013).

3. Cybersecurity assessment frameworks

There are seven international and seventy-nine national documents on risk assessment/management (methods, standards, guidelines, frameworks and tools) published by various organisations around the world and listed in the guidelines developed by the European Union Agency for Cybersecurity (ENISA) (Publications Office of the European Union, 2018). While some of these standards, guidelines or frameworks are developed for all industries without having sector-specific aspects in mind, some are targeted at specific industries such as finance, energy or oil & gas. However, ENISA's guidelines do not include any cyber assessment framework that focuses on the risks to which one is exposed in construction projects.

As the use of BIM/CDE tools and procedures increases, the need for a tailored framework for cybersecurity risk assessment increases. As digital collaboration and information exchange reach their peak in the design phase, especially in design-build and IPD projects (Ma et al., 2018), a security-focused approach is of paramount importance. Therefore, this chapter focuses on selecting a generic cyber assessment framework so that it can later, in Section 4, be adapted to the design phase context in BIM-enabled construction projects.

Even though most of the available cybersecurity assessment frameworks use qualitative methods, there are also some quantitative ones. An example of quantitative methods is Factor Analysis of Information Risk (FAIR), explained in detail in Freund and Jones's (2014) book. They explain why a quantitative approach is necessary and present how to measure cybersecurity risks using the FAIR model. Another quantitative approach was proposed by Hubbard and Seiersen (2016). Their method aims to improve the existing scoring systems (i.e., Common Vulnerability Scoring System) and make them more measurable.

In this paper, the focus is on the qualitative frameworks since they are considered the initial step before going into a more detailed quantitative analysis. For this reason, four qualitative frameworks/standards were chosen to be reviewed in the following subsections; Framework for Improving Critical Infrastructure Cybersecurity v1.1 by National Institute of Standards and Technology [NIST] (2018), ISO/IEC 27005 (ISO, 2018), Global Technology

Audit Guide (GTAG), Assessing Cybersecurity Risk: Roles of the Three Lines of Defense (Ames et al., 2016), and Cyber Assessment Framework v3.0 by NCSC (NCSC, 2019).

3.1. NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1

The framework from the National Institute of Standards and Technology (NIST) is a comprehensive and advanced framework for reducing cybersecurity risks to critical infrastructures (CIs) (Barrett, 2018). It is developed based on other references such as frameworks, guidelines or specifications. The framework consists of three main components: Framework Core, Framework Implementation Tiers, and Framework Profile.

In the Framework Core, there are four sections: Functions (identify, protect, detect, respond, and recover), Categories, Subcategories and Informative References. The Informative References section includes documents from other organisations that explain how to achieve cybersecurity objectives. The Framework Implementation Tiers component provides an overview of how organisations view cybersecurity risks. On the other hand, the Framework Profile component helps organisations develop cybersecurity risk strategies that are aligned with their resources and business goals.

In summary, this framework by NIST does not include a checklist of questions for conducting a cyber assessment. Instead, it guides organisations in developing their cybersecurity strategies and provides references to find detailed information on each security aspect.

3.2. ISO/IEC 27005: Information technology – Security techniques – Information security risk management

ISO/IEC 27005 (ISO, 2018) is an international set of standards that contains guidelines for risk management in the area of information security. It was developed to be used by companies from all industries. It describes the process of information security risk management by defining all steps and the activities in each phase. Risk assessment is covered in three components: risk identification, risk analysis and risk evaluation. Risk handling follows the risk assessment process and consists of four options: risk modification, risk retention, risk avoidance and risk-sharing.

In summary, this standard by ISO and IEC describes how to develop risk management processes for information security and defines limits; however, it does not provide an assessment framework with a list of questions to be answered by organisations.

3.3. Global Technology Audit Guide (GTAG), Assessing Cybersecurity Risk: Roles of the Three Lines of Defense

The guide (Ames et al., 2016) from the Institute of Internal Auditors (IIA) addresses cybersecurity risks and threats for all types of organisations and provides an approach to conducting cybersecurity risk assessments. It highlights the importance of ensuring the robust operation of each of the three lines of defence separately. The first line of defence covers the management of risks, data, processes and controls; the second line of defence ensures the effectiveness of the first line of defence; the third line of defence assesses the effectiveness of the first and second lines of defence.

This guide presents a framework for risk assessment in the field of cybersecurity. The framework has six components: Cybersecurity Governance, Inventory of Information Assets, Standard Security Configurations, Information Access Management, Prompt Response and Remediation, and Ongoing Monitoring. Suggestions are made for each component of the framework rather than providing a checklist for conducting a risk assessment.

3.4. NCSC – Cyber Assessment Framework v3.0

This comprehensive framework (NCSC, 2019) of the United Kingdom's National Cybersecurity Centre (NCSC) is designed to be used by organisations themselves or by third parties to assess the cybersecurity functions of organisations. The assessment structure is built around four main objectives: managing security risks, protecting against cyber-attacks, detecting cybersecurity events and minimising the impact of cybersecurity incidents.

In total, there are fourteen principles under four main objectives, and these principles are grouped into thirty-nine contributing outcomes for detailed assessment. For each contributing outcome, a set of good practice indicators are listed in tables to assess whether the contributing outcome is achieved, partially achieved or not achieved by the organisation. The good practice indicators are presented as clear statements in the form of a checklist, which makes them easier and more convenient to use. Table 1 contains a list of all fourteen principles that take place in the assessment framework.

Table 1. List of principles in the cyber assessment framework from NCSC

Objectives	#	Principles
Managing security risk	1	Governance
	2	Risk Management
	3	Asset Management
	4	Supply Chain
Protecting against cyber-attack	5	Service Protection Policies and Processes
	6	Identity and Access Control
	7	Data Security
	8	System Security
	9	Resilient Networks and Systems
	10	Staff Awareness and Training
Detecting cybersecurity events	11	Security Monitoring
	12	Proactive Security Event Discovery
Minimising the impact of cybersecurity incidents	13	Response and Recovery Planning
	14	Lessons Learned

Table 2. Comparison between the reviewed cybersecurity frameworks

	Framework for Improving Critical Infrastructure Cybersecurity by NIST	ISO/IEC 27005	GTAG, Assessing Cybersecurity Risk	Cyber Assessment Framework by NCSC
Targeted organisations	It mainly targets CIs, as the title indicates.	It can be used by all types of organisations from any sector.	It can be used by all types of organisations from any sector.	It can be used by all types of organisations from any sector.
Format and ease of use	It does not come in a ready-to-use format. It requires the responsible organisation to go over the provided reference documents and create their own assessment based on their requirements.	It does not come in a ready-to-use format. Instead, it provides guidelines for organisations to develop their risk management processes.	It does not come in a ready-to-use format. Instead, it provides suggestions about each of the six components that it contains.	It comes in a ready-to-use format. The good practice indicators are presented in a clear and structured way, which makes it easy to use.
Comprehensive-ness	It is a comprehensive document that addresses both IT and OT-related cybersecurity issues.	It is a comprehensive document that addresses only IT-related cybersecurity (information security) issues.	It contains only brief proposals for each of its six components. Therefore, it is not as extensive as the other three documents reviewed in this paper.	It is a comprehensive document that addresses both IT and OT-related cybersecurity issues.
Self-sufficiency	It makes use of the existing cybersecurity frameworks. Therefore, it is not self-sufficient.	It relies on two other ISO/IEC standards: ISO/IEC 27000 and ISO/IEC 27001. Therefore, it is not self-sufficient.	It does not require any additional documents. Therefore, it is self-sufficient.	It does not require any additional documents. Therefore, it is self-sufficient.

3.5. Comparison

Table 2 presents a comparison between the frameworks reviewed above to get a better understanding of their differences and justify the decision made in Section 4.

4. Cybersecurity assessment of AECO design cyberspace

Based on the study in the previous section, Cyber Assessment Framework v3.0 (NCSC, 2019) is selected as the most appropriate for the following reasons:

– All concerns are presented in a well-organised and easy-to-use checklist format, which is missing in the other three documents reviewed.

– It deals comprehensively with cyber-security issues under thirty-nine items, while the framework from the IIA (Section 3.3) contains only brief proposals for each of its six components.

– It is self-sufficient. Unlike the framework from NIST and the standard from ISO/IEC, it is not necessary to use other standards/methodologies.

– It provides a ready-to-use assessment framework rather than describing how the assessment should be performed, unlike NIST and ISO/IEC documents reviewed in the previous sections.

In the subsections below, we assess the issues in a BIM/CDE environment across the fourteen NCSC principles presented in Section 3.4. Each principle is first discussed and then the guiding questions are presented. These guiding questions are adaptations from the original framework to the design phase of BIM-enabled construction projects. The customisation considers the stakeholder, organisational, and technological specifics of construction projects using BIM/CDE. Adapted security issues are stated as questions to be answered by a person in charge of cybersecurity.

The discussion is dedicated to suggesting possible solutions to specific security issues of BIM design process. Best practices relevant to the design phase and BIM/CDE processes are provided to support the key points. Since the practical aspects may vary from project to project according to the requirements of each case, the goal is to discuss possible solutions, rather than giving definite answers. Discussion paragraphs include many suggestions from PAS 1192-5 (BSI, 2015) as it is a comprehensive document addressing security threats in digital built environments.

4.1. Discussion of the Principles and Guiding Questions

4.1.1. Governance

According to the recommendations of PAS 1192-5, a Built Asset Security Manager (BASM) shall be appointed by the asset owner or the employer if the asset is identified as sensitive. BASM position can be a full-time job if the project is large-scale and complex; otherwise, it can be handled by a project member equipped with security-related knowledge and experience as a part-time responsibility (BSI, 2015). BASM shall be responsible for developing: the built asset security strategy (BASS), the built asset security management plan (BASMP), the security breach/incident management plan (SB/IMP), and the built asset security information requirements (BASIR) defined in PAS 1192-5. This role is not precisely equivalent to any roles mentioned in the guiding questions below. However, BASM may assign security-related roles to the project members with sufficient knowledge to distribute the responsibilities for maintaining a secure environment as well as delegating risk management decision-makers. Moreover, BASM can be supported by a third-party cybersecurity consultant company that regularly provides the current threat landscape. Even though BASM is accountable for all security decisions, someone from the senior project management shall still track the overall security level of the project and raise awareness about the recent security concerns.

Adapted guiding questions:

- Is there an executive in the project management team who is in charge of the security issues in the project, leads the security discussions in coordination meetings, and points out security-related concerns of IT infrastructure and CDE of the IPD project?
- Are project members (with sufficient security-related knowledge) assigned the roles for maintaining the security of the project before the initiation or using any external services?
- Are there decision-making project members who are delegated by the project management and aware of the risk management strategy of the project to make decisions when necessary?

4.1.2. Risk management

PAS 1192-5 recommends developing three main strategies and plans to manage security risks of built assets in BIM environment: the built asset security strategy (BASS), the built asset security management plan (BASMP), and the security breach/incident management plan (SB/IMP). The built asset risk management strategy is suggested as well, as a part of the BASS to specify the method of conducting risk assessments for identifying potential vulnerabilities and threats. Risk assessments shall be updated dynamically by following the latest threats, particularly against CDEs, design authoring tools, and databases that store critical project information. The latest vulnerabilities discovered by the global cybersecurity community can be tracked on MITRE's Common Vulnerabilities and Exposures (CVE) database (MITRE, 2021). The project type can define the detail level of risk assessments since the effect of a data breach is proportional to the sensitivity of the project and the significance of the information stored in the CDE.

Adapted guiding questions:

- Are possible security risks that may interrupt stable design processes or compromise sensitive design information identified by considering the possible consequences?
- Are possible security threats specifically related to the requirements of the current project, software and hardware utilised for BIM processes, and design workflows considered for risk assessments? Are risk management decision-makers assigned by the BASMP aware of critical outcomes of the assessments?
- Are risk assessment criteria updated when there is a change in the utilised software or hardware such as CDE, design tools, database systems, and network systems, or when there are known changes in construction-related threats?
- Is the project confident about the employed measurements for maintaining robust security of project IT systems? Is the project confident of its security level to be verified by a third-party assessor?

4.1.3. Asset management

Tangible resources such as data storage hardware and Wi-Fi routers can be considered as security-critical assets during the design phase of projects. Inventories of tangible resources shall be managed with respect to their security impact on the project. If the project is utilising an in-house server for the CDE, keeping the hardware infrastructure of the server secure can be critical. The most critical tangible assets should be protected against potential adverse events such as fire and flood.

Adapted guiding questions:

- Are all resources with vital importance on security (such as project computers, data servers, if applicable), and supporting equipment (such as uninterruptable power supply (UPS) or cooling devices) inventoried by their effects on the critical functions of the project? Is the inventory managed and updated in a security-minded fashion?

4.1.4. Supply chain

Intellectual property produced by the in-house design team, design subcontractors, and consultants during the design phase and stored in CDE can be the target of cyber attackers depending on the type of the project. PAS 1192-5 recommends cautiously managing user access levels to CDE, databases, and other data exchange platforms when sharing information with suppliers. Especially the confidential project information should be stored in a different storage level that external suppliers cannot access. Having detailed information about the other projects of suppliers and their business relationships with companies can provide valuable tips to discover possible malicious intentions from suppliers. Security requirements expected to be met by suppliers shall be mentioned explicitly in supplier contracts to protect intellectual property and prevent intrusions. PAS 1192-5 suggests developing a security breach/incident management plan (SB/IMP) to take prompt actions when needed, and a similar incident management plan can be requested from the supplier as a requirement in the contract if the work includes the sharing of sensitive project information.

Adapted guiding questions:

- Is there detailed security-critical information about your partners (such as design and engineering subcontractors, surveying subcontractors, or cost estimation consultants) regarding their other current projects or partnerships they are involved? Is this information about your suppliers included in your risk assessments?

- Is there adequate protection from cybersecurity attacks against networks and sensitive data (such as confidential design details and quantity information) shared with partners during the design phase?
- Are all partners aware of security requirements they need to fulfil to protect the sensitive information shared with them and to access the project network and CDE without violating security rules? Are these security requirements stated unambiguously in partner contracts?
- Do you and your partners have incident management procedures to follow in case of a data breach or an interruption to CDE? Is an incident management procedure included in partner contracts as a requirement?

4.1.5. Service protection policies and processes

PAS 1192-5 suggests developing a built asset security management plan (BASMP) that identifies policies, processes, and procedures to maintain security during the lifecycle of the project. As an example, a policy can be necessary for managing user access to CDE, and a process related to user access can identify the mechanism to accept or reject access requests by users. On the other hand, a procedure related to user access application may indicate the required information from users, such as their role, the access duration, and the privileges needed. The effectiveness of these policies, processes, and procedures may decrease in time with new cyber threats; therefore, regular reviews shall take place for evaluating the performance of these rules. PAS 1192-5 recommends a holistic approach for security that encompasses people, technology tools, and processes since the security measures cannot be effective without due diligence from the individuals.

Adapted guiding questions:

- Are security policies and procedures to follow throughout the lifecycle of the project identified in BIM Execution Plan (BEP) considering the sensitivity of the built asset and the confidentiality of the data to be stored in CDE and shared with stakeholders?
- Are security policies and procedures reviewed and updated regularly as well as in case of changes in the threat landscape or experiencing a significant cyber incident?
- Are security policies and procedures integrated with other project policies and procedures carefully followed by the project stakeholders and regularly evaluated to assess their effectiveness?
- Are security policies and procedures communicated to all project members to create awareness about the security due diligence, the confidentiality level of different types of information and the requirements of working in a shared data environment?

4.1.6. Identity and access control

Controlled access to CDE by project members, suppliers, and consultants during the design phase is required to ensure the confidentiality, integrity, and availability of sensitive project data. A user access management system and a device identity management system can be developed before the project initiation to be active during the design phase and other project phases. Accounts with privileged user access to CDE and the accounts connecting to CDE from mobile devices, such as mobile phones and tablets, shall be closely monitored to detect any suspicious event in time. While providing robust security for project PCs with required configurations and directly connected to the project network can be relatively manageable, mobile devices that can access CDE via mobile applications can be more challenging to handle. Therefore, these devices shall be particularly considered critical in a BIM environment. PAS 1192-5 points out the recent trend of "bring your own device (BYOD)" as a security concern for holding sensitive information and suggests necessary measurements to ensure the removal of critical information after the demobilisation of these devices. In case of using personal devices for work purposes and connecting to CDE, required security software should be installed beforehand. Another significant matter to manage can be third parties such as design subcontractors, cost consultants, and construction subcontractors that request access permission to CDE. Access shall be granted to these third parties after rigorous security checks, especially when working with a company for the first time. As mentioned previously in Section 4.1.4, these security checks should include the other projects of the suppliers and their business relationships.

Adapted guiding questions:

- Is the access to CDE and other data sharing systems limited to authorised and authenticated project members with personally granted user access?
- Is there a more robust authentication system for project members with administrative access rights (such as department managers or IT personnel) and users who need access from remote locations due to the requirements of the project? Are these privileged accounts monitored and reviewed regularly?
- Are the devices authorised to make administrative changes to the CDE and that have full read/write/modify access to all project data limited to internal project network with limited access from/to outside world?
- Is there a robust device management system controlling all connections to the CDE and project network to limit access to known devices only and granting access to supplier or consultant devices when sharing of CDE is required?
- Is there a robust user access management system ensuring the minimum required level of permissions to project members, reviewing these permissions regularly and keeping the record of all authorised and unauthorised access to CDE and project network?

4.1.7. Data security

PAS 1192-5 defines sensitive information as the information that may cause damage (such as loss of intellectual property, financial loss, and reputation loss) to the organisation when lost, altered, or disclosed. During the design phase of construction projects, sensitive information can include the design details if the project is classified as sensitive, quantity details to be used in the bill of quantities, and any other information that may provide a competitive advantage to competitors if disclosed. Therefore, utilising a system to assess and record the sensitivity of all information stored in CDE from the beginning of the project can be advantageous while granting access to project members and third parties, and defining access limits. In case of using mobile devices such smart phones and tablets to access data – which becomes more and more popular on construction sites – the organisation should be able to delete all sensitive information stored in them remotely when necessary.

Adapted guiding questions:

- Do you have a detailed identification of your sensitive project information stored in CDE (such as confidential design details, bill of quantities, and commercial information) which would cause damage if tampered or accessed by competitors or malevolent parties?
- Is there robust data protection for the transmission of sensitive project data over trusted and non-trusted carriers?
- Is there robust data protection for stored data in CDE which would cause competitive disadvantage, loss or disclosure of intellectual property, financial losses, or reputation damage if accessed by malicious third parties?
- Do you have a system to control (or wipe all the sensitive information when necessary) all mobile devices (such as mobile phones, tablets, and project laptops) that can access CDE?
- In case of disposal of a project device or equipment with storage, do you erase all information permanently to prevent any possible disclosure of sensitive project information?

4.1.8. System security

Developing a system to assess and record the sensitivity of all project information from the beginning, as suggested in the Data Security section, can be useful for creating various security zones for different levels of sensitivity. This way of designing segregated zones for each level of sensitivity can improve the resilience of the critical project systems. Moreover, providing a high level of protection to all project information without assessing the information sensitivity may significantly increase the total security cost of the project. Vulnerabilities of critical software used in the project (e.g., design authoring software, CDE platform, technical analysis software) and operating systems shall be followed to take timely mitigation actions. IT personnel responsible for maintaining the technical security in the project shall be responsible for following these announced vulnerabilities and patches if available. The latest security configurations for software and operating systems shall be carefully followed to minimise the probability of cyber incidents.

Adapted guiding questions:

- Is the CDE utilised in the project designed in a way to support robust security by creating various security zones for different levels of information sensitivity and allowing easy recovery after a possible attack? Is there zoning established to take into account people working in more than one project at the same time, using more than one CDE?
- Are configurations of CDE and other data sharing systems that hold sensitive information updated regularly to the latest versions to maintain security?
- Are there any dedicated and isolated devices to make administrative changes to the project network and CDE? Are these changes only managed by privileged accounts assigned to a limited number of trusted project personnel with IT experience?
- Are the latest announced vulnerabilities by software companies for utilised design authoring tools, operating systems, and CDE platforms carefully followed to be able to perform required mitigations and patch if necessary? Do you or a third-party security consultant make regular vulnerability tests to your systems to detect possible vulnerabilities?

4.1.9. Resilient networks and systems

Boyes (2013) defines resilience as being ready for any kind of threat to be able to continue the main business functions. In the design and cybersecurity context, resilience can be defined as being able to maintain the design work critical for the timeline of the project in case of possible cyber incidents. Developing a security breach/incident management plan (SB/IMP), as suggested by PAS 1192-5, can be a solution for providing resilience in construction projects. SB/IMP includes having a process to follow in case of experiencing a breach or incident, having knowledge about the disaster recovery plan of CDE service provider, if applicable, and having contractually binding liabilities with subcontractors and consultants in case of incidents caused by them (BSI, 2015). Critical documents and information produced during the design phase can be treated with special attention in terms of disaster recovery to maintain the essential functions and not delay the main design deliveries after a possible incident.

Adapted guiding questions:

- Are your project network and CDE capable of returning to functional status in the minimum possible time after experiencing a cyber incident without delaying the ongoing design work? Do you have a disaster recovery procedure to follow after a possible cyber incident? Do you have periodical tests for the resilience of your systems?
- Are the systems utilised for the main design works (that directly affect the project schedule) treated separately from the supporting project work (such as business administration functions) in terms of security?

- Is there an automated backup system for critical project data that may have an adverse schedule impact if modified by malicious individuals or lost? Is there robust protection provided for these backups?

4.1.10. Staff awareness and training

PAS 1192-5 suggests conducting security awareness training for the project personnel to create a security-minded culture within the project. In addition to the general security awareness training, role-based security training is also recommended for key roles in the project, such as information manager, procurement personnel, and supplier or contractor employees responsible for security (BSI, 2015). According to the M-Trends 2021 report (FireEye, 2021), phishing attacks account for 23% of intrusions, making it the second most common initial infection vector. Therefore, organisations should pay particular attention to conduct phishing awareness trainings and performing regular phishing tests on employees. The personnel who constantly fail phishing tests may constitute a major risk for the organisation. Lastly, a rewarding system for personnel, discovering and reporting cybersecurity issues may improve security awareness. Receiving recognition for helping to maintain a secure environment can be motivating for the project staff.

Adapted guiding questions:

- Are all project employees aware of the security priorities of the project and cybersecurity threats that they may face? Are they recognised for addressing cybersecurity issues of the software and information systems utilised in the project?
- Is there a cybersecurity training routine for all the stakeholders in the project regardless of their roles and responsibilities?

4.1.11. Security monitoring

In the design phase of construction projects, there may be many partners and project personnel using the project network and CDE. Therefore, it is of utmost importance to track logging data to detect potential threats and suspicious activities. Keeping all the software updated for virus signatures and indicators of compromise is one of the measures to be taken for detecting unexpected activity. If an external company provides the CDE service, their measures for monitoring the logging data and automatic security alerts shall be checked with them. Responsibilities for following logging data to project information systems can be assigned to the IT personnel. In the case of hosting the CDE in-house, having a robust security monitoring system can alleviate the risks of potential cyber-attacks against the CDE.

Adapted guiding questions:

- Do you have a robust security monitoring system tracking all logging by project personnel and supplier devices to identify suspicious activities in the information system?
- Is log data protected and only accessible by a limited group of project personnel that needs it for business reasons?
- Do suspicious logs and activities in your project network and CDE, provided either by an external host or in-house, trigger alerts?
- Do you regularly check the updates for virus signatures and compromise indicators for the design software and CDE platform you are using?
- Is there a team in your IT department responsible for monitoring log data and suspicious activities?

4.1.12. Proactive security event discovery

Having mechanisms to detect abnormalities in information systems can prevent malicious activities as well as hostile reconnaissance. According to PAS 1192-5, during hostile reconnaissance, malevolent parties can be looking for physical vulnerabilities, the security level of the information systems, and some hints that can be used for social engineering. Therefore, detecting suspicious activities in the reconnaissance stage may help in avoiding attacks. Since social engineering takes advantage of human vulnerabilities, a failure of project security guards to detect suspicious activity can lead to a cybersecurity incident. For this reason, training the security guards against such attempts can protect the project from further cyber-attacks. In order to detect abnormalities in the CDE platforms that are hosted by external software companies, the support of the service provider can be helpful.

Adapted guiding questions:

- Do you have a detection mechanism for abnormalities in the project network and CDE which makes use of experienced incidents and threats from previous projects and current known threats?
- Are there routine abnormality checks for the project network and CDE to detect potential malicious activities by hackers, competitors, or insiders?

4.1.13. Response and recovery planning

Having a security breach/incident management plan (SB/IMP) as recommended by PAS 1192-5 can be a solution to maintain the critical design activities after an incident. Incident response plans shall be developed based on the risks particular to the type of project, location of the project, and sensitivity of the information stored in the CDE. A robust plan to follow for the worst-case scenarios is necessary for the resilience of the information systems of the project and not having adverse schedule impacts. Having the resources necessary for running the incident response plan with full functionality is another significant matter for quick recovery. Training the IT staff about developing and running response plans and employing state-of-the-art cybersecurity technologies capable of promptly returning the system to its initial state can be beneficial for performing incident response activities effectively.

Adapted guiding questions:

- Is there a functional incident response plan that covers potential attacks against the project network and CDE directed to maintaining critical design activities after incidents?

- Are there enough resources available for incident response activities (such as skilled staff, IT infrastructure for incident response) and cybersecurity incident response consultancy if required?
- Are there routine tests for checking the effectiveness of response plans, supported by the experiences from previous projects and experiences of other organisations if available?

4.1.14. Lessons learned

Analysing the causes of each incident after the occurrence is a good practice for preventing the recurrence of similar incidents and taking quick actions in case of future circumstances. Keeping a record of lessons learned and regularly updating it shall be a part of the project's routines; the results of the root cause of analysis after cyber incidents can be a vital part of the lessons learned. Cyber threat information sharing is a well-accepted practice in both public and private sectors (Nweke & Wolthusen, 2020). A similar approach can be employed in the AECO industry to share the cybersecurity-related lessons learned among the companies/projects to improve cyber intelligence on a global scale.

Adapted guiding questions:

- Do the lessons learned processes and procedures in your project include conducting root cause analysis after cyber incidents?
- Are all the lessons learned items after cyber incidents recorded in detail to improve the security of project information systems, including the CDE?

4.2. Evaluation method

NIST (2018) suggests that companies have cybersecurity risk profiles showing the alignment of their actions with the business requirements, priorities, and risk appetite. This section proposes two different profiles for evaluation, namely Current Profile and Target Profile, as mentioned in NIST's framework. As the profile names indicate, the Current Profile shows the extent to which the existing cybersecurity-related measures are taken. On the other hand, the Target Profile presents the actions and measures required to accomplish the desired level of cybersecurity. In order to compare these two profiles and create a pathway from the Current to Target Profile, a scoring system based on NIST's implementation tiers was employed. NIST suggests the following implementation tiers: Tier 1 – Partial, Tier 2 – Risk Informed, Tier 3 – Repeatable, and Tier 4 – Adaptive. Based on these tiers, the scorecard shown in Table 3 is proposed to evaluate the previously mentioned principles by answering the guiding questions with the provided scores. The scorecard includes one more level of implementation for the assessment purpose, "No Implementation", which corresponds to a score of 0. The scores shown in Table 3 do not aim to turn the assessment into a quantitative one. Their sole purpose is to provide a means to demonstrate the degree of implementation and make the comparison between the two profiles easier.

Using the scores in Table 3, the person responsible for cybersecurity in the organisation can answer the guiding questions provided in the previous subsections according to the existing cybersecurity practices. The result of this evaluation will show the Current Profile. The next step is to define the Target Profile depending on the organisation's priorities, allocated budget for cybersecurity, and risk appetite. When both profiles are determined, the final step is to build an organisation-wide strategy to reach the Target Profile. In order to visualize the gap between the two profiles, a radar chart can be utilized, as demonstrated in Figure 4. The radar chart example in Figure 4 uses hypothetical Current and Target Profile scores.

Table 3. Proposed scorecard for the evaluation

Implementation level	Description	Score
No implementation	There is no implementation in place.	0
Partial	The risks are managed in an ad hoc way. There are no formalised cybersecurity practices.	1
Risk Informed	There is an awareness of cybersecurity risks, and cybersecurity exercises are approved by management; however, there are no organisation-wide policies.	2
Repeatable	There are organisation-wide policies and procedures to manage cybersecurity risks. Cybersecurity exercises are regularly updated according to the requirements and risk appetite of the organisation.	3
Adaptive	The organisation-wide cybersecurity exercises, policies, and procedures are continuously adapted to the latest technology, advances, and threat landscape.	4

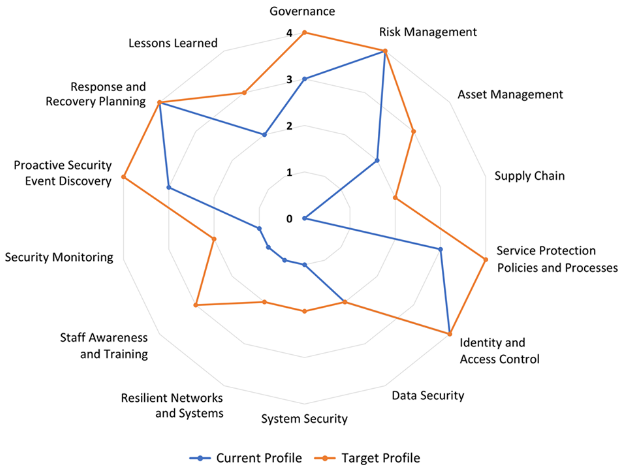

Figure 4. Radar chart

Conclusions, discussion, and future work

In collaborative BIM environments implemented in a CDE, pursuing IPD, the use of centralised data exchange systems improves efficiency, helps save time, and improves communication between the parties involved. However, sharing data with third parties such as subcontractors, suppliers, consultants, and other project partners via centralised data networks as well as relying on cloud services significantly increases the risk of external and internal cyber-attacks. These attacks can lead to financial loss, disruption of operations and loss of reputation.

Digital collaboration reaches its peak in the design phase of construction projects. It raises concerns about change tracking in design files, intellectual property ownership, and the confidentiality of sensitive project information. These concerns should be addressed during the design phase through a cybersecurity assessment framework to identify vulnerabilities and assess the security level of the project. In the absence of a sector-specific framework, there are many frameworks that can be, to some extent, used in the construction industry.

Based on an analysis of four such frameworks, in this paper we have used the Cyber Assessment Framework of the National Cyber Security Centre of the United Kingdom as a foundation. The main reasons were that it provides clear guidelines in the form of a checklist. It addresses concerns in sufficient detail and does not require access to additional documents. A total of fourteen cybersecurity principles taken from the original framework were adapted to the requirements of BIM/CDE ecosystem and discussed to provide recommendations on how to address the risks. Moreover, an evaluation method that includes a scorecard was proposed to define the Current and Target Profiles of organisations. The profiles were illustrated in radar chart

We find the framework useful for an initial overview of cybersecurity issues in the construction industry. It is also useful to pinpoint the specific challenges of cybersecurity in construction. In the analysis in Section 4, we are finding that particularly the principles 1 (Governance), 4 (Supply Chain), 6 (Identity and Access control), 7 (Data Security), and 8 (System Security) are lacking the specifics of design environments in construction.

In construction design, governance (1) is not about the governance of cybersecurity in an organisation but rather governance of a unique, dynamic, temporal, multi-stakeholder, virtual organisation. The supply chain (4) is, in fact, a dynamic network of partners involved in the project that form a virtual organisation. Successful collaboration and integrated project delivery require smooth access to information and to other resources. Cybersecurity measures would create obstacles to that. Further, the supply chain is not static, and elements of the virtual organisation may be simultaneously partnering with other virtual organisations or can work with competitors with future projects. This creates a challenge for identity management and particularly access control (6). The cybersecurity of one BIM/CDE project cannot be addressed in isolation from other BIM/CDE projects.

A particular challenge to data security (7) is the nature of data storage that BIM technology currently uses. The entire model developed by many partners can be one single file. Technically – using traditional cybersecurity technology – that can only be protected as a whole. It will be up to the software companies that are developing the BIM modellers to manage the data as a relational or object-oriented database where access rights can be defined for each table, field, class of objects, and even more precisely. This would also include access to reusable representations of objects which is important for the protection of intellectual property. The system security (8) would have to be tightly coupled with that, creating overlapping security zoning in the real organisations and in the virtual organisations. The delimitation between the zones would cut right through BIM models and even through individual objects.

Finally, cybersecurity adds another layer of complexity to already highly complicated construction design projects, creating obstacles to smooth collaboration, integrated project delivery, and teamwork by creating digital locks and fences, additional paperwork, additional organisational efforts, and extensions to execution plans or contracts. The list of fourteen principles in Section 4 is long and the number of measures to be taken calls for a huge effort. But this is not all. In the original NCSC framework, fourteen main principles are divided into thirty-nine individual assessments. Further work is needed, on one hand, to see how those can be addressed. And on the other hand, a cost-benefit analysis is required to see how much security is actually worth.

Further theoretical work should consider developing a construction-specific framework that would take into account the particularities and dynamic nature of partners that design collaboratively, the variety of actors involved, and the overlapping boundaries and jurisdictions of participants.

Funding

The presented work was in part financially supported by the Slovenian Research Agency via research programme eConstruction [P2-0210].

Author contributions

MSS and ŽT conceived the study and were responsible for the overall outline and research direction. ŽT and RK were responsible for analysis and data interpretation. ŽT wrote the first draft of the article.

Disclosure statement

We, the authors of this paper, declare that we are not aware of any competing financial interests or personal relationships that may have influenced the work presented in this paper.

References

Abdirad, H., & Pishdad-Bozorgi, P. (2014). Developing a framework of metrics to assess collaboration in integrated project delivery. In *Proceedings of the 50th Annual International Conference of the Associated Schools of Construction*. Virginia Polytechnic Institute and State University, VA, US.

AIA National. (2007). *Integrated project delivery: A guide*. The American Institute of Architects. https://www.aia.org/resources/64146-integrated-project-delivery-a-guide

Ames, B. C., Foster, F. R., Glynn, C., Lynn, M., Nakama, D., Penrose, T., & Rai, S. (2016). *Assessing cybersecurity risk: Roles of the three lines of defense*. Institute of Internal Auditors (IIA). https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity/gtag-assessing-cybersecurity-risk.pdf

Azhar, S. (2011). Building information modeling (BIM): Trends, benefits, risks, and challenges for the AEC industry. *Leadership and Management in Engineering*, *11*(3), 241–252. https://doi.org/10.1061/(ASCE)LM.1943-5630.0000127

Barrett, M. P. (2018). *Framework for improving critical infrastructure cybersecurity*. National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA.

Bishop, M. (2004). *Introduction to computer security*. Addison-Wesley Professional.

Boyes, H. (2013). *Resilience and cyber security of technology in the built environment*. The Institution of Engineering and Technology.

Boyes, H. (2014). Building information modelling (BIM): Addressing the cyber security issues. *Engineering & Technology Reference*. https://doi.org/10.1049/etr.2014.9001

Boyes, H. (2015). Security, privacy, and the built environment. *IT Professional*, *17*(3), 25–31. https://doi.org/10.1109/MITP.2015.49

British Standards Institution. (2013). *Specification for information management for the capital/delivery phase of construction projects using building information modelling (incorporating corrigendum No. 1)* (PAS 1192-2:2013).

British Standards Institution. (2015). *Specification for security-minded building information modelling, digital built environments and smart asset management* (PAS 1192-5:2015).

buildingSMART. (n.d.). *Industry foundation classes (IFC)*. buildingSMART Technical. https://technical.buildingsmart.org/standards/ifc/

Construction Users Roundtable. (2004). *Collaboration, integrated information and the project lifecycle in building design, construction and operation*. https://kcuc.org/wp-content/uploads/2013/11/Collaboration-Integrated-Information-and-the-Project-Lifecycle.pdf

Cybersecurity and Infrastructure Security Agency. (2009, May 6). *What is cybersecurity?* https://us-cert.cisa.gov/ncas/tips/ST04-001

Davis, A. (2015). Building cyber-resilience into supply chains. *Technology Innovation Management Review*, *5*(4), 19–27. https://doi.org/10.22215/timreview/887

Eastman, C. M., Eastman, C., Teicholz, P., Sacks, R., & Liston, K. (2008). *BIM handbook: A guide to building information modeling for owners, managers, designers, engineers and contractors*. John Wiley & Sons. https://doi.org/10.1002/9780470261309

Eastman, R., Versace, M., & Webber, A. (2015). *Big data and predictive analytics: On the cybersecurity frontline*. International Data Corporation (IDC). https://v2.itweb.co.za/whitepaper/Whitepaper_SAS_Cyber_Security.pdf

European Union Agency for Cybersecurity. (2015). *Definition of cybersecurity – Gaps and overlaps in standardisation* (Report/Study TP-01-15-934-EN-N). https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Falk, C. (2004). Gray hat hacking: Morally black and white. In *2004 Cyber Security Group (CSG) Training Conference*.

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

Freund, J., & Jones, J. (2014). *Measuring and managing information risk: A FAIR approach* (1st ed.). Butterworth-Heinemann.

Glavach, D., LaSalle-DeSantis, J., & Zimmerman, S. (2017). Applying and assessing cybersecurity controls for direct digital manufacturing (DDM) systems. In L. Thames & D. Schaefer (Eds.), *Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing* (pp. 173–194). Springer International Publishing. https://doi.org/10.1007/978-3-319-50660-9_7

Hubbard, D. W., & Seiersen, R. (2016). *How to measure anything in cybersecurity risk* (1st ed.). John Wiley & Sons. https://doi.org/10.1002/9781119162315

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security – A survey. *IEEE Internet of Things Journal*, *4*(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

Ilozor, B. D., & Kelly, D. J. (2012). Building information modeling and integrated project delivery in the commercial construction industry: A conceptual study. *Journal of Engineering, Project, and Production Management*, *2*(1), 23–36. https://doi.org/10.32738/JEPPM.201201.0004

International Organization for Standardization. (2018). *Information technology-Security techniques–Information security risk management* (ISO Standard No. ISO/IEC 27005).

International Organization for Standardization. (2013). *Information security management* (ISO Standard No. ISO/IEC 27001:2013).

Kabay, M. E. (2015). History of computer crime. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer security handbook* (pp. 2.1–2.41). John Wiley & Sons, Inc. https://doi.org/10.1002/9781118851678.ch2

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

Ma, Z., Zhang, D., & Li, J. (2018). A dedicated collaboration platform for Integrated Project Delivery. *Automation in Construction*, *86*, 199–209. https://doi.org/10.1016/j.autcon.2017.10.024

Mahamadu, A.-M., Mahdjoubi, L., & Booth, C. (2013). Challenges to BIM-cloud integration: Implication of security issues on secure collaboration. In *2013 IEEE 5th International Conference on Cloud Computing Technology and Science* (Vol. 2, pp. 209–214). https://doi.org/10.1109/CloudCom.2013.127

Mantha, B. R. K., & de Soto, B. G. (2019). Cyber security challenges and vulnerability assessment in the construction industry. In *Proceedings of the Creative Construction Conference 2019* (pp. 29–37). https://doi.org/10.3311/CCC2019-005

MITRE. (2021). *CVE*. https://cve.mitre.org/

Mutis, I., & Paramashivam, A. (2019). Cybersecurity management framework for a cloud-based BIM model. In I. Mutis & T. Hartmann (Eds.), *Advances in informatics and computing in civil and construction engineering* (pp. 325–333). Springer International Publishing. https://doi.org/10.1007/978-3-030-00220-6_39

Nawari, N. O., & Ravindran, S. (2019). Blockchain technology and BIM process: Review and potential applications. *Journal of Information Technology in Construction (ITcon)*, *24*(12), 209–238.

National Cybersecurity Centre. (n.d.). *What is cyber security?* https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

National Cybersecurity Centre. (2016). *Common cyber attacks: Reducing the impact*.

National Cybersecurity Centre. (2019). *Cyber assessment framework v3.0*. https://www.ncsc.gov.uk/files/NCSC_CAF_v3.0%20.pdf

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity v1.1*. Gaithersburg, MD. https://doi.org/10.6028/NIST.CSWP.04162018

Nweke, L. O., & Wolthusen, S. (2020). Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection. In *12th International Conference on Cyber Conflict* (*CyCon*) (pp. 63–78). https://doi.org/10.23919/CyCon49761.2020.9131721

Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information*. Wiley.

Parker, D. B. (2015). Toward a new framework for information security? In *Computer Security Handbook* (pp. 3.1–3.23). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781118851678.ch3

Parn, E. A., & 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

Peltier, T. R. (2005). *Information security risk analysis*. Auerbach Publications. https://doi.org/10.1201/9781420031195

Publications Office of the European Union. (2018). *Guidelines on assessing DSP and OES compliance with the NISD security requirements: Information security audit and self – assessment/management frameworks*. http://op.europa.eu/en/publication-detail/-/publication/78f2a620-f909-11e8-9982-01aa75ed71a1/language-en

Rogers, M. K. (2005). The development of a meaningful Hacker Taxonomy: A two dimensional approach. In *NIJ National Conference 2005*.

Smith, G. E., Watson, K. J., Baker, W. H., & Pokorski II, J. A. (2007). A critical balance: Collaboration and security in the IT-enabled supply chain. *International Journal of Production Research*, *45*(11), 2595–2613. https://doi.org/10.1080/00207540601020544

Stewart, J. M., Chapple, M., & Gibson, D. (2015). *CISSP: Certified information systems security professional study guide* (7th ed.). Sybex, a Wiley brand.

Thames, L., & Schaefer, D. (2017). Industry 4.0: An overview of key benefits, technologies, and challenges. In L. Thames & D. Schaefer (Eds.), *Cybersecurity for industry 4.0: Analysis for design and manufacturing* (pp. 1–33). Springer International Publishing. https://doi.org/10.1007/978-3-319-50660-9_1

Thaseen, S., Cherukuri, A. K., Ahmad, A., Cherukuri, A. K., & Ahmad, A. (2019). Improving security and privacy in cyber-physical systems. In Y. Maleh, M. Shojafar, A. Darwish, & A. Haqiq (Eds.), *Cybersecurity and privacy in cyber physical systems* (pp. 3–43). CRC Press. https://doi.org/10.1201/9780429263897-2

Turk, Ž. (2020). Interoperability in construction – Mission impossible?. *Developments in the Built Environment*, 100018. https://doi.org/10.1016/j.dibe.2020.100018