ISSN 1392-3730/eISSN 1822-3605

VILNIUS TECH
Vilnius Gediminas Technical University

JOURNAL of CIVIL ENGINEERING and MANAGEMENT

2025
Volume 31
Issue 8
Pages 926–954
https://doi.org/10.3846/jcem.2025.25213

IDENTIFYING CYBER RISK FACTORS ASSOCIATED WITH CONSTRUCTION PROJECTS

Dongchi YAO[1,2]✉, Borja GARCÍA DE SOTO[1,2], Mike WILKES[3]

[1]*S.M.A.R.T. Construction Research Group, Division of Engineering, New York University Abu Dhabi (NYUAD), Experimental Research Building, Saadiyat Island, P.O. Box 129188, Abu Dhabi, United Arab Emirates*
[2]*Department of Civil and Urban Engineering, Tandon School of Engineering, New York University (NYU), New York, United States*
[3]*Department of Computer Science and Engineering, Tandon School of Engineering, New York University (NYU), New York, United States*

Article History:
- received 1 February 2024
- accepted 14 July 2025

Abstract. As construction projects adopt increasingly interconnected digital technologies, their cyber-attack surface expands, making comprehensive cyber risk management essential to prevent incidents, mitigate risks, and minimize potential losses resulting from such attacks. However, the necessary risk factors for this purpose are lacking. Therefore, the study aims to develop a comprehensive set of project-level cyber risk factors tailored to the complexities of construction projects, identified through a systematic and flexible seven-step methodological framework: (1) a literature review of construction and cybersecurity sources to identify initial factors; (2) initial definition of risk categories; (3) internal evaluation and expert input to refine these factors; (4) distribution of a detailed expert questionnaire for rating; (5) expert evaluations through meetings and feedback sessions to enhance validity; (6) elimination of lower-scoring factors; and (7) establishment of quantitative scales for precise risk assessment. The findings include the 32 identified risk factors into five groups: project information, project structure, information technology (IT), operational technology (OT), and management and human aspects. The contributions include providing a set of risk factors that serve as cybersecurity management references and inputs for future quantitative risk assessments, offering a checklist used for proactive risk management, and introducing a framework adaptable for identifying factors of other risks.

Keywords: construction cybersecurity, digital transformation, risk factors, risk assessment, industry-specific vulnerabilities.

✉Corresponding author. E-mail: ***dongchi.yao@nyu.edu***

1. Introduction

1.1. Background

The advent of Construction 4.0 marks the construction industry's transition into the digital era, characterized by the integration of digital tools such as Building Information Modeling (BIM) and automation/robotic systems, along with cyber-physical systems (CPS) and digital twins (Kurtz, 2019). These innovations enhance efficiency and productivity by enabling real-time data exchange, monitoring, and management. However, this integration also exposes the industry to heightened cybersecurity vulnerabilities. Various forms of attacks, including data breaches, phishing, and ransomware, exploit these vulnerabilities, presenting significant cyber risks to construction projects. Therefore, strengthening cybersecurity becomes paramount. It is not merely about protecting data but is also instrumental in ensuring the holistic physical, operational, and financial integrity of construction projects amidst the complexities of the digital revolution.

1.2. Problem statement

The construction industry lags behind other sectors in cybersecurity, with its vulnerabilities becoming evident in real-world incidents (Badi & Nasaj, 2024). Over the past decade, the industry has experienced a dramatic rise in cyber incidents, especially in five categories: ransomware, phishing, insider threats, data breaches, and supply chain attacks (Deloitte, 2022; Yao & García De Soto, 2024a). Table 1 highlights representative cyberattacks from the past years, underscoring the urgent need for the construction industry to strengthen its cybersecurity measures to ensure the successful delivery of projects. In the UAE, cyberattacks have surged across various industries, with

ransomware emerging as a predominant threat. Reports indicate that over half of the cyber incidents in the UAE involve ransomware, primarily targeting sectors such as government, energy, and information technology, with the construction sector also being increasingly vulnerable (CPX, 2024). A survey conducted by Freshfields, Accuracy, and NYU Abu Dhabi revealed that 73% of respondents in the Middle East construction sector reported an increase in cyberattacks since 2020 (Rosenberg et al., 2024). The escalation of ransomware and related cyber threats is far more than an IT nuisance; it poses an enterprise-wide risk that can stall projects, inflate costs, and erode contractual trust. Effective mitigation therefore needs to be framed as a comprehensive cyber risk management endeavour that (i) aligns technical safeguards with corporate strategy, (ii) meets emerging national and sector-specific regulations, and (iii) embeds digital-governance practices throughout the project life cycle. By integrating these dimensions, construction firms can transform fragmented cybersecurity measures into a coherent risk management programme that safeguards project performance and strengthens organisational resilience.

A complete risk management process involves three phases: (1) identifying risks, (2) assessing their potential impact and likelihood, then prioritizing them, and (3) responding to risks by applying strategies that include acceptance, monitoring, mitigation, transfer, and more (Zou et al., 2007). Similarly, in the context of construction projects, cyber risk management begins with cyber risk identification, which involves determining the associated risks (e.g., ransomware, phishing, etc.) that might affect the projects and identifying the risk factors for each risk. It helps establish the context and scope of risk management. Risk factor identification requires in-depth domain knowledge of both construction projects and cybersecurity. A comprehensive and accurate set of risk factors is crucial in establishing a solid foundation for risk management. It enhances the understanding of cyber risks within the industry and provides practitioners with insights into which aspects to prioritize ahead of time.

However, as stated in Section 2, there is a significant gap in the literature: no research identifies a comprehensive set of cybersecurity risk factors tailored to construction projects. Current studies suffer from several shortcomings. First, only a limited number address cybersecurity in the construction sector, and these often remain generalized, without pinpointing specific risk factors. Second, existing cyber risk assessments rely heavily on subjective assumptions about stakeholders rather than thorough analyses of risk factors; consequently, no definitive set of risk factors is provided. Moreover, while many studies have identified and categorized risk factors for other construction-relat-

Table 1. Cyber incident examples in the last five years

Year	Victim	Attack Nature	Consequence	Reference
2018	Ingérop	Data breach/theft	65 GB of data related to nuclear power plants stolen, over 11,000 files from a dozen projects accessed, and personal details of more than 1,000 employees compromised.	Cyware (2018)
2019	Bird Construction	Data breach	MAZE claims to have stolen 60 GB of data from the company, which landed 48 contracts worth $406 million with Canada's Department of National Defense between 2006 and 2015.	Coble (2020)
2019	Marous Brothers Construction	Email fraud	When the major renovation project of the St. Ambrose Catholic Church was about to be completed, there were financial issues, and the $1.7 million payment that should have been made to the contractor was not received. This situation stems from the theft of email communication content,	Sawyer and Rubenstone (2019)
2020	Bouygues Construction	Ransomware attack	Forced the company to shut down its systems worldwide due to a ransomware attack at the end of January 2020.	Korman (2020)
2020	Bam Construct & Interserve	Ransomware attack	Bam Construct faced ransomware encrypting files for ransom, and Interserve suffered a data breach potentially affecting 100,000 employees, with suspicions of targeting its anti-pandemic efforts.	Price (2020)
2021	Colonial Pipeline	Cyberattack using a compromised password	Networks accessed using a compromised password, shutting off the largest fuel pipeline in the US until a $4.4 million ransom was paid, marking its first complete shutdown in 57 years.	Turton and Mehrotra (2021)
2022	Interserve Group Ltd	Data breach	Issued a £4.4 million fine for failing to secure the personal information of its staff, constituting a breach of data protection law.	Steel (2022)
2022	The Knauf Group	Ransomware attack	Resulted in emails and product-ordering software being taken offline, disrupting customer communications.	The Stack (2022)
2023	Huntington Ingalls Industries	Unauthorized access to data	Unauthorized access to sensitive consumer data, including personal, financial, and medical information, reported.	JDSUPRA (2023)
2023	Simpson Manufacturing Co., Inc.	Malicious activity	IT infrastructure and applications disrupted, with steps taken to stop and remediate the activity.	Kunert (2023)

ed issues such as financial, environmental, and operational, none focus on cybersecurity-specific risks, effectively neglecting cybersecurity concerns. This gap is especially troubling given the growing reliance on digital technologies in construction, where cybersecurity is paramount.

1.3. Research question and objectives

Therefore, our study's research question is: "What are the project-level cybersecurity risk factors, specifically tailored to construction projects, that can address the industry's current gap in comprehensive cybersecurity risk assessments?". Two objectives are outlined to answer this question: (1) developing a comprehensive set of project-level cyber risk factors through a systematic methodology that combines literature review, expert evaluation, and questionnaire surveys; and (2) pinpointing the advantages of the identified risk factors for future cyber risk assessments, which includes incorporating the network structure of projects, integrating both macro and micro project aspects, allowing for a more quantitative risk assessment, and infusing information on construction-unique vulnerabilities into the risk assessment models.

These identified risk factors can be applied to a wide range of cyber threats, including but not limited to ransomware, phishing, data breaches, insider attacks, and supply chain attacks. By systematically developing and validating these factors, our study extends prior risk factor identification efforts. Our approach provides a more comprehensive set of factors that capture the unique dynamics of construction projects ranging from project structure to communication patterns, to IT-related considerations, and thus offers a robust foundation for future research and practical applications. Overall, this paper comprehensively investigates and addresses the research question proposed, thus confirming the hypothesis that a tailored set of project-level cyber risk factors can indeed fill the identified gap in the construction industry's cyber risk assessments.

1.4. Contributions

For the first time, a comprehensive set of 32 project-level cyber risk factors specifically tailored to the construction industry has been systematically identified using the proposed seven-step framework. This represents a major breakthrough, as it addresses a previously overlooked research area and enables more proactive and quantitative cyber risk assessments in a rapidly digitizing sector. This addresses a critical need in an industry where cyber incidents have surged by over 5,000% in less than a decade, causing significant financial and operational disruptions. By providing a systematic methodology framework for risk factor identification, the study enables practitioners and researchers alike to pinpoint and prioritize potential vulnerabilities before they escalate. The importance of these findings and who stands to benefit from them are expounded as follows:

(1) Impact on Scholars: Future cyber risk assessments can utilize the newly developed set of risk factors as an evidence-based foundation, reducing reliance on ad hoc or generalized assumptions. This not only advances scholarly discourse on construction cybersecurity but also facilitates more quantifiable research in an area where empirical data have been scarce.

(2) Benefit to Industry Stakeholders: Construction firms, project managers, and technology vendors can adopt the identified risk factors as a proactive "checklist" to fortify their security measures. By systematically addressing the vulnerabilities unique to construction projects, companies can potentially save millions of dollars in direct cyber-incident costs (e.g., data breaches, ransomware payments) and indirect expenses (e.g., project delays, reputational damage). This increased operational resilience not only protects critical infrastructure but also enhances stakeholder confidence in an industry rapidly embracing digital transformation.

(3) Relevance to Broader Risk Categories: While tailored to cybersecurity, the framework can be extended to the project risk management for other forms of risks, facilitating a more integrated and holistic approach to assessing threats in modern construction environments.

The remainder of this paper is as follows: Section 2 discusses the unique cybersecurity challenges in the construction industry and reviews related studies. Section 3 elaborates on the methodology, including the rationale for treating each construction project as a network and introducing the seven-step framework for risk factor identification. Section 4 presents the final set of cybersecurity risk factors, systematically categorized and accompanied by corresponding scales for quantitative assessment. Section 5 offers a comprehensive discussion. Section 6 concludes the study.

2. Related works

2.1. Cybersecurity challenges and cyber risk factor necessity

The construction industry is grappling with unique cybersecurity challenges beyond those commonly faced in the IT sector. These distinct vulnerabilities stem from the inherently multifaceted and dynamic nature of construction projects. First, fluid team changes along the phases of construction projects might disrupt communication and security protocols, increasing breach risks due to unfamiliarity and oversights from phase-specific tasks and specialization (Mantha & García de Soto, 2019). Second, a diverse workforce with varied cybersecurity awareness can lead to security lapses, with less informed individuals prone to errors or phishing attacks (Kurtz, 2019). Third, the widespread communications networks among stakeholders elevate the risk of data breaches. The breadth of these

networks can lead to misinterpretations, unauthorized access, and leaks (Nyamuchiwa et al., 2022). Fourth, digital transformation, especially in supply chains, amplifies information exchange. Vulnerabilities resulting from those imposed by external participants and associated weak communication protocols can be propagated and intensified, escalating the risk of exploitation by cyber attacks (Kurtz, 2019; Parn & Edwards, 2019). Lastly, the common practice of personnel working across multiple projects can lead to the blurring of project boundaries, elevating the risk of unintentional data leaks or unauthorized access (Yao & García de Soto, 2023). Given these distinct vulnerabilities and their interactive effects, a tailored set of risk factors is a must for effective industry-specific cyber risk management. The identification of such risk factors is important because it enables a structured understanding of where and how vulnerabilities emerge, helping to prioritize areas of concern and allocate resources efficiently. Without a clear set of identified risk factors, efforts to mitigate cybersecurity threats are likely to be fragmented and reactive, leaving construction projects exposed to significant and preventable risks. However, despite the growing urgency, such comprehensive work remains absent, leaving a critical gap in the industry's ability to address evolving cyber threats systematically.

2.2. Limited and fragmented studies on construction cybersecurity

In contrast to the well-explored realms of traditional risks, cybersecurity in construction remains a relatively uncharted territory. Pargoo and Ilbeigi (2023) pointed out the deficiency in the field by conducting a scoping review that identified only 45 works related to cybersecurity in construction. A majority of these publications, such as Bello and Maurushat (2020), El-Sayegh et al. (2020), García de Soto et al. (2022a), Mantha and García de Soto (2019) engage in broad discussions, accentuating the necessity for specialized, in-depth research to boost the industry's defense and resilience against cybersecurity threats. However, these discussions often lack actionable insights or practical frameworks tailored to the specific dynamics of construction projects. Additionally, while contributions have been made in areas such as blockchain technology for data decentralization (Parn & Edwards, 2019; Shemov et al., 2020), machine learning algorithms for data-driven anomaly detection (Pan et al., 2019; Parn & Edwards, 2019; Sheikh et al., 2019), threat modeling for attack path simulation and assessment (Mantha et al., 2021; Shibly & García de Soto, 2020), and the use of CVSS scores for assessing stakeholder vulnerabilities (Mantha & García de Soto, 2021), these solutions focus on narrow, technical issues.

Recent works have started to address broader challenges, such as insider threats and multi-stakeholder coordination (Lalropuia et al., 2025), the development of machine learning–centric frameworks for risk assessment (Yao & García De Soto, 2024a, 2024b, 2024c), the role of language models in cybersecurity management (Yao & García De Soto, 2024c), and the organizational factors influencing cybersecurity effectiveness (Badi & Nasaj, 2024). Researchers have also begun to investigate emerging topics like the use of ChatGPT in construction projects and its attendant cybersecurity issues (Sonkor & García De Soto, 2024). While recent advances acknowledge the multifaceted nature of cyber threats, they often address technical or organizational elements in isolation rather than presenting a unified strategy that integrates risk identification, assessment, and response. Yet, developing such a cohesive framework fundamentally depends on the systematic identification of cyber risk factors, a process not realized in current literature. In particular, no comprehensive set of cyber risk factors has been consolidated to reflect the unique vulnerabilities of construction projects, including fluid team dynamics, extensive stakeholder networks, and cross-project interactions. This omission perpetuates the absence of an integrated, end-to-end approach, leaving the industry limited in its ability to conduct truly systematic and holistic cyber risk management.

2.3. Relevant cyber risk assessment studies in construction

One of the purposes of setting risk factors is to provide inputs into the risk assessment model, which is essential for conducting the risk assessment process. Therefore, the literature on cyber risk assessment in construction is further explored to identify any cybersecurity-related risk factors. Within the limited body of research on construction cybersecurity, three studies are related. Mantha and García de Soto (2019) advocated for using agent-based models to understand and quantify stakeholders' vulnerabilities and to simulate their propagation within the complex interactions of communication networks, but the vulnerability score is just based on assumptions, not on the specific risk factors related to the proposed stakeholders, which leads to a lack of granularity and the result of subjectivity. In another work (Mantha & García de Soto, 2021), they applied the CVSS scoring method to provide a systematic way of evaluating the vulnerabilities of stakeholders in construction networks. The CVSS score approach covers Confidentiality, Integrity, and Availability aspects, but the assessment of each aspect is still based on overall judgment and assumptions without any risk factor analysis related to the stakeholders. Shibly and García de Soto (2020) developed attack trees for threat modeling to propagate and calculate the likelihood of the threat. However, their assessment is specifically aimed at an industrial-grade robotic arm system for an offsite 3D printer, not at the project level, and thus lacks generalization ability. In conclusion, while these three studies contribute to the understanding of cyber risk assessment in the construction industry, they each have limitations. None of them provide a comprehensive set of risk factors at the project level that can be both flexibly adapted to various scenarios and generalized across different contexts.

2.4. Insights from broader risk factor identification and methodological approaches

In contrast, the construction industry has seen a comprehensive body of research that addresses a diverse array of other risks. These studies, including investigations into financial risks (Abd El-Karim et al., 2017; Baloi & Price, 2003; Chileshe & Boadua Yirenkyi-Fianko, 2012; Sharma & Goyal, 2022), environmental and safety risks (Aghaei et al., 2022; Hwang et al., 2017), supply chain risks (Rudolf & Spinler, 2018), procurement risks (Chan et al., 2011; Rudolf & Spinler, 2018), technological application risks (Goh et al., 2021; Zou et al., 2007), operational and management risks, time performance risks (Abd El-Karim et al., 2017; Assaf & Al-Hejji, 2006; Gondia et al., 2020), and a combination of these (Jarkas & Haupt, 2015; Sharaf & Abdelwahab, 2015; Renuka et al., 2014; Wuni et al., 2022; Zou et al., 2007; Zou & Zhang, 2009) have each introduced a tailored set of risk factors. These factors are categorized based on specific criteria, aiming not only to enhance the understanding of the associated risks but also to facilitate their effective assessment and management. For instance, Sharma and Goyal (2022) not only identified 55 risk factors related to cost overrun in construction projects but also implemented a fuzzy logic-based assessment to prioritize these risks. Similarly, Hwang et al. (2017) identified 42 risk factors impacting environmental and safety risks in green residential constructions, providing insights specifically tailored to this niche area. Assaf and Al-Hejji (2006) categorized 53 risk factors into groups such as owner-related, consultant-related, and design-related, employing these classifications to predict project delays effectively. Moreover, Zou et al. (2007) documented 85 risk factors in Chinese construction projects, encompassing a wide spectrum including cost, time, quality, and beyond, illustrating the depth and breadth of risk considerations necessary for comprehensive project management.

However, despite this extensive coverage of traditional risks, none of these studies explicitly addresses cyber risk factors. This indicates an urgent need for targeted research that captures the unique vulnerabilities of construction projects in an increasingly digitized environment. That said, the methodologies and categorizations developed in these broader risk studies could help incorporate cybersecurity considerations into general risk management after adaptation. From a methodological standpoint, advanced multi-criteria decision-making (MCDM) approaches under fuzzy environments have proven effective in managing complex risk scenarios in various sectors. In the IT outsourcing domain, for instance, Ebrahimnezhad et al. (2017b) introduced an extended analytical hierarchy process that accommodates incomplete interval-valued data, while Ebrahimnejad et al. (2017a) developed an interval-valued hesitant fuzzy decision method that integrates service costs and risks for prioritizing alternatives. Mousavi and Gitinavard (2019) further contributed by proposing an extended multi-attribute group decision model that integrates multiple criteria into a collective decision-making process. Additionally, Hamzeh et al. (2020) introduced an imprecise earned duration model that incorporates risk considerations directly into project scheduling. Although these sophisticated methodologies demonstrate promise, there is a critical gap in adapting them to systematically identify, categorize, and manage cyber risks within the complex, multi-stakeholder context of construction projects.

2.5. Summary

In summary, although progress has been made in understanding and mitigating various cyber risks in construction, there is still a lack of a complete set of cyber risk factors that reflects the industry's unique vulnerabilities and can be used for thorough risk assessment. This gap demonstrates the necessity for focused research to systematically identify these factors. This study addresses this need by aiming to develop a detailed set of cyber risk factors that cover the multifaceted aspects of construction projects. The novelty of this paper lies in its comprehensive approach to addressing this overlooked area of research, providing a tailored set of cyber risk factors for construction projects at the project level. By bridging this gap, the study contributes to advancing both theoretical understanding and practical applications in cybersecurity for the construction sector.

3. Methodology

This section presents our methodology for identifying cybersecurity risk factors in construction projects. First, we explain the rationale for conceptualizing each project as a network in Section 3.1, drawing on the work of the work of Mantha and García de Soto (2019). This network-based perspective provides the foundation for a seven-step methodology expounded in Section 3.2, which systematically identifies key cyber risk factors in construction projects.

3.1. Project as network

The project structure plays a crucial role in cybersecurity, as it determines the complexity of communication among stakeholders and reveals potential weak points where attacks could occur within a network. Simply put, the organization of a project can indicate its level of security or vulnerability to cyber threats. To represent the project structure effectively, relevant literature on construction projects was reviewed, and the work of (Mantha & García de Soto, 2019) was identified as particularly relevant. In their study, construction projects were modeled using an agent-based model (ABM) network to represent the interactions and relationships among stakeholders. Inspiration was drawn from their network modeling approach, adapting it in this study to simulate and analyze the interactions among stakeholders within a project structure. For a comprehensive understanding of their methodology and findings (please refer to Mantha & García de Soto, 2019).

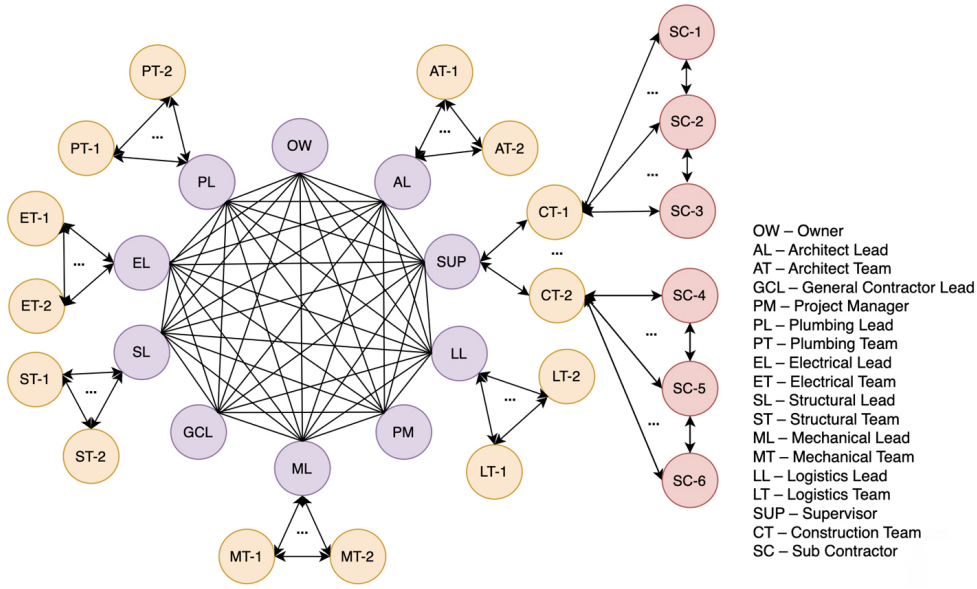

Figure 1. Network graph of a construction project (adapted from Mantha & García de Soto, 2019)

To better explain the project network concept, an Integrated Project Delivery (IPD) project is used as an example and depicted in Figure 1. The figure shows the project structure as a three-ring communication network, where teams (including owners, contractors, subcontractors, and others) are shown as nodes (circles), and their data exchanges via email, messaging, video calls, or project-management software appear as directed edges (arrows). In the innermost ring, Layer 1 represents core leadership and contains 10 teams connected by 90 channels; the middle ring, Layer 2, represents primary delivery partners and comprises 14 sub-teams with 20 channels; and the outer ring, Layer 3, captures specialist subcontractors and suppliers, linking 6 sub-teams through 10 channels. The IPD project's dense interconnections encourage collaboration yet significantly enlarge the attack surface. Each additional channel becomes a potential entry point for malicious actors, and shared data can allow a breach in one team to cascade across the network. These structural characteristics make encrypted communication, continuous monitoring, and tightly defined access controls essential. Asking project managers to create similar network graphs for their own delivery models reveals structural vulnerabilities early and supports proactive cybersecurity planning.

3.2. The 7-step framework

This section outlines the systematic methodology used to identify a comprehensive set of ready-to-use risk factors for construction projects. We employed three key methods including literature review, expert evaluation, and a structured questionnaire survey (Meyer & Reniers, 2022), and ensured reliability and validity through a multi-step process involving iterative refinement. The process, illustrated in Figure 2, was conducted in two primary stages: the initial identification of risk factors through an extensive literature review, followed by refining these factors through expert feedback obtained via questionnaires and consultations. Our approach is aligned with the NIST Cybersecurity Framework (National Institute of Standards and Technology [NIST], 2024), which advocates for a structured and comprehensive methodology to identify, assess, and manage cybersecurity risks. This alignment ensures our study maintains a systematic approach tailored to the complex nature of construction projects. Additionally, principles of the Delphi Method (Galanis, 2018) were integrated by employing iterative rounds of expert consultation and feedback, refining and achieving consensus on the identified risk factors to enhance robustness and credibility. Data collection (outlined in Step 4 of Section 3.2) was carried out using comprehensive questionnaires that incorporated risk factors identified through the literature review, refined further by expert input through structured scoring and iterative consultations. The target population for our study (described in Step 5) consisted of industry experts specializing in both cybersecurity and construction. These experts were carefully selected through purposive sampling based on their extensive experience and relevance to the study topic. The data analysis methods (outlined in Steps 6 and 7) synthesized expert scores and feedback, using a combination of quantitative and qualitative evaluations to refine, validate, and categorize the risk factors.

Step 1. Literature review

The study began with a broad search of the literature covering risk factors in construction projects. Although numerous papers were initially scanned, 18 key publications were ultimately selected for their explicit, relevant insights aligned with the study's objectives, as detailed in Section 2. The remaining unselected works either addressed risk factors in non-construction settings or discussed broader themes without providing actionable, construction-focused considerations. The 18 selected sources offer

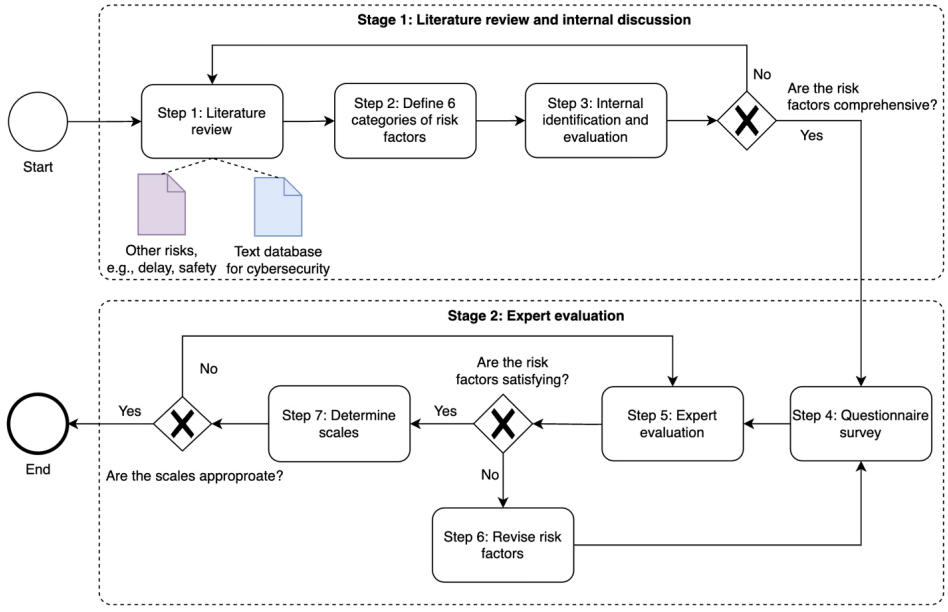

Figure 2. The process of risk factor identification

insights into risk factors related to project delays, supply chain issues, and beyond. Our objective was to extrapolate and adapt pertinent factors that align with the broader scopes of project management and operation for our study. These factors cover a range of aspects, including human and management dynamics, operational elements, external influences, and regulatory frameworks, collectively offering a rich, diversified foundation of insights for our analysis. Additionally, six textual sources concerning cybersecurity in the construction industry were investigated, which were published in our previous work as a database containing a large number of sentences (Yao & García de Soto, 2023). These sources, compiled from six types of construction cybersecurity literature, including news articles and blogs, LexisNexis databases, academic papers, books (chapters), specifications/standards, and company reports, collectively comprise 802 K text sentences. They provide a comprehensive exploration of cybersecurity challenges and risks prevalent in the construction industry.

Step 2. Define risk factor categories

After reviewing the literature, six aspects of a construction project were initially identified, collectively providing a comprehensive view of the cybersecurity landscape. These aspects are expounded as follows:

(1) Basic Information of the Project: This category includes general project information like company size, current project phase, and other foundational details. Understanding these elements is vital as it sets the stage for evaluating the cybersecurity posture of the project.

(2) Project Structure: This refers to the organization and communication patterns of project teams and sub-teams. It's crucial to analyze this structure to comprehend the complexity and connectivity, which, in turn, influences the project's cybersecurity vulnerabilities and strengths.

(3) Cybersecurity Scores: Teams within the project are evaluated and scored based on their cybersecurity status. These scores, while offering insights into each team's cybersecurity posture, collectively provide a comprehensive view of the project's overall cybersecurity health, indicating areas of strength and vulnerability.

(4) Project Context: This category considers elements like governmental regulations and the construction company's financial health, which can externally influence the project. Assessing these factors is vital to understanding the impact of external pressures and resources on the project's cybersecurity resilience.

(5) Information Technology (IT) Factors: This category assesses the project's robustness and cybersecurity awareness from the perspective of information technology, focusing on factors such as the existence of a specialized IT department, the regularity of app updates, etc.

(6) Operational Technology (OT) Factors: This category evaluates the security measures in place for protecting physical and digital assets crucial to the project. Analyzing factors like access control mechanisms and the security of critical digital assets offers insights into the project's operational security and efficiency.

Step 3. Internal identification and evaluation of risk factors

For each category, the literature was recurrently reviewed, referring back to Step 1, to identify as many relevant risk factors as possible with the goal of achieving a compre-

hensive compilation. Simultaneously, regular internal discussions were conducted to assess these factors, totaling ten discussions over one month. In each discussion session, the previously identified risk factors were assessed based on four criteria: (1) their relevance to cybersecurity, (2) their significance in contributing to cyber risk, (3) the ease of understanding for industry professionals, and (4) the simplicity in collecting associated information. These criteria guided the decision on whether to include each factor. If disagreements arose regarding certain risk factors, they were tentatively retained on the list. Later, feedback on these disputed factors was sought from external experts to gain additional insights. Ultimately, a list of 62 preliminary risk factors was compiled, as outlined in Appendix, with 9, 9, 6, 11, 16, and 11 factors allocated to each respective category. Throughout the study, each risk factor is formulated as a question. This approach enhances comprehension when presented to experts and industry practitioners, leading to higher response accuracy. The clarity aids experts in offering insightful feedback and promotes efficient data collection from the industry, particularly when selecting specific scales of risk factors, a process detailed in Step 7.

Step 4. Data collection with questionnaire survey

A detailed questionnaire was developed and presented to experts to gather feedback on the 62 identified cybersecurity risk factors. This questionnaire served as the primary data collection method, designed to ensure a comprehensive gathering of expert insights and feedback. It is meticulously structured as follows:

- The basic information of the expert, including name, email, position/title.
- An executive summary of around 400 words provides background information, making it easy for company practitioners to understand our goals and objectives.
- The body is divided into six sections, each representing a specific category of risk factors, accompanied by an explanation of that category.
- Under each section are the corresponding risk factors initially identified (totaling 62), each accompanied by a definition, an in-depth definition, and an explanation of its potential impact on project cybersecurity. For clarity, textual descriptions, illustrative graphics, or mathematical derivations were included where applicable.
- Each risk factor is followed by a multiple-choice scoring question, with options ranging from 1 to 5 (five levels). A level of 5 indicates the expert's perception that it is highly reasonable to include this risk factor in the cybersecurity evaluation.

Step 5. Expert evaluation

The questionnaire with 62 risk factors was presented to three experts, purposively selected based on qualifications including substantial industry experience, senior-level roles, and proven expertise in cybersecurity or construction:

- Cybersecurity Experts. Two of these experts specialize in cybersecurity and are affiliated with a New York-based cybersecurity company, each bringing over 20 years of industry experience. This firm's focus on evaluating and monitoring organizational security postures offered deep, data-driven insights into the viability of each risk factor from a cybersecurity standpoint. Both experts scored each factor on a 1–5 scoring system and provided qualitative feedback during online meetings and email exchanges, ensuring a comprehensive review of technical and operational feasibility.
- Construction Expert. The third expert specializes in construction and works at a leading construction company in the Middle East, with over 8 years of experience. This UAE-based company has delivered complex, multi-sector projects (airports, retail, hospitality, high-rise buildings, themed developments) across regions such as Saudi Arabia, Ethiopia, and Oman. The expert evaluated each factor for practical applicability and clarity within typical construction workflows, also providing a 1–5 rating to reflect its relevance and providing qualitative feedback. Communication occurred primarily through email and phone calls, capturing critical industry-specific considerations like project phasing, sub-team structures, and resource constraints.

By ensuring both cybersecurity and construction professionals from different regions were included, we aimed to achieve diversity in industry representation and geographical context. All experts' feedback was equally weighted: their 1–5 ratings were averaged, and factors scoring below 3 were revised or removed. This balanced approach allowed us to integrate technical rigor with on-the-ground realities. Table 2 summarizes the experts' profiles and the collaborative five-month review process, which involved online meetings, emails, and phone calls. Recordings and correspondences were retained (with permission) to ensure transparency throughout iterative risk factor revisions. In subsequent communications, after finalizing the risk factors, all three experts provided feedback on the scale design of these factors, as detailed in Step 7.

Step 6. Revise risk factors

The finalization of risk factors follows an iterative, staged process grounded in the Delphi method (Galanis, 2018), which is designed to systematically collect and refine expert opinions. This approach is closely linked to step 5 of our methodology. After collecting scores and initial feedback, adjustments were made to the risk factors in the questionnaire, including their explanation, scope, and the time span certain risk factors cover, among other aspects. Transparency was prioritized by documenting every significant change and ensuring each adjustment aligned with feedback from field experts. Our data analysis method involved a combination of quantitative and qualitative analysis, synthesizing expert scores to determine the average ratings for each factor and using qualitative expert feedback to guide iterative refinements. The iterative refinement process involved evaluating each piece of feedback

Table 2. Overview of expert information and collaborative process

No.	Expertise	Position Level	Affiliation	Location	Years of Experience	Communication Method	Tasks and Feedback	Quantity
1	Cybersecurity	Senior	A cybersecurity scoring company	New York, U.S.	30+	Online ZOOM meetings & Email	Score and provide feedback on risk factors and their scales	■ 12 meetings ■ 60 emails ■ 2 phone calls
2	Cybersecurity	Senior	A cybersecurity scoring company	New York, U.S.	10+	Online ZOOM meetings & Email		
3	Construction	Senior	A construction company	Dubai, UAE	8+	Email and phone calls	Provide feedback on risk factors and their scales	

based on its significance, feasibility, and relevance to project objectives. Modifications were made following multiple rounds of discussions with experts to ensure that each change was practical and data-driven.

Consultations with experts were conducted at each stage to confirm the appropriateness of existing risk factors and to add new ones, if recommended. This feedback-driven, evidence-based approach enabled us to systematically incorporate expert insights and refine the decision-making process. After final discussions, any risk factor with an average score below 3 was removed, as this threshold was chosen to ensure that only those factors deemed at least moderately significant by expert consensus would be retained in the analysis. A notable example is the unanimous recommendation by all experts to eliminate the "Cybersecurity Scores" category whose average was below 3 due to the inherent difficulties in quantifying such metrics within the study's context.

Appendix consolidates the average scores of the original risk factors alongside the experts' recommended actions. The table includes the initial numbering of each risk factor, a summary of expert feedback, the action taken, and a newly assigned number for any retained factors. For instance, for Risk Factor 1.5, "What is the total number of people involved in the project?", the experts suggested excluding all individuals not directly involved in cyber risk assessment, since labor does not necessarily increase vulnerabilities. Instead, the focus should be on those with access to critical systems and data rather than the entire project personnel. The average score for this factor is 4, thus it has been retained and revised to "What is the total number of people involved in the project (labor excluded)?".

Step 7. Determine the scales of risk factors

In risk assessment, a quantitative approach is often preferred over a qualitative one, as it yields more numerically based and, thus, objective results. However, this approach requires quantified or fine-grained risk factor inputs, an element often missing in existing literature, including (Gondia et al., 2020; Mantha & García de Soto, 2019, 2021; Shibly & García de Soto, 2020). As an illustration, in the study of predicting project delay risk (Gondia et al., 2020), the authors subjectively classify risk factors as high or low risk without offering numerically-based or substantial evidence to back their classifications. Our study aims to take a more numerical approach by incorporating risk factor scales (Assaf & Al-Hejji, 2006), where each risk factor is categorized into distinct levels, categories, or numerical values, paving the way for more quantitative future risk assessments. For instance, risk factor 1.3 – the percentage of the total project budget for cybersecurity management – can be divided into six scales: <= 1%, 1%–2%, 2%–3%, 3%–4%, 4%–5%, > 5%. Similarly, risk factor 1.4 – the project duration – can be divided into five distinct time intervals: <= 3, 3–6, 6–12, 12–24, and > 24 months.

The scales for each risk factor were initially proposed using our team's domain knowledge and an extensive review of construction-related literature. To ensure a more systematic and objective approach, these preliminary scales were then embedded into the final questionnaire and shared with our panel of experts (see Step 4). Their feedback informed an iterative refinement procedure, in which each expert provided detailed comments on the clarity, practicality, and representativeness of the proposed intervals. After each consultation round, we systematically documented suggested amendments ranging from minor adjustments in the boundary values to more substantial changes in how a factor was represented (e.g., discrete levels vs. continuous numerical ranges). We reconvened with the experts to discuss points of divergence and consolidate a consensus on final thresholds. Throughout this process, objective criteria (such as alignment with industry standards, data availability, and ease of measurement) guided the acceptance or rejection of each proposed modification. This consensus-building approach, anchored in documented evidence and multiple feedback loops, ensured that every scale accurately mirrors field realities without sacrificing interpretability. The outcome is a set of refined scales presented in Tables 4–8, which strike a careful balance between the granularity required for effective analysis and the practicality needed for implementation.

4. Results

After completing the methodological steps outlined in Section 3.2, a final set of 32 risk factors was identified, which have been re-categorized into 5 aspects: (1) Overall information of the project; (2) Project structure; (3) IT factors; (4) OT factors; (5) Management and human factors. This new categorization minimizes overlap among distinct categories while ensuring comprehensive coverage of construction project characteristics. The finalized set of risk factors is listed in Tables 4–8, with counts of 7, 4, 9, 5, and 7, respectively. Importantly, Categories 3, 4, and 5 are tai-

lored to evaluate a specific company and the project phase it is involved in, necessitating the consideration of its subteams. This led us to assign risk factors 3.1 and 3.2 to Category 3, even though they were initially intended for Category 1. This strategic reclassification aids companies engaged in future data collection to comprehend that these two factors, and the ones following, are aimed at assessing the distinct phase their company is involved in, ensuring targeted and relevant responses. Tables 3–7 display the finalized risk factors along with their original numbering from the initial version. Additionally, each risk factor includes a hypothetical real-world example to make it more accessible and understandable to practitioners.

Table 3. Category 1: Overall project information

No.	Risk factor	Explanation	Hypothetical Example of Real-World Manifestation	Scales	Previous No.
1.1	What is the country of the project?	This identifies the specific country where the primary construction activities take place, as different countries have varying regulations, standards, and cybersecurity implications that can impact project operations.	In regions with strict data sovereignty laws, all project data must be stored locally and encrypted to comply with national regulations. A multinational firm building a facility in Country X had to overhaul its data storage architecture, delaying the project's timeline.	Asia, Europe, Africa, North America, South America, Antarctica, and Oceania. Information about the country was initially requested, and the continent was then derived from it.	1.9
1.2	What is the project budget?	Refers to the total approved financial allocation for the project, which can influence decisions, risk management strategies, and resource availability throughout the project lifecycle.	A large commercial complex faced cost overruns and cut its cybersecurity training program, leaving systems more susceptible to phishing attacks. Months later, a ransomware incident occurred, halting critical design communications.	<= $100,000, $ 100,000–$ 500,000, $ 500,000–$ 1 million, $ 1 million–$ 5 million, > $5 million	Newly added
1.3	What is the percentage of the total project budget for cybersecurity management?	Measures the proportion of the project's overall budget that is specifically allocated to managing cybersecurity, covering areas such as technology, staffing, and risk mitigation strategies.	A billion-dollar highway project allotted less than 1% to cybersecurity, resulting in inadequate monitoring tools and a major security breach. Attackers then accessed proprietary construction schedules and caused significant delays.	<= 1%, 1%–2%, 2%–3%, 3%–4%, 4%–5%, > 5%	4.4
1.4	What is the project duration?	Represents the total timeframe from the start to the completion of the project, and it can include planned, adjusted, or actual durations, impacting resource allocation, scheduling, and risk exposure.	A multi-year rail infrastructure project encountered evolving cyber threats, requiring extra security upgrades mid-project. Because the timeline was extended, newly introduced collaborative tools became a fresh target for attackers.	<= 3 months, 3–6 months, 6–12 months, 12–24 months, > 24 months	Newly added
1.5	What is the total number of people involved in the project (labor excluded)?	Considers the total number of personnel, excluding on-site labor, who are directly involved in managing and executing the project, including roles such as management, technical staff, and consultants.	A hospital expansion with a large management team struggled with inconsistent cybersecurity practices. Confusion around role-based access controls led to unauthorized file sharing, ultimately exposing sensitive building specifications.	<= 50, 51–100, 101–200, 201–300, 301–400, > 400	1.5
1.6	What is the project type?	Identifies the specific category or nature of the construction project, which may determine its scope, complexity, and applicable risk factors.	A high-security military facility build demanded stringent encryption and background checks. In contrast, a private residential project had fewer controls but was targeted by social engineers posing as subcontractors due to lax verification procedures.	Transportation Infrastructure Projects, Government Projects, Healthcare Projects, Large-Scale Commercial Projects, Residential Projects, Other types	Newly added
1.7	Whether there is a dedicated cybersecurity legal team for the project?	Specifies whether there is a legal team focused solely on managing and addressing cybersecurity-related legal matters for the project, either through in-house resources or external consultants.	When a major contractor suffered a data breach, its in-house legal cybersecurity team swiftly navigated reporting obligations and regulatory inquiries. Without that specialized team, the breach response would have been delayed, incurring additional fines and reputational damage.	Yes, No, Unsure	4.2

Table 4. Category 2: Project structure

No.	Risk factor	Explanation	Hypothetical Example of Real-World Manifestation	Scales	Previous No.
2.1	What is the project delivery method?	Refers to the specific approach used for delivering the project, which outlines the contractual relationships and workflow between involved parties, impacting coordination, risk management, and project execution.	An Integrated Project Delivery (IPD) approach allowed real-time data sharing among architects, engineers, and contractors. However, it also gave a subcontractor unauthorized visibility into sensitive designs due to poor segregation protocols.	Design-Bid-Build (DBB), Design-Build (DB), Construction Manager at Risk (CMAR), Construction Management Multi-Prime (CMMP), Public-Private Partnership (PPP or P3), Integrated Project Delivery (IPD), Design/Build/Operate/Maintain (DBOM), Other types	2.1
2.2	What is the number of sub-teams at different layers of the project?	Considers the number of sub-teams working within various levels or functional layers of the project, reflecting the organizational structure and distribution of tasks and responsibilities.	A hospital construction involved multiple layers of subcontractors, from medical device installers to HVAC specialists. Poor coordination of security roles across these teams led to accidental exposure of confidential blueprints on a publicly accessible server.	Eight layers, each layer's choices are: <= 10, 11–20, 21–30, 31–40, > 40, N/A ("N/A" means this layer is not existent)	2.2
2.3	What is the number of communication channels at different layers in the project?	Represents the number of established communication channels, such as mobile devices, PCs, tablets, and software platforms like email and messaging apps, used at different levels within the project. This indicates the complexity and flow of information among project stakeholders, impacting communication efficiency and coordination.	A project used multiple platforms including email, mobile apps, and cloud drives, where each channel had different encryption standards. Attackers exploited the least-secure channel (a free file-sharing app) to infiltrate the entire network.	Eight layers, each layer's choices are: <= 50, <= 100, <= 150, <= 200, < 250, <= 300, > 300, N/A ("N/A" means this layer is not existent)	2.4
2.4	What is the percentage of teams overlapping in different projects?	Measures the proportion of teams that are concurrently involved in multiple projects, highlighting the extent of resource sharing and potential implications for project focus and capacity.	A contractor simultaneously worked on a government data center and a corporate office build, reusing staff across both projects. One employee mistakenly shared classified blueprints from the government job on the corporate project's shared drive, leading to a confidentiality breach.	<= 20%, 21%–40%, 41%–60%, 61%–80%, 81%–100%	4.9

Table 5. Category 3: IT factors

No.	Risk factor	Explanation	Hypothetical Example of Real-World Manifestation	Scales	Previous No.
3.1	What is the scale of your company?	Describes the size or scale of your company based solely on the number of full-time employees, which can influence the company's capacity and approach to risk management.	A small family-run firm lacked any dedicated IT security team, leaving it vulnerable to a simple phishing attack that compromised sensitive documents for months before discovery.	Five choices: <= 30, 31–60, 61–100, 101–150, > 150	1.2
3.2	What is the phase of the construction project when your company is involved?	Indicates the specific phase of the construction project when your company is involved, such as design, construction, or other stages, which can shape project scope and risk exposure.	An engineering consultant joined a build during final commissioning and found that critical cybersecurity measures (like network segmentation) were overlooked in earlier phases, making remediation costly and time-consuming.	Planning and Bidding phase, Design phase, Construction phase, Maintenance & Operation phase, Demolition phase	1.3

End of Table 5

No.	Risk factor	Explanation	Hypothetical Example of Real-World Manifestation	Scales	Previous No.
3.3	Is there a dedicated IT team for the project?	Identifies whether there is a dedicated IT team specifically assigned to manage and support the project's technological and cybersecurity needs.	A skyscraper project without an on-site IT team faced repeated malware intrusions on contractor laptops. Response times were slow, allowing malicious software to spread to project scheduling systems.	Yes, No, Unsure	5.8
3.4	What is the total number of critical digital assets?	Refers to the total number of critical digital assets associated with the project, including essential data, systems, hardware, software or resources that require protection from cyber threats.	In constructing a new airport terminal, the unprotected Building Information Modeling (BIM) system was deemed critical only after hackers exfiltrated partial design data. This oversight forced an emergency security upgrade mid-project.	<= 50, 51–200, 201–400, 401–600, > 600	6.1
3.5	What is the total number of user endpoints of digital devices for the project?	Specifies the total count of user endpoints, such as computers, smartphones, and tablets, that are connected to and used within the project.	Contractors frequently used personal smartphones for daily logs, introducing vulnerabilities. An infected phone passed malware into the main project network, halting operations for days.	<= 50, 51–200, 201–400, 401–600, > 600	5.2
3.6	What is the percentage of digital devices with firewalls or intrusion detection systems involved in the project?	Measures the proportion of digital devices within the project that are equipped with firewalls or intrusion detection systems to provide cybersecurity protection.	A commercial complex project found that half of their servers lacked updated firewall rules, enabling attackers to pivot across the internal network and access sensitive contract documents unnoticed.	<= 20%, 21%–40%, 41%–60%, 61%–80%, 81%–100%	6.5
3.7	What is the network type used for the project: Public or Private?	Indicates whether the network used for project-related activities is a public or private network, which impacts security measures and data access.	At a remote construction site relying on public Wi-Fi, attackers intercepted unencrypted data transmissions, exposing confidential project schedules and budgets.	Public network, Private network, Both public and private network	6.4
3.8	What is the percentage of individuals who fail phishing tests after completing mandatory training?	Represents the percentage of individuals who fail phishing tests after undergoing mandatory cybersecurity training, reflecting the effectiveness of the training.	Despite mandatory cybersecurity training, a new intern inadvertently clicked a phishing link, compromising the file server. The incident underscored the need for continuous, scenario-based training.	<= 20%, 21%–40%, 41%–60%, 61%–80%, 81%–100%	5.12
3.9	What is the estimated Mean Time to Respond (MTTR) in hours?	Specifies the estimated Mean Time to Respond (MTTR) to cybersecurity incidents, expressed in hours, representing the average time taken to detect, contain, and resolve issues.	A hotel construction project took over 48 hours to detect and contain a ransomware attack, causing extended downtime for critical design management software and inflating project costs.	Within 1 hour, 1–4 hours, 4–8 hours, 8–24 hours, Above 24 hours	5.15

Table 6. Category 4: OT factors

No.	Risk factor	Explanation	Hypothetical Example of Real-World Manifestation	Scales	Previous No.
4.1	What is the total number of important OT equipment involved?	Refers to the total number of important OT equipment used in the project, which may include machines, control systems, and other critical assets requiring protection and management.	In a water treatment plant expansion, outdated SCADA systems lacked basic security patches, allowing hackers potential control over valve operations.	<= 30, 31–60, 61–90, 91–120, 121–150, > 150	6.2
4.2	What is the level of physical access control mechanism to OT equipment?	Indicates the strength or comprehensiveness of the physical access control mechanisms in place to secure access to OT equipment, such as locks, security systems, or personnel protocols.	A substation upgrade failed to enforce badge-only entry to critical control rooms, enabling a disgruntled staff member to tamper with machinery without detection.	Level 1, Level 2, Level 3, Level 4, Level 5	6.7
4.3	What is the percentage of OT equipment isolated from the project's general network?	Measures the proportion of OT equipment that is segregated or isolated from the general project network, which can reduce exposure to cyber risks and external threats.	A manufacturing facility project segmented its OT network from the internet, thwarting a ransomware worm that had infiltrated its corporate IT environment.	<= 20%, 21%–40%, 41%–60%, 61%–80%, 81%–100%	6.11
4.4	What is the average age of the important OT equipment, in years?	Specifies the average age, in years, of important OT equipment, as older equipment may present different risk profiles and require specialized maintenance and security measures.	A dam construction project used 20-year-old turbines that were incompatible with modern security patches, prompting the need for a costly custom firewall solution to avoid a complete equipment overhaul.	<= 1, 1–3, 4–7, 8–10, > 10	6.3
4.5	What is the level of authentication mechanism to access the HMI (Human Machine Interface)?	Evaluates the robustness of authentication mechanisms used to access the HMI, which serves as the interface connecting operators to machinery or control systems. Stronger measures, such as multi-factor or biometric authentication, enhance security, restrict access to authorized personnel, and protect the integrity and safety of critical processes.	A new production line had only basic password logins for its control interface, allowing a former employee to gain remote access and alter operational settings, causing production delays.	Level 1, Level 2, Level 3, Level 4, Level 5	6.9

Table 7. Category 5: Management and human factors

No.	Risk factor	Explanation	Hypothetical Example of Real-World Manifestation	Scales	Previous No.
5.1	What is the average level of commitment to corporate governance, ethical practices and cybersecurity policy?	Reflects the overall level of adherence and commitment by the organization to corporate governance, ethical practices, and established cybersecurity policies, impacting the project's risk culture and compliance standards.	An underfunded contractor cut corners on cybersecurity policies; a later data breach revealed that employees shared passwords openly and no one was held accountable for repeated violations.	Level 1, Level 2, Level 3, Level 4, Level 5	4.3
5.2	What is the average frequency of security training per year?	Indicates how often security training sessions are conducted for project stakeholders over the course of a year, affecting awareness, knowledge, and responsiveness to cyber threats.	After implementing monthly interactive security workshops, a complex stadium renovation saw a significant drop in phishing incidents and unauthorized USB device usage on site.	<= 10, 11–20, 21–30, 31–40, 41–50, > 50	5.11
5.3	Do you allow password reuse for any project-related software, systems, or accounts (e.g., project management tools, email, internal networks, file storage, etc.)?	Determines whether project-related software, systems, or accounts permit the reuse of passwords, which can impact security protocols and the potential for breaches.	A multinational developer let teams reuse passwords across multiple cloud services. When one set of credentials was compromised, attackers immediately accessed contract management portals, delaying contract sign-offs.	Yes, No	5.13

End of Table 7

No.	Risk factor	Explanation	Hypothetical Example of Real-World Manifestation	Scales	Previous No.
5.4	Does internet access within your construction project require Multi-Factor Authentication (MFA) or utilize other methods such as biometrics or face recognition?	Specifies whether internet access within the construction project employs MFA or advanced security methods like biometrics or facial recognition to enhance access control.	A university expansion project required MFA for accessing design software remotely, preventing unauthorized logins even after a staffer's password was exposed on a phishing site.	Yes, No	6.8
5.5	What is the percentage of people who have access to sensitive information in the project?	Measures the proportion of individuals within the project who have access to sensitive information, highlighting potential exposure and data security considerations.	At a high-security data center project, nearly all project participants had admin-level file privileges, resulting in a near-breach when one user's account was hijacked via a spear-phishing attack.	<= 10%, 11%–30%, 31%–50%, 51%–70%, 71%–90%, 91%–100%	1.6
5.6	What is the average team member variability over a 3-month period?	Represents the average degree of change or turnover in team membership over a three-month period, indicating workforce stability and its impact on continuity and project risks.	Rapid turnover in a mega-mall construction project caused delays in revoking old user accounts. A former subcontractor retained access to shared drives for months, unnoticed, downloading confidential design revisions.	<= 20%, 20%–40%, 40%–60%, 60%–80%, 80%–100%	4.10
5.7	What is the average socioeconomic level of the people involved in the project?	Describes the average socioeconomic level of individuals involved in the project, referring to their economic status, educational background, and job roles. This can influence project dynamics, risk exposure, and security practices by shaping access to resources, familiarity with cybersecurity measures, and overall engagement based on their social and economic contexts.	A rural project hired community members unfamiliar with cybersecurity basics, leading to repeated accidental disclosures of internal documents via unsecure messaging apps. Management introduced tailored, on-site cybersecurity briefings to mitigate risks.	Level 1, Level 2, Level 3, Level 4, Level 5	4.7

5. Analyses and discussions

This section discusses the critical cybersecurity risk factors impacting construction projects, categorized to provide a clearer explanation and understanding of these factors and their actual impacts. Additionally, the potential advantages of these risk factors for future cyber risk assessment models are discussed. Recommendations are offered to stakeholders, including project managers, IT teams, construction companies, and regulatory bodies, to enhance cybersecurity resilience. Lastly, limitations and directions for future work are outlined.

5.1. Implications of the identified risk factors

5.1.1. Category (1): Overall information of the project

This category (Table 3) encompasses seven factors that offer a comprehensive outlook on the project's foundational elements. They collectively give insights into the project's environmental, financial, temporal, and human aspects, along with legal considerations, setting the context for a tailored cyber risk assessment. It is recommended to involve a project manager familiar with the overall project to provide the necessary data.

The foundational elements of a construction project significantly shape its cybersecurity landscape. Geographical location (Risk Factor 1.1) determines the regulatory compliance requirements and influences the threat environment, necessitating region-specific security strategies. Project budget (Risk Factor 1.2) and the percentage allocated to cybersecurity (Risk Factor 1.3) directly affect the resources available for implementing solid security measures. Limited budgets may constrain investments in advanced IT infrastructure, security technologies, and skilled personnel, increasing vulnerability to cyberattacks. Project duration (Risk Factor 1.4) impacts the continuity and adaptability of cybersecurity defenses; longer projects require sustained vigilance and regular updates to security protocols to counter evolving threats. The number of people involved (Risk Factor 1.5) introduces more potential access points and the risk of insider threats, necessitating comprehensive access controls and continuous cybersecurity training. Project type (Risk Factor 1.6) influences the specific cybersecurity challenges and regulatory obligations, as different project categories (e.g., infrastructure vs. residential) have unique security needs. Lastly, having a dedicated cybersecurity legal team (Risk Factor 1.7) ensures that legal and regulatory aspects of cybersecurity

are adequately addressed, reducing the risk of non-compliance and enhancing the project's ability to respond to legal challenges arising from cyber incidents. Collectively, these factors demonstrate the importance of integrating cybersecurity considerations into the early stages of project planning and budgeting (Deloitte, 2022; García de Soto et al., 2022b).

5.1.2. Category (2): Project structure

Four factors in this category (Table 4) provide an overview of the project's organizational and communication architecture. They highlight the structural complexity and interconnectedness that could influence the project's vulnerability to cyber threats. A network graph, similar to Figure 1, can be drawn to visually depict these relationships, aiding in comprehending the risk factors and deriving needed statistical figures. It is recommended to involve a project manager familiar with the overall project to help with data collection.

The organizational and communication architecture of a construction project plays a vital role in its cybersecurity posture. The project delivery method (Risk Factor 2.1) determines the level of collaboration and information sharing among stakeholders, which can either enhance or compromise data security. For instance, methods like Integrated Project Delivery (IPD) involve higher levels of information exchange, increasing the need for stringent security protocols. The number of sub-teams at different layers (Risk Factor 2.2) affects the distribution of cybersecurity responsibilities and the consistency of security practices across the project. A higher number of sub-teams can lead to fragmented security measures, making it harder to maintain uniform protection standards. Additionally, the number of communication channels (Risk Factor 2.3) correlates with the complexity of information flow; more channels can create additional vulnerabilities and require strong encryption and monitoring to prevent data breaches. The percentage of teams overlapping in different projects (Risk Factor 2.4) introduces risks related to resource sharing and information leakage between projects. Overlapping teams may inadvertently compromise the security of multiple projects if not properly managed, highlighting the need for clear boundaries and dedicated cybersecurity protocols for each project. Overall, the project structure must be meticulously designed to minimize vulnerabilities and ensure cohesive cybersecurity management across all organizational layers (Mantha & García de Soto, 2019, 2021).

5.1.3. Category (3): IT factors

Nine elements in this category (Table 5) explore the company's IT infrastructure and behaviors, highlighting the integral role of IT in managing cybersecurity. These factors are crucial as they can reflect specific IT vulnerabilities of this company, enabling targeted defense strategies. By evaluating IT factors and forming dedicated mitigation strategies, companies can enhance cyber resilience, ensuring project security against evolving cyber threats, making them essential for informed cybersecurity planning. It is recommended to involve both the project manager of this company and an IT professional to help with data collection.

IT infrastructure is the backbone of modern construction projects, and its security is paramount. The scale of the company (Risk Factor 3.1) influences the capacity to deploy comprehensive cybersecurity measures; larger companies may have more resources but also attract more sophisticated attacks, while smaller companies might struggle with limited cybersecurity expertise and budgets. The phase of the construction project when the company is involved (Risk Factor 3.2) affects the type of cybersecurity measures needed; different phases, such as design or construction, have distinct data protection and system security requirements. Having a dedicated IT team (Risk Factor 3.3) enhances the project's ability to respond swiftly to cyber threats, whereas the absence of such a team can lead to delayed incident responses and increased vulnerability. The total number of critical digital assets (Risk Factor 3.4) and user endpoints (Risk Factor 3.5) expand the potential attack surface, necessitating solid asset management and endpoint security solutions to protect sensitive data and systems. The percentage of digital devices with firewalls or intrusion detection systems (Risk Factor 3.6) indicates the depth of defensive measures in place; higher percentages correlate with stronger protection against unauthorized access and cyber threats. The network type (Risk Factor 3.7) determines the baseline security controls required, with private networks typically offering better security than public ones. Phishing test failure rates (Risk Factor 3.8) reflect the effectiveness of cybersecurity training and the human element in security breaches, highlighting the need for ongoing education and awareness programs. Finally, the Mean Time to Respond (MTTR) (Risk Factor 3.9) measures the project's resilience in handling cyber incidents; shorter MTTRs signify a more agile and prepared cybersecurity team capable of minimizing damage from breaches. Together, these IT factors delineate the technical and operational capabilities essential for maintaining a secure and resilient construction project environment (Bello & Maurushat, 2020; NIST, 2024).

5.1.4. Category (4): OT factors

This category (Table 6), containing five factors, centers on the project's operational technology. It looks at the equipment and systems important for managing physical processes, underscoring their vulnerability and the essentialness of strategic measures to enhance security and prevent unauthorized access. Important OT equipment in construction includes Industrial Control Systems (ICS); Programmable Logic Controllers (PLCs); Human-Machine Interfaces (HMIs); sensors and actuators; communication networks and specific protocols; Building Management Systems (BMS); access control, security systems such as surveillance cameras and intrusion detection systems; en-

vironmental monitoring systems; control panels and field devices; SCADA systems; and remote monitoring and control systems (Sonkor & García de Soto, 2021). It is recommended to involve a manager well-acquainted with the company and deeply involved in the project during this phase to help with data collection.

OT systems are integral to managing the physical processes in construction projects, and their security is critical to preventing operational disruptions. The total number of important OT equipment (Risk Factor 4.1) directly correlates with the potential attack surface; more OT devices mean more points that need to be secured against cyber intrusions. The level of physical access control mechanisms (Risk Factor 4.2) to OT equipment determines how well unauthorized physical access is prevented, which is essential for safeguarding sensitive systems from tampering or sabotage. The percentage of OT equipment isolated from the project's general network (Risk Factor 4.3) enhances security by limiting the exposure of critical systems to broader network vulnerabilities, thereby containing potential threats within segmented environments. The average age of important OT equipment (Risk Factor 4.4) affects security as older devices may lack modern security features and are more susceptible to exploitation due to outdated software and hardware vulnerabilities. Finally, the level of authentication mechanisms to access the Human-Machine Interface (HMI) (Risk Factor 4.5) is crucial for ensuring that only authorized personnel can interact with critical control systems, thereby preventing unauthorized modifications and maintaining system integrity. These OT factors collectively highlight the need for comprehensive security strategies that protect both the digital and physical aspects of construction project operations, ensuring uninterrupted and secure project execution (Sonkor & García de Soto, 2021).

5.1.5. Category (5): Management and human factors

Seven factors in this category (Table 7) explore the company's governance, ethical standards, and cybersecurity culture. It shows the vital role of human elements and management practices in bolstering the project's overall cybersecurity posture, emphasizing a holistic approach that combines technology and human effort. It is recommended to involve a manager well-acquainted with the company and deeply involved in the project during this phase to help with data collection.

The governance, ethical standards, and human elements within a construction project profoundly influence its cybersecurity effectiveness. The average level of commitment to corporate governance, ethical practices, and cybersecurity policy (Risk Factor 5.1) sets the tone for the entire project's security culture; high commitment levels foster a proactive approach to cybersecurity, ensuring that policies are strictly followed and integrated into daily operations. The average frequency of security training per year (Risk Factor 5.2) affects the overall cybersecurity awareness and preparedness of the project team; frequent training helps keep security practices top-of-mind and equips team members with the latest knowledge to counter emerging threats. Allowing or disallowing password reuse (Risk Factor 5.3) has direct implications for password security; prohibiting reuse reduces the risk of credential-based breaches by ensuring that compromised passwords do not provide access to multiple systems. The implementation of Multi-Factor Authentication (MFA) or other advanced authentication methods (Risk Factor 5.4) significantly strengthens access controls, making unauthorized access more difficult and enhancing overall security. The percentage of people who have access to sensitive information (Risk Factor 5.5) must be carefully managed to minimize the risk of data breaches and insider threats; stricter access controls ensure that only authorized personnel can view or manipulate sensitive data. Team member variability over a 3-month period (Risk Factor 5.6) impacts cybersecurity continuity; high turnover can lead to knowledge gaps and inconsistencies in security practices, necessitating reliable onboarding and offboarding procedures. Lastly, the average socioeconomic level of the people involved in the project (Risk Factor 5.7) can influence cybersecurity behaviors and attitudes; understanding the socioeconomic backgrounds of team members can help tailor training and support to address varying levels of cybersecurity awareness and competency. Collectively, these management and human factors emphasize the importance of fostering a strong security culture, ensuring continuous education, and implementing reliable access and identity management practices to safeguard the project against both external and internal cyber threats (García de Soto et al., 2022b; Pargoo & Ilbeigi, 2023).

5.2. Potential advantages for future risk models

The established set of risk factors presents four potential advantages that could enhance future cyber risk assessment models, as outlined below:

(1) Capturing project structure dynamics. This study adopts a view of the project as a multi-layered network to provide a detailed understanding of its complex structure and associated cybersecurity vulnerabilities. Each layer comprises various teams, sub-teams, and communication channels. Based on this perspective, specific risk factors in Category 2 were identified, capturing statistical features related to the spread of sub-teams and communication channels within the project's layered network. This detailed, layer-specific information could enhance future risk assessment models by better representing the dynamic and complex nature of modern construction projects. Incorporating this structural information may improve the accuracy and reliability of risk predictions, addressing gaps in existing studies, such as those noted by Shibly and García de Soto (2020), which do not fully consider a project's layered structure in risk assessments.

(2) Enhancing specificity with contextual insight. Risk factors in Categories 1 and 2 provide a broad overview of the project, capturing general information to establish a foundational context for risk assessment models. Meanwhile, risk factors in Categories 3, 4, and 5 are derived from specific project phases, with data sourced directly from the involved companies, offering phase-specific detail. This integration of broad contextual data and phase-specific insights has the potential to enhance the model's ability to make more granular risk predictions tailored to a company's specific project phase while preserving the overall project context. Such an approach may contribute to risk predictions that are both comprehensive and applicable across distinct project phases, offering potential advancements in cyber risk assessment.

(3) Enabling a more quantitative risk assessment. Many works, including Gondia et al. (2020), Kalinin et al. (2021), Mantha and García de Soto (2019), mainly used qualitative analysis for risk assessment, where expert opinions and subjective judgments determined whether a risk factor, a stakeholder, or a system was considered risky without a concrete numerical standard for reference. Our study allows for more quantitative risk assessments by segmenting each risk factor into distinct scales and requiring data collection before determining the risk status. For example, Risk Factor 4.3 – the percentage of OT equipment isolated from the general network – is divided into five scales: <= 20%, 21%–40%, 41%–60%, 61%–80%, and 81%–100%. After data about OT equipment isolation is collected, it is compared with the predefined scales to determine the risk status of the risk factor, eliminating ambiguity and subjectivity as these scales have been vetted and validated. Although the interpretation of these scales is still influenced by the risk analyzer's criteria, establishing these criteria beforehand ensures that the numerical values-based assessments are more objective. This approach augments the consistency and comparability of risk evaluations across various contexts.

(4) Addressing unique industry vulnerabilities. Alongside risk factors that address general vulnerabilities, some are specifically aligned with the distinct challenges faced by the construction industry, as described in Section 2. These correlations are detailed in Table 8, which explains how these risk factors may be effective. By incorporating a diverse set of risk factors, this approach aims to balance general cybersecurity concerns with the unique challenges specific to the construction sector.

5.3. Scenario-based cyber risk mitigation

Building on the 32 identified risk factors, practical scenario-based analyses can illustrate how construction projects may effectively address and mitigate cyber threats. For example, consider a large infrastructure project utilizing Integrated Project Delivery (IPD). In a phishing-attack scenario, multiple sub-teams could be targeted, with compromised credentials spreading laterally if mandatory user training (Risk Factor 5.2) and well-built password policies (5.3) are insufficient. Integrating these risk factors into project protocols would underline the need for active monitoring, multi-factor authentication (5.4), and thorough oversight of privileged access to prevent widespread credential misuse. A different scenario emphasizes the significance of OT vulnerability. When aging OT equipment (4.4) operates without frequent patching or isolation (4.3), malicious actors may exploit such gaps to disrupt control systems or steal sensitive data. Here, the identified risk factors guide stricter segmentation of outdated machinery and highlight the necessity of consistent maintenance schedules, thereby reducing the risk of cascading failures across multiple project layers. Moreover, overlapping teams (2.4) and limited firewall or intrusion-detection coverage (3.6) illustrate

Table 8. Correlation mapping between industry vulnerabilities and risk factors

Construction Industry Vulnerability	Risk Factors	Explanation
Fluidity of Team Compositions	2.1–2.4	These factors address the project's structural and communication dynamics, revealing the challenges induced by changing team compositions and structures. This reflects the adaptability needed in various phases of construction projects.
Diverse Workforce	1.5, 3.8, 5.2	These factors provide insights into the diversity of the workforce's cybersecurity awareness. It highlights potential gaps and vulnerabilities, emphasizing the need for targeted training and awareness programs.
Widespread communications networks	2.3	This factor illuminates the expansive and multi-layered communication networks in construction projects, pinpointing potential vulnerabilities and areas for enhanced data protection and communication security.
Frequent Information/Data Exchange	3.4–3.9, 4.1–4.5	These IT and OT factors are pivotal in evaluating the risks and vulnerabilities emerging from the extensive digital information exchange, underscoring the need for robust, tailored security protocols.
Blurring of Project Boundaries	2.4, 5.5	These factors identify the potential for overlapping team roles and access to sensitive information across projects, signaling heightened risks of data leaks and the need for stringent access and information management protocols.

how simultaneous projects can inadvertently share vulnerabilities, emphasizing that centralized network governance and continuous monitoring are critical for containing risks. Similarly, subcontractor integration can introduce additional weak points if third-party cybersecurity measures are inadequate, pointing to the importance of vendor audits and binding cybersecurity clauses. By mapping actual project configurations to these scenarios, stakeholders can pinpoint high-risk conditions and develop tangible defensive strategies. Tabletop exercises, for instance, allow project managers to assess how quickly staff respond to simulated breaches and whether communication channels remain effective under pressure. Such proactive evaluations not only validate the relevance of the risk factors but also foster adaptive learning, allowing continuous improvement in both technical defenses and managerial decision-making. Ultimately, these scenarios provide a practical framework for how construction firms can transform static risk factor lists into actionable, context-sensitive interventions throughout all phases of a project.

5.4. Managerial implications and recommendations

This section discusses managerial insights and recommendations for strengthening cybersecurity in construction projects. By aligning these strategies with the roles of project managers, IT and cybersecurity teams, construction companies, and regulatory bodies, stakeholders can address key vulnerabilities and enhance overall security. Building on the systematic categorization of risk factors, this guidance provides practical methods for integrating strong defenses throughout each phase of a construction project.

- **Project Managers can integrate the identified risk** factors into every project phase, including planning, design, construction, and maintenance, by conducting regular, comprehensive assessments that consider evolving threats, new technologies, and regulatory shifts. This approach allows managers to design specific mitigation measures for vulnerabilities, including scenarios where longer project durations heighten exposure to cyber threats or where complex structures necessitate stringent access controls and carefully monitored communication protocols. Continual oversight of IT and OT integration ensures that protective measures remain current as the project advances.
- **IT and Cybersecurity Teams** benefit from using the risk factors to guide the prioritization of security measures, such as deploying endpoint protection, segmenting critical systems, and enforcing strict access control protocols. Continuous user education, supported by mandatory phishing tests and refresher sessions, helps reduce human error vulnerabilities. The quantitative scales attached to each risk factor offer a framework for setting resource allocation priorities, focusing on high-risk areas first and continually evaluating improvements through metrics like incident response times and reductions in user errors.
- **Construction Companies** can reinforce their overall cybersecurity posture by devising a holistic strategy that treats each project as a network of interrelated risks. Periodic cybersecurity audits identify and address both shared and phase-specific weaknesses, while ongoing employee training programs emphasize management and human factors to mitigate insider threats and promote alignment with cybersecurity policies. Establishing cross-departmental committees dedicated to risk management and rapid response ensures cohesive coordination between IT/OT teams and other functional areas, thereby streamlining cyber defense efforts.
- **Regulatory Bodies and Policy Makers** can adopt these risk factors as a baseline for developing solid, enforceable guidelines that reflect the unique characteristics of construction projects. Key regulatory measures may include mandating advanced authentication protocols, implementing network segmentation for critical OT systems, and requiring incident response planning. Additionally, setting physical security standards for large-scale projects and continuously monitoring critical assets ensures a well-rounded defensive posture. Regular updates to these regulations, informed by emerging technologies and newly discovered threats, maintain their relevance and effectiveness, while engagement with industry stakeholders facilitates practical and consistent implementation.

5.5. Comparison with ISO/IEC 27001

To illustrate the practical value of our findings, we demonstrate how the construction-specific risk factors identified in this study map onto internationally recognized security requirements. This comparison is intended to confirm that the factors are both novel to the construction context and fully interoperable with established governance frameworks. We benchmark these cyber-risk factors against ISO/IEC 27001:2022 (International Organization for Standardization & International Electrotechnical Commission [ISO/IEC], 2022), a leading standard for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). Although our study primarily aligns with the NIST Cybersecurity Framework, referencing an additional recognized standard increases its rigor and comprehensiveness. ISO/IEC 27001:2022 (ISO/IEC, 2022) organizes security controls into four categories (organizational, people, physical, and technological) to address various aspects of risk management, such as asset inventory, supplier relationships, and incident response. Some of these controls may seem broad compared to our construction-centric factors, but they still provide a valuable benchmark for ensuring a holistic approach to cybersecurity practices.

Table 9 compares our construction-specific cyber risk factors with these ISO/IEC 27001:2022 (ISO/IEC, 2022) control areas. This crosswalk reveals both alignment and unique considerations: for instance, "country of the project" and "project type" map to legal and contextual requirements, while factors like budget allocations, turnover, and phishing vulnerabilities highlight organizational and human-centric risks. Our emphasis on operational technology (OT) security, which includes equipment age, physical access controls, and network isolation, adds construction-specific detail not always highlighted in generic standards. While our factors largely mirror ISO 27001's categories, there are opportunities to expand on areas like encryption, supplier risk management, and asset disposal. Overall, these insights confirm that our proposed factors balance the specialized needs of construction projects with recognized best practices in information security management, enhancing both credibility and applicability.

Table 9. Mapping of construction-specific risk factors to ISO/IEC 27001:2022 controls

No.	Risk Factor	Relevant ISO/IEC 27001:2022 Control(s)	Notes on Alignment / Potential Gaps
1.1	What is the country of the project?	■ A.5.2 Information Security Roles and Responsibilities ■ A.5.27 Compliance with Legal, Regulatory, and Contractual Requirements	Different regions impose diverse legal requirements on cybersecurity. Ensuring compliance with local regulations is consistent with ISO 27001's emphasis on organizational roles/responsibilities and legal adherence.
1.2	What is the project budget?	■ A.5.7 Budgeting and Resource Allocation (Implied within Organizational Controls)	While ISO 27001 does not specify exact budgeting for security, it expects adequate resources for risk mitigation. This factor indicates financial readiness to address identified cybersecurity risks.
1.3	What is the percentage of the total project budget for cybersecurity management?	■ A.5.7 Budgeting and Resource Allocation ■ A.5.1 Policies for Information Security	Allocating a dedicated cybersecurity budget aligns with ISO 27001's requirement that the organization must provide sufficient resources to implement and maintain its ISMS and related controls.
1.4	What is the project duration?	■ A.5.5 Information Security in Project Management	Longer or evolving projects may require ongoing security reviews. ISO 27001 demonstrates integrating security considerations throughout the entire project lifecycle.
1.5	What is the total number of people involved in the project (labor excluded)?	■ A.6.1 Screening ■ A.6.2 Information Security Awareness, Education, and Training	Large teams raise the need for thorough background checks and consistent security training. ISO 27001 calls for both screening and regular awareness programs.
1.6	What is the project type?	■ A.5.1 Policies for Information Security	Distinct project types (e.g., infrastructure vs. residential) can present unique threats. ISO 27001 prescribes tailoring security policies to the specific context of operations.
1.7	Whether there is a dedicated cybersecurity legal team for the project?	■ A.5.3 Segregation of Duties ■ A.5.4 Contact with Authorities ■ A.5.27 Compliance with Legal, Regulatory, and Contractual Requirements	Having a dedicated legal team enhances compliance with laws, regulations, and incident reporting. ISO 27001 supports defining responsibilities clearly, including legal and regulatory contacts.
2.1	What is the project delivery method?	■ A.5.5 Information Security in Project Management	Different delivery methods (e.g., IPD) alter communication flows and potential vulnerabilities. ISO 27001 advocates security integration in all forms of project/contract management.
2.2	What is the number of subteams at different layers of the project?	■ A.5.2 Information Security Roles and Responsibilities ■ A.5.3 Segregation of Duties	Complex organizational structures require clear delineation of security tasks and duties. ISO 27001 emphasizes segregation of responsibilities to minimize risk.
2.3	What is the number of communication channels at different layers in the project?	■ A.8.9 Network Security ■ A.8.10 Encryption ■ A.8.11 Secure Data Transmission	Multiple channels increase points of vulnerability. ISO 27001 focuses on securing network traffic, potentially through encryption and robust channel management.
2.4	What is the percentage of teams overlapping in different projects?	■ A.5.8 Relationship Management ■ A.5.28 Security Requirements for Using External ICT Services	Overlapping teams could expand the attack surface and resource-sharing challenges. ISO 27001 addresses external relationships and consistent security requirements across multiple engagements.
3.1	What is the scale of your company?	■ A.5 Organizational Controls	Larger organizations often require more sophisticated governance structures. ISO 27001's organizational controls must be scaled appropriately.
3.2	What is the phase of the construction project when your company is involved?	■ A.5.5 Information Security in Project Management	Early-phase involvement can mitigate design-level risks. Later phases require monitoring and compliance checks. ISO 27001 emphasizes a lifecycle approach to security.

Continue of Table 9

No.	Risk Factor	Relevant ISO/IEC 27001:2022 Control(s)	Notes on Alignment / Potential Gaps
3.3	Is there a dedicated IT team for the project?	■ A.5.2 Information Security Roles and Responsibilities ■ A.6.2 Information Security Awareness, Education, and Training	Ensuring specialized IT/cyber support is a best practice for robust control implementation. ISO 27001 prescribes clearly assigned security responsibilities and adequate expertise/training.
3.4	What is the total number of critical digital assets?	■ A.5.8 Inventory of Information and Other Associated Assets ■ A.8.2 Information Classification	ISO 27001 requires classifying and safeguarding important information assets. Identifying critical digital assets is fundamental to risk assessment.
3.5	What is the total number of user endpoints of digital devices for the project?	■ A.8.1 Access Control ■ A.8.3 End-User Devices	Each endpoint (laptop, smartphone, etc.) represents a potential entry point. ISO 27001's technical controls require device security and proper access management.
3.6	What is the percentage of digital devices with firewalls or intrusion detection systems involved in the project?	■ A.8.13 Protection of Information Systems ■ A.8.14 Logging and Monitoring	ISO 27001 emphasizes deploying protective technologies (e.g., firewalls, IDS) and monitoring to detect anomalies.
3.7	What is the network type used for the project: Public or Private?	■ A.8.9 Network Security	Public networks carry different risks (e.g., open Wi-Fi hotspots). ISO 27001 advocates secure network architecture, segmentation, and proper encryption protocols.
3.8	What is the percentage of individuals who fail phishing tests after completing mandatory training?	■ A.6.2 Information Security Awareness, Education, and Training ■ A.8.14 Logging and Monitoring	Phishing susceptibility is a critical human-factor risk. ISO 27001 calls for targeted training and continuous monitoring of suspicious activity.
3.9	What is the estimated Mean Time to Respond (MTTR) in hours?	■ A.5.6 Information Security Incident Management Planning and Preparation ■ A.5.22 Business Continuity Management	Quick response times reduce impact. ISO 27001 integrates incident response and business continuity measures to handle disruptions effectively.
4.1	What is the total number of important OT equipment involved?	■ A.5.8 Inventory of Information and Other Associated Assets ■ A.8.9 Network Security (if OT systems are network-connected)	Incorporating OT devices in asset inventory is often overlooked. ISO 27001 expects organizations to account for all critical assets, including OT.
4.2	What is the level of physical access control mechanism to OT equipment?	■ A.7.1 Physical Security Perimeter ■ A.7.2 Physical Entry Controls	Restricting physical access to critical OT assets mitigates tampering risks. ISO 27001 emphasizes robust physical controls.
4.3	What is the percentage of OT equipment isolated from the project's general network?	■ A.8.9 Network Security	Segregating OT from IT can limit lateral movement in an attack scenario. ISO 27001 supports network segmentation principles to reduce risk.
4.4	What is the average age of the important OT equipment, in years?	■ A.8.15 Access, Use, and Maintenance of Assets	Older OT hardware may lack patches or vendor support. ISO 27001 requires continuous assessment of assets' security posture throughout their lifecycle.
4.5	What is the level of authentication mechanism to access the HMI (Human Machine Interface)?	■ A.8.1 Access Control ■ A.8.2 Identification, Authentication, and Access Management	Critical OT interfaces (HMI) should employ strong or multi-factor authentication. ISO 27001 prescribes rigorous access management to sensitive systems.
5.1	What is the average level of commitment to corporate governance, ethical practices and cybersecurity policy?	■ A.5.1 Policies for Information Security ■ A.5.2 Information Security Roles and Responsibilities ■ A.5.6 Incident Management	High-level commitment to cybersecurity and ethics forms the backbone of a culture of security. ISO 27001 deems leadership support and clearly defined policies crucial.
5.2	What is the average frequency of security training per year?	■ A.6.2 Information Security Awareness, Education, and Training	Regular training fosters security awareness and skills. ISO 27001 strongly recommends ongoing, systematic training programs for all staff.
5.3	Do you allow password reuse for any project-related software, systems, or accounts (e.g., project management tools, email, internal networks, file storage, etc.)?	■ A.8.2 Identification, Authentication, and Access Management	Password reuse is a known vulnerability. ISO 27001 requires secure authentication methods, including prohibiting unsafe practices like reusing credentials across systems.

End of Table 9

No.	Risk Factor	Relevant ISO/IEC 27001:2022 Control(s)	Notes on Alignment / Potential Gaps
5.4	Does internet access within your construction project require Multi-Factor Authentication (MFA) or utilize other methods such as biometrics or face recognition?	■ A.8.2 Identification, Authentication, and Access Management	Strong authentication measures, such as MFA or biometrics, reduce unauthorized access risks. ISO 27001 stresses layered access controls for critical services.
5.5	What is the percentage of people who have access to sensitive information in the project?	■ A.8.1 Access Control ■ A.8.2 Identification, Authentication, and Access Management	Limiting access to sensitive data aligns with the principle of least privilege. ISO 27001 advises organizations to grant data access based on role necessity.
5.6	What is the average team member variability over a 3-month period?	■ A.6.1 Screening ■ A.6.2 Information Security Awareness, Education, and Training ■ A.8.2 Identification, Authentication, and Access Management	High turnover or frequent changes demand robust onboarding/offboarding processes. ISO 27001 requires regular updates to access privileges, security education, and user management.
5.7	What is the average socioeconomic level of the people involved in the project?	■ A.6.2 Information Security Awareness, Education, and Training	While not explicitly covered, workforce demographics can influence training needs, risk perception, and susceptibility to social engineering. ISO 27001 encourages tailoring awareness programs to the audience.

5.6. Limitations and future works

This study's primary advantages include its extensive coverage and depth, evidenced by an initial pool of 62 factors derived from a large textual dataset. Strong expert consensus led to a final selection of 32 factors, achieving an average rating of 3.9 (standard deviation 0.5), which indicates strong agreement on their importance. The iterative validation process, involving over 12 online meetings across approximately five months, further supported the method's reliability and thoroughness. Nevertheless, there are limitations. The small expert panel, which consists of two from a U.S. cybersecurity firm and one from a Middle Eastern construction company, restricts the diversity of perspectives and may limit the global applicability of the findings in capturing varied cyber risk perceptions. Moreover, an emphasis on quantitative scales of risk factors could overlook qualitative nuances, such as organizational culture and stakeholder dynamics, that can significantly influence cybersecurity risks. Besides addressing these limitations, future research will also employ the identified risk factors to establish a predictive risk assessment model tailored to construction projects, integrating ideas from existing risk-based decision-making frameworks (Ebrahimnejad et al., 2017a, 2017b; Hamzeh et al., 2020; Mousavi & Gitinavard, 2019). For instance, these works have demonstrated how fuzzy logic, interval-valued hesitant fuzzy information, and multi-criteria decision analysis can successfully handle uncertainty in IT outsourcing and project scheduling contexts. Building on those insights, the planned model will incorporate empirical validation and comparative analysis to evaluate its effectiveness and scalability. Specifically, it will fuse historical data, real-time analytics, and industry-specific indicators for cyber threats to develop phase-specific mitigation strategies. By enabling more precise risk identification and proactive measures, this model aims to bolster both resilience and cybersecurity posture within the construction sector.

6. Conclusions

This study presents a comprehensive set of 32 project-level cybersecurity risk factors tailored to the construction industry, filling a critical gap where past research has largely overlooked the sector's unique vulnerabilities. A seven-step framework guided the process, beginning with an extensive literature review and proceeding through iterative Delphi-based expert survey evaluations and refinements. By modeling construction projects as multi-layered networks, this study allows for capturing the complex interdependencies among diverse stakeholders, sub-teams, and communication channels. The final risk factors were organized into five categories, including Overall Project Information, Project Structure, IT, OT, and Management and Human Factors. By defining quantitative scales for each factor, these risk factors enable more quantitative cyber risk assessments, marking a departure from qualitative evaluations that rely heavily on subjective assumptions. Through an iterative approach of expert feedback, the reliability and practical relevance of these risk factors were validated, illustrating how each factor could directly impact project cybersecurity. This study integrates these factors into scenario-based analyses and analyzes managerial implications so that construction stakeholders can get insights of how to adopt proactive, context-specific defenses addressing both IT and OT vulnerabilities. Moreover, benchmarking against ISO/IEC 27001 demonstrates the relevance and rigor of these factors, highlighting their alignment with recognized standards. Overall, the study provides contributions to both academia and industry by facilitating more

systematic, quantitative, and context-aware management of cyber risks in an increasingly digitized construction environment.

Acknowledgements

This study was supported by different Centers at NYUAD. It was supported by the Center for Sand Hazards and Opportunities for Resilience, Energy, and Sustainability (SHORES), funded by Tamkeen under the NYUAD Research Institute Award CG013; the Center for Cyber Security at New York University Abu Dhabi (CCS-AD), funded by Tamkeen under the NYUAD Research Institute Award G1104; and the Center for Interacting Urban Networks (CITIES), funded by Tamkeen under the NYUAD Research Institute Award CG001. We also thank the experts from ALEC Engineering & Contracting LLC (ALEC) in Dubai, especially Mr. Sabyasachi Jana, and SecurityScorecard in New York, especially Dr. Jared Smith, for participating in our questionnaire survey, supporting the evaluation of risk factors, and providing insightful feedback.

Author contributions

Dongchi Yao led the study's conceptualization, research design, data analysis, and manuscript drafting. He also coordinated the submission process as the corresponding author. Borja García de Soto contributed to methodology development, risk factor identification, and manuscript revision, with a focus on industry-specific insights. Mike Wilkes provided feedback on risk factor identification, suggestions for paper composition, and additional industry-specific insights. All authors collaborated throughout all stages of the research, reviewed the final manuscript, and approved it, ensuring the integrity and accuracy of the work.

Disclosure statement

The authors declare that there are no conflicts of interest regarding the publication of this paper. All authors have reviewed the content and agreed upon the submission, ensuring that there are no financial or personal relationships influencing the work presented.

References

Abd El-Karim, M. S. B. A., Mosa El Nawawy, O. A., & Abdel-Alim, A. M. (2017). Identification and assessment of risk factors affecting construction projects. *HBRC Journal*, *13*(2), 202–216. https://doi.org/10.1016/j.hbrcj.2015.05.001

Aghaei, P., Asadollahfardi, G., & Katabi, A. (2022). Safety risk assessment in shopping center construction projects using fuzzy fault tree analysis method. *Quality and Quantity*, *56*, 46–59. https://doi.org/10.1007/s11135-021-01115-9

Assaf, S. A., & Al-Hejji, S. (2006). Causes of delay in large construction projects. *International Journal of Project Management*, *24*(4), 349–357. https://doi.org/10.1016/j.ijproman.2005.11.010

Badi, S., & Nasaj, M. (2024). Cybersecurity effectiveness in UK construction firms: An extended McKinsey 7S model approach. *Engineering, Construction and Architectural Management*, *31*(11), 4482–4515. https://doi.org/10.1108/ECAM-12-2022-1131

Baloi, D., & Price, A. D. F. (2003). Modelling global risk factors affecting construction cost performance. *International Journal of Project Management*, *21*(4), 261–269. https://doi.org/10.1016/S0263-7863(02)00017-0

Bello, A., & Maurushat, A. (2020). Technical and behavioural training and awareness solutions for mitigating ransomware attacks. In R. Silhavy (Ed.), *Advances in intelligent systems and computing*: *Vol. 1226*. *Applied Informatics and Cybernetics in Intelligent Systems* (*CSOC 2020*) (pp. 164–176). Springer, Cham. https://doi.org/10.1007/978-3-030-51974-2_14

Chan, D. W. M., Chan, A. P. C., Lam, P. T. I., Yeung, J. F. Y., & Chan, J. H. L. (2011). Risk ranking and analysis in target cost contracts: empirical evidence from the construction industry. *International Journal of Project Management*, *29*(6), 751–763. https://doi.org/10.1016/j.ijproman.2010.08.003

Chileshe, N., & Boadua Yirenkyi-Fianko, A. (2012). An evaluation of risk factors impacting construction projects in Ghana. *Journal of Engineering, Design and Technology*, *10*(3), 306–329. https://doi.org/10.1108/17260531211274693

Coble, S. (2020, January 27). Major Canadian military contractor compromised in ransomware attack. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/bird-construction-compromised-in/

CPX. (2024, March 11). *UAE Cyber Security Council and CPX unveil Cybersecurity Report 2024*: *A call to action against rising cyber threats*. https://www.cpx.net/media-center/press-releases/state-of-cybersecurity-in-the-uae/?utm_source=chatgpt.com

Cyware. (2018). *Hackers hit French firm Ingerop stealing 65 GB data relating to nuclear power plants*. https://cyware.com/news/hackers-hit-french-firm-ingerop-stealing-65-gb-data-relating-to-nuclear-power-plants-f193b9ba/

Deloitte. (2022). *Building cybersecurity in the construction industry*. https://www2.deloitte.com/ce/en/pages/real-estate/articles/ce-building-cybersecurity-in-the-construction-industry.html

Ebrahimnejad, S., Naeini, M. A., Gitinavard, H., & Mousavi, S. M. (2017a). Selection of IT outsourcing services' activities considering services cost and risks by designing an interval-valued hesitant fuzzy-decision approach. *Journal of Intelligent & Fuzzy Systems*, *32*(6), 4081–4093. https://doi.org/10.3233/JIFS-152520

Ebrahimnezhad, S., Gitinavard, H., & Sohrabvandi, S. (2017b). A new extended Analytical Hierarchy Process technique with incomplete interval-valued information for risk assessment in IT outsourcing. *International Journal of Engineering*, *30*(5), 739–748.

El-Sayegh, S., Romdhane, L., & Manjikian, S. (2020). A critical review of 3D printing in construction: Benefits, challenges, and risks. *Archives of Civil and Mechanical Engineering*, *20*, Article 34. https://doi.org/10.1007/s43452-020-00038-w

Galanis, P. (2018). The Delphi method. *Archives of Hellenic Medicine*, *35*(4), 564–570.

García de Soto, B., Agustí-Juan, I., Joss, S., & Hunhevicz, J. (2022a). Implications of Construction 4.0 to the workforce and organizational structures. *International Journal of Construction Management*, *22*(2), 205–217. https://doi.org/10.1080/15623599.2019.1616414

García de Soto, B., Turk, Ž., Maciel, A., Mantha, B., Georgescu, A., & Sonkor, M. S. (2022b). Understanding the significance of cybersecurity in the construction industry: survey findings. *Journal of Construction Engineering and Management*, *148*(9), Article 04022095. https://doi.org/10.1061/(ASCE)CO.1943-7862.0002344

Goh, G. D., Sing, S. L., & Yeong, W. Y. (2021). A review on machine learning in 3D printing: Applications, potential, and challenges. *Artificial Intelligence Review*, *54*(1), 63–94. https://doi.org/10.1007/s10462-020-09876-9

Gondia, A., Siam, A., El-Dakhakhni, W., & Nassar, A. H. (2020). Machine learning algorithms for construction projects delay risk prediction. *Journal of Construction Engineering and Management*, *146*(1), Article 04019085. https://doi.org/10.1061/(ASCE)CO.1943-7862.0001736

Hamzeh, A. M., Mousavi, S. M., & Gitinavard, H. (2020). Imprecise earned duration model for time evaluation of construction projects with risk considerations. *Automation in Construction*, *111*, Article 102993. https://doi.org/10.1016/j.autcon.2019.102993

Hwang, B. G., Shan, M., Phua, H., & Chi, S. (2017). An exploratory analysis of risks in green residential building construction projects: the case of Singapore. *Sustainability*, *9*(7), Article 1116. https://doi.org/10.3390/su9071116

International Organization for Standardization, & International Electrotechnical Commission. (2022). *Information security, cybersecurity and privacy protection – Information security management systems – Requirements* (ISO/IEC Standard No. 27001:2022). https://www.iso.org/standard/27001

Jarkas, A. M., & Haupt, T. C. (2015). Major construction risk factors considered by general contractors in qatar. *Journal of Engineering, Design and Technology*, *13*(1), 165–194. https://doi.org/10.1108/JEDT-03-2014-0012

JDSUPRA. (2023, April 19). *Huntington Ingalls Industries files official notice of data breach affecting 43,643 individuals*. https://www.jdsupra.com/legalnews/huntington-ingalls-industries-files-3524071/

Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. *Machines*, *9*(4), Article 78. https://doi.org/10.3390/machines9040078

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

Kunert, P. (2023, October 12). US construction giant unearths concrete evidence of cyberattack. *The Register*. https://www.theregister.com/2023/10/12/simpson_manufacturing_security_incident/?td=readmore

Kurtz, S. (2019). Cybersecurity vulnerabilities in the construction industry. *Total IT Information Technology*. https://totalit.com/cybersecurity-vulnerabilities-in-the-construction-industry/

Lalropuia, K., Goyal, S., García De Soto, B., Yao, D., & Sonkor, M. S. (2025). Mitigating malicious insider threats to common data environments in the architecture, engineering, and construction industry: an incomplete information game approach. *Journal of Cybersecurity and Privacy*, *5*(1), Article 5. https://doi.org/10.3390/jcp5010005

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

Mantha, B. R. K., & García de Soto, B. (2021). Assessment of the cybersecurity vulnerability of construction networks. *Engineering, Construction and Architectural Management*, *28*(10), 3078–3105. https://doi.org/10.1108/ECAM-06-2020-0400

Mantha, B., 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*, Article 102682. https://doi.org/10.1016/j.scs.2020.102682

Meyer, T., & Reniers, G. (2022). *Engineering risk management*. De Gruyter. https://doi.org/10.1515/9783110665338

Mousavi, S. M., & Gitinavard, H. (2019). An extended multi-attribute group decision approach for selection of outsourcing services activities for information technology under risks. *International Journal of Applied Decision Sciences*, *12*(3), Article 227. https://doi.org/10.1504/IJADS.2019.100437

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework* (*CSF*) *2.0*. https://doi.org/10.6028/NIST.CSWP.29.pol

Nyamuchiwa, K., Lei, Z., & Aranas, C. (2022). Cybersecurity vulnerabilities in off-site construction. *Applied Sciences*, *12*(10), Article 5037. https://doi.org/10.3390/app12105037

Pan, Z., Hariri, S., & Pacheco, J. (2019). Context aware intrusion detection for building automation systems. *Computers & Security*, *85*, 181–201. https://doi.org/10.1016/j.cose.2019.04.011

Pargoo, N. S., & Ilbeigi, M. (2023). A scoping review for cybersecurity in the construction industry. *Journal of Management in Engineering*, *39*(2), Article 03122003. https://doi.org/10.1061/JMENEA.MEENG-5034

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

Price, D. (2020). Bam construct and Interserve hit by cyber attacks. *Construction News*. https://www.constructionnews.co.uk/contractors/bam-construct/bam-construct-hit-by-cyber-attack-13-05-2020/

Renuka, S. M., Umarani, C., & Kamal, S. (2014). A review on critical risk factors in the life cycle of construction projects. *Journal of Civil Engineering Research*, *4*(2A), 31–36.

Rosenberg, K., Reindorf, J., Merali, Z., & Mohsen, E. (2024, April 3). Cybercrime risk in the Middle East construction industry. *Freshfields*. https://riskandcompliance.freshfields.com/post/102j4a8/cybercrime-risk-in-the-middle-east-construction-industry?utm_source=chatgpt.com

Rudolf, C. A., & Spinler, S. (2018). Key risks in the supply chain of large-scale engineering and construction projects. *Supply Chain Management*, *23*(4), 336–350. https://doi.org/10.1108/SCM-09-2017-0292

Sawyer, T., & Rubenstone, J. (2019). Construction cybercrime is on the rise. *Engineering News-Record* (*ENR*). https://www.enr.com/articles/46832-construction-cybercrime-is-on-the-rise

Sharaf, M. M. M., & Abdelwahab, H. T. (2015). Analysis of risk factors for highway construction projects in Egypt. *Journal of Civil Engineering and Architecture*, *9*(5), 526–533. https://doi.org/10.17265/1934-7359/2015.05.004

Sharma, S., & Goyal, P. K. (2022). Fuzzy assessment of the risk factors causing cost overrun in the construction industry. *Evolutionary Intelligence*, *15*(4), 2269–2281. https://doi.org/10.1007/s12065-019-00214-9

Sheikh, A., Kamuni, V., Patil, A., Wagh, S., & Singh, N. (2019). Cyber attack and fault identification of HVAC system in building management systems. In *2019 9th International Conference on Power and Energy Systems* (*ICPES*), Perth, WA, Australia. IEEE. https://doi.org/10.1109/ICPES47639.2019.9105438

Shemov, G., García de Soto, B., & Alkhzaimi, H. (2020). Blockchain applied to the construction supply chain: A case study with threat model. *Frontiers of Engineering Management*, *7*(4), 564–577. https://doi.org/10.1007/s42524-020-0129-x

Shibly, M. U. R. M., & García de Soto, B. (2020, October 14). Threat modeling in construction: an example of a 3D concrete printing system. In *Proceedings of the 37th International Symposium*

on Automation and Robotics in Construction (ISARC 2020) (pp. 625–632), Kitakyushu, Japan. https://doi.org/10.22260/ISARC2020/0087

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), Article 04021172. https://doi.org/10.1061/(ASCE)CO.1943-7862.0002193

Sonkor, M. S., & García De Soto, B. (2024). Using ChatGPT in construction projects: Unveiling its cybersecurity risks through a bibliometric analysis. *International Journal of Construction Management*, *25*(7), 741–749. https://doi.org/10.1080/15623599.2024.2355782

Steel, L. (2022, November 24). Data protection: Security breach results in £4.4m fine for Interserve. *Wright Hassall*.

The Stack. (2022, July 20). *Plasterboard giant Knauf Group pummelled by ransomware*. https://www.thestack.technology/knauf-group-ransomware-attack-plasterboard-shortage/

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

Wuni, I. Y., Shen, G. Q. P., & Mahmud, A. T. (2022). Critical risk factors in the application of modular integrated construction: A systematic review. *International Journal of Construction Management*, *22*(2), 133–147. https://doi.org/10.1080/15623599.2019.1613212

Yao, D., & García de Soto, B. (2023, July). A corpus database for cybersecurity topic modeling in the construction industry. In *Proceedings of the 40th International Symposium on Automation and Robotics in Construction* (*ISARC 2023*) (pp. 537–544), Chennai, India. https://doi.org/10.22260/ISARC2023/0072

Yao, D., & García De Soto, B. (2024a). Assessing cyber risks in construction projects: A machine learning-centric approach. *Developments in the Built Environment*, *20*, Article 100570. https://doi.org/10.1016/j.dibe.2024.100570

Yao, D., & García De Soto, B. (2024b). Cyber risk assessment framework for the construction industry using machine learning techniques. *Buildings*, *14*(6), Article 1561. https://doi.org/10.3390/buildings14061561

Yao, D., & García De Soto, B. (2024c). Enhancing cyber risk identification in the construction industry using language models. *Automation in Construction*, *165*, Article 105565. https://doi.org/10.1016/j.autcon.2024.105565

Zou, P. X. W., & Zhang, G. (2009). Managing risks in construction projects: Life cycle and stakeholder perspectives. *International Journal of Construction Management*, *9*(1), 61–77. https://doi.org/10.1080/15623599.2009.10773122

Zou, P. X. W., Zhang, G., & Wang, J. (2007). Understanding the key risks in construction projects in China. *International Journal of Project Management*, *25*(6), 601–614. https://doi.org/10.1016/j.ijproman.2007.03.001

APPENDIX

Table A1. The initial identification of risk factors related to project basic information (Category 1)

No.	Risk factor	Feedback from experts	Average Score	Action	New No.
1.1	Is your construction company global or local?	Rather than broadly categorizing companies as global or local, it would be more useful to look at company scale in more granular segments based on factors like number of employees. This allows for a more nuanced risk assessment to determine what controls are needed for companies of different sizes and scopes.	2	deleted	–
1.2	What is the scale of your construction company?	Remove limitation to construction companies, as data collection may include design, architecture, engineering, or maintenance firms with similar cyber risk factors.	4	revised	3.1
1.3	What is the current phase of the construction project?	Project phase is a valid cyber risk factor as differing stages present unique considerations and vulnerabilities requiring security controls adapted to current activities.	5	kept	3.2
1.4	What is the weather of the current project phase?	We would remove weather as a risk factor, as it is not directly related to cybersecurity vulnerabilities or controls needed. The focus should be on project activities rather than external climate conditions.	1	deleted	–
1.5	What is the total number of people involved in the project?	Do not include all people involved in assessing cyber risk. Labor does not necessarily increase vulnerabilities. Focus should be on those with access to critical systems and data rather than total project personnel.	4	revised	1.5
1.6	What is the percentage of people who have access to sensitive information?	The percentage granted access to sensitive data is a valid risk factor, as more access increases threats of unauthorized disclosure, therefore determining priorities for access controls.	5	kept	5.5
1.7	What is the percentage of FTE (full time employees) involved in the project?	We suggest to remove the percentage of FTEs as a risk factor. The focus should be on access controls for those needing access to critical systems rather than full-time status. Insider threats are better mitigated through security protocols and auditing controls rather than limiting FTE numbers.	1	deleted	–
1.8	What is the percentage of people having worked over 10 years?	We suggest not include tenure length as a definitive risk factor, as it is uncertain whether long-tenured employees inherently pose higher insider threat risks. More important factors are strong security controls and practices applied evenly regardless of years of service.	1	deleted	–
1.9	What is the region of the project?	Rather than broadly assessing region, we would suggest specifying country as the risk factor to allow for more granular cybersecurity analysis tied to the specific threats, regulations, and resources within individual nations involved in the project.	5	revised	1.1

Table A2. The initial identification of risk factors related to project structure (Category 2)

No.	Risk factor	Feedback from experts	Average Score	Action	New No.
2.1	What is the project delivery method?	We agree the project delivery method should be included as a risk factor. Different approaches have implications on collaboration, access controls, communication channels, and security protocols between parties, which directly impact the overall cybersecurity posture. The delivery method provides useful insight into vulnerabilities.	5	kept	2.1
2.2	What is the number of sub-teams at different layers of the project?	While the number of sub-teams at each layer provides some useful insight, we would only partially include this as a risk factor. More sub-teams don't necessarily correlate to more vulnerabilities. Effective communication and cybersecurity practices are more indicative of risk than team quantity. This should be considered in conjunction with other factors to avoid assumptions.	3	kept	2.2
2.3	What is the total number of teams in the project?	This can be derived from the risk factor 2.2.	1	deleted	–
2.4	What is the number of communication channels at different layers in the model?	The number of communication channels at each layer should be included as a cyber risk factor. More pathways for interaction and data exchange introduce complexity and potential vulnerabilities that need to be addressed through tailored security controls. Quantifying these channels is valuable for assessing where risks may emerge.	4	kept	2.3

End of Table A2

No.	Risk factor	Feedback from experts	Average Score	Action	New No.
2.5	What is the total number of communication channels among teams in the project?	This can be derived from the risk factor 2.2.	1	deleted	–
2.6	What is the average communication strength of channels at each layer?	While communication strength is important, we would be hesitant to include this as a quantified risk factor. Assessing the abstract concept of channel "strength" introduces ambiguity and subjectivity. More objective factors like protocols, access controls, and auditing would better indicate concrete vulnerabilities. Quantifying communication effectiveness seems challenging and less actionable.	2	deleted	–
2.7	What is the overall communication strength of all channels?	Same as above	2	deleted	–
2.8	What is the average maturity of communication channels at different layers?	Same as above	1	deleted	–
2.9	What is the overall maturity of all communication channels?	Same as above	1	deleted	–

Table A3. The initial identification of risk factors related to cybersecurity scores of teams (Category 3)

No.	Risk factor	Feedback from experts	Average Score	Action
3.1	What is the average risk score at each layer of model?	While assessing risk scores per team and layer provides useful cybersecurity insights, quantifying these specific metrics presents challenges. Risk scores require clearly defined criteria and models to assign meaningful values representing security posture. Without explanation of how scores are calculated for teams, factors based on averages, spreads, and outliers become difficult to objectively quantify. We would suggest focusing on more concrete metrics until risk scoring methods are established, and you can just ignore these factors for now.	2	deleted
3.2	What is the average risk score over all the teams in the project?			
3.3	To what extent are the risk scores spread out among the different teams in the project?			
3.4	What is the percentage of teams that have high risk scores (higher than 70)?			
3.5	What is the highest value of risk scores over all the teams?			
3.6	The IQR metric of the risk scores over all teams			

Table A4. The initial identification of risk factors related to project context (Category 4)

NO.	Risk factor	Feedback from experts	Average Score	Action	New No.
4.1	What is level of the cybersecurity impact and stakeholder engagement regarding cybersecurity?	Duplicated with 4.3	2	deleted	–
4.2	Whether there is a dedicated cybersecurity legal team?	A dedicated cybersecurity legal team is crucial to ensure compliance, guide responses, manage risks, and add legal expertise to bolster resilience – their inclusion enables comprehensive risk assessment.	5	kept	1.7
4.3	What is the level of commitment to corporate governance and ethical practices regarding cybersecurity?	Gauging the commitment to corporate governance and ethical cyber practices is crucial, as robust adherence to regulations, accountability, and principled decision-making fosters stakeholder trust. However, weak governance jeopardizes reputation, success, and legal compliance, making this factor integral for comprehensively evaluating cyber risk.	5	kept	5.1
4.4	What is the percentage of total project budget for cybersecurity management?	The percentage of total budget allocated to cybersecurity management is crucial to enable robust threat reduction and avoid data breaches, system downtime, financial losses, and reputation damage from insufficient funding. Including this budget factor allows comprehensive evaluation and mitigation of project cyber risks.	5	kept	1.3

End of Table A4

NO.	Risk factor	Feedback from experts	Average Score	Action	New No.
4.5	What is the level of financial risk?	We suggest excluding financial risk level from the cyber risk model, as financial instability impacts general project success but does not directly correlate with technical, procedural or human cyber risks. Diluting the model's focus, it is better evaluated separately through financial analysis to maintain precision identifying core cyber vulnerabilities.	2	deleted	–
4.6	What is the frequency of daily information exchange?	While frequent information exchange enables collaboration, it can heighten cyber risks from increased phishing, breach, and access threats. However, as data collection on exchange frequency poses challenges, removing this factor enhances the model's feasibility. Though a helpful indicator, omitting it simplifies data gathering to focus on assessing obtainable risk metrics.	2	deleted	–
4.7	What is the average socioeconomic level of the involved people?	We recommend including the average socioeconomic level, as disparities can influence cybersecurity attitudes and behaviors, introducing risks from uneven awareness and practices. Tracking this factor identifies potential knowledge gaps, enabling tailored training and policies to promote security. Inclusion provides useful insights despite challenges obtaining sensitive information.	3	kept	5.7
4.8	What is the degree of variation of the socioeconomic level of the involved people?	While workforce diversity can influence collaboration and awareness, gauging socioeconomic variation does not provide direct cyber risk insights. This subjective factor dilutes the model's focus on technical vulnerabilities. Excluding it sharpens precision by concentrating solely on core cyber threats.	2	deleted	–
4.9	What is the percentage of teams overlapping in different projects?	We suggest keeping this factor, because personnel and resource sharing inherently amplifies risks from divided priorities causing gaps, inconsistent practices, unauthorized data access, and process interdependencies across projects.	4	kept	2.4
4.10	What is the average level of team member variability?	As frequent composition changes escalate cyber risks from new vulnerabilities and departures leaving gaps, we recommend incorporating this factor, but with a time period specified. Specifying a timeframe provides contextual insight on personnel fluctuation impacts. Tracking variability in a set period strengthens risk evaluation by signaling gaps in practices and knowledge.	4	revised	5.6
4.11	What is the average churn rate of all teams?	We suggest excluding average team churn rate, as turnover frequency has minimal direct correlation with project cyber risks. While impacting knowledge retention, churn rate is better assessed as a general HR metric. Removing churn sharpens focus on technical and procedural vulnerabilities rather than indirect HR factors.	1	deleted	-

Table A5. The initial identification of risk factors related to IT (Category 5)

No.	Risk factor	Feedback from experts	Average Score	Action	New No.
5.1	Is the IT staff under-resourced for the size of the project?	We recommend excluding the IT staff resourcing factor because the criteria for adequate staffing levels is highly subjective, making consistent risk evaluation across projects difficult.	2	deleted	–
5.2	What is the number of user endpoints of digital devices?	We suggest to keep endpoint device count as it provides vital visibility into access points, enabling assessment of the attack surface scale. More endpoints expand exposure, so quantifying unique devices through inventories allows comprehensive evaluation of access-related cyber risks and guides safeguards.	5	kept	3.5
5.3	What is the average computer/laptop security score?	We recommend dropping the average laptop/computer security score factor since consistently rating the strength of protections on diverse devices is really hard to do. The subjectivity in scoring different system safeguards makes it difficult to objectively quantify security levels across an array of computers and laptops.	1	deleted	–
5.4	What is the ratio of Windows system vs non-Windows?	The security of a system depends more on its implemented security controls than the operating system itself. Both Windows and non-Windows systems have vulnerabilities. Thus, factors like regular updates, secure configurations, and user practices often outweigh the inherent security of the operating system.	2	deleted	–

End of Table A5

No.	Risk factor	Feedback from experts	Average Score	Action	New No.
5.5	What is the ratio of Android vs non-Android systems?	We recommend removing this factor. Rather than focus on the operating system, robust security requires proper management, user behavior, and prudent practices regardless of platform. Neither Android nor non-Android is inherently more secure, so this ratio does not provide meaningful risk insights.	2	deleted	–
5.6	Whether 90% of the computers/laptops have 90% of its applications are up to date?	Indeed, monitoring whether 90% of computers/laptops have 90% of their applications up-to-date can be challenging due to privacy and data collection concerns. Additionally, such statistics would require continuous, real-time tracking, which isn't practical or ethical in many contexts. Hence, it's recommended to remove this factor.	2	deleted	–
5.7	What is the construction-related APP/software maturity level?	Assessing the maturity level of construction-related apps or software can be quite subjective and variable, as it depends on many factors such as the specific software in question, its version, the use case, the user, and more. Therefore, this factor is not universally applicable or consistently measurable.	2	deleted	–
5.8	Is there a dedicated IT team for the project?	We suggest keeping the dedicated IT team factor because their specialized skills and sole focus on the project enables faster, tailored incident response and security controls. This builds greater familiarity with the environment and accountability for protection.	5	kept	3.3
5.9	What is the level of stringency of cybersecurity policy?	duplicated with 5.1	2	deleted	–
5.10	What is the level of commitment to cybersecurity policy?	duplicated with 5.1	2	deleted	–
5.11	What is the average frequency of security training per year among all teams?	The average frequency of security training per year is a crucial factor to keep. This directly reflects an organization's commitment to security awareness and the preparedness of its teams. Regular training updates employees on new threats, reinforces security protocols, and cultivates a culture of vigilant cybersecurity behavior.	5	kept	5.2
5.12	What is the percentage of people who fail phishing tests a second time after completing required training?	Indeed, the factor "fail a second time after training" is too narrow. We recommend revising it to "fail after completing required training". This broader approach still evaluates training effectiveness and the team's susceptibility to phishing, offering valuable insights into potential security vulnerabilities.	4	revised	3.8
5.13	What is the percentage of password reuse among employees in the project?	Quantifying the exact "percentage" may pose data privacy and collection challenges. It's better to focus on "whether there is a policy against password reuse". This revision still emphasizes the importance of good password practices without requiring intrusive data collection.	4	revised	5.3
5.14	Whether there is any presence of exploitable critical findings in annual pen testing?	The factor "presence of exploitable critical findings in annual pen testing" should be removed as it oversimplifies security assessment. Security is dynamic and depends on various factors, not just the presence or absence of critical findings at a particular point in time. A zero-critical-findings result today doesn't guarantee security tomorrow.	2	deleted	–
5.15	What is the estimated mean time to respond (MTTR) of the project, in hours?	Mean Time to Respond (MTTR) is an essential factor, as it measures the response efficiency to cyber incidents. A lower MTTR signifies quicker threat resolution, minimizing potential damage. Therefore, it's crucial to continually monitor and aim to reduce MTTR for enhanced cybersecurity resilience.	3	kept	3.9
5.16	What is the number of production-impacting incident tickets per month in the project?	We recommend removing this factor as the number of production-impacting incidents monthly might not be available or disclosed, especially by organizations lacking a dedicated cybersecurity department. This data is typically sensitive and may remain confidential due to privacy and security concerns.	2	deleted	–

Table A6. The initial identification of risk factors related to OT (Category 6)

No.	Risk factor	Feedback from experts	Average Score	Action	New No.
6.1	What is the total number of critical digital assets in the project?	Including the total number of important digital assets strengthens cyber risk assessment by providing crucial visibility into sensitive data vulnerabilities. Quantifying these assets enables strategic prioritization of security efforts and protections to mitigate critical threats.	5	kept	3.4
6.2	What is the total number of important OT equipment and devices?	The inclusion of this risk factor is insightful. Quantifying essential OT assets is key for evaluating potential exposure, prioritizing protection, and allocating resources effectively. This enhances your model's ability to address and mitigate cyber threats efficiently.	4	kept	4.1
6.3	What is the average age of the important OT equipment?	Considering the average age of crucial OT equipment as a risk factor is prudent. It provides insight into possible vulnerabilities due to aging infrastructure, including security gaps, maintenance challenges, and performance decrease. It aids in identifying upgrade needs, which promotes reliable and secure OT operations, reducing risks from obsolete equipment.	3	kept	4.4
6.4	Whether the project uses Public Network or Private Network?	Inclusion of the network type (public vs private) in your risk assessment is valuable. It helps expose vulnerabilities, guides decisions on network architecture, and shapes data protection strategies. By considering this factor, you can better strategize secure practices and mitigate risks associated with public network usage.	5	kept	3.7
6.5	What is the percentage of digital devices with firewalls or intrusion detection systems involved in the project?	The inclusion of the percentage of devices with firewalls or intrusion detection systems is crucial. This metric provides a measure of the project's cybersecurity posture, reflecting the extent of safeguards against unauthorized access and threats. This will enhance network security evaluation and resource allocation.	5	kept	3.6
6.6	What is the percentage of firewalls and endpoint detection systems with the latest security updates?	While the percentage of updated security systems is an important metric for cybersecurity, acquiring such specific, up-to-date data might prove challenging due to privacy concerns, system complexity, or resource limitations. Therefore, removing this factor could streamline your risk assessment process without significantly compromising its effectiveness.	2	deleted	–
6.7	What is the level of physical access control mechanism?	Assessing the level of physical access control is key, especially regarding OT equipment. Such control mechanisms play an important role in preventing unauthorized access to sensitive systems and data. By specifically focusing on OT equipment access, you further tailor the risk assessment to the unique cybersecurity needs of OT environments.	3	revised	4.2
6.8	Whether the access to internet requires Multi-Factor Authentication (MFA)?	Including MFA for internet access is an excellent idea for a risk factor. Enhancing it with additional methods like biometrics or face recognition increases security, ensuring robust authentication controls and reducing unauthorized access. This further strengthens the assessment's ability to implement comprehensive protections for sensitive data.	4	revised	5.4
6.9	What is the level of authentication mechanism to access the HMI (Human Machine Interface)?	The level of authentication mechanism for HMI access is an important factor. It provides insight into potential vulnerabilities, ensuring authorized access and control. This evaluation can significantly enhance cybersecurity, thereby ensuring the project's integrity and safety.	4	kept	4.5
6.10	What is the percentage of OT equipment in proximity to personnel during operation?	While the proximity of OT equipment to personnel provides context about potential physical tampering risks, the quantitative data might be difficult to assess and its impact on cybersecurity is relatively indirect. This factor could add complexity without substantial benefits, making it a candidate for removal to maintain the model's focus and efficiency.	1	deleted	–
6.11	What is the percentage of OT equipment isolated from project's general network?	Assessing the extent of OT equipment isolation from the general network is a commendable inclusion. This metric provides valuable insights into system segregation, contributing to improved cyber resilience. It allows for better threat containment and impact reduction, making it a crucial factor in preserving both system functionality and security.	4	kept	4.3