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), 6 MetroTech Center, Brooklyn, NY 11201, United States
[3] Department of Computer Science and Engineering, Tandon School of Engineering, New York University (NYU), 6 MetroTech Center, Brooklyn, NY 11201, United States

Email: dongchi.yao@nyu.edu, garcia.de.soto@nyu.edu, mwilkes@nyu.edu

Abstract: With the rapid digitalization of construction projects, incidents of cyberattacks are surging. A comprehensive approach to identifying and managing cyber risks in construction is essential. This study employs a systematic methodology to identify cyber risk factors tailored to construction projects. These 32 identified risk factors reflect general vulnerabilities prevalent in the IT sector and those arising from the complex and dynamic nature of construction projects specific to the construction industry. The risk factors are grouped into five categories: 7 about overall project information, 4 about project structure, 9 about IT, 5 about OT, and 7 about management and human aspects, which can be used to assess a diverse range of cyber risks. Each risk factor is divided into specific numerical or ordinal scales, allowing for a more quantitative risk assessment approach. The long-term goal of this study is to incorporate the identified risk factors into a future cyber risk assessment model, which is intended to be implemented in web or mobile applications utilized by construction practitioners for effective cyber risk management.

Keywords: *Construction Cybersecurity; Digital Transformation; Risk Factors; Risk Assessment; Industry-Specific Vulnerabilities*

1.0 Introduction

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 [1]. 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.

However, the construction industry is lagging behind other industries when it comes to cybersecurity, and its vulnerabilities become starkly evident when examining real-world incidents. The industry has seen a dramatic increase in cyber incidents from nearly 10 in 2013 to almost 520 in 2022—a 5100% rise. This rise is notable in five specific types of cyber risks: ransomware, phishing, insider attacks, data breaches, and supply chain attacks [2]. For example, Bouygues Construction suffered a ransomware attack where attackers held 200GB of data ransom, causing project delays as systems were shut down to prevent further damage [3]. Bird Construction experienced a similar attack with a ransom demand of $9,000,000 CAD to decrypt the 60GB of project data held hostage [4]. These incidents underscore the urgent need for the construction industry to bolster its cybersecurity management to ensure the successful delivery of projects, which calls for the implementation of a comprehensive and effective cyber risk management approach.

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 [5]. 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 notable gap. While ample literature exists on identifying risk factors for other types of risks in construction, such as delay and safety risks, there is a dearth of literature focused on industry-specific cyber risk factors. This gap is not aligned with the extensive utilization of digital technologies in construction projects where cybersecurity is of paramount importance.

Therefore, our study aims to bridge this significant research gap by developing a set of cyber risk factors tailored to the characteristics of construction projects. These risk factors can be applied to a wide range of cyber risks, including but not limited to ransomware, phishing, data breaches, insider attacks, and supply chain attacks. Two objectives are outlined to achieve the goal: (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. Our study will contribute to the existing body of knowledge by (1) providing a systematic methodology framework that can be applied to identify risk factors for other risks, (2) offering a set of risk factors that can serve as a reference for future cyber risk assessments by scholars, and (3) presenting a set of risk factors that construction practitioners can use as a checklist for proactive risk management.

The remaining of this paper is structured as follows: Section 2 addresses the unique cybersecurity challenges in construction and reviews existing literature. Section 3 elaborates on the concept of treating the project as a network structure. Section 4 details the steps and methods of our risk factor identification. Section 5 delves into each risk factor, underscoring their importance to project cybersecurity. Section 6 explores the advantages of these factors in future cyber risk assessments. Section 7 concludes this study and outlines areas for future research.

2.0 Related works

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 [6]. Second, a diverse workforce with varied cybersecurity awareness can lead to security lapses, with less informed individuals prone to errors or phishing attacks [1]. 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 [7]. 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 [1][8]. 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 [9]. Given these distinct vulnerabilities and their interactive effects, a tailored set of risk factors is a must for effective industry-specific cyber risk management. However, such work is still notably absent.

In contrast, the construction industry has witnessed extensive studies addressing a variety of other risks, including financial risks [10]–[13], environmental and safety risks [14], [15], supply chain risks [16], procurement risks [16], [17], technological application risks [5], [18], operational and management risks [19], time performance risks [12], [20], [21], and a mix of these [5], [22]–[26]. Each of these studies introduces a tailored set of risk factors, categorized based on specific criteria, aiming to either enhance the understanding of associated risks or facilitate their assessment. For example, Sharma and Goyal [10] identified 55 risk factors associated with cost overrun risk in construction projects and then conducted a fuzzy assessment on the risk; Hwang et al. [14] identified 42 risk factors associated with environmental and safety risks in green residential construction to enhance understanding of the risks in this specific scenario; Assaf and Al-Hejji [21] identified 53 risk factors, categorizing them into groups such as owner-related, consultant-related, and design-related risks. These factors were then employed to predict the risk of project delays; Zou et al. [5] identified 85 risk factors targeting construction projects in China, covering various types of risks, including

cost, time, quality, and more. However, none of them provide a subset of risk factors for cyber risk, and almost none of them mention risk factors related to cybersecurity.

Compared to the well-explored realms of traditional risks, cybersecurity in construction remains a relatively uncharted territory. In 2023, Pargoo and Ilbeigi [27] underscored 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 [28], [29], [30], [6], engage in broad discussions, accentuating the necessity for specialized, in-depth research to boost the industry's defense and resilience against cybersecurity threats. Additionally, some contributions suggest specific technical solutions like blockchain technology for data decentralization [8], [31], machine learning algorithms for data-driven anomaly detection [8], [32], [33], threat modeling for attack path simulation and assessment [34], [35], framework development for cyber risk identification [36], and the use of CVSS scores for assessment of stakeholder vulnerabilities [37]. Despite these advancements, there is not a single work offering a complete qualitative or quantitative cyber risk assessment that encompasses risk identification, assessment, and response, and a comprehensive set of cyber risk factors, analogous to those for other types of risks, remains absent.

Within the limited body of research on cyber risk assessment in the construction industry, three particular studies are notably related. Mantha and García de Soto [6] advocated for using agent-based models to understand and quantify stakeholders' vulnerabilities and to simulate their propagation within the complex interactions of communication networks. In another work [37], they applied the CVSS scoring method to provide a systematic way of evaluating the vulnerabilities of stakeholders in construction networks. Shibly and García de Soto [34] 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 the three studies are related to cyber risk assessment, none provide a set of risk factors at a project level that can be flexibly adapted and generalized.

In summary, although progress has been made in understanding and mitigating various cyber risks in construction, a complete set of cyber risk factors that reflects the industry's unique vulnerabilities and can be used for thorough risk assessment has yet to be established. This gap underscores the need 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 covers the multifaceted aspects of construction projects.

3.0 Project as network

The project structure is crucial for cybersecurity because it outlines how complex the communication is among stakeholders and shows the potential weak points where attacks could occur within a network. In simpler terms, the way a project is organized can highlight how secure or vulnerable it is to cyber threats [6]. We draw inspiration from [6], where project dynamics are portrayed through an agent-based model and involved stakeholders are simulated to assess the vulnerability propagation. Similarly, we conceptualize the project structure as a network where various teams are interlinked, exchanging information via communication channels. Figure 1 illustrates this. Every team in a construction project (owners, contractors, subcontractors, etc.) is depicted as nodes (represented by circles). The edges (indicated by arrows) exemplify the communications/data exchanges among them through mediums like emails, texts, video calls, or software. The graph is organized into three distinct layers (rings), each identified by a unique color and encompassing diverse teams or sub-teams. The network graph helps us understand the project's structure and how cyber risk is distributed across all teams involved. It provides additional data that enhances the risk assessment model, making it easier to identify and address potential cybersecurity issues in the project network.

The example graph (Figure 1) delineates three layers with varying numbers of teams (sub-teams) and communication channels. In this particular case, Layer 1 has 10 sub-teams (purple circles) and 90 channels (arrows); Layer 2 comprises 14 sub-teams (yellow circles) and 20 channels (arrows); Layer 3 consists of 6 sub-teams (red circles) and 10 channels (arrows). Different project delivery methods yield diverse structures and network graphs. Figure 1 illustrates the Integrated Project Delivery (IPD) delivery method, which involves a complex network of connected teams and sub-teams, creating a dynamic and complicated digital ecosystem. In contrast, other delivery methods, such as Design-Bid-Build (DBB), can result in a more sequential and linear network graph due to their more straightforward and less complex communication

patterns. When collecting data, it is beneficial to guide the project manager or interviewee in creating a rough network graph like this to extract useful information.

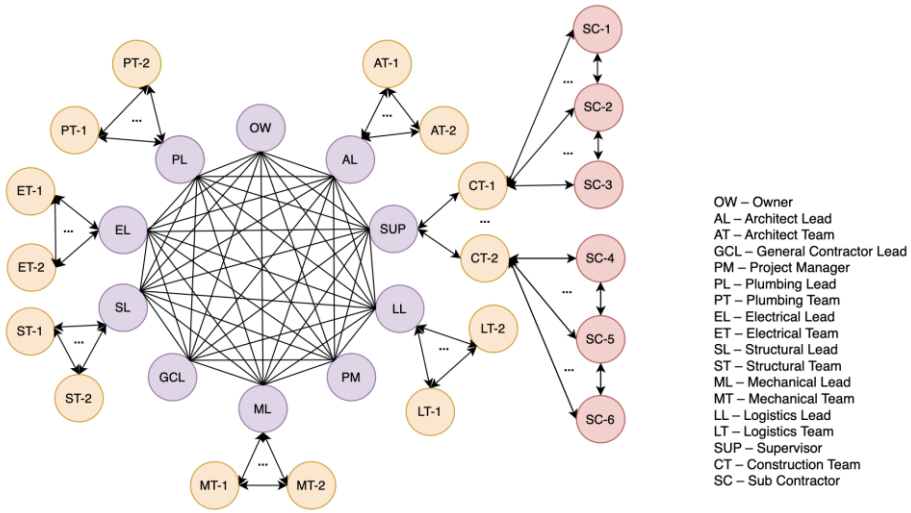

Figure 1. Network graph of a construction project (adapted from [6])

4.0 Steps and methods

This section presents the steps and methods used in our study to systematically identify a ready-to-use comprehensive set of risk factors that encompass various aspects of a construction project. Among the existing methods for identifying risk factors [38], we chose a combination of three: literature review, expert evaluation, and questionnaire survey for a well-rounded analysis and identification. The entire process of identifying risk factors can be visualized in Figure 2, which can be broadly divided into two stages: initial identification of risk factors based on literature review, followed by refining them through questionnaires and expert opinions.

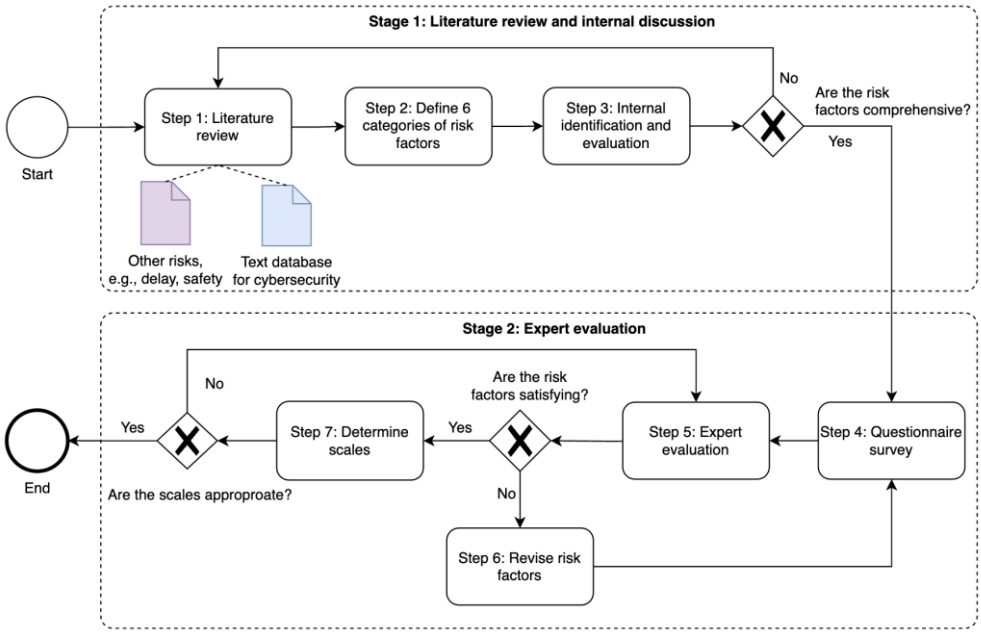

Figure 2. The process of risk factor identification

Step 1: Literature review

We began our study with a thorough review of the 18 publications on various types of risks in construction projects, as detailed in Section 2.0. These sources offer 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, we

investigated six textual sources concerning cybersecurity in the construction industry, published in our previous work as a database containing a large number of sentences [9]. These sources, collected from six types of construction cybersecurity literature, offer an in-depth exploration of cybersecurity challenges and risks in construction. Table 1 presents a statistical overview of these sources.

Table 1. Statistical information of the text database

Text source	Number of documents	Number of sentences	Total number of sentences
News articles and blogs	75 websites	71 K	802 K
LexisNexis databases	3,968 pieces of news	596 K	
Academic papers	78 files	26 K	
Books (chapters)	13 files	73 K	
Specifications/Standards	37 files	22 K	
Company reports	46 files	14 K	

Step 2: Define risk factor categories

After reviewing the literature, we initially identified six aspects of a construction project that collectively offer a comprehensive view of the cybersecurity landscape, which 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 is 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, we recurrently reviewed the literature, referring back to Step 1, to identify as many relevant risk factors as possible with the goal of achieving a comprehensive compilation. Simultaneously, we conducted regular internal discussions to assess these factors, totaling ten discussions over one month. In each discussion session, we assessed the previously identified risk factors considering 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 informed our decision on whether to include each factor. If there were disagreements on including certain risk factors, we kept them tentatively on the list. Later, we sought feedback on these disputed factors from external experts to gain additional insights. Ultimately, we compiled a list of 62 preliminary risk factors, as outlined in Table 3, 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: Questionnaire survey

We developed a detailed questionnaire that was presented to experts to gather feedback on the 62 identified cybersecurity risk factors. This questionnaire 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, we have included textual descriptions, illustrative graphics, or mathematical derivations 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 was presented to three experts, two of whom specialize in cybersecurity and are affiliated with a cybersecurity company based in New York, U.S., with an average of over 20 years of industry experience. They were requested to provide a score ranging from 1 to 5, indicating their perception of the level of reasonability for including each risk factor from a cybersecurity perspective. We conducted online meetings and email communications to discuss the questionnaire, collect the scoring, and gather feedback. The third expert specializes in construction and is associated with one of the leading construction companies in the Middle East, with over 8 years of experience. This expert provided feedback on the comprehensibility and appropriateness of the factors within the context of the construction industry at the same time. Communication with this expert was primarily conducted through email and phone calls. In later communications, after finalizing the risk factors, all three experts provided feedback on the scale design of these factors, detailed in Step 7.

Engaging experts from both cybersecurity and construction sectors enriches the validity and applicability of our identified risk factors. Their diverse insights ensure a well-rounded, cross-industry perspective, enhancing the robustness and relevance of the factors in both contexts. Table 2 provides a summarization of the experts and the collaborative process. Spanning approximately five months, this collaborative phase involved online meetings, emails, and phone calls. We have retained the recordings of these communications and copies of email correspondences, with permission, for future reference during the iterative risk factor revision process.

Table 2. Overview of expert information and collaborative process

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

Step 6: Revise risk factors

The finalization of risk factors is an iterative, staged process closely linked to step 5. After collecting scores and initial feedback, we adjusted the risk factors in the questionnaire, including their explanation, scope, and time span certain risk factors cover, among others. We then continued to consult with experts on these revisions to confirm if the risk factors were appropriately refined at each stage; in the meantime, new risk factors, if any, were added as suggested. This approach allowed us to systematically incorporate feedback and align with expert insights. After concluding all discussions and communications, we eliminated risk factors with an average score below 3. One significant removal is the previous category, "Cybersecurity Scores." This change was prompted by all experts' advice, indicating that the risk factors within this category, primarily concerning the cybersecurity scoring of each team, are challenging to quantify and, therefore, not

practical and should be eliminated from this study. We consolidate the average scores of the original risk factors and the suggested actions from the experts in Table 3. We originally planned to include a summary of the feedback in the table, but it has been omitted due to page constraints.

Table 3. Initial list of risk factors and expert feedback

Category	NO.	Risk factor	Score	Action
1. Basic Information of the Project	1.1	Is your construction company global or local?	2	deleted
	1.2	What is the scale of your construction company?	4	revised
	1.3	What is the current phase of the construction project?	5	kept
	1.4	What is the weather of the current project phase?	1	deleted
	1.5	What is the total number of people involved in the project?	4	revised
	1.6	What is the percentage of people who have access to sensitive information?	5	kept
	1.7	What is the percentage of FTE (full-time employees) involved in the project?	1	deleted
	1.8	What is the percentage of people with over 10 years working in the organization?	1	deleted
	1.9	What is the region of the project?	5	revised
2. Project Structure	2.1	What is the project delivery method?	5	kept
	2.2	What is the number of sub-teams at different layers of the project?	3	kept
	2.3	What is the total number of teams in the project?	1	deleted
	2.4	What is the number of communication channels at different layers in the project?	4	kept
	2.5	What is the total number of communication channels among teams in the project?	1	deleted
	2.6	What is the average communication strength of channels at each layer?	2	deleted
	2.7	What is the overall communication strength of all channels?	2	deleted
	2.8	What is the average maturity of communication channels at different layers?	1	deleted
	2.9	What is the overall maturity of all communication channels?	1	deleted
3. Cybersecurity Scores	3.1	What is the average risk score at each layer of the project?	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		
4. Project Context	4.1	What is the level of the cybersecurity impact and stakeholder engagement regarding cybersecurity?	2	deleted
	4.2	Whether there is a dedicated cybersecurity legal team?	5	kept
	4.3	What is the level of commitment to corporate governance and ethical practices regarding cybersecurity?	5	kept
	4.4	What is the percentage of the total project budget for cybersecurity management?	5	kept
	4.5	What is the level of financial risk?	2	deleted
	4.6	What is the frequency of daily information exchange?	2	deleted
	4.7	What is the average socioeconomic level of the involved people?	3	kept
	4.8	What is the degree of variation in the socioeconomic level of the involved people?	2	deleted
	4.9	What is the percentage of teams overlapping in different projects?	4	kept
	4.10	What is the average level of team member variability?	4	revised
	4.11	What is the average churn rate of all teams?	1	deleted
5. Information Technology (IT) Factors	5.1	Is the IT staff under-resourced for the size of the project?	2	deleted
	5.2	What is the number of user endpoints of digital devices?	5	kept
	5.3	What is the average computer/laptop security score?	1	deleted
	5.4	What is the ratio of Windows system vs non-Windows?	2	deleted
	5.5	What is the ratio of Android vs non-Android systems?	2	deleted
	5.6	Whether 90% of the computers/laptops have 90% of its applications are up to date?	2	deleted
	5.7	What is the construction-related APP/software maturity level?	2	deleted
	5.8	Is there a dedicated IT team for the project?	5	kept
	5.9	What is the level of stringency of cybersecurity policy?	2	deleted
	5.10	What is the level of commitment to cybersecurity policy?	2	deleted

Table 3. (continued)

Category	NO.	Risk factor	Score	Action
5. Information Technology (IT) Factors	5.11	What is the average frequency of security training per year among all teams?	5	kept
	5.12	What is the percentage of people who fail phishing tests a second time after completing the required training?	4	revised
	5.13	What is the percentage of password reuse among employees in the project?	4	revised
	5.14	Is there any presence of exploitable critical findings in annual pen testing?	2	deleted
	5.15	What is the estimated mean time to respond (MTTR) of the project in hours?	3	kept
	5.16	What is the number of production-impacting incident tickets per month in the project?	2	deleted
6. Operational Technology (OT) Factors	6.1	What is the total number of critical digital assets in the project?	5	kept
	6.2	What is the total number of important OT equipment and devices?	4	kept
	6.3	What is the average age of the important OT equipment?	3	kept
	6.4	Type of Network used in the project (Public Network or Private Network?)	5	kept
	6.5	What is the percentage of digital devices with firewalls or intrusion detection systems involved in the project?	5	kept
	6.6	What is the percentage of firewalls and endpoint detection systems with the latest security updates?	2	deleted
	6.7	What is the level of the physical access control mechanism?	3	revised
	6.8	Does access to the internet require Multi-Factor Authentication (MFA)?	4	revised
	6.9	What is the level of authentication mechanism to access the HMI (Human Machine Interface)?	4	kept
	6.10	What is the percentage of OT equipment in proximity to personnel during operation?	1	deleted
	6.11	What is the percentage of OT equipment isolated from the project's general network?	4	kept

As a result, we arrived at a final set of 32 risk factors, 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 Table 4, with counts of 7, 4, 9, 5, and 7, respectively. Importantly, Categories 3, 4, and 5 are tailored to evaluate a specific company and the project phase it is involved in, necessitating the consideration of its sub-teams. 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. Table 4 displays the finalized risk factors along with their corresponding numbering in the initial version. A detailed explanation of each risk factor and its implications for project cybersecurity will be covered in Section 5.

Table 4. List of selected risk factors (32 total)

Category	NO.	Risk factor	Scales	Previous No.
1. Overall project information	1.1	What is the country of the project?	Asia, Europe, Africa, North America, South America, Antarctica, and Oceania. We initially asked for information about the country, and then derived the continent.	1.9
	1.2	What is the project budget?	<= $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?	<= 1%, 1% - 2%, 2% - 3%, 3% - 4%, 4% - 5%, > 5%	4.4
	1.4	What is the project duration?	<= 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)?	<= 50, 51 - 100, 101 - 200, 201 - 300, 301 - 400, > 400	1.5
	1.6	What is the project type?	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?	Yes, No, Unsure	4.2

Table 4. (continued)

Category	NO.	Risk factor	Scales	Previous No.
2. Project structure	2.1	What is the project delivery method?	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?	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?	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?	<= 20%, 21% - 40%, 41% - 60%, 61% - 80%, 81% - 100%	4.9
3. IT factors	3.1	What is the scale of your company?	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?	Planning and Bidding phase, Design phase, Construction phase, Maintenance & Operation phase, Demolition phase	1.3
	3.3	Is there a dedicated IT team for the project?	Yes, No, Unsure	5.8
	3.4	What is the total number of critical digital assets?	<= 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?	<= 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?	<= 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?	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?	<= 20%, 21% - 40%, 41% - 60%, 61% - 80%, 81% - 100%	5.12
	3.9	What is the estimated Mean Time to Respond (MTTR) in hours?	Within 1 hour, 1 - 4 hours, 4 - 8 hours, 8 - 24 hours, Above 24 hours	5.15
4. OT factors	4.1	What is the total number of important OT equipment involved?	<= 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?	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?	<= 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?	<= 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)?	Level 1, Level 2, Level 3, Level 4, Level 5	6.9

Table 4. (continued)

Category	NO.	Risk factor	Scales	Previous No.
5. Management and human factors	5.1	What is the average level of commitment to corporate governance, ethical practices and cybersecurity policy?	Level 1, Level 2, Level 3, Level 4, Level 5	4.3
	5.2	What is the average frequency of security training per year?	<= 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.)?	Yes, No	5.13
	5.4	Does internet access within your construction project require Multi-Factor Authentication (MFA) or utilize other methods such as biometrics or face recognition?	Yes, No	6.8
	5.5	What is the percentage of people who have access to sensitive information in the project?	<= 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?	<= 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?	Level 1, Level 2, Level 3, Level 4, Level 5	4.7

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 [6], [20], [34], [37]. As an illustration, in the study of predicting project delay risk [20], 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 [21], 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 initial determination of these scales was based on our expertise and fundamental understanding of construction projects. They were incorporated into the final version of the questionnaire with 32 risk factors presented to the experts, as outlined in Step 4. The determination of the final scales also underwent an iterative process. The feedback and insights garnered from them prompted refinements to the scales—some were expanded, others narrowed, and certain risk factors transitioned from level representation to numerical representation. The iterative refinements and expert validations have shaped the final scales that strike a balance between detailed granularity and practical feasibility. The finalized scales for each risk factor are presented in Table 4.

5.0 Understanding cybersecurity implications of 32 risk factors

This section delves into the impact of each risk factor on the cybersecurity of construction projects, aiding in a deeper comprehension of their significance. Table 4 provides a detailed breakdown of the scales associated with each risk factor.

5.1 Category (1): Overall Information of the Project

This category 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.

- **Risk factor 1.1: What is the country of the project?** The project's country influences its cybersecurity due to varied regulations, technology infrastructure, and cyber threat levels in different

nations. Each country's unique cybersecurity regulations and threat landscape necessitate tailored security measures. Therefore, the location can impact the complexity and nature of security strategies needed to mitigate potential cyber risks effectively.

- **Risk factor 1.2: What is the project budget?** The overall project budget is a relevant cybersecurity risk factor, as limited funding may constrain resources allocated to IT infrastructure, security controls, auditing, training, and expertise. Larger budgets allow more investment in robust cybersecurity measures and skilled personnel to implement best practices.
- **Risk factor 1.3: What is the percentage of the total project budget for cybersecurity management?** The allocation to cybersecurity affects a project's defense capability. Insufficient funds can lead to vulnerabilities, while adequate investment ensures robust security measures, skilled personnel, and effective responses to cyber threats, safeguarding project integrity and data security.
- **Risk factor 1.4: What is the project duration?** Project duration impacts cybersecurity due to evolving threats. Longer projects face changing, potentially escalating cyber threats requiring ongoing adaptations in security measures. Shorter timelines may minimize exposure but still necessitate comprehensive security plans to protect against breaches.
- **Risk factor 1.5: What is the total number of people involved in the project? (labor excluded)** The number of non-labor participants correlates with cybersecurity risk. More individuals increase potential points of vulnerability due to human error or insider threats. Managing and training a larger group in cybersecurity protocols becomes vital to mitigate risks of breaches and data leaks.
- **Risk factor 1.6: What is the project type?** Different project types present distinct cybersecurity challenges. Infrastructure, residential, commercial, or industrial projects each have unique security needs and vulnerabilities. Identifying the project type helps tailor cybersecurity measures to specific risks and regulatory requirements, enhancing the effectiveness of security protocols.
- **Risk factor 1.7: Whether there is a dedicated cybersecurity legal team?** A cybersecurity legal team signifies enhanced preparedness and response to legal issues arising from cyber threats. Their absence can expose the project to regulatory non-compliance, liability risks, and inadequate legal response during cybersecurity incidents, impacting project security and integrity.

5.2 Category (2): Project Structure

Four factors in this category 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.

- **Risk factor 2.1: What is the project delivery method?** Different delivery methods (e.g., Design-Bid-Build (DBB), Integrated Project Delivery (IPD)) have varying levels of collaboration, contractual relationships, and information sharing among stakeholders. The specific delivery method can impact the project's cybersecurity posture by affecting access to sensitive information, communication channels, and the implementation of security protocols.
- **Risk factor 2.2: What is the number of sub-teams at different layers of the project?** The number of sub-teams at various project layers can be an indicator of cyber risk. Typically, outer-layer sub-teams (shown in Figure 1), potentially smaller with limited cybersecurity resources, pose more risks. Inner-layer teams are often larger, better equipped, and more aware of cybersecurity. Thus, tracking sub-teams across layers helps in targeted risk management.
- **Risk factor 2.3: What is the number of communication channels at different layers in the project?** This factor gauges the security implications of the number of communication channels within each layer of the project. A higher count can amplify vulnerabilities due to increased data exchange points, necessitating enhanced security protocols to protect sensitive information and maintain system integrity at each layer.
- **Risk factor 2.4: What is the percentage of teams overlapping in different projects?** The percentage of teams working on multiple projects simultaneously (overlap) increases cyber risks through shared resources, people, and potential security gaps. More overlap raises breach, gap, and dependency risks, requiring management to mitigate threats. Team overlaps matters because shared resources and personnel heighten cyber vulnerabilities.

Categories (1) and (2) emphasize the general information of the project, whereas Categories (3), (4), and (5) are tailored to specific phases of the project and are particularly relevant to the specific company engaged in those phases. This approach ensures that the risk assessment model to be established is comprehensive, incorporating both generic project data and phase-specific data. Furthermore, Categories (3) through (5) must take into account all sub-teams during the data-gathering process to ensure a thorough and accurate assessment.

5.3 Category (3): IT factors

Nine elements in this category 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.

- **Risk factor 3.1: What is the scale of your company?** Larger firms often have more resources for advanced security measures but can be targets for cyberattacks due to their visibility and data value. In contrast, smaller companies, though less visible, may be more vulnerable due to limited security resources and expertise despite potentially having fewer threats to contend with.
- **Risk factor 3.2: What is the phase of the construction project when your company is involved?** The project phase influences cybersecurity needs. For example, the design phase may focus on data protection and privacy, while the construction phase phases might emphasize system security and integrity. Each phase presents unique cyber challenges, requiring tailored strategies to mitigate risks effectively.
- **Risk factor 3.3: Is there a dedicated IT team for the project?** A dedicated IT team enhances real-time response and management of cybersecurity issues. Without it, a project may face delayed responses to threats, increased vulnerabilities, and potential breaches, impacting the security and integrity of project data and systems.
- **Risk factor 3.4: What is the total number of critical digital assets?** The quantity of critical digital assets indicates the potential risk exposure. These assets encompass various data types, including BIM files, project plans, management data, contracts, communication platforms, and databases. More assets mean increased vulnerability points, requiring enhanced security measures to ensure the integrity and confidentiality of sensitive data and systems amidst various cyber threats. We can estimate the total count by considering the number of stored digital documents across various project management systems, including cloud storage, PCs, and mobile devices used for the project. Consider the number of stored digital documents such as BIM files, project plans, contracts, and other relevant files. While it may not provide an exact count, this estimation method gives a reasonable understanding of the overall volume of digital assets.
- **Risk factor 3.5: What is the total number of user endpoints of digital devices for the project?** As the number of connected devices, such as laptops and smartphones, increases in a network, so does the attack surface. Each additional device provides another potential entry point for cyber threats, making the network more vulnerable to security breaches. To acquire accurate data on user endpoints, we can utilize a centralized information or inventory system that catalogs all devices within a project. This resource allows for the identification and counting of every unique device, including laptops, desktops, and smartphones, integral to the digital infrastructure.
- **Risk factor 3.6: What is the percentage of digital devices with firewalls or intrusion detection systems involved in the project?** The percentage of devices with firewalls or intrusion detection systems reflects the project's defense depth against cyber threats. A higher percentage indicates stronger security, while lower figures suggest potential vulnerabilities and the need for enhanced protective measures.
- **Risk factor 3.7: What is the network type used for the project: Public or Private?** Choosing between a public or private network impacts a project's cybersecurity. Public networks can be vulnerable to attacks due to easier access, while private networks offer enhanced security controls but may be costly and complex to manage. Each type requires specific security approaches.

- **Risk factor 3.8: What is the percentage of individuals who fail phishing tests after completing mandatory training?** The percentage of individuals failing phishing tests post-training indicates the effectiveness of education programs and the remaining vulnerability to phishing attacks, highlighting areas for improvement in training and awareness to enhance cybersecurity defenses.
- **Risk factor 3.9: What is the estimated Mean Time to Respond (MTTR) in hours?** The MTTR estimates the average time required for the project team, including sub-teams, to respond to and resolve cybersecurity incidents. It is calculated by tracking the time from the moment an incident is detected to the time it is fully resolved. Add up the response and resolution times for all incidents, then divide by the total number of incidents to get the average MTTR. This process should be done for the team and all sub-teams, and the results should be averaged to get an overall MTTR for the project.

5.4 Category (4): OT factors

This category, containing five factors, centers on the project's operational technology. It looks at the equipment and systems pivotal 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; environmental monitoring systems; control panels and field devices; SCADA systems; and remote monitoring and control systems [39]. 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.

- **Risk factor 4.1: What is the total number of important OT equipment involved?** The number of critical OT equipment pieces is directly proportional to the potential attack surface. A higher count indicates an increased risk, necessitating more complex and robust security protocols to mitigate the risks of operational disruptions, data breaches, and system failures, thereby ensuring the operational continuity and integrity of the construction project.
- **Risk factor 4.2: What is the level of physical access control mechanism to OT equipment?** Evaluating physical access control mechanisms, including secure entry points, surveillance, and ID badges, is vital to prevent unauthorized physical access to sensitive systems and data. More stringent controls like biometrics and visitor audits indicate a higher security level. Robust physical access control is crucial for maintaining cybersecurity.
- **Risk factor 4.3: What is the percentage of OT equipment isolated from the project's general network?** Measuring the percentage of operational technology assets separated from the general network assesses the extent of critical system isolation. Higher levels of OT equipment segregation into distinct networks enhance cyber resilience by preventing unauthorized access, containing threats, and minimizing impacts to maintain functionality.
- **Risk factor 4.4: What is the average age of the important OT equipment, in years?** The average age indicates potential vulnerabilities from aging infrastructure, like inadequate security, maintenance issues, and decreased performance. Tracking average age helps identify needs for upgrades, maintenance, and resources to ensure reliable, secure OT operations and mitigate risks from outdated equipment.
- **Risk factor 4.5: What is the level of authentication mechanism to access the HMI (Human Machine Interface)?** This factor is crucial given the pivotal role HMI plays as the interface connecting operators to machinery or plant control systems. It evaluates the strength of authentication protocols for HMI access. Higher levels indicate robust measures like multi-factor or biometric verification. Including this evaluates potential vulnerabilities, ensuring only authorized access and control through the HMI. Assessing the HMI access authentication mechanism enhances cybersecurity and safeguards the project's integrity and safety.

5.5 Category (5): Management and Human Factors

Seven factors in this category explore the company's governance, ethical standards, and cybersecurity culture. It underscores 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.

- **Risk factor 5.1: What is the average level of commitment to corporate governance, ethical practices and cybersecurity policy?** This reflects a project's commitment to incorporating principles of good governance and ethics into its cybersecurity efforts. It encompasses compliance with laws and regulations, transparency, accountability, and the making of ethical decisions. A strong commitment bolsters stakeholder trust and contributes to the project's success, whereas inadequate governance may result in reputational harm and legal complications.
- **Risk factor 5.2: What is the average frequency of security training per year?** The average yearly cybersecurity training frequency for all teams indicates how proactively knowledge and skills are enhanced. More frequent sessions promote awareness, inform on threats and best practices, and foster a culture of security. Regular training enables teams to effectively contribute to the project's overall security posture.
- **Risk factor 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.)?** Including this factor is crucial because password reuse can significantly heighten cybersecurity risk. It measures the project's vulnerability to unauthorized access and potential breaches. Assessing this aspect enables the implementation of stringent password policies to enhance overall security and data protection.
- **Risk factor 5.4: Does internet access within your construction project require Multi-Factor Authentication (MFA) or utilize other methods such as biometrics or face recognition?** The use of MFA, biometrics, or face recognition enhances security by adding layers of authentication, reducing unauthorized access risks. The absence or inadequacy of these measures can increase vulnerabilities, emphasizing the need for robust authentication to secure internet access and protect sensitive project data and systems.
- **Risk factor 5.5: What is the percentage of people who have access to sensitive information in the project?** Here, sensitive information refers to any data that is protected against unwarranted disclosure, such as personal identification information, financial records, and proprietary project details. A larger percentage of people with access to sensitive data increases the risk of breaches. It underscores the need for stringent access controls and security protocols to protect sensitive information, minimize insider threats, and ensure that data confidentiality and integrity are maintained throughout the project's lifecycle.
- **Risk factor 5.6: What is the average team member variability over a 3-month period?** Team member variability refers to the extent of changes in team composition during a project. More frequent changes increase cyber risks, as new members may introduce vulnerabilities while departing members leave gaps. Frequent team changes impact security practices and knowledge retention. A higher level of variability indicates more frequent team changes, increasing project cybersecurity risks.
- **Risk factor 5.7: What is the average socioeconomic level of the people involved in the project?** This refers to the collective economic and social standing of the project's personnel, measured by income, education, and occupation. It is essential for assessing potential disparities in cybersecurity awareness and practices. Individuals with higher socioeconomic statuses often exhibit better cybersecurity attitudes and behaviors, influencing the overall project's cyber risk.

6.0 Enhancing cyber risk assessment

The established set of risk factors offers four advantages for cyber risk assessment models, which are expounded as follows.

(1) Capturing project structure dynamics. In our study, we innovate by viewing the project as a multi-layered network, providing a detailed understanding of its complex structure and associated cybersecurity vulnerabilities. Each layer includes a variety of teams, sub-teams, and communication channels. From these, we have identified specific risk factors in Category 2 that extract statistical features concerning the spread of sub-teams and communication channels across the project's layered network. This detailed, layer-specific information enhances future risk assessment models, enabling them to capture the dynamic and complex nature of modern construction projects. Including this structural information can improve the accuracy and

reliability of the predictions of the risk assessment model, setting our approach apart from previous studies [34], which neglect the importance of a project's layered structure in assessing risks.

(2) Enhancing specificity with contextual insight. Risk factors in Categories 1 and 2 offer a broad overview of the project, ensuring a comprehensive encapsulation of general information and establishing a foundational context for the risk assessment model. In contrast, risk factors in Categories 3, 4, and 5 derive from specific project phases, with data sourced directly from the companies involved, ensuring phase-specific specificity. This integration of broad and detailed data boosts the model's efficacy in making nuanced risk predictions that are specific to the phase the company is involved in without losing the contextual information of the project. As a result, the model makes risk predictions that are both comprehensive and applicable across distinct project phases, marking an advancement in the field of cyber risk assessment.

(3) Enabling a more quantitative risk assessment. Many works, including [6], [20], and [40], 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. In addition to the risk factors addressing general vulnerabilities, some align with the distinct vulnerabilities of the construction industry, as delineated in Section 2. These correlations are explicitly mapped in Table 5, with an explanation of how these risk factors can be efficacious. By analyzing diverse risk factors, the model can balance between addressing general cybersecurity concerns while simultaneously addressing challenges specific to the construction sector.

Table 5. Correlation 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.

7.0 Conclusions

This study adopts a systematic approach to identify 32 risk factors tailored for assessing cyber risks in construction projects, which are grouped into five categories: Overall Information of the Project, Project Structure, IT Factors, OT Factors, and Management and Human Factors. These factors, capturing both general vulnerabilities and distinct vulnerabilities linked to construction projects, are capable of evaluating a broad spectrum of cyber risks. The identified risk factors offer four advantages for cyber risk assessment in this domain: Treating the project as a network allows for the capture of complex project structures and, consequently, the associated cybersecurity vulnerabilities inherent in each layer's dynamics. The integration of both broad and phase-specific data enhances the model's predictive specificity to project phases without

compromising the overall project's contextual insight, ensuring tailored and context-aware risk assessments. The incorporation of risk factor scales facilitates a more quantitative risk assessment, boosting objectivity and consistency in risk evaluations and mitigating the influence of subjective judgments and expert biases. The inclusion of industry-specific risk factors ensures that the model is not only comprehensive but also tailored to address unique vulnerabilities inherent to the construction sector. However, a limitation exists: the specific risk degree associated with each scale of each risk factor has not been determined. For instance, the varying risk degrees for different project countries remain undefined. A simple method would be to calculate the proportion of cyber incidents in each country, but acquiring such comprehensive and accurate data is challenging. Addressing this issue is reserved for future research, which will assess various qualitative and quantitative methods to determine the most effective approach.

Acknowledgments

This work was supported by the Center for Cyber Security (CCS), funded by Tamkeen under the NYUAD Research Institute Award G1104. It was conducted in collaboration with the NYUAD Center for Interacting Urban Networks (CITIES), funded by Tamkeen under the NYUAD Research Institute Award CG001. We 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.

References

[1] S. Kurtz, "Cybersecurity Vulnerabilities in the Construction Industry," Total IT Information Technology. Accessed: Mar. 19, 2021. [Online]. Available: https://totalit.com/cybersecurity-vulnerabilities-in-the-construction-industry/

[2] Deloitte, "Building cybersecurity in the construction industry." Accessed: Sep. 30, 2023. [Online]. Available: https://www2.deloitte.com/ce/en/pages/real-estate/articles/ce-building-cybersecurity-in-the-construction-industry.html

[3] A. Barbaschow, "Bouygues Construction falls victim to ransomware," ZDNET. Accessed: Sep. 30, 2023. [Online]. Available: https://www.zdnet.com/article/bouygues-construction-falls-victim-to-ransomware/

[4] Tunney Catharine, "Ransomware attack on construction company raises questions about federal contracts," CBC News. Accessed: Sep. 30, 2023. [Online]. Available: https://www.cbc.ca/news/politics/ransomware-bird-construction-military-1.5434308

[5] P. X. W. Zou, G. Zhang, and J. Wang, "Understanding the key risks in construction projects in China," *International Journal of Project Management*, vol. 25, no. 6, pp. 601–614, Aug. 2007, doi: 10.1016/j.ijproman.2007.03.001.

[6] B. R. K. Mantha and B. García de Soto, "Cyber security challenges and vulnerability assessment in the construction industry," in *Proceedings of the Creative Construction Conference 2019*, Budapest University of Technology and Economics, 2019, pp. 29–37. doi: 10.3311/CCC2019-005.

[7] K. Nyamuchiwa, Z. Lei, and C. Aranas, "Cybersecurity Vulnerabilities in Off-Site Construction," *Applied Sciences (Switzerland)*, vol. 12, no. 10, May 2022, doi: 10.3390/app12105037.

[8] E. A. Parn and D. Edwards, "Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence," *Engineering, Construction and Architectural Management*, vol. 26, no. 2. 2019. doi: 10.1108/ECAM-03-2018-0101.

[9] D. Yao and B. García de Soto, "A corpus database for cybersecurity topic modeling in the construction industry," Jul. 2023. doi: 10.22260/ISARC2023/0072.

[10] S. Sharma and P. K. Goyal, "Fuzzy assessment of the risk factors causing cost overrun in construction industry," *Evol Intell*, vol. 15, no. 4, pp. 2269–2281, Dec. 2022, doi: 10.1007/s12065-019-00214-9.

[11] D. Baloi and A. D. F. Price, "Modelling global risk factors affecting construction cost performance," *International Journal of Project Management*, vol. 21, no. 4, 2003, doi: 10.1016/S0263-7863(02)00017-0.

[12] M. S. B. A. Abd El-Karim, O. A. Mosa El Nawawy, and A. M. Abdel-Alim, "Identification and assessment of risk factors affecting construction projects," *HBRC Journal*, vol. 13, no. 2, pp. 202–216, Aug. 2017, doi: 10.1016/j.hbrcj.2015.05.001.

[13] N. Chileshe and A. Boadua Yirenkyi-Fianko, "An evaluation of risk factors impacting construction projects in Ghana," *Journal of Engineering, Design and Technology*, vol. 10, no. 3, pp. 306–329, Oct. 2012, doi: 10.1108/17260531211274693.

[14] B. G. Hwang, M. Shan, H. Phua, and S. Chi, "An exploratory analysis of risks in green residential building construction projects: The case of Singapore," *Sustainability (Switzerland)*, vol. 9, no. 7, 2017, doi: 10.3390/su9071116.

[15] P. Aghaei, G. Asadollahfardi, and A. Katabi, "Safety risk assessment in shopping center construction projects using Fuzzy Fault Tree Analysis method," *Qual Quant*, vol. 56, no. 1, 2022, doi: 10.1007/s11135-021-01115-9.

[16] C. A. Rudolf and S. Spinler, "Key risks in the supply chain of large scale engineering and construction projects," *Supply Chain Management*, vol. 23, no. 4, 2018, doi: 10.1108/SCM-09-2017-0292.

[17] D. W. M. Chan, A. P. C. Chan, P. T. I. Lam, J. F. Y. Yeung, and J. H. L. Chan, "Risk ranking and analysis in target cost contracts: Empirical evidence from the construction industry," *International Journal of Project Management*, vol. 29, no. 6, 2011, doi: 10.1016/j.ijproman.2010.08.003.

[18] G. D. Goh, S. L. Sing, and W. Y. Yeong, "A review on machine learning in 3D printing: applications, potential, and challenges," *Artif Intell Rev*, vol. 54, no. 1, pp. 63–94, Jan. 2021, doi: 10.1007/s10462-020-09876-9.

[19] P. Rezakhani, "Classifying Key Risk Factors in Construction Projects," *The Bulletin of the Polytechnic Institute of Jassy, Construction and Architecture Section*, vol. 62, no. 2, 2012.

[20] A. Gondia, A. Siam, W. El-Dakhakhni, and A. H. Nassar, "Machine Learning Algorithms for Construction Projects Delay Risk Prediction," *J Constr Eng Manag*, vol. 146, no. 1, Jan. 2020, doi: 10.1061/(ASCE)CO.1943-7862.0001736.

[21] S. A. Assaf and S. Al-Hejji, "Causes of delay in large construction projects," *International Journal of Project Management*, vol. 24, no. 4, pp. 349–357, May 2006, doi: 10.1016/j.ijproman.2005.11.010.

[22] A. M. Jarkas and T. C. Haupt, "Major construction risk factors considered by general contractors in Qatar," *Journal of Engineering, Design and Technology*, vol. 13, no. 1, 2015, doi: 10.1108/JEDT-03-2014-0012.

[23] S. M. Renuka, C. Umarani, and S. Kamal, "A Review on Critical Risk Factors in the Life Cycle of Construction Projects," *Journal of Civil Engineering Research*, vol. 4, no. 2A, 2014.

[24] I. Y. Wuni, G. Q. P. Shen, and A. T. Mahmud, "Critical risk factors in the application of modular integrated construction: a systematic review," *International Journal of Construction Management*, vol. 22, no. 2, 2022, doi: 10.1080/15623599.2019.1613212.

[25] P. X. W. Zou and G. Zhang, "Managing risks in construction projects: Life cycle and stakeholder perspectives," *International Journal of Construction Management*, vol. 9, no. 1, 2009, doi: 10.1080/15623599.2009.10773122.

[26] Mahmoud Mohamed Mahmoud Sharaf and Hassan T. Abdelwahab, "Analysis of Risk Factors for Highway Construction Projects in Egypt," *Journal of Civil Engineering and Architecture*, vol. 9, no. 5, 2015, doi: 10.17265/1934-7359/2015.05.004.

[27] N. Salami Pargoo and M. Ilbeigi, "A Scoping Review for Cybersecurity in the Construction Industry," *Journal of Management in Engineering*, vol. 39, no. 2, Mar. 2023, doi: 10.1061/JMENEA.MEENG-5034.

[28] A. Bello and A. Maurushat, "Technical and Behavioural Training and Awareness Solutions for Mitigating Ransomware Attacks," in *Advances in Intelligent Systems and Computing*, vol. 1226 AISC, 2020, pp. 164–176. doi: 10.1007/978-3-030-51974-2_14.

[29] S. El-Sayegh, L. Romdhane, and S. Manjikian, "A critical review of 3D printing in construction: benefits, challenges, and risks," *Archives of Civil and Mechanical Engineering*, vol. 20, no. 2. 2020. doi: 10.1007/s43452-020-00038-w.

[30] B. García de Soto, I. Agustí-Juan, S. Joss, and J. Hunhevicz, "Implications of Construction 4.0 to the workforce and organizational structures," *International Journal of Construction Management*, vol. 22, no. 2, pp. 205–217, Jan. 2022, doi: 10.1080/15623599.2019.1616414.

[31] G. Shemov, B. García de Soto, and H. Alkhzaimi, "Blockchain applied to the construction supply chain: A case study with threat model," *Frontiers of Engineering Management*, vol. 7, no. 4, pp. 564–577, Dec. 2020, doi: 10.1007/s42524-020-0129-x.

[32] A. Sheikh, V. Kamuni, A. Patil, S. Wagh, and N. Singh, "Cyber Attack and Fault Identification of HVAC System in Building Management Systems," in *2019 9th International Conference on Power and Energy Systems (ICPES)*, IEEE, Dec. 2019, pp. 1–6. doi: 10.1109/ICPES47639.2019.9105438.

[33] Z. Pan, S. Hariri, and J. Pacheco, "Context aware intrusion detection for building automation systems," *Comput Secur*, vol. 85, pp. 181–201, Aug. 2019, doi: 10.1016/j.cose.2019.04.011.

[34] M. U. R. Mohamed Shibly and B. García de Soto, "Threat Modeling in Construction: An Example of a 3D Concrete Printing System," in *37th International Symposium on Automation and Robotics in Construction*, Oct. 2020. doi: 10.22260/ISARC2020/0087.

[35] B. Mantha, B. García de Soto, and R. Karri, "Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment," *Sustain Cities Soc*, vol. 66, no. December 2020, p. 102682, Mar. 2021, doi: 10.1016/j.scs.2020.102682.

[36] Ž. Turk, B. García de Soto, B. R. K. Mantha, A. Maciel, and A. Georgescu, "A systemic framework for addressing cybersecurity in construction," *Autom Constr*, vol. 133, p. 103988, Jan. 2022, doi: 10.1016/j.autcon.2021.103988.

[37] B. R. K. Mantha and B. García de Soto, "Assessment of the cybersecurity vulnerability of construction networks," *Engineering, Construction and Architectural Management*, vol. 28, no. 10, pp. 3078–3105, Nov. 2021, doi: 10.1108/ECAM-06-2020-0400.

[38] T. Meyer and G. Reniers, *Engineering Risk Management*. 2022. doi: 10.1515/9783110665338.

[39] M. S. Sonkor and B. García de Soto, "Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective," *J Constr Eng Manag*, vol. 147, no. 12, Dec. 2021, doi: 10.1061/(ASCE)CO.1943-7862.0002193.

[40] M. Kalinin, V. Krundyshev, and P. Zegzhda, "Cybersecurity Risk Assessment in Smart City Infrastructures," *Machines*, vol. 9, no. 4, p. 78, Apr. 2021, doi: 10.3390/machines9040078.