Implementation of the Cybersecurity Incident Severity Scale (CISS) to Assess Cyber Incidents in the Construction Sector

Dongchi Yao[1], Bharadwaj R. K. Mantha[2], Borja García de Soto[1]

[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 Environmental Engineering, University of Sharjah, Sharjah, UAE
dongchi.yao@nyu.edu, rmantha@sharjah.ac.ae, garcia.de.soto@nyu.edu

Abstract –

As the construction industry adopts digital technologies, cybersecurity risks are rising. However, the absence of a standardized incident reporting framework has resulted in limited disclosure of cybersecurity incidents and a lack of a centralized database. This prevents construction companies from learning from past events and developing effective cyber risk management strategies. To address this issue, this study applies the Cybersecurity Incident Severity Scale (CISS) model to assess the severity of cyber incidents within the construction sector. The CISS model uses a structured, semi-quantifiable approach to generate an integrated score, evaluating dimensions such as safety and financial impacts to provide a comprehensive understanding of an incident's consequences. A real-world construction cyber incident serves as a case study to demonstrate the model's applicability. By promoting standardized reporting, the CISS model can improve data collection, ensure consistent reporting across organizations, and enable meaningful comparisons over time and across regions.

Keywords –

Cyber Incidents; Severity Score; Construction 4.0; Construction Projects; Cyber Attacks

1 Introduction

The Construction 4.0 integrates the Internet of Things (IoT), Building Information Modeling (BIM), artificial intelligence (AI), and other digital technologies. These have transformed the industry by improving efficiency and collaboration. Although phishing, ransomware, and other cyber risks are prevalent in every sector involving digitalization, the construction industry faces unique cybersecurity challenges. Construction projects often involve many stakeholders, such as owners, contractors, and suppliers, who rely on BIM and IoT to exchange data in real time. This high level of coordination enlarges the cyberattack surface because each partner or device might be an attack entry point. The supply chain's fragmentation, the tight project schedule, and the limited budget make it hard to implement unified cybersecurity standards and regulations for different parties. Cyberattacks not only lead to data loss but interrupt physical site operations, delay the project, and may cause physical and financial harm. Through IoT equipment and smart machines, increased connectivity exacerbates these vulnerabilities, impacting time, cost, and safety. As for the cloud-based BIM platform and collaborative tools based on sensitive data analysis, strong security is necessary. AI-driven analytics must be protected to avoid tampering. Furthermore, ongoing digitalization needs updates to protect emerging techniques and processes. Multiple stakeholders with different cybersecurity awareness, expertise, and standards make it complicated to maintain a unified defense [1].

To effectively manage these cyber incident risks, the construction sector must implement comprehensive, effective, and robust cybersecurity strategies informed by lessons from past incidents. However, such progress is limited, and one primary reason is the absence of a standardized incident reporting framework. Without such a framework, the disclosure and documentation of cyber incidents remain fragmented and inconsistent across various projects and organizations, leading to a lack of a centralized database. This also hinders the analysis of trends, the identification of recurring vulnerabilities, and the design of effective preventive measures. Consequently, the industry misses out on critical insights essential for developing cybersecurity practices to address existing and emerging threats [1].

Global cybersecurity incident reporting frameworks vary significantly, offering lessons for the construction sector. The EU's NIS2 Directive [2] mandates rapid notifications and uniform reporting across member states, while Singapore's Cybersecurity Act [3] imposes a two-hour window for incident reporting. China's draft measures emphasize quick initial and follow-up reports [4] and Australia and India also enforce stringent

timelines to safeguard critical infrastructure [5]. In the United States, the Cyber Incident Reporting for Critical Infrastructure Act [6] aims to unify reporting across sectors. Despite the push for standardization, current frameworks rely on qualitative evaluations that overlook the complex threat landscape in construction. Without standardized quantitative metrics, comparing data across projects remains difficult. This limits thorough data collection and obscures key vulnerabilities. A comprehensive, quantitative approach could enhance security status and strengthen cross-sector collaboration.

To address this challenge, Conard (2024) proposed the Cybersecurity Incident Severity Scale (CISS) [7] to provide a semi-quantifiable and standardized metric for evaluating cybersecurity incident severity. We apply this approach to construction projects by utilizing it to assess and score the severity of cybersecurity incidents that uniquely impact this sector. By incorporating data related to the cybersecurity incident of the project as the inputs, this model derives a single severity score, making the assessment more evidence-based and objective. With a standardized severity score derived from uniform data inputs, stakeholders can quickly assess and learn from cybersecurity incidents, facilitating the sharing of materials and lessons across groups and organizations. This, in turn, enhances the overall efficiency of cybersecurity incident data preservation and collection.

2 Related Works

2.1 Industrial Cybersecurity Solutions

Cybersecurity is a rapidly evolving field, where practical knowledge and insights often originate from industry solutions. For instance, Willis Towers Watson's (WTW) "Cyber Quantified" platform [8] helps organizations model and quantify cyber risk exposures using insurance analytics and real-world benchmarks, while Marsh & McLennan's "Cyber Risk Analytics Center" [9] utilizes proprietary datasets to evaluate potential losses and guide mitigation strategies. Widely recognized annual reports such as Verizon's Data Breach Investigations Report (DBIR) [10] highlight patterns in attack vectors, adversary tactics, and breach trends. CrowdStrike's Global Threat Report [11] similarly maps the evolving threat landscape across diverse sectors. The Threat Landscape publications [12] of an EU commercial agency called ENISA offer industry-driven insights that complement academic literature. From a broader industrial perspective, frameworks such as the IAEA's guidance on "Computer Security for Nuclear Security" [13] demonstrate how other critical infrastructure sectors assess and manage risk severity. Collectively, these sources demonstrate the prevalence of real-world cyber threats and the necessity for practical assessment mechanisms. However, when it comes to the construction industry, research on cybersecurity, particularly the systematic scoring and comparison of incident severity, remains sparse. This indicates a clear need for deeper investigation within this sector.

2.2 Lack of Incident Severity Scoring Studies Within the Construction Industry

Awareness of cybersecurity within the construction industry, though increasing, remains relatively underdeveloped compared to other sectors. This is evidenced by the limited body of research dedicated to the topic. A 2023 scoping review by Pargoo and Ilbeigi [14] identified only 45 studies focused on cybersecurity within the construction industry, which can be broadly categorized into: discussions, reviews and solutions.

Among specific solutions, several studies focus on risk assessment of the entities (software, hardware, stakeholders, etc.) in construction projects. Mantha and García de Soto [15], for example, utilized agent-based models to examine how vulnerabilities spread among stakeholders in a construction network of projects. However, this remains at a very preliminary stage, lacking real-world case study validation, and the score assignment process is relatively subjective. In another study [16], they applied the CVSS to score stakeholders' vulnerabilities in construction networks based on the Confidentiality, Integrity, and Availability (CIA) Triad. Nevertheless, its manual and subjective score assignment process limits swift adaptability across different project contexts. Subsequently, Mantha et al. [17] enhanced their agent-based model from [15] by introducing seven more detailed steps to assess vulnerability spread among entities in construction projects, but the quantitative aspect has not significantly improved, and a large portion of the vulnerability score assignments remains non-data-driven. More recently, Yao and García de Soto [18] proposed a machine-learning-centric approach to assess the probability of cyber risks across project phases but lacked extensive case studies for validation.

Besides each study's limitations, they all focus on the vulnerability of entities and the probability of cybersecurity incidents to these entities within projects, failing to address the potential impact of incidents on the projects themselves. This gap highlights the need for comprehensive research on assessing the impact of cybersecurity incidents within construction projects.

2.3 Scoring Methods in Other Industries

Scoring methods have been widely adopted across diverse fields to quantify and communicate the severity of incidents, offering insights for robust cybersecurity scoring in construction. In the financial sector, the Data Envelopment Analysis (DEA)-based system [19]

synthesizes financial ratios into a "credibility score," helping institutions gauge credit risk and streamline decisions. Similarly, the IHS Markit Banking Risk Rating System (RRS) [20] employs a 0-100 scale to evaluate structural risk factors, detecting critical vulnerabilities early on. While quantitative, these approaches may overlook nuanced qualitative elements crucial for a holistic risk perspective. In public health, the NIH Stroke Scale [21] exemplifies a more granular clinical tool by assessing neurological function in stroke patients, but its specialized application underscores the challenges of designing universally applicable scoring systems. Transportation also illustrates how scoring or categorization frameworks must remain flexible. For example, the SAE Levels of Driving Automation [22] provide standardized automation categories but require ongoing adjustments as technology rapidly evolves.

In cybersecurity, the Common Vulnerability Scoring System (CVSS) [23] ranks software vulnerabilities on a 0–10 scale, guiding remediation priorities but potentially missing broader organizational effects. Insurance approaches like Willis Towers Watson's "Cyber Quantified" [8] translate threats into financial impacts using proprietary analytics, focusing on underwriting yet illustrating how data-driven methods can be adapted elsewhere, including construction. Across critical infrastructure, the U.S. National Cyber Incident Scoring System (NCISS) [24] developed by CISA is recognized as a best-practice for evaluating and prioritizing cyber incidents. It assigns severity ratings based on threat actor capabilities, potential critical infrastructure impacts, and disruption scale, offering a structured approach to triage. These scoring methods each contribute valuable methodologies for assessing various types of risks and incidents. However, their applicability to the construction sector, particularly for capturing the multi-stakeholder, project-based nature of construction projects, remains an open question, emphasizing the need for tailored or adapted scoring systems.

2.4 The CISS Model by Conard

In 2024, Conard [7] proposed the Cybersecurity Incident Severity Scale (CISS) model, drawing from established frameworks with potential applications in the construction sector for severity assessment. It aims to foster a uniform incident reporting scheme for cybersecurity incidents across various industries. The model integrates elements from scoring systems in other industries, focusing on standardized, detailed, and practical assessments. It evaluates factors such as data type, system criticality, individual harms, and organizational impacts, providing a comprehensive understanding of cybersecurity incidents. Additionally, the model must be adaptable to evolving risks and offer granular classifications for precision. International standardization, like those in transportation and public health, is crucial to support global collaboration and consistent cybersecurity threat mitigation. CISS is especially relevant for construction, where cybersecurity breaches can cause financial losses, operational disruptions, and stakeholder repercussions. Its holistic, semi-quantitative approach captures the sector's multi-dimensional nature, ensuring precise severity evaluations. Applying the CISS model would help address gaps in consistent incident reporting and severity assessment.

3 The CISS Model

For a more standardized cybersecurity incident severity assessment model in the construction industry, we considered Conard [7]'s CISS framework as a starting point because it provides a structured calculation methodology and includes critical factors such as financial repercussions, operational disruptions, and harm to individuals. Regarding the calculation method, the CISS model quantifies an incident's impact using a structured assessment pathway incorporating severity and criticality assessments. This is also useful for construction, where cybersecurity incidents may not only disrupt IT systems but also affect physical safety, project schedules, and contractual obligations. Regarding the factors, these align well with the key cybersecurity risks in construction, where incidents often impact supply chains, project timelines, collaborative digital platforms (e.g., BIM), and IoT-enabled smart construction sites. As a preliminary study, we apply the proven CISS framework to assess cyber incidents in construction. This helps ensure that our model is compatible with other sectors while demonstrating its practicality for the construction industry. However, we also recognize the need for future adaptations, such as integrating more granular construction-specific considerations due to the complexity of multi-stakeholder networks, supply chain vulnerabilities, and regulatory requirements.

3.1 Overview of the CISS Score

The overview of the scoring mechanism is shown in Figure 1. The CISS score (Y) is calculated using a weighted approach based on severity score(S), criticality score (C), and their weights β_1, β_2 using Equation 1.

$$Y = \beta_1 S + \beta_2 C \quad (1)$$

S is computed based on the financial score, individual score, and operational score, whereas C is measured based on the National Critical Function (NCF) score and National Security Impact (NSI) score. More information about each score is provided below. However, as the purpose of this paper is to implement and apply this scoring system within the context of construction, only a brief overview is included. The reader is encouraged to

refer to [7] for a more detailed description.

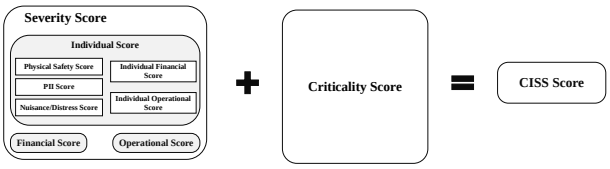

Figure 1. Overview of the CISS Scoring methodology adopted from [7]

Using the current estimation process, which incorporates a weighted approach and proposed scales, the overall CISS scores range from 0 to 10, where 0 indicates no impact, and 10 represents a very high impact. Table 1 outlines the various impact levels, corresponding score ranges, and their descriptions.

Table 1. Overview of different impact levels, corresponding score ranges, and description for CISS

Impact Level	Score Range	Description
No Impact	0	No observable impact or disruption to information and/or operations
Minor Impact	1-2	Minimal impact with no significant consequences; minor disruptions or inconveniences that do not affect core information and/or operations
Low Impact	3-4	Noticeable disruptions with limited consequences to information and/or operations
Medium Impact	5-6	Significant disruptions affecting critical information and/or operations
High Impact	7-8	Severe disruptions with major impacts on critical information and/or operations, potentially hindering recovery efforts
Very High Impact	9-10	Catastrophic disruptions causing long downtime, substantial losses, or permanent damage to information and/or operations

3.2 CISS Score Calculations

3.2.1 Severity Score (*S*)

According to [7], the Severity score evaluates the impact of an incident by combining three components, namely individual score, financial score, and operational score. This comprehensive metric provides insight into the scale and intensity of the incident. These are aggregated by considering an average, ensuring a balanced representation of the harm caused to individuals, financial systems, and organizational operations.

Individual Score: It evaluates the harm to affected individuals across five subcategories: physical safety, personally identifiable information (PII) breaches, nuisance/distress, financial harm, and operational harm. Each subcategory is scored on a scale from 0 (no impact) to 10 (extreme impact) and combined with population scores that account for the number of people affected. For example, physical safety measures range from minor injuries requiring first aid to fatalities, while PII breaches evaluate the sensitivity of compromised data, from basic contact information (low impact) to highly sensitive records like health data or legal information (high impact). Nuisance/distress measures emotional or psychological harm, while financial harm reflects direct monetary losses to individuals. Operational harm assesses disruptions to daily tasks, such as accessing essential services or managing personal responsibilities. These are also aggregated using the average of all the subcategories, reflecting both the severity of harm and the scale of those affected. This ensures a nuanced understanding of the incident's impact on individuals.

Financial Score: It quantifies monetary repercussions stemming from a security incident, using a scale from 0 (losses under $100K) to 10 (losses over $1B). These levels are informed by empirical breach reports, insurance data, and industry benchmarks, which ensures incremental levels of financial severity. Assessors factor in direct expenses such as investigation, legal actions, and response measures, as well as indirect costs tied to reputational damage or diminished customer trust. Because incidents can grow in scope as hidden liabilities appear, the Financial Score is recalculated whenever new data emerges. This dynamic nature allows stakeholders to grasp evolving fiscal burdens, guiding decisions on resource allocation and risk mitigation strategies. Ultimately, this score provides a consistent metric for comparing economic impacts.

Operational Score: It measures the extent to which an incident disrupts an organization's core functions on a scale of 0 to 10. It accounts for both the breadth (how many processes or systems are affected) and the duration (how long these disruptions persist). Minor issues such as short outages in non-critical applications receive lower scores, while incidents that halt production lines, obstruct customer services, or compromise safety protocols could reach the highest. Recovery progress influences the score, which may shift as incident response teams implement fixes or uncover new complications. By examining factors like system interdependencies, infrastructure resilience, and contingency procedures, the score provides a structured view of how deeply an incident impacts essential operations.

3.2.2 Criticality Score (*C*)

The criticality score, according to [7], evaluates the systemic importance of the affected systems by combining two dimensions, National Critical Function (NCF) and National Security Impact (NSI), into a single metric. Each dimension is scored on a 0–10 scale, with 0 indicating no impact and 10 representing a severe, prolonged effect on core national assets. The final

criticality score is an average of these two components.

The NCF evaluates the disruption to essential services, such as power grids, telecommunications, water supply, or financial transactions. The scoring scale ranges from short, localized interruptions, such as a brief internet outage scoring near 0–2, to multi-day failures across multiple interdependent services, such as energy, transportation, and emergency response, scoring 8–10. The framework often references established guidelines, such as the U.S. Cybersecurity and Infrastructure Security Agency (CISA)'s NCF pillars (Connect, Distribute, Manage, Supply) [25], but it is adaptable to country-specific classifications. The cascading effects of a single disruption can create ripple effects in other sectors, particularly if critical infrastructure is shared, thereby amplifying the overall severity.

The NSI assesses the sensitivity of any exposed or compromised data from unclassified but sensitive information to highly classified documents that, if leaked, could threaten national security. The scoring scale assigns higher values as data classification levels escalate. For example, a score of 0 signifies that no classified data was involved, a score of 4 might reflect unauthorized access to need-to-know information, and a score of 8–10 indicates a breach of Secret or Top Secret materials. The global adaptability of this scale allows organizations to align scoring with their own national standards, as classification systems vary by country. For instance, organizations may categorize data as "Confidential," "Secret," "Top Secret," or use equivalent local labels.

4 Implementation

To illustrate the applicability of the CISS model, we analyzed a real incident from a leading engineering and contracting firm in the UAE. During the 24-month construction phase of a $5 million commercial building project, phishing attempts occurred approximately every two months. One incident highlighted the effectiveness of the company's proactive cybersecurity measures. The attack was detected by the company's spam filtering system and promptly reported to the IT team, allowing for swift containment with only minor impacts. Thanks to robust defenses, including employee awareness training and immediate response protocols, the company ensured no data was compromised, and there were no significant operational, financial, or reputational damages. This incident underscores the critical role of structured cybersecurity practices in managing threats, maintaining operational continuity, and safeguarding stakeholder trust with minimal disruption.

4.1 Severity Score (S)

Individual Score. The phishing incident's individual impact was assessed across multiple dimensions to determine its severity. For physical safety, no harm occurred and thus no one was affected. In the Personally Identifiable Information (PII) category, PII with moderate sensitivity (e.g., contact details, employment information) was breached, affecting 10 employees. For nuisance/distress, about 100 employees (mostly IT staff, managers, and those who reported phishing attempts) were affected. Personal communication data (e.g., personal emails and messages) was stolen, causing inconveniences and disrupting daily routines. No financial losses were reported, so no one was financially impacted. For operational harm, about 150 employees (mainly IT and operational staff) experienced disruptions while managing phishing emails, delaying tasks like accessing online communication services. Table 2 shows a detailed breakdown of these dimensions. The integrated individual score, the average of all dimensions, is 1.5.

Table 2. Breakdown of Individual Score

Dimension	Impact Score	# of People Impacted	People Score	Ave. Score	Indv. Score
Physical Safety	0	0	0	0	1.5
PII Impact	2	10	2	2	
Nuisance/ Distress	3	100	2	2.5	
Financial Harm	0	0	0	0	
Operational Harm	4	150	2	3	

Financial Score. Although the phishing attacks led to some minor incidental costs (e.g., investigation and staff time), the overall financial impact remained below the $100k threshold set by [7]. As such, the Financial Score for this incident was 0, largely due to the company's proactive defenses (e.g., spam filtering) that effectively mitigated the threat.

Operational Score. In contrast, the Operational Score is 5, indicating significant disruptions to the firm's operations. The phishing incident required operational adjustments, such as workarounds and managing delays, underscoring its major impact on day-to-day processes even if it did not result in substantial financial losses.

The severity score can be computed by taking the average (as suggested in [7]) of the individually estimated scores as follows. However, it is worth noting that several other methods can be used, more of which are detailed in the discussion section.

$$Severity\ Score = \left(\frac{Individual\ Score + Financial\ Score + Operational\ Score}{3}\right) = \left(\frac{1.5 + 0 + 5}{3}\right) = 2.17$$

4.2 Criticality Score (C)

The incident occurred in a normal commercial

building project, which had no direct impact on critical infrastructure or cascading effects on national operations. Therefore, the NCF score is 0. Similarly, no sensitive or classified information was exposed, so the NSI score is 0, so the incident posed no risk to national security.

$$Criticality\ Score = \frac{NCF\ Score + NSI\ Score}{2} = \frac{0+0}{2} = 0$$

4.3 Overall CISS Score

The overall CISS score is derived from the Severity Score and Criticality Score with a weighted combination of 0.9 and 0.1, respectively, as suggested by [7]. Although several other weights can be considered, extensive set of correlative experiments conducted showed the significance of these weights and hence the usage for this implementation.

$$CISS\ Score = 0.9 * Severity\ Score + 0.1 * Criticality\ Score$$
$$= (0.9 * 2.17) + (0.1 * 0.0) = 1.95$$

The final CISS score is 1.95, indicating the incident had a small impact without significant consequences. It only caused minor disruptions or inconveniences without affecting core information or operations.

5 Discussion

5.1 Model Efficacy

The CISS score of 1.95 indicates that the phishing attack on the company only caused a minor impact. This score closely aligns with the reality of the case study, reflecting the effectiveness of proactive mitigation measures such as spam filtering systems and employee awareness. These measures successfully prevented any significant financial, operational, or security consequences. The score's consistency with the facts of the case demonstrates the efficacy of the proposed model in accurately assessing the impact of the phishing incident. By quantifying the relatively low severity and negligible criticality of the incident, the model effectively underscores its ability to provide a realistic and data-driven evaluation of cybersecurity risks. This correlation between the calculated score and the actual case outcomes further validates the model's robustness and utility in real-world scenarios.

5.2 Suggestions for Model Adaptation

Scoring Granularity. The severity score should be derived through systematic analysis of evidence across multiple hierarchical layers, each corresponding to specific causative factors or events, inspired by frameworks like the IHS Markit RRS [20] and the NIH Stroke Scale [21]. For example, the scoring can incorporate metrics such as individual repercussions and assessing the impact on personnel. It can be quantified by evaluating both the number of affected individuals and the severity of harm incurred. This multi-dimensional approach ensures a highly granular assessment, enabling the identification and consideration of nuanced factors that might otherwise be overlooked.

Adaptive Evolution. The model must prioritize adaptability to address the evolving cyber risks in construction. Inspired by frameworks like the SAE Levels of Driving Automation [22], which are updated to reflect technological advancements, the scoring model should also evolve in terms of its structure, dimensions, and inputs. This ensures responsiveness to emerging technologies, such as AI-powered design tools, and to evolving threats targeting interconnected systems. By maintaining this flexibility, the model can integrate new threat vectors and technologies, providing an up-to-date framework for assessing cybersecurity incidents in construction projects. This adaptability enhances resilience and promotes industry-wide collaboration.

Threshold Customization. Our study used predefined thresholds as illustrative baselines to reflect typical financial, operational, and stakeholder impacts. While these cutoffs effectively demonstrate how the model can be applied in practice, they should not be viewed as universally applicable. Different regions, project scales, and regulatory environments may require notably different threshold values to capture the true impact of cybersecurity incidents. We therefore recommend that future applications of this model begin with a calibration phase, during which these thresholds are adjusted based on local conditions, expert judgments, and available incident data. This can ensure that the model retains its relevance and accuracy as it is extended to broader contexts or more diverse construction project scenarios.

5.3 Insights and Implications

The CISS provides a standardized framework for reporting and assessing cybersecurity incidents. Using structured inputs, it ensures consistent data collection, produces a unified severity score, and facilitates reliable documentation across different organizations. The resulting quantitative metric helps prioritize and triage incidents, enabling meaningful comparisons of severity over time and across regions. By analyzing these scores, stakeholders can learn from the past, promote best practices, and respond to evolving cyber threats. CISS can also align cybersecurity efforts across public and private sectors, helping policymakers develop targeted regulations and allocate resources effectively. Through its common framework for assessment and reporting, CISS fosters transparency and accountability among clients, partners, and regulators. This standardized approach enhances industry resilience, promotes global

coordination, and protects critical infrastructure, making it valuable for the construction industry and beyond.

Many modern construction contracts, such as those using standard forms like FIDIC or NEC, now include clauses requiring specific cybersecurity standards and rigorous protocols for data protection. They may mandate compliance with recognized frameworks or set requirements for incident reporting. By integrating the CISS model into these contractual clauses, contractors can standardize severity assessments, ensuring compliance and fostering transparency. This alignment clarifies responsibilities and promotes uniformity across projects, facilitating more robust monitoring, response, and documentation of cyber incidents. Furthermore, embedding the CISS score into contractual deliverables encourages proactive adoption of best practices, reinforcing project security and stakeholder trust. Future work can investigate additional ways to link CISS metrics with emerging contractual obligations.

5.4 Limitations and Future Work

While the CISS model's applicability to construction has been demonstrated, several limitations exist, and further improvements are needed.

(1) The model's broad applicability can sometimes overlook industry-specific nuances due to the lack of context-specific factors in the model. In the construction sector, critical factors such as project delays, supply chain disruptions, and stakeholder confidence play a significant role but are not directly accounted for within the model's current dimensions. Addressing these industry-specific aspects would make the model more effective in reflecting the unique risks and impacts of construction-related cybersecurity incidents, enhancing its accuracy and relevance in this context.

(2) Another limitation of the CISS implementation is its reliance on weighted averaging, which can oversimplify the cybersecurity incidents. By converting impact dimensions into a single score through weighted averaging, granular interactions and cascading effects may be overlooked, hiding critical insights. However, this approach serves as a starting point to demonstrate how the CISS model can be applied in construction. In the future, more sophisticated weighting schemes or multi-criteria decision-making approaches could be integrated into the model to capture the complexity of cyber incidents more accurately in construction.

(3) Another technical limitation is the model's inability for real-time updates, a key aspect given fast-paced IT developments and evolving cyber threats. Although the current CISS model relies on static or post-incident data, construction environments shift quickly. By enabling real-time data inputs like IoT sensor feeds and continuous project updates, the model could provide near-instantaneous threat detection and adaptive scoring, aligning more closely with proactive cybersecurity strategies. As IT technology advances and threats grow more sophisticated, real-time adaptability will be crucial to safeguarding construction projects by enhancing situational awareness and rapid response capabilities.

(4) Using a single case study may limit the model's generalization, which may overlook the diversity of potential incident types, project scales, and organizational contexts. Consequently, certain scoring factors and contextual details within the model may not fully capture all conditions, which necessitates more extensive data and multiple examples to validate and refine the scoring model. Further research with a range of real-world incidents would help ensure that the scoring methodology is robust and reflective of the complex realities faced by different construction projects.

6 Conclusion

This study addresses the research gap regarding the lack of cybersecurity incident severity assessments and the absence of standardized measurement and reporting within the construction industry. By applying the CISS model, this study provides an integrated score for evaluating the severity of cyber incidents in construction projects. The model assesses severity based on financial, operational, and individual impacts, while criticality considers NCFs and the potential exposure of classified information. These dimensions collectively provide a comprehensive evaluation of a cybersecurity incident's impact and significance. Through a case study involving a real-world phishing incident at a construction company, the model demonstrates its applicability in assessing cybersecurity incidents within the construction context. The implications of this research include promoting the adoption of an existing structured framework for consistent and standardized incident reporting, enabling uniform data collection, supporting meaningful incident comparisons over time and across diverse contexts, fostering collaboration across organizations and regions, and ultimately contributing to industry-wide efforts to enhance cybersecurity resilience and coordination.

Acknowledgments

This research was partially 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 ALEC Engineering & Contracting LLC, particularly Mr. Sabyasachi Jana, for providing project-related information.

References

[1] 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

[2] "DHS-CISA & DG CONNECT Cyber Incident Reporting Comparison Report," DHS, DG CONNECT, Mar. 2024. Accessed: Nov. 20, 2024. [Online]. Available: https://www.dhs.gov/publication/comparative-assessment-dhs-harmonization-cyber-incident-reporting-federal-government

[3] Baker McKenzie, "Global Data Privacy and Cybersecurity Handbook," Baker McKenzie. Accessed: Nov. 22, 2024. [Online]. Available: https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook/asia-pacific/singapore/topics/breach-notification-requirements

[4] China Briefing, "China's Cybersecurity Regulator Issues Draft Measures on Incident Reporting," China Briefing. Accessed: Nov. 15, 2024. [Online]. Available: https://www.china-briefing.com/news/chinas-cybersecurity-regulator-issues-draft-measures-on-incident-reporting/

[5] Australian Cyber Security Centre (ACSC), "Report a Cyber Security Incident," Australian Cyber Security Centre (ACSC). Accessed: Nov. 29, 2024. [Online]. Available: https://www.cyber.gov.au/report-and-recover/report/report-a-cyber-security-incident

[6] "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements; Extension of Comment Period," Federal Register. Accessed: Oct. 23, 2024. [Online]. Available: https://www.federalregister.gov/documents/2024/05/06/2024-09505/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements-extension-of

[7] C. F. Conard, "Quantifying the Severity of a Cybersecurity Incident for Incident Reporting," Graduate Theses, Massachusetts Institute of Technology, Cambridge, Massachusetts, United States, 2024. Accessed: Dec. 17, 2024. [Online]. Available: https://hdl.handle.net/1721.1/157124

[8] Willis Towers Watson, "Cyber Quantified," Willis Towers Watson. Accessed: Mar. 03, 2025. [Online]. Available: https://www.wtwco.com/en-us/solutions/products/cyber-quantified

[9] Marsh McLennan, "Marsh McLennan Cyber Risk Intelligence Center," Marsh McLennan. Accessed: Mar. 03, 2025. [Online]. Available: https://www.marshmclennan.com/solutions/cyber-resilience/cyber-risk-intelligence-center.html

[10] Verizon, "2024 Data Breach Investigations Report," Verizon, 2024. Accessed: Feb. 27, 2025. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir

[11] CrowdStrike, "CrowdStrike 2024 Global Threat Report," CrowdStrike, 2024. Accessed: Mar. 01, 2025. [Online]. Available: https://www.crowdstrike.com/global-threat-report

[12] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2024," ENISA, Sep. 2024. Accessed: Mar. 01, 2025. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[13] International Atomic Energy Agency, "Computer Security for Nuclear Security," IAEA, 2021. [Online]. Available: https://www.iaea.org/publications/13629/computer-security-for-nuclear-security

[14] N. Salami Pargoo and M. Ilbeigi, "A Scoping Review for Cybersecurity in the Construction Industry," *Journal of Management in Engineering*, vol. 39, no. 2, p. 03122003, Mar. 2023, doi: 10.1061/JMENEA.MEENG-5034.

[15] 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.

[16] 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.

[17] B. R. K. Mantha, M. S. Sonkor, and B. García de Soto, "Investigation of the cyber vulnerabilities of construction networks using an agent-based model," *Developments in the Built Environment*, vol. 18, p. 100452, Apr. 2024, doi: 10.1016/j.dibe.2024.100452.

[18] D. Yao and B. García De Soto, "Cyber Risk Assessment Framework for the Construction Industry Using Machine Learning Techniques," *Buildings*, vol. 14, no. 6, p. 1561, May 2024, doi: 10.3390/buildings14061561.

[19] A. B. Emel, M. Oral, A. Reisman, and R. Yolalan, "A credit scoring approach for the commercial banking sector," *Socio-Economic Planning Sciences*, vol. 37, no. 2, pp. 103–123, Jun. 2003, doi: 10.1016/S0038-0121(02)00044-7.

[20] IHS Markit, "Banking Risk Ratings Methodology," S&P Global. Accessed: Dec. 08, 2024. [Online]. Available: https://www.spglobal.com/_assets/documents/marketplace/ihs-markit-banking-risk-ratings-methodology.pdf

[21] Naureen, "NIH Stroke Scale - NurseBrain®," NurseBrain®. Accessed: Dec. 12, 2024. [Online]. Available: https://nursebrain.com/2021/12/nih-stroke-scale/

[22] R. Harrington, C. Senatore, J. Scanlon, and R. Yee, "The Role of Infrastructure in an Automated Vehicle Future," *Bridge*, vol. 40, pp. 48–55, Jun. 2018.

[23] S. Radack, "The Common Vulnerability Scoring System (CVSS)," National Institute of Standards and Technology.

[24] Cybersecurity and Infrastructure Security Agency (CISA), "CISA National Cyber Incident Scoring System (NCISS)," CISA, 2023. Accessed: Mar. 02, 2025. [Online]. Available: https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss

[25] Cybersecurity and Infrastructure Security Agency (CISA), "National Critical Functions (NCF) Framework," CISA, 2024. Accessed: Feb. 25, 2025. [Online]. Available: https://www.cisa.gov/topics/risk-management/national-critical-functions