International Journal of Scientific and Management Research
Volume 8 Issue 8 (August) 2025
ISSN: 2581-6888
Page: 37-51

Analysis of Cybersecurity Issues in Construction Industry in Digital Transformation

Benjamin O. Uwakweh[1], Ajeka Friday[2], Opeoluwa Adigun[3], & Chukwuemeka Chuka-Maduji[4]
[1]Department of Built Environment, North Carolina A&T State University, **USA.**
[2]Department of Computer Systems Technology, North Carolina A&T State University, **USA.**
[3]Department of Computer Systems Technology, North Carolina A&T State University, **USA.**
[4]Department of Computer Systems Technology, North Carolina A&T State University, **USA.**
DOI - http://doi.org/10.37502/IJSMR.2025.8805

Abstract

The construction industry is undergoing a profound digital transformation, driven by technologies such as Building Information Modeling (BIM), Internet of Things (IoT), drones, and 3D printing. While these innovations bring significant efficiency and productivity gains, they also introduce new cybersecurity risks. This study systematically reviews literature and industry reports to identify the most critical cybersecurity threats facing the construction industry, including ransomware, distributed denial-of-service (DDoS) attacks, and supply chain breaches. The findings reveal that ransomware remains the most financially damaging, with significant operational and reputational consequences, while human error and third-party vulnerabilities are the primary amplifiers of breach costs. The paper proposes three strategic mitigation measures—comprehensive employee training, AI-driven threat detection, and centralized security information and event management (SIEM) systems—adapted from the NIST framework to the specific context of construction. The main limitation of this study is its reliance on secondary data, which may not capture rapidly evolving threat landscapes or region-specific risks. Future empirical research should validate and refine the proposed strategies across diverse construction environments. By addressing these vulnerabilities, the construction industry can better secure its digital assets and safeguard critical infrastructure.

Keywords: Cybersecurity, Construction industry, Digital transformation

1.0 Introduction

In recent years, digitalization and technological advancements have reshaped virtually every sector, and the construction industry is no exception. The integration of Building Information Modeling (BIM), Internet of Things (IoT) applications, cloud-based project management systems, and advanced robotics has accelerated the industry's transition into the era of Construction 4.0. While these innovations enable improved efficiency, collaboration, and precision, they also expose construction operations to an evolving set of cybersecurity threats.

Despite the significant benefits of digital tools, the construction industry remains a late adopter compared to sectors such as finance or healthcare. Existing literature and industry reports reveal that cybersecurity frameworks tailored to construction are scarce, and there is limited empirical research examining the intersection of cybersecurity and construction-specific

processes (Salami Pargoo & Ilbeigi, 2023; Mantha & García de Soto, 2021). This knowledge gap is concerning given the sensitive nature of construction data, which may include design blueprints, bidding information, and operational control systems for critical infrastructure.

By clearly identifying the threats, vulnerabilities, and practical strategies for mitigation, this paper aims to contribute to both academic literature and industry practice. The practical implications include a more resilient digital infrastructure for construction firms, reduced risk of operational disruption, and improved compliance with international security standards. This addresses a critical gap in both scholarly research and professional application, offering a foundation for future empirical studies and industry-wide adoption.

1.1 Cybersecurity

Over the years, the acceptable terminology used to describe the security aspects of digital conversations has constantly evolved. The beginning of this century saw the introduction of phrases such as Information Security, Computer Security, or IT Security (Schatz, Bashroush, and Wall, 2017). Cybersecurity is the practice of protecting digital assets, information, and systems from unauthorized access, damage, or theft (Craigen et al, 2014). It includes a broad range of fundamental concepts and best practices, including encryption, intrusion detection and access control. The continuously shifting threat landscape in the digital age calls for consistent vigilance to safeguard against cyberattacks, data breaches, and other security risks. Cybersecurity is thus a crucial aspect in ensuring the integrity and confidentiality of data, which is especially relevant in the context of the construction industry's increasing reliance on digital technologies.

1.2 Types of Threats in Cybersecurity

Cybersecurity threats are prone in the following areas, bank, schools, government sectors, and organization database. The effect of these threats is disastrous because it affects both financial and data management (Emmanuel S. Dandaura, 2015)

i. Denial of Service (DoS) Attack: Cyber threat attack form that shuts down a machine or network, making it inaccessible to its intended user(s). The two general DoS attack methods are accomplished by flooding the target with traffic for the server to buffer, causing them to slow down and eventually stop, or sending it information that triggers a crash (Dietmar P. F. Möller, 2020).
ii. Distributed Denial of Service (DDoS): Cyber threat attack to disrupt normal traffic of targeted server, service or network by overwhelming the target or its surrounding infrastructure with heavy internet traffic (Dietmar P. F. Möller, 2020).
iii. Advanced Persistent Threat (APT): Network cyber threat attack in which unauthorized persons access a network and stay there undetected in the long term. The primary intent of APT is to steal data, disrupt business operation and damage infrastructures. APT attackers coordinate their activities with the security measures of their targeted private or public organization and often attack them several times. APT groups often receive instruction and support from governments or government agencies (Dietmar P. F. Möller, 2020).
iv. Social engineering: Social engineering is a manipulative tactic employed by attackers to deceive individuals into revealing private information or engaging in

actions that compromise security (Benson, V., McAlaney, J., & Frumkin, L. A., 2019). By exploiting human behavior and gaining trust, attackers aim to extract personal data like passwords or financial information or manipulate victims into performing actions they would not typically do, such as opening malicious email attachments or clicking on harmful links (Lezzi, M., Lazoi, M., & Corallo, A., 2018).

v. Phishing: Phishing is a social engineering technique that, using various methodologies, aims to influence the target of the attack to reveal personal information, such as an email address, username, password, or financial information. This information is then used by the attacker to the detriment of the victim (Stavroulakis, P., & Stamp, M., 2010)

1.3 Construction Industry

Currently, the construction industry is undergoing a digital transformation that is completely changing the way projects are planned, executed, and managed (Garcia de Soto et al, 2022). This revolution is driven by the adoption of digital technologies and data-driven processes, such as Building Information Modeling (BIM), the Internet of Things (IoT), and cloud-based project management systems. To effectively analyze the digital transformation currently going on in construction, efforts will span various project phases, from design to maintenance, with the widespread use of Information Computer Technology (Sonkor and Garcia de Soto, 2021). These digital environments, unlike the previous phase of construction, facilitate the sharing of design specifics, work instructions, and project information among participants of a construction project (Salami Pargoo, 2023). Equally, the emergence of autonomous and remotely controlled machinery creates a spiral bound effect in Operational Technologies (OT), posing crucial cybersecurity concerns, particularly in collaborative work environments between humans and machines (Turk et al., 2022).

Industrial Control Systems (ICS) are interconnected with the internet in construction equipment. This raises significant vulnerabilities, exposing project participants to potential cyberattacks. The reliance on Building Automation, Fire and Life Safety, and closed-circuit television systems during the operation and maintenance phase heightens the impact of cyberattacks on construction and building systems (Turk et al., 2022).

1.4 Slow Adoption of New Technologies in Construction

The Construction industry generally operates with little funds available to acquire or invest in new technologies for project management. For most firms to implement emerging technologies, they will have to hire new personnel who are educated and knowledgeable, who can help train others and help the requisite components. All these increase the cost of doing business. Further, most firms are reluctant to be trail blazers when they cannot effectively predict the return of investment (ROI). Finally, there are risks associated with adopting new technologies; sometimes these risks may be prohibitive because they may require larger investments to effectively integrate them into the business operations and practices. These adoption processes may disrupt normal operations such as bidding submission, estimating, and may impact their competitive strategies. Thus, the integration and infusion of new technology must be done thoughtfully and by professionals who not only understand the technology but also all the critical processes that are at the core of that firm.

1.5 Objective of the Study

The primary objective of this paper is to provide a comprehensive review of the existing literature that focuses on the intersection of cybersecurity and the construction industry. This aims to bring to light the specific challenges, threats, and vulnerabilities that construction professionals and stakeholders encounter as they navigate the current digital landscape in discharging their duties. By examining the literature, we intend to gain a deeper and better understanding of the cybersecurity issues that are crucial to the safety and security of construction operations in an increasingly digital world.

2.0 Literature Review

Any comprehensive literature review of cybersecurity would be grossly incomplete without traversing the length and breadth of various fields including engineering, political science, psychology, management, sociology, and education (Craigen, Diakun-Thibault & Purse, 2014). However, cybersecurity is not only limited to these disciplines. There is also evidence of cybersecurity in law, public administration, healthcare, policy development, and accounting. Consequently, the point of intersection of cybersecurity with various sectors, and industries is a complex and critical aspect of contemporary global operations. In the healthcare sector, the safekeeping of patient records and medical data is not only essential for ensuring privacy but also important for maintaining the integrity of healthcare systems (Kim, 2022). However, in healthcare, the function of cybersecurity extends beyond the scope of data protection to safeguarding medical devices and by extension, the prevention of potential threats to patient safety (Luna et al., 2016). In finance, institutions face an ever-evolving landscape of cyber threats, which ranges from sophisticated phishing schemes to ransomware attacks (Uddin, et al., 2022). The protection of sensitive financial information and the stability of financial transactions are crucial. The potential impact of the application of cybersecurity in the finance sector is not only on individual users but also on the broader economic landscape (Lagazio and Cushman, 2014). The energy sector is increasingly reliant on interconnected systems and Industrial Internet of Things (IIoT) devices. As such, it must prioritize cybersecurity to protect critical infrastructure (Hossein Motlagh et al., 2020). A potential cyberattack on power grids or oil and gas facilities will be catastrophic for society. Possible consequences will extend beyond financial losses to encompass significant societal disruptions and potential threats to national security (Pleta et al., 2020). The emergence of Industry 4.0 in the manufacturing industry has led to increased automation and interconnected production processes (Gorecky, et al., 2014). This has resulted in efficiency gain and cybersecurity challenges, as ensuring the reliability of supply chains, securing intellectual property, and preventing disruptions to production have become the paramount issues in the industry (Del Giorgio Solfa, 2022). With crucial education reforms taking the center stage in global conversations, the education sector is not immune to cybersecurity concerns. Major educational institutions are currently housing vast amounts of sensitive student data. The potential occurrence of cyber threats targeting academic institutions can lead to major data breaches, jeopardizing the privacy of students and potentially disrupting academic operations (Fouad, 2022). The government is not left out. Government entities and systems face unique cybersecurity challenges tied to national security interests. The task of protecting classified information, critical infrastructure, and ensuring the continuity of essential government functions have become imperative conversations in governance (Kim, 2017).

Managed service companies who monitor and respond to cyberattacks have been clear about the significance of the risk to the industry. For example, ReliaQuest's 2023 Annual Cyber-Threat Report, the construction industry ranked number one on the most-targeted sectors list followed by transportation with an average of 226 incidents per year. See Fig. 1.

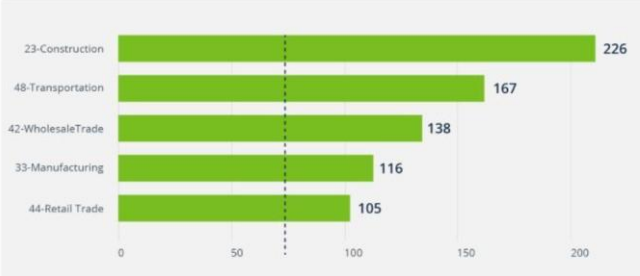

Fig.1: annual cyber-threat report (ReliaQuest's 2023)

Consequently, a recurring theme across these diverse, evolving sectors are challenges related to mitigating ransomware attacks, addressing vulnerabilities in complex supply chains, and implementing robust incident response plans (Masip-Bruin et al., 2021). As industries traverse the pathways of digitization and interconnection, the intersection of cybersecurity has become foundational in ensuring the resilience, privacy, and integrity of operations across a broad spectrum of professional domains. Conclusively, these innovations underscore the need for ongoing collaboration, information sharing, and the development of innovative cybersecurity solutions to navigate this complex and dynamic landscape effectively.

The global average cost of a data breach spiked and increased by 10% in one year, reaching USD 4.88 million, the biggest jump since the pandemic (IBM cost of data breach report, 2024). Business disruption and post-breach response activities drove most of this yearly cost increase. See Fig. 2.

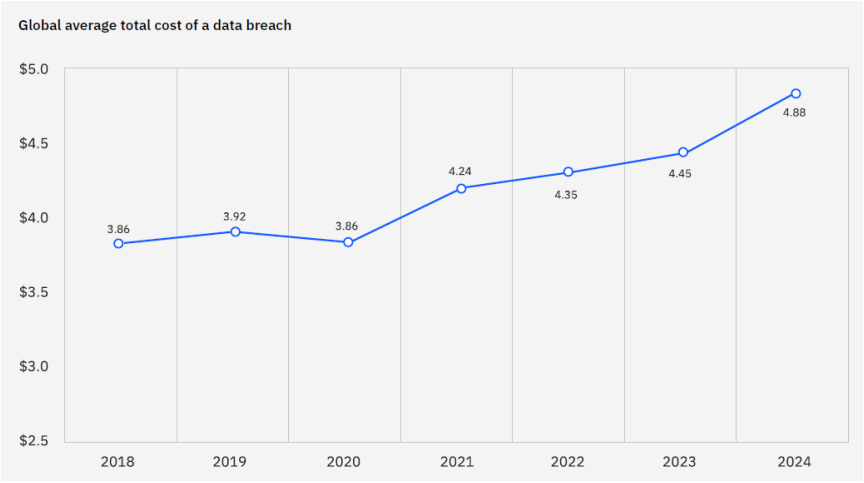

Fig. 2: Global average total cost of data breach measure in USD millions (IBM cost of a data breach report, 2024).

Cybersecurity, as a field, encompasses a wide array of topics, including threat actors, attack vectors, security frameworks, and emerging trends (Ham, 2021). It is essential to have a fundamental understanding of these concepts as they form the basis for addressing cybersecurity issues in the construction industry. Ghelani (2022) stated that cyber threats are

dynamic and diverse, ranging from traditional malware and phishing attacks to more sophisticated threats like ransomware, advanced persistent threats (APTs), and insider threats. The construction industry must be vigilant against these threats to protect sensitive data, project plans, and critical infrastructure.

The amount an organization spends on extortion attacks can vary based on the type of attack such as ransomware, data exfiltration and destructive as well as the way the organization responds. All three types of attacks were examined, including ransomware, where data is encrypted and a ransom demanded; data exfiltration, where data is stolen and the organization sometimes extorted; and destructive, where attackers delete data and destroy systems for their own objectives. Fig. 3 presents the cost of the three types of attack described above.

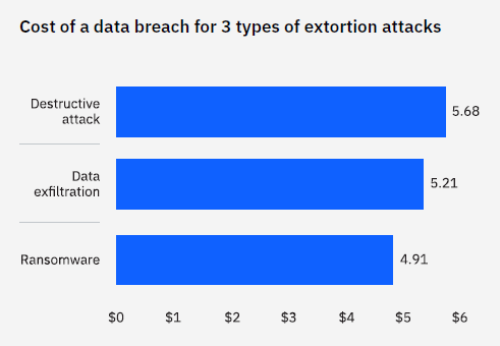

Fig. 3: cost of data breach for extortion attacks (IBM Cost of a Data Breach Report, 2024).

Ransomware operators continue to use double extortion tactics across all industries globally, with the US emerging as the most targeted country in 2023. Ransomware cost more than $400 million in the first six months of the year (Alessandro Mascellino, 2023) but Deloitte Global Cyber Threat Intelligence (CTI) observed an encouraging decline in ransomware payments globally, particularly in the health care and financial services sectors (Deloitte Global Cyber Threat Intelligence, 2024). Sophisticated ransomware operators are increasingly using zero-day exploits as their initial access vector, with 36 percent of victims' ransom. Security frameworks such as NIST (National Institute of Standards and Technology) and ISO 27001 provide essential guidelines and best practices for securing digital assets (Shen, 2014; Khaleefa & Al-Mashhadi, 2022).

2.1 Analysis of Literature

The aim of this section is to identify common themes, specific insights, and the implications of the existing research on the intersection of cybersecurity and the construction industry's digital transformation. The literature reveals that the construction industry, like many others, is grappling with a rapidly evolving threat landscape. Cyber threats such as data breaches, ransomware attacks, and supply chain vulnerabilities pose significant risks. These threats can lead to data loss, project delays, financial losses, and damage to the industry's reputation (Mantha and De Soto, 2019).

One recurring theme in the literature is the critical importance of proactive cybersecurity measures. Effective cybersecurity practices are not only about defending against known threats but also about being prepared for new and unforeseen challenges. This preparedness involves robust network security, access controls, employee training, and incident response plans (Mutis and Paramashivam, 2019). Furthermore, collaboration between industry stakeholders,

including contractors, subcontractors, and suppliers, is essential to address supply chain risks effectively.

3.0 Cybersecurity Issues in Construction

The integration of digital technologies in the construction industry has introduced specific cybersecurity challenges. These challenges include the protection of sensitive project data, the security of construction equipment connected to the Internet, and safeguarding of critical infrastructure against cyberattacks.

The construction industry undergoing a significant digital transformation known as Construction 4.0 is increasingly reliant on communication and information technologies, creating what is known as a construction network (Qian and Papadonikolaki, 2021). The adoption of digital tools and interconnected systems has led to the rise of Construction 4.0, providing advantages such as increased efficiency, precision, and collaboration. However, this transformation brings about new challenges, particularly in the realm of cybersecurity. In a study by Mantha and García de Soto, the authors assessed the cybersecurity vulnerability of construction networks, highlighting the critical importance of addressing cybersecurity concerns in the Construction 4.0 landscape (Mantha and García de Soto, 2021). In his study, a new methodology was introduced, utilizing the Common Vulnerability Scoring System (CVSS) to calculate scores and assess the likelihood of cybersecurity incidents based on communication frequencies within a construction network.

3.1 Challenges in the Construction Industry

The construction industry, with its unique and dynamic characteristics, presents distinct challenges in the realm of cybersecurity, necessitating a tailored approach to address specific areas of concern (Turk et al., 2022). One of the main challenges faced is security breaches in construction projects, which are also applicable to both Information Technology (IT) and Operational Technology (OT) attacks. The underreporting of incidents complicates the quantification of cyberattacks, and this is often blocked from public purview to preserve the reputation of involved firms. Major examples of such incidents include stolen blueprints, fraudulent deposit collections, identity theft, and phishing attacks on construction participants. OT attacks, specifically targeting critical infrastructure, have caused physical damage to processes or equipment and one such prominent example is Stuxnet's impact on an Iranian nuclear plant (Turk et al., 2022). Another challenge in construction is that every project is a fundamental unit of production, and each project is inherently unique across all dimensions. The processes are aided by a unique collection of resources like companies, software tools, engineers, consultants, contractors, and subcontractors. Unlike manufacturing industries which are designed to produce a series of similar products, construction projects result in individual, often bespoke buildings, introducing an element of complexity that demands a nuanced cybersecurity approach (Turk et al., 2022). Another hurdle that can be problematic is when the construction industry seeks economies through scale, replication, and repetition. Therefore, identifying repetitive elements, whether they are building parts or sub-processes, introduces a challenge for security. This quest for repetitive elements underscores the industry's attempt to streamline processes and achieve efficiency while simultaneously creating a dynamic security landscape (Turk et al., 2022). Finally, the existing traditional approach to cybersecurity encompasses providing security for systems with clear and distinct boundaries. However, most construction projects exhibit overlapping and fluid boundaries. It takes a combination of

institutional and human actors to participate in multiple projects simultaneously, rendering existing traditional system boundaries less effective. Individuals, majorly affiliated with various companies, congregate to work on multiple projects concurrently, illustrating the complex interplay of overlapping boundaries. In this context, existing traditional security measures, which are largely dependent on clear-cut system boundaries, may prove to be inadequate, leading to potential vulnerabilities across interconnected projects and entities (Turk et al., 2022).

3.2 Temporal nature of construction projects

Construction projects are both unique and temporary. For many projects, existence is only for the duration of design or construction. Unlike ongoing and permanent systems, these projects have a defined lifecycle, adding another layer of complexity to cybersecurity considerations. The temporal nature of construction projects makes it necessary to adapt security measures to the project's specific timeline, aligning with its transient nature (Turk et al., 2022).

Essentially, the construction industry's peculiarities, marked by project uniqueness, the pursuit of repetitive elements, and fluid boundaries, requires cybersecurity frameworks to account for these specifics. The conventional paradigms of securing well-defined systems are challenged by the dynamic and overlapping nature of construction projects, urging the development of nuanced and adaptive cybersecurity strategies (Turk et al., 2022). Yet another key concern is the potential exposure of project plans and blueprints to unauthorized access. Building Information Modeling (BIM) systems, which are central to many construction projects, can be attractive targets for cybercriminals seeking to exploit vulnerabilities in project designs (Loukaka and Rahman, 2020). Furthermore, Internet of Things (IoT) devices, such as connected construction equipment and sensors, can introduce vulnerabilities that, if not adequately secured, might lead to operational disruptions or data breaches (Khurshid et al., 2023). Supply chain risks are another prominent issue in construction cybersecurity. The complex network of suppliers and contractors in construction projects can provide entry points for attackers seeking to compromise the integrity of the supply chain (Mantha and De Soto, 2019).

3.3 Digital Issues in Construction

The adoption of technologies like Building Information Modeling (BIM) and the Internet of Things (IoT) is revolutionizing traditional construction practices. BIM, for instance, offers a collaborative and data-driven approach to construction projects, allowing stakeholders to work on a shared digital model. IoT applications provide real-time data on equipment performance, environmental conditions, and more, thereby enhancing decision-making and project efficiency (Mantha and De Soto, 2019). However, this digitalization introduces a new layer of complexity. Managing, securing, and optimizing these digital tools are crucial for construction projects' success. Balancing the advantages of digitalization with the potential risks and challenges is central to ensuring the security and resilience of the construction industry in the digital era.

3.4 Cost of Cyber-Attack in Construction

The repercussions of a cyber-attack on a construction company can be severe and far-reaching.

i. Reputational damage is a critical concern, as clients and partners may lose trust in a company's ability to secure its operations and data. Reputation is paramount in the architectural/engineering/ construction (AEC) sector, which means the fallout from a cyber-attack can be devastating. Clients may choose to work with competitors perceived to have better security practices, leading to lost business opportunities (Construction Drive, 2024)

ii. Operational damage can be devastating, too. Project delays caused by ransomware or denial-of-service (DoS) can lead to significant financial losses and contractual penalties. Even a short disruption can have cascading effects, impacting multiple projects and stakeholders (Construction Drive, 2024)

3.5 Protection Strategies

To overcome these cyber threats, construction companies must holistically protect their attack surface. Below are some of identified protection strategies (Construction Drive, 2024):

i. People: Vetting employees reduces the insider threat, as does implementing access controls. Educating employees to improve their cybersecurity awareness is also crucial, but make sure the security awareness training features bite-sized and accessible content tailored to the needs of busy construction workers.

ii. Supply chain security: Vetting subcontractors, using least-privilege access and conducting periodic supplier cybersecurity reviews are vital for supply chain security. Subcontractors play a crucial role in construction projects, but their cybersecurity practices vary widely. Ensuring subcontractors adhere to the same stringent security standards as the primary contractor is essential.

iii. Threat detection and response: Threat detection involves applying robust threat intelligence across your infrastructure with 24x7 monitoring of software and hardware across your entire infrastructure, from endpoints to networks and cloud nodes. Advanced threat detection technologies, such as machine learning and artificial intelligence, can help identify and respond to threats in real time. These technologies can analyze vast amounts of data to detect anomalies and potential security incidents, allowing construction companies to respond quickly and effectively.

3.6 Factors that Increased Breach Costs

The top three factors that amplified breach costs were security system complexity, security skills shortage and third-party breaches, which can include supply chain breaches. See Fig. 4.

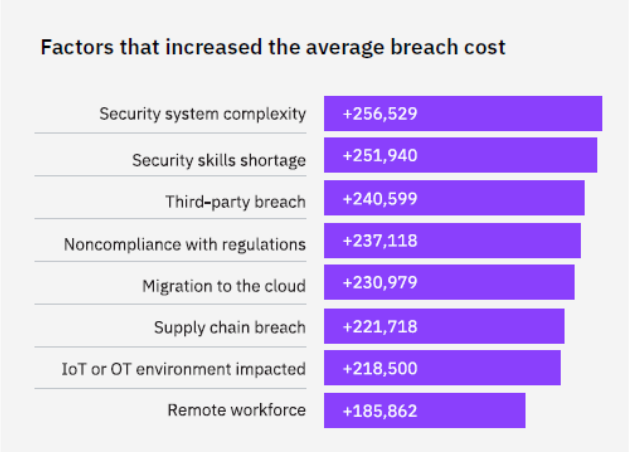

Fig. 4: factors that increase average breach cost (IBM Cost of a Data Breach Report, 2024).

The average cost of a data breach jumped to USD 4.88 million from USD 4.45 million in 2023, a 10% spike and the highest increase since the pandemic (IBM Cost of Data Breach report, 2024). A rise in the cost of lost business, including operational downtime and lost customers, and the cost of post-breach responses, such as staffing customer service help desks and paying higher regulatory fines, drove this increase.

3.7 Factors that Reduced Breach Costs

Employee training and the use of AI and machine learning insights were the top factors mitigating average data breach costs in their analysis. Employee training continues to be an essential element in cyber defense strategies, specifically for detecting and stopping phishing attacks. AI and machine learning insights closely followed in second place. See Fig. 5.

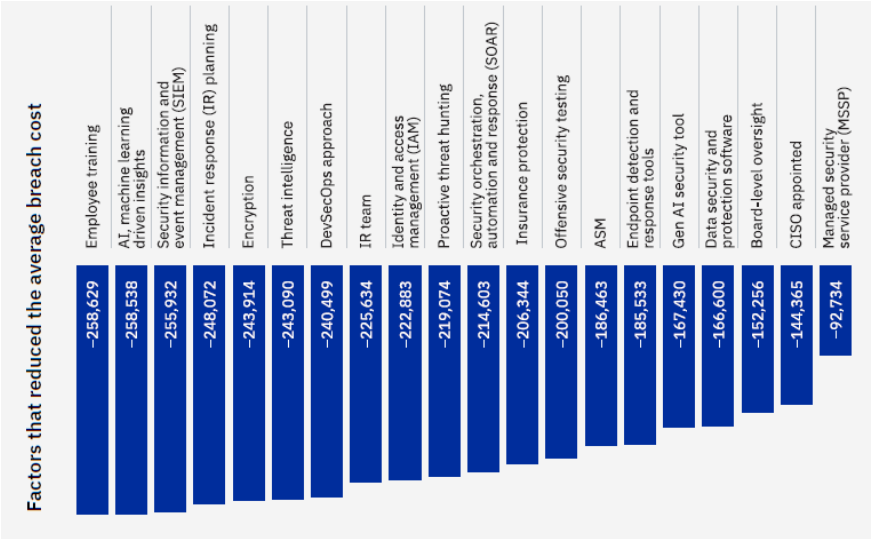

Fig. 5: Factors that reduced average breach cost (IBM Cost of a Data Breach Report, 2024).

3.8 National Institute of Standards and Technology (NIST) Cybersecurity Framework

NIST framework was developed in response to a presidential Executive Order which called for a set of standards for organizations to lower cyber risk (Executive Office of the President, 2013). The NIST cybersecurity framework has become a globally adopted standard that can be implemented in many organizations regardless of their industry, size, and level of cyber

maturity (Navid & Mohammad, 2023). The framework divides the cybersecurity management process into five main functions: (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover. In addition, each function is subdivided into multiple categories (Barrett 2018). Table 1 introduces the functions, their descriptions, and categories.

Table 1. Functions and categories of NIST cybersecurity framework

Function	Description of function	Category
Identify (ID)	Develop organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	Business environment Governance Risk assessment Risk management strategy Supply chain risk management
Protect (PR)	Develop and implement appropriate safeguards to ensure delivery of services.	Identity management and access control Awareness and training Data security Information protection processes and procedures Maintenance Protective technology
Detect (DE)	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.	Anomalies and events Security continuous monitoring Detection processes
Respond (RS)	Develop and implement appropriate activities to take action regarding a detected cybersecurity event.	Response planning Communications Analysis Mitigation Improvements
Recover (RC)	Develop and implement appropriate activities to maintain plans for resilience and restore capabilities/services that were impaired due to a cybersecurity event.	Recovery planning Improvements Communications

4.0 Discussion

The findings of this review indicate that the construction industry faces an evolving set of cybersecurity threats, with ransomware, distributed denial-of-service (DDoS) attacks, and supply chain breaches emerging as the most critical. Ransomware incidents in particular can have severe operational, financial, and reputational impacts, which are amplified by the industry's heavy reliance on time-sensitive project delivery. DDoS attacks, while less common, can disrupt access to cloud-based project management systems and delay workflows across multiple stakeholders.

A recurring theme in the literature is the industry's slow adoption of advanced cybersecurity measures compared to other sectors. This lag is attributed to budget constraints, lack of specialized personnel, and the perceived complexity of integrating security protocols without

disrupting project schedules (Mantha & De Soto, 2019; Turk et al., 2022). Additionally, the unique nature of construction projects, characterized by temporary collaborations among multiple contractors and subcontractors, creates complex and overlapping system boundaries that challenge traditional IT security models.

The adaptation of the NIST cybersecurity framework to construction-specific contexts offers a viable path forward. By aligning construction processes with the NIST functions—Identify, Protect, Detect, Respond, and Recover—companies can structure their security programs to address vulnerabilities at each project stage. However, literature suggests that such frameworks must be supplemented with sector-specific guidelines that account for the transient and multi-stakeholder nature of construction networks.

From a practical perspective, the integration of AI and machine learning technologies into threat detection and response systems can significantly reduce breach costs and detection times (IBM, 2024). Likewise, consistent employee training programs, tailored to the realities of construction workflows, remain essential for mitigating risks associated with human error and social engineering attacks.

Overall, this discussion underscores that while effective solutions exist, their adoption in the construction industry remains inconsistent. The challenge lies in balancing operational efficiency with the rigorous security controls necessary to protect sensitive data and infrastructure in an increasingly digitized environment.

5.0 Conclusion

This study has examined the cybersecurity challenges confronting the construction industry in the context of digital transformation. By synthesizing insights from academic literature and industry reports, it has identified ransomware, DDoS attacks, and supply chain vulnerabilities as the most pressing threats. These threats are exacerbated by human error, inadequate supply chain vetting, and the unique, temporary nature of construction projects.

6.0 Recommendations

After studying the factors that increase and reduce data breaches, this study therefore recommends the top three mitigating strategies for overcoming cybersecurity issues in construction.

i. Implementing employee training strategy for mitigating cyber-attacks, as human error is often the weakest link in an organization’s security defenses. To strengthen organization's cybersecurity posture, it is recommended to implement comprehensive employee training programs focusing on the following key areas: recognizing phishing attacks, password security, social engineering awareness, incident reporting and response, and physical security measures.

ii. Employ Artificial Intelligence (AI) and machine learning (ML) strategy which offer powerful solutions for mitigating cyber-attacks by providing advanced insights, automating threat detection, and improving response times.

iii. Implement security information and event management (SIEM) tool for mitigating cyber-attacks which provide centralized, real-time monitoring, analysis, and response capabilities for an organization’s IT security infrastructure.

References

1) Alessandro Mascellino. (2023). China unleashes AI-powered image generation for influence operations.
2) Barrett, M. P. (2018). Framework for improving critical infrastructure cybersecurity version 1.1. *National Institute of Standards and Technology*.
3) Benson, V., McAlaney, J., & Frumkin, L. A. (2019). Emerging threats for the human element and countermeasures in the current cyber security landscape. In Cyber law, privacy, and security: Concepts, methodologies, tools, and applications. *IGI Global*, 1264–1269.
4) Construction Drive. (2024). Safeguarding the construction industry with effective cybersecurity.
5) Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10).
6) Dandaura, E. S. (2015). Cyberspace governance: The imperative for national and economic security. International Conference on Cyberspace Governance: The Imperative for National & Economic Security. https://doi.org/10.13140/rg.2.1.2407.8321
7) Del Giorgio Solfa, F. (2022). Impacts of cyber security and supply chain risk on digital operations: Evidence from the pharmaceutical industry. *International Journal of Technology, Innovation and Management (IJTIM), 2*.
8) Deloitte Global Cyber Threat Intelligence. (2024). Annual cyber threat trend.
9) Executive Office of the President. (2013). Improving critical infrastructure cybersecurity. *Federal Register, 78*(33), 11737–11744.
10) Fouad, N. S. (2022). The security economics of edTech: Vendors' responsibility and the cybersecurity challenge in the education sector. *Digital Policy, Regulation and Governance, 24*(3), 259–273.
11) García de Soto, B., Turk, Ž., Maciel, A., Mantha, B., Georgescu, A., & Sonkor, M. S. (2022). Understanding the significance of cybersecurity in the construction industry: Survey findings. Journal of Construction Engineering and Management, 148(9), 04022095.
12) Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A review.
13) Gorecky, D., Schmitt, M., Loskyll, M., & Zühlke, D. (2014). Human-machine-interaction in the industry 4.0 era. *In 2014 12th IEEE International Conference on Industrial Informatics (INDIN)*, 289–294.
14) Ham, J. V. D. (2021). Toward a better understanding of cybersecurity. *Digital Threats: Research and Practice, 2*(3), 1–3.
15) Hossein Motlagh, N., Mohammadrezaei, M., Hunt, J., & Zakeri, B. (2020). Internet of Things (IoT) and the energy sector. *Energies, 13*(2), 494.
16) IBM. (2024). Cost of a data breach report.
17) Khaleefah, A. D., & Al-Mashhadi, H. M. (2023). Methodologies, requirements and challenges of cybersecurity frameworks: A review. *International Journal of Wireless and Microwave Technologies*, 13, 1–13.

18) Khurshid, K. et al. (2023). An in-depth survey demystifying the Internet of Things (IoT) in the construction industry: Unfolding new dimensions. *Sustainability, 15*(2), 1275.
19) Kim, J. (2017). Cyber-security in government: Reducing the risk. *Computer Fraud & Security, 2017*(7), 8–11.
20) Kim, L. (2022). Cybersecurity: Ensuring confidentiality, integrity, and availability of information. *In Nursing informatics: Health informatics, interprofessional and global perspective*, 391–410.
21) Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. *Computers & Security*, 45, 58–74.
22) Loukaka, A., & Rahman, S. S. (2020). Security professionals must reinforce detect attacks to avoid unauthorized data exposure. *Information Technology in Industry, 8(*1).
23) Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care, 24*(1), 1–9.
24) Mantha, B. R., & de Soto, B. G. (2019). Cyber security challenges and vulnerability assessment in the construction industry. *In Creative Construction Conference*, 29–37.
25) Mantha, B. R., & García de Soto, B. (2021). Assessment of the cybersecurity vulnerability of construction networks. *Engineering, Construction and Architectural Management, 28*(10), 3078–3105.
26) Masip-Bruin, X., et al. (2021). Cybersecurity in ICT supply chains: Key challenges and a relevant architecture. *Sensors, 21*(18), 6057.
27) Möller, D. P. F. (2020). Cybersecurity in digital transformation: Scope and applications. *Springer*. https://doi.org/10.1007/978-3-030-60570-4
28) Mutis, I., & Paramashivam, A. (2019). Cybersecurity management framework for a cloud-based BIM model. In Advances in informatics and computing in civil and construction engineering: Proceedings of the 35th CIB W78 2018 Conference: IT in design, construction, and management, *Springer*, 325–333
29) Plėta, T., Tvaronavičienė, M., Della Casa, S., & Agafonov, K. (2020). Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases. Insights into Regional Development, 2(3).
30) Qian, X., & Papadonikolaki, E. (2021). Shifting trust in construction supply chains through blockchain technology. Engineering, Construction and Architectural Management, 28(2), 584–602.
31) ReliaQuest. (2023). Annual cyber-threat report.
32) Salami Pargoo, N., & Ilbeigi, M. (2023). A scoping review for cybersecurity in the construction industry. *Journal of Management in Engineering, 39*(2), 03122003.
33) Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law, 12*(2), 8.
34) Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. *Scitech Lawyer, 10*(4), 16.
35) Sonkor, M. S., & García de Soto, B. (2021). Operational technology on construction sites: A review from the cybersecurity perspective. *Journal of Construction Engineering and Management, 147(*12), 04021172.

36) Stavroulakis, P., & Stamp, M. (Eds.). (2010). Handbook of information and communication security. *Springer*.
37) Turk, Ž., de Soto, B. G., Mantha, B. R., Maciel, A., & Georgescu, A. (2022). A systemic framework for addressing cybersecurity in construction. *Automation in Construction,* 133, 103988.
38) Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Management, 22*(4), 239–309.