International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 1, Jan-Feb 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cybersecurity in Construction Industry

Matthew N. O. Sadiku[1], Paul A. Adekunte[2], Janet O. Sadiku[3]

[1]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[2]International Institute of Professional Security, Lagos, Nigeria
[3]Juliana King University, Houston, TX, USA

ABSTRACT

The construction industry faces several cybersecurity threats due to its unique nature. The industry is increasingly becoming a prime target for cyberattacks. Data breaches, supply chain attacks, and ransomware pose significant threats. For years, cybersecurity experts have warned construction industry and workers that they are targets for ransomware attacks, phishing theft, data breaches, and theft of sensitive information. Cyber criminals see the construction sector as a potential weak and easy target to attack. By prioritizing cybersecurity, construction companies can protect their financial health, maintain business continuity, and preserve their hard-earned reputations. This paper discusses the role of cybersecurity in the construction industry.

KEYWORDS: *security, cybersecurity, space exploration, space colonization, space system*

How to cite this paper: Matthew N. O. Sadiku | Paul A. Adekunte | Janet O. Sadiku "Cybersecurity in Construction Industry" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-1, February 2025, pp.102-111, URL: www.ijtsrd.com/papers/ijtsrd73814.pdf

IJTSRD73814

INTRODUCTION

The construction industry, a cornerstone of global infrastructure development, is undergoing a digital transformation, but this progress comes with increased cybersecurity vulnerabilities. The industry is now confronting a new frontier of threats emanating from the digital realm. Today, the built environment is designed, constructed, and managed using digital technology, making it increasingly exposed to cyber security risks. The construction industry grapples with ensuring the security of its physical assets and its digital infrastructure. As a result, the industry has experienced massive losses including stolen or misdirected funds.

From building neighborhood homes to mile-long suspension bridges, construction is the foundation of the growth and essential to the development and advancement of any nation. The construction industry is at a crossroads of innovation and vulnerability.

Although digital innovations can help ensure that projects remain under budget on construction sites, the growing digitalization may present additional challenges.

Although smartphones, laptops, and tablets are widely used in the construction industry to monitor data, transfer information, and send communications to employees and clients, it can be challenging to enact widespread security measures with so many devices. Projects often involve numerous partners, increasing the complexity of managing cybersecurity across different systems. This complexity presents numerous entry points for cybercriminals seeking to exploit vulnerabilities within interconnected systems. Figure 1 shows a typical construction site [1], while Figure 2 shows some construction workers [1].

OVERVIEW ON CYBERSECURITY

Cybersecurity refers to a set of technologies and practices designed to protect networks and information from damage or unauthorized access. It is vital because governments, companies, and military organizations collect, process, and store a lot of data. As shown in Figure 3, cybersecurity involves multiple issues related to people, process, and technology [2]. Figure 4 shows different components of cybersecurity [3].

A typical cyber attack is an attempt by adversaries or cybercriminals to gain access to and modify their target's computer system or network. Cybercriminals or ethical hackers are modern-day digital warriors, possessing extraordinary skills and knowledge to breach even the most impregnable systems. A typical cybercriminal is shown on Figure 5 [5]. Cyber attacks are becoming more frequent, sophisticated, dangerous, and destructive. They are threatening the operation of businesses, banks, companies, and government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists) [5].

The cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity. A security incident is an act that threatens the confidentiality, integrity, or availability of information assets and systems [6]. These are known as the pillars of information assurance.

- *Availability*: This refers to availability of information and ensuring that authorized parties can access the information when needed. Attacks targeting availability of service generally leads to denial of service.
- *Authenticity*: This ensures that the identity of an individual user or system is the identity claimed. This usually involves using username and password to validate the identity of the user. It may also take the form of what you have such as a driver's license, an RSA token, or a smart card.
- *Integrity*: Data integrity means information is authentic and complete. This assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or corruption. When integrity is targeted, nonrepudiation is also affected.
- *Confidentiality*: Confidentiality ensures that measures are taken to prevent sensitive information from reaching the wrong persons. Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings.
- *Nonrepudiation*: This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.

Good practices for cybersecurity in construction companies should include all of these elements.

Everybody is at risk for a cyber attack. Cyber attacks vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). The following are typical examples of cyber attacks or threats [7]:

- *Malware*: This is a malicious software or code that includes traditional computer viruses, computer worms, and Trojan horse programs. Malware can infiltrate your network through the Internet, downloads, attachments, email, social media, and other platforms. Spyware is a type of malware that collects information without the victim's knowledge.
- *Phishing*: Criminals trick victims into handing over their personal information such as online passwords, social security number, and credit card numbers.
- *Denial-of-Service Attacks*: These are designed to make a network resource unavailable to its intended users. These can prevent the user from accessing email, websites, online accounts or other services.
- *Social Engineering Attacks*: A cyber criminal attempts to trick users to disclose sensitive information. A social engineer aims to convince a user through impersonation to disclose secrets such as passwords, card numbers, or social security number.
- *Man-In-the-Middle Attack*: This is a cyber attack where a malicious attacker secretly inserts him/herself into a conversation between two parties who believe they are directly communicating with each other. A common example of man-in-the-middle attacks is eavesdropping. The goal of such an attack is to steal personal information.

These and other cyber attacks or threats are shown in Figure 6 [8]. Sources of cyber threats are displayed in Figure 7 [9].

The social and financial importance of cybersecurity is increasingly being recognized by businesses, organizations, and governments. Cybersecurity involves reducing the risk of cyber attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available [10]. Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Cybersecurity experts have shown that passwords are highly vulnerable to cyber threats, compromising personal data, credit card records, and even social security numbers. Governments and international organizations play a key role in

cybersecurity issues. Securing the cyberspace is of high priority to the US Department of Homeland Security (DHS). Vendors that offer mobile security solutions include Zimperium, MobileIron Skycure, Lookout, and Wandera.

CYBERSECURITY IN CONSTRUCTION

Cybersecurity attacks are making headlines these days, and the construction industry is not immune. In reality, all types of businesses are a target for cyberattacks. The way the construction industry operates makes construction companies especially vulnerable to attack. Integrating digital technologies has also put the industry at a higher risk for damages caused by cyberattacks. From data breaches compromising sensitive project information to sophisticated ransomware attacks disrupting operations, the construction industry finds itself at the intersection of technological innovation and cybersecurity vulnerability. Construction cybersecurity is a crucial part of business for all companies in the industry and will continue to be vital in the coming years.

As shown in Figure 8, cybersecurity in an important consideration in construction [11]. Cybercriminals love to target the construction industry for the following reasons [12]:

- The frequent transfer of sensitive information, such as blueprints, client, financial, and personal information, which can all be stolen or used as ransom.
- The unique structure of construction, with many remote workers (on site) and office locations, constantly communicating through digital networks and mobile devices such as emails and texts.
- Being an industry with a historically low perception of risk regarding cyber threats. Many contractors or workers underestimate how big of a target they are, leading to underinvestment in protective measures.
- The complexity of the construction industry, involving many different possible points of failure, such as subcontractors, suppliers, clients, and workers.

There are several aways cyber-attacks could impact a construction company: (i) ransomware; (ii) fraudulent wire transfer; (iii) downtime or business interruption; (iv) breach of intellectual property; and (v) breach of bid data. Here are common cybersecurity threats in the construction industry [13,14]:

- *Data Breaches*: Construction companies handle vast amounts of sensitive data, including financial information, intellectual property, project designs, and client details. Data breaches can occur through hacking, malware, or social engineering attacks, leading to significant financial losses and reputation damage.
- *Supply Chain Attacks*: Construction projects involve diverse players, including architects, engineers, subcontractors, and suppliers, each contributing to the intricate tapestry of a project's lifecycle. Each entity represents a potential entry point for cybercriminals to infiltrate the network, compromise sensitive information, or disrupt operations.
- *Internet of Things (IoT) Vulnerabilities*: The increasing adoption of IoT devices in construction, such as connected sensors, drones, and wearable technology, introduces new cybersecurity risks. These devices often lack robust security measures and can be exploited by attackers. Construction companies increasingly focus on securing IoT devices by implementing network segmentation,
- *Ransomware*: Ransomware, or when a threat actor holds a computer system hostage for payment, can limit a construction company's access to critical systems and potential delay work at Project. Ransomware attacks have become a significant concern for the construction industry. Cybercriminals use malicious software to encrypt critical files and demand payment for their release, disrupting project timelines and causing financial harm. The most common delivery source for ransomware to infect an operating system is via phishing emails that seek to induce the reader to download malware.
- *Fraudulent Wire Transfers:* The number of repeated payments throughout a project involving many trade contractors, the prevalent use of apps to automatically process monthly payments, and the extensive use of tablets on job sites make the industry vulnerable to cybersecurity incidents. As construction companies become increasingly reliant on online banking and wire transfers, they become susceptible to wire fraud. Fraudulent wire transfers, often the result of social engineering, present a substantial risk the construction industry, who are often moving large sums of capital around. Falling victim to fraudulent wire transfer not only presents dire fiscal issues for a construction company but can also lead to server reputation harm.
- *Physical Security Risks*: Construction sites are often physically exposed and vulnerable to theft,

vandalism, and unauthorized access. Cyber-physical attacks targeting equipment or building systems, such as HVAC or access control systems, can disrupt operations and compromise safety.

- *Business Interruption:* Operational disruptions are another significant effect of cyber incidents. The construction industry is heavily reliant on the ability to deliver projects on a deadline. A cyber-attack on a construction company's software or equipment could potentially cause a delay in the project while the cyber-attack is properly addressed.
- *Breach of Intellectual Property:* If a construction company is holding highly sensitive blueprints or schematics in its computer system, breach of these computer systems could result in major reputational damage and potential lawsuits.
- *Breach of Bid Data:* Any breach can lead to financial loss, legal repercussions, and a damaged reputation. If a construction company holds information regarding its bidding strategies on a computer system, access and acquisition of these files could lead to a loss of a competitive edge.
- *Data Theft:* If data is lost or stolen, operations can be severely disrupted, leading to project delays. The construction industry faces frequent attacks to steal intellectual property and private data. Cyber criminals commit data theft because social security and credit card numbers, as well as personal information of employees, vendors, and customers are very valuable to them. Whether acquired through ransomware or other hacking mechanisms, data theft is a serious issue. Some construction entities deal with sensitive and confidential intellectual property such as blue prints, designs, patents and bid information. Sophisticated hackers recognize the value of such information, and there is no limit to what they will do to extort their victims.

COMBATING CYBERSECURITY IN CONSTRUCTION

Escalating cyber threats, tightening regulations, and increasing reliance on technology has created a need for rapid cyber maturity and tailored risk transfer solutions so that construction firms can better weather these challenges. To combat these threats, construction professionals are implementing various cybersecurity measures:

- *Proactive Steps to Boost Cybersecurity:* A proactive approach to cyber security risks is essential. Construction companies must recognize the growing cyber threats they face and take proactive steps to safeguard their operations. Just as cybercriminals develop increasingly sophisticated hacking methods, cybersecurity companies continue to evolve the cybersecurity measures and systems available for company use. Partner with cybersecurity professionals who understand the unique challenges of the construction industry. They can provide tailored solutions, conduct penetration testing, and offer ongoing support to enhance your security posture. Have strong plans in place for the "what if" scenarios and ensure everyone is trained in the risk/response strategies and their immediate implementation.
- *Implement an Incident Response Plan:* Determine actions to be taken after a potential cyberattack to mitigate losses. Create an incident response plan, a plan of action for what your company will do if it falls victim to a cyber-attack. You need to be ready to take immediate action to mitigate damages. Determine which individuals in your company will be responsible for taking key actions, and have a point person designated to lead the charge.
- *Secure Supply Chain Management:* Work closely with subcontractors and suppliers to ensure they adhere to robust cybersecurity standards. Incorporate cybersecurity clauses in contracts and conduct regular audits to verify compliance. Using foresight can help mitigate the possible cybersecurity risks of working with subcontractors and suppliers.
- *Choosing the Right Software:* Adding robust cybersecurity measures to cover all devices and users is vital, but choosing the right software can help to shore up security from within.
- *Education:* Educate all of your team members about cybersecurity risks. Let them understand the cyber risks affecting your industry and how to identify and report social engineering attempts. Make sure that your personnel understand this risk and other vulnerabilities by conducting periodic training and workshops. It is likely not enough to just train your employees. You should periodically evaluate whether the lessons are sticking by sending mock phishing emails to see how well your employees perform. Make sure that your employees know who the point person is at your company to contact in the event of a cybersecurity breach.
- *Insurance:* Even with a robust cybersecurity defense, no system is immune to attacks. Consider having cyber liability insurance in place

to help recover from worst case scenario outcomes. Cyber insurance helps mitigate exposure to cyber-related losses, filling gaps that may be left over from other policies (e.g., commercial property insurance, general liability insurance, etc.). If you suffer a data breach, your coverage may help you cover the costs of hiring attorneys, forensic IT consultants, and other crisis management costs that you may incur. Insurance may cover losses from fraudulent wire transfers and may also assist in negotiating and paying a ransom.

BENEFITS

A successful cyberattack can lead to damaging intellectual property theft, sensitive data breaches, ransomware, spyware, malware, disruption, and supply chain disorder. Government agencies and industry organizations play a crucial role in enhancing cybersecurity across the construction sector. By integrating cybersecurity into every phase of the project lifecycle, a company can protect sensitive data and maintain operational integrity. Other benefits include [15]:

- *Network Security*: Construction companies are deploying robust network security solutions, such as firewalls, intrusion detection systems, and encryption protocols, to safeguard their digital infrastructure from unauthorized access and malware attacks.
- *Supply Chain Management*: Implementing stringent cybersecurity requirements for vendors and subcontractors can help mitigate the risk of supply chain attacks. Contracts should include clauses addressing data protection and cybersecurity standards.
- *Secure IoT Deployment*: Construction firms increasingly focus on securing IoT devices by implementing network segmentation, regularly updating firmware, and monitoring device activity for signs of compromise.
- *Physical Security Measures*: Physical security measures such as surveillance cameras, access controls, and perimeter fencing can help deter unauthorized access to construction sites and protect valuable equipment and materials.
- *Regulatory Compliance:* Adhering to industry-specific cybersecurity regulations and standards, such as the NIST Cybersecurity Framework or GDPR, can help construction companies establish comprehensive cybersecurity policies and practices.
- *Ensuring Project Continuity:* Cyberattacks can disrupt project timelines, leading to delays and financial losses. By implementing robust cybersecurity protocols, construction companies can ensure the continuity of their projects and maintain the trust of clients and stakeholders.
- *Safeguarding Intellectual Property:* Architectural designs, proprietary construction methodologies, and sensitive project data are intellectual property treasures. Cybersecurity measures are essential to prevent the theft or compromise of these assets, preserving the competitive edge of construction firms.
- *Adherence to Regulatory Standards:* As the digital landscape evolves, so do regulatory standards. Cybersecurity is not only a defense against attacks but also a means of staying compliant with industry-specific regulations, avoiding legal repercussions.

CHALLENGES

Apart from handling a lot of big data, to operate, the construction industry relies on remote working, and often, a BYOD (bring your own device) culture, both of which are ways of working that create extra vulnerabilities within an IT infrastructure. It is urgent for construction companies to act to protect themselves from the devastating attacks which threaten to jeopardize project timelines, financial stability, reputations, and sensitive data. Other challenges include [15]:

- *Lack of Cybersecurity Infrastructure:* An entity without appropriate cyber hygiene and cyber architecture signifies an entity that is easy to attack and extort. Monetarily driven cyber criminals will be able to apply little effort for maximum gain. Many construction companies have not properly invested in cybersecurity and pay dearly when they experience an attack.
- *Target for Sensitive Information:* Cybercriminals may be able to access confidential data and then use this sensitive information to enact ransomware attacks. For nation states seeking to gain valuable infrastructure information, intellectual property, or entrance to critical public works, the construction industry is the weak link and an easy target for access. The threat actors seek to extort money, and the construction industry presents a big, lucrative target.
- *Integration of New Technologies:* Engineering and construction services have supported technologies such as artificial intelligence, building information modelling (BIM), machine learning, IoT, and robotics. The integration of new technologies makes processes so much easier and more efficient, yet it also introduces new

challenges, making cybersecurity more essential than ever. Data privacy risk is often overlooked in the race to embrace new technologies, creating a significant risk.

- *Legacy Systems:* Many construction companies still rely on outdated software and hardware, which are more susceptible to vulnerabilities. Integrating these legacy systems with newer technologies without proper security measures can open the door to cyber threats. Support on legacy systems is a significant problem in the construction industry. Legacy or end-of-life operating systems present significant opportunities for cybercriminals.
- *Third-party Risk*: Construction companies often rely on multiple subcontractors and third-party vendors, which increases the potential for cybercriminals to target less secure partners. Once a third-party vendor's system is breached, attackers can gain entry into the main company's network, compromising sensitive data. Third-party cyber risk includes potential data breaches due to vulnerabilities within a vendor's IT environment and can lead to financial, reputational, and regulatory/compliance consequences.
- *Lack of Cybersecurity Regulations:* The construction industry has historically not been subject to mandatory cyber regulatory requirements or scrutiny. For many decades, it seemed the construction sector did not have many regulations in place for data security, whereas sectors like financial services are subject to stringent regulation. To date the construction industry has avoided the strict data privacy and security regulations that industries such as healthcare and banking have faced. The limited regulation and guidance in the construction industry may have contributed to less focus on cybersecurity than in other industries. However, the US government has been increasingly regulating and requiring government contractors to comply with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.
- *Data Breach Expenses:* When a threat actor accesses or acquires Personal Identifiable Information as defined by applicable law, your company has suffered a data security incident. Cyber liability insurance policies typically cover the costs of hiring of lawyers, forensic IT security vendors, public relations, or crisis communication costs to assist you in handling your response.
- *Cybersecurity Training:* Human error accounts for a high proportion of cybersecurity infractions. All employees, subcontractors, and temporary workers should be thoroughly trained in cyberattack prevention essentials. Training employees on good security practices —such as regularly installing software updates, creating strong passwords, utilizing multi-factor authentication on all devices, and encrypting sensitive data, can prevent slip-ups that might have severe effects.
- *Reputational Damage:* Trust is paramount in the construction industry. A breach can erode client confidence, leading to loss of future business opportunities and long-term harm to the company's reputation. The reputational damage that often comes with data breaches further burdens construction companies. Also, any blueprints, designs, methodology, patents, or other proprietary intellectual property is at serious risk if appropriate steps to mitigate cyberattacks are not taken.
- *Protection of Digital Assets:* With the industry's increased reliance on building information modelling (BIM), IoT devices, and cloud-based solutions, the protection of digital assets has never been more critical. Cybersecurity measures serve as a shield against unauthorized access and data breaches.

CONCLUSION

The construction industry is confronted with various cybersecurity challenges as it continues to adopt digital technologies and innovative solutions. The industry's digital evolution requires a proactive and comprehensive approach to cybersecurity. Cybersecurity should be of the utmost importance for construction firms today, but the industry should exercise caution. Embracing cybersecurity is no longer an option, but a necessity. By investing in cybersecurity, construction companies can build not just structures, but also resilience.

The construction industry faces an increasing threat from cyberattacks. Cybersecurity is becoming more essential as the danger and potential risks continue to rise and evolve. It should be fundamental to a strong corporate governance strategy that supports building trust among stakeholders. As the digital transformation accelerates, construction companies must recognize that cybersecurity is critical to their bottom line and business continuity.

REFERENCES

[1] "Why is cyber security important in the construction industry?" August 2024,

https://k3techs.com/why-is-cyber-security-important-in-the-construction-industry/#:~:text=Protecting%20Your%20Projects%20from%20Digital%20Threats&text=Any%20breach%20can%20lead%20to,essential%20to%20protect%20valuable%20data.&text=Therefore%2C%20it%20is%20crucial%20for,invest%20in%20robust%20cybersecurity%20measures.

[2] P. Singh, "A layered approach to cybersecurity: People, processes, and technology- explored & explained," July 2021, https://www.linkedin.com/pulse/layered-approach-cybersecurity-people-processes-singh-casp-cisc-ces

[3] M. Loi et al., "Cybersecurity in health – disentangling value tensions," *Journal of Information, Communication and Ethics in Society,* June 2019, https://www.emerald.com/insight/content/doi/10.1108/JICES-12-2018-0095/full/html

[4] M. Adams, "Unlocking the benefits of ethical hacking: The importance of ethical hackers in cybersecurity," April 2023, https://www.businesstechweekly.com/cybersecurity/network-security/ethical-hacking/

[5] M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi, "A primer on cybersecurity," *International Journal of Advances in Scientific Research and Engineering*, vol. 3, no. 8, Sept. 2017, pp. 71-74.

[6] M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Smart grid cybersecurity," *Journal of Multidisciplinary Engineering Science and Technology*, vol. 3, no. 9, September 2016, pp.5574-5576.

[7] "FCC Small Biz Cyber Planning Guide," https://transition.fcc.gov/cyber/cyberplanner.pdf

[8] "The 8 most common cybersecurity attacks to be aware of," https://edafio.com/blog/the-8-most-common-cybersecurity-attacks-to-be-aware-of/

[9] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports,* vol. 7, November 2021, https://www.sciencedirect.com/science/article/pii/S2352484721007289

[10] Y. Zhang, "Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment," *Doctoral Dissertation,* University of Toledo, 2015.

[11] "Construction cyber risk in the construction industry: An important consideration," August 2016, https://esub.com/blog/construction-cyber-risk-in-the-construction-industry/

[12] F. Osborn, "Safeguarding your construction company from cyber threats," September 2024, https://www.foundationsoft.com/learn/safeguarding-your-construction-company-from-cyber-threats/

[13] "Combatting cyber threats in the construction industry," February 2024, https://www.captechu.edu/blog/combatting-cyber-threats-construction-industry

[14] "Why the construction industry is being impacted by cyberattacks, and what to do about it," https://www.agc.org/sites/default/files/Galleries/enviro_members_file/CLE%20Paper_%20Cyber%20Attacks%20and%20the%20Construction%20Industry.pdf

[15] D. Anderson, B. Q. Choi, and J. Valdez, "Building defenses against cyber risk in the construction sector," March 2024, https://woodruffsawyer.com/insights/cybersecurity-in-construction

Figure 1 A typical construction site [1].

Figure 2 Construction workers [1].

Figure 3 Cybersecurity involves multiple issues related to people, process, and technology [2].

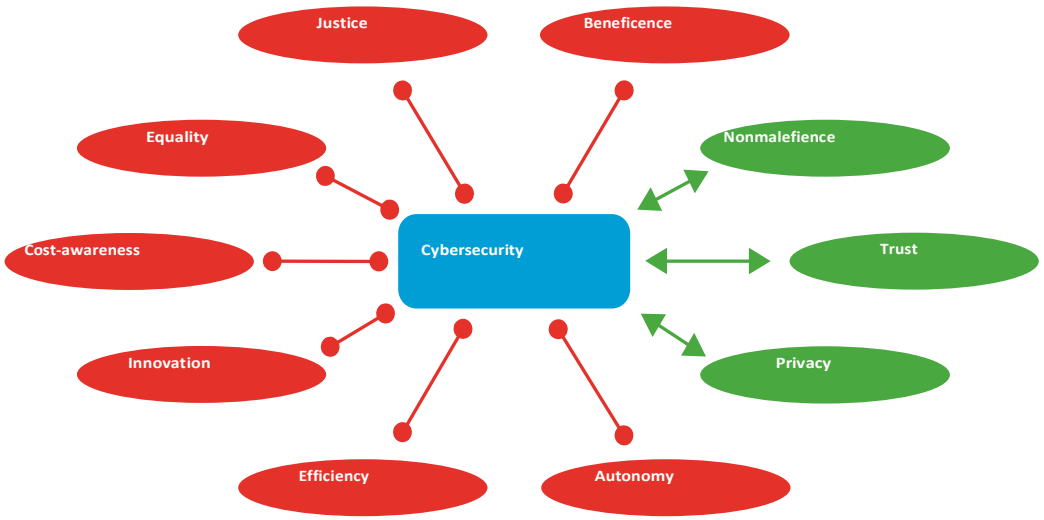

Figure 4 Different components of cybersecurity [3].(Green: supportive; red: in tension)

Figure 5 A typical cybercriminal [4].

Figure 6 Common types of cybersecurity threats [8].

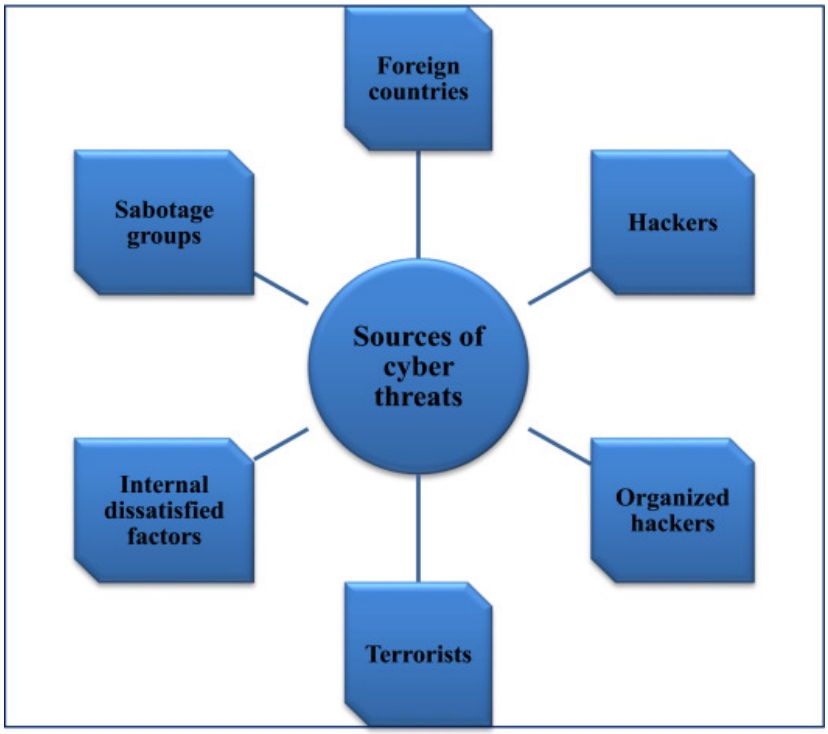

Figure 7 Sources of cyber threats [9].

Figure 8 Cybersecurity in an important consideration in construction [11].