frontiers in Built Environment

ORIGINAL RESEARCH
published: 26 May 2021
doi: 10.3389/fbuil.2021.612668

Cybersecurity in Construction: Where Do We Stand and How Do We Get Better Prepared

Bharadwaj R. K. Mantha[1,2] *and Borja García de Soto*[2]*

[1] *Department of Civil and Environmental Engineering, University of Sharjah, Sharjah, United Arab Emirates,* [2] *S.M.A.R.T. Construction Research Group, Division of Engineering, New York University Abu Dhabi (NYUAD), Saadiyat Island, United Arab Emirates*

The architecture, engineering, and construction (AEC) industry is increasingly becoming digital and more prone to cyber-attacks. Although there are several studies and standards in the cybersecurity domain, experts suggest that domain-specific studies need to be conducted to address the unique challenges faced within each of the different industries. Therefore, several cybersecurity studies have been undertaken for various industries, such as healthcare, manufacturing, telecommunication, and energy. However, this type of study is largely missing in the AEC industry due to different reasons, including lack of awareness. To address that, this study aims to (a) compare and analyze the number of cybersecurity-related documents in the AEC industry with several other industries, and (b) extract and analyze the cybersecurity-related documents data to identify potential future research trends and topics for the AEC community. The Web of Science (WOS) database, consisting of significant and influential journal publications, was used for document retrieval. VOSviewer was used to identify key research topics and trends in the cybersecurity domain and define future cybersecurity research in the AEC industry. WOS document retrieval results that compared the total number of publications corroborated the little to no attention received to cybersecurity investigation in the AEC industry. In addition, the VOSviewer analysis revealed three significant areas of research in the cybersecurity community that provide a reasonably justified roadmap for conducting cybersecurity research in the AEC industry. This study could greatly benefit the AEC research community and potential reaping benefits to the industry by creating more awareness among different stakeholders.

Keywords: cyber security, construction digitalization, text mining, cyber-physical systems, construction automation

OPEN ACCESS

Edited by:
Hongling Guo,
Tsinghua University, China

Reviewed by:
Joaquín Ordieres Meré,
Polytechnic University of Madrid, Spain
Andrew Agapiou,
University of Strathclyde, United Kingdom

***Correspondence:**
Borja García de Soto
garcia.de.soto@nyu.edu

Specialty section:
This article was submitted to Construction Management, a section of the journal Frontiers in Built Environment

Received: *30 September 2020*
Accepted: *18 March 2021*
Published: *26 May 2021*

Citation:
Mantha BRK and García de Soto B (2021) Cybersecurity in Construction: Where Do We Stand and How Do We Get Better Prepared. Front. Built Environ. 7:612668. doi: 10.3389/fbuil.2021.612668

INTRODUCTION

Cybersecurity can be defined as an aggregation of tools, policies, methods, approaches, best practices, and frameworks that help protect the organizations and their assets [International Telecommunication Union (ITU), 2008]. Although the digital revolution dates back to the early 1970s, research in cybersecurity did not receive much attention until the 1990s. The size of the cybersecurity industry is consistently growing, and it is projected to grow even more. For example, the global cybersecurity market is projected to grow to approximately 250 billion dollars by 2023 (Holst, 2020). This is significant because

of the detrimental implications of cyberattacks over the past decade. For example, the Identity Theft Resource Center (ITRC) reported that the data breaches and records exposed from 2005 to 2018 have increased multifold from 157 to 1,244 million and 67 to 447 million, respectively (ITRC, 2018). As a result, the economic impact of cybercrime is also steadily increasing. For instance, the average cost of cybercrime has increased by almost 30% for the United States, Japan, and the United Kingdom from 2017 to 2018 (Ponemon Institute and Accenture Securuty, 2019). The economic implications are also significant. The average annual cost due to cyberattacks in 2018 for the countries mentioned above was $27.37, $13.57, and $11.46 million, respectively. The same report details the economic impacts of cyberattacks for different sectors such as banking, insurance, and healthcare, which account for almost $19, $16, and $12 million, respectively. Unfortunately, due to scant attention given to understand the implications of such attacks in the architecture, engineering, and construction (AEC) industry, statistics are not available for that specific sector. However, among the reported values, the authors believe that the corresponding financial impact on the AEC sector might have been incorporated into the public and energy sector categories which include civil and infrastructure projects, such as bridges, tunnels, pipelines, dams, and government facilities.

Cybersecurity Research in Other Industries

Since the digital revolution in the 1990s, several tools, standards, methods, and frameworks have been developed to address the growing concern of working in the cyber environment and cyber-related incidents. Some of these are tailored to the specific needs and applications within the computer science and information technology (IT) industry, while others are generic that can apply to any industry. Two of the most commonly used generic frameworks include the national institute of standards and technology (NIST) framework for improving critical infrastructure cybersecurity (NIST, 2018) and international organization for standardization's information security management systems (i.e., series of 27000s code of practices including the ISO/IEC 27000:2018) (ISO, 2018).

Experts suggested the need to conduct domain-specific studies to address the unique challenges faced with the integration of digital tools and technologies into different sectors. Therefore, over the past couple of decades, many sectors, including manufacturing, healthcare, financial, and defense, have rapidly adopted and incorporated cybersecurity in their overall risk management approach with the help of uniquely tailored tools, methods, standards, and frameworks. For example, the center for internet security (CIS) developed a framework to prevent the most commonly occurred cyber-attacks in the healthcare sector (CIS, 2019). In addition, Hutchins et al. (2015) developed a cybersecurity risk identification framework for the manufacturing industry. The New York department of financial services (NYDFS) released a new set of regulations that mandates the cybersecurity requirements on all covered financial institutions (NYDFS, 2017). It is thus evident that industry-specific studies are beneficial to identify, monitor, and manage domain-specific risks.

Cybersecurity Research in the AEC Industry

Compared to other industries, the AEC industry is, in general, the least digitize. This can be attributed to the resistance to change, which has been one of the main reasons for the slow-paced digitalization of the AEC industry. However, this is changing due to the incorporation of several digital tools, technologies, and methods such as robotics, data analytics, additive manufacturing (AM), artificial intelligence (AI), internet of things (IoT), machine learning (ML), digital twins, and drones. Previous studies within the construction research community have investigated the need and incorporation of these technologies; however, little attention has been given to the cybersecurity implications.

A few studies and standards have been developed and tailored specifically for this industry. Brooks et al. (2020) investigated the knowledge of facility management personnel to comprehensively understand and mitigate cybersecurity vulnerabilities in the building automation control systems (BACS). Parn and Edwards (2019) suggested the use of blockchain technology to mitigate the risk of digital built environment vulnerabilities. Mutis and Paramashivam (2019) proposed the use of Cloud-BIM (building information model) to overcome the limitations and security vulnerabilities of the standalone BIM models, especially data breaches. Similarly, Hammi and Bouras (2018) identified the significance of cybersecurity implications of BIM and proposed the integration of BIM and blockchain in the university curriculum. Boyes (2015), on the other hand, examined the cyber-resilience issues of global supply chains considering the cybersecurity threat and vulnerability attributes. In addition, ISO (2020) and (IET, 2013) provide standards and a code of practice to improve cybersecurity and resilience in the built environment. However, one of the common limitations afflicting most of the studies and standards mentioned above is that they mainly focused on the design or operation and maintenance phases, and the investigation during the construction phase is still very limited. Although there are few studies conducted to address cybersecurity concerns during the construction phase as described below, there is still a considerable knowledge gap and significant potential to conduct research in this area, especially taking into consideration the rapid adoption of new technologies.

With a few exceptions, the publications related to understanding cybersecurity aspects in the construction sector are limited. For example, Mantha and García de Soto (2019) investigated the spread of vulnerability in construction networks using an agent-based modeling approach. They considered two construction networks, one resembling a traditional delivery system in which construction participants are more segregated (e.g., Design-Bid-Build or DBB) and another with higher integration and combination among the different stakeholders (e.g., Integrated Project Delivery or IPD). The results showed that the spread of the vulnerability (i.e., the number of impacted project participants) was higher in IPD-like

configurations. Mantha et al. (2021) proposed a preliminary cybersecurity threat model tailored to the AEC industry. To that end, they laid out threat models for each of the life cycle phases of a construction project and presented a case study for the commissioning phase. Mantha et al. (2020) tried to quantify the cyber vulnerability in construction projects by implementing the Common Vulnerability Scoring System (CVSS). The goal was to assess project participants' vulnerability, hence improving the security level of construction networks. Mohamed Shibly and García de Soto (2020) investigated different existing threat modeling methods, such as STRIDE, OCTAVE, PASTA, and VAST, to see which one would be a good fit for applications in construction projects. Based on that, they developed a preliminary threat modeling approach relevant to the construction industry that could be adopted to investigate the implementation of new technologies. As a proof-of-concept of the threat model and to provide insights into different threats that new technologies might have, they used an industrial-grade robotic arm system to 3D print construction elements off-site. Their study also helps to raise awareness about the cybersecurity implications of implementing such technologies and operational technology attacks in the AEC industry. Shemov et al. (2020) discussed the main challenges faced in the construction supply chain (CSC) and proposed a blockchain platform to enhance security. Using a hypothetical CSC scenario, they performed a partial threat analysis on a blockchain model to identify potential attacks and countermeasures required to prevent them. Their analysis showed that blockchain is a viable solution to the challenges in the CSC regardless of the risks associated with the security and robustness of the flow of information and data protection; however, they indicated that it would also be possible for malicious attacks to be executed, which could impact construction participants. Pärn and García de Soto (2020) did a review of the cyber-space and cyber-physical attacks to identify the motivations for hacking and the different types of hackers against the background of Construction 4.0. García de Soto et al. (2020) emphasized the significance and overlap of the construction cybersecurity and the European Union's Critical Infrastructure Protection (EUCIP) and suggested possible ways to improve the increasingly vulnerable cyber-security situation of the built environment.

Thus, it can be said that there is potential to conduct more comprehensive and thorough studies within the AEC industry, like in the other industries. There is room to develop frameworks, tools, best practices, and methods within the AEC industry to tackle the cybersecurity issues for all the different phases that might impact not only the business continuity, productivity, safety, privacy, and quality aspects but also the reputation of different stakeholders involved.

Need for Cybersecurity Research in the AEC Industry

With construction rapidly moving toward incorporating digital tools and technologies, cybersecurity issues, particularly cyber-attacks, will rise. Based on the types of attacks, they can be categorized as IT (e.g., impacting the IT infrastructure or digital ecosystem) or operational technology (OT) (e.g., impacting the operational tasks or processes). In some cases, both are applicable since the attacks could be initiated with an IT-based attack and concluded with an OT-based attack. A few examples of past reported incidents for the IT and OT based attacks include heating, ventilation, and air conditioning (HVAC) system and Building Management Systems (BMS) (Sheikh et al., 2019), hacking of a complete BMS system of the Google office in Australia (Ben, 2013), unauthorized access of Target's (a United States-based retailer) network through the mechanical contractor doing retrofit work on the HVAC system which lead to the exposure of about 40 million debit and credit card accounts (Krebs, 2014; Shu et al., 2017), stolen construction plans and specifications of the Australian Secret Intelligence Services (ASIS) (Motley and Mas, 2017), data breach of personal sensitive information of employees of two well-known United States based construction companies Turner and Whiting-Turner (iSqFt, 2016; Watson, 2018), compromised trade secrets of a construction elevator and escalator manufacturing firm (Motley and Mas, 2017), attempt to steal the proprietary information regarding the one armed brick layer (Pash, 2018), and, loss of about 17.2 million euros and 1.7 million United States dollars by Konecranes and Marous Brothers Construction due to unwarranted payments and wire fraud (Watson, 2018; Sawyer and Rubenstone, 2019). In another cyberattack, 65 GB (gigabytes) of data from nuclear power plants were stolen by hackers. More than 11,000 project-related documents and more than a thousand employee-related sensitive information was compromised (Cyware Social, 2018). More recently, Bouygues Construction suffered a ransomware attack, forcing the company to shut down its systems worldwide (Manucaster, 2020). Bam Construct had to shut down its website and some other systems due to a cyberattack, while Interserve suffered a major data breach. As many as 100,000 employees may have been affected by the attack (Warrington, 2020). In a recent incident in Florida, United States, hackers tried to poison the entire water supply (Collier, 2021).

As can be expected, most of the attacks indicated above occurred due to vulnerabilities and inconsistencies during the same life cycle phase of a project. However, it is also worthy to note that some of these attacks occurred due to vulnerabilities and inconsistencies in other phases. Therefore, caution needs to be exercised to understand, analyze, and develop countermeasures for the root cause of the cyber-attacks. A comprehensive understanding of the different project phases and their interdependencies is required to devise an effective cybersecurity risk management plan.

In addition, it is not uncommon that several cybersecurity-related incidents never get reported due to their potential implications on market reputation and competition. According to the global 2020 State of Cybersecurity Survey report by the Information Systems Audit and Control Association, cybercrime is significantly underreported. 62% of the respondents indicated that cybercrime is consistently underreported, despite legal or regulatory requirements requiring companies to report such cases (ISACA, 2020). Due to the inherent nature of the AEC industry, lack of cyber-related best practices can cause severe

implications on the physical asset during its construction, facilities already constructed, people using these facilities, people working on the construction sites, and so on. This will have not only financial implications but also the potential to compromise human lives. Therefore, there is a critical need to investigate these implications in the construction research community and devise action plans to mitigate these risks.

Text Mining to Assist in the Determination of the Future Research Roadmap

Several studies conducted in the past couple of decades in other industries focused on addressing cybersecurity issues and concerns. The volume and diversity of publications are increasing every year. Accurate and reliable identification of the most studied and emerging research topics and trends can assist future cybersecurity research in the AEC industry (Neff and Corley, 2009). This acts as a preliminary step toward enabling a fully autonomous knowledge discovery process from the large sets of textual data (i.e., full-length manuscripts or articles) (Ding et al., 2018). This is also widely known as KDD or knowledge discovery in databases. The idea is to gather potentially useful information from the unstructured or semi-structured article database with text mining approaches.

Text mining approaches can be an effective way to identify research trends and topics successfully. For example, Chen et al. (2018) did a data-driven review using text mining on scientific literature and social media to achieve an unbiased way to assess the use of automation technologies in the construction industry. They used VOSviewer (where VOS stands for visualization of similarities) and RapidMiner Studio to determine the most promising research areas by analyzing scientific publications. Nie and Sun (2017) identified research trends in the design of products and services with text mining approaches such as clustering and bibliometric analysis. The proposed methodology takes advantage of the bibliometric data and network analysis techniques to perceive significant academic divisions. Overall, four academic branches within the design research were proposed and extensively discussed based on the results from this approach. Using a similar approach, Oh and Lee (2017) analyzed 869 articles to identify interdisciplinary research directions. Jiang et al. (2016) employed topic modeling techniques to explore the trends in the hydropower studies conducted in the past (about 1,726 articles were analyzed). In addition, Rezaeian et al. (2017) claimed that text mining can be used to realize science foresight with the help of topic extraction from large amounts of data. Zhang and Liao (2015) analyzed relevant data from Web of Science (WOS) in VOSviewer and showed the link between building controls and indoor thermal comfort.

It is evident from the previous studies that text mining is a useful tool to identify research topics and trends based on previously published journal articles, conference proceedings, and engineering reports (i.e., text data). To the best of the authors' knowledge, this has not been done in the AEC industry, particularly concerning cybersecurity. This study aims to identify potential future research topics and cybersecurity trends that the construction research community can focus on moving forward. Therefore, the objectives of this research are to (a) compare and analyze the number of cybersecurity-related documents in the AEC industry with several other industries (or sectors) such as manufacturing, defense, and telecommunications, and (b) extract and analyze the cybersecurity-related documents data to identify potential future research trends and topics for the AEC community.

METHODOLOGY

Figure 1 shows the overall methodology process employed in this study. As can be observed, it is broadly divided into two parts. The objective of Part 1 is to retrieve and analyze documents in the cybersecurity domain, mainly focusing on the comparison of the number of documents among different industries such as manufacturing, healthcare, banking/insurance, defense, and construction. For this study, the WOS core collection database was used. It consists of all the significant and influential journals and is widely used for similar studies (Song et al., 2016; Zhao, 2017; Tang et al., 2019). The objective of Part 2 is to analyze the structured text (i.e., title, abstract, and keywords) of the documents in the cybersecurity domain and identify some of the key research topics and trends that have been researched. To perform the analysis, VOSviewer version 1.6.15 (VOSviewer, 2020) was used because of the ease of implementation, visualization, and usability (Van Eck and Waltman, 2010; Hosseini et al., 2018; Wang et al., 2019; Ozturk, 2020). The idea is to take inspiration from key topics and pave the way for a future research roadmap to conduct cybersecurity-related research in the AEC industry. It has to be noted that WOS and VOSviewer are incidental for the context of this study. A similar analysis could still be performed using other databases such as Google Scholar and Scopus and visualization or analysis tools such as Gephi, CiteSpace, CoPalRed, BibExcel, VantagePoint, or Sci2 (Cobo et al., 2011).

Determine Cyber Security Keywords

Since the goal is to retrieve and analyze cybersecurity-related documents, all different variants of the words "cyber security," "cyber attack," "cyber threat," "hack," and "cyber vulnerability" were identified as the keywords for the search criteria. The different variants used were with and without spaces, with and without hyphenations, singular and plural, and words that begin with a specific string of characters (i.e., using wildcards, such as * to represent unknown characters). For example, hack* would search for all the words that start with hack, such as hacking, hacker, and hacked, but also hackneyed or hacksaw, which are not relevant for this study, hence need to be excluded.

Retrieve Documents

The goal of this step is to retrieve all the documents based on the keywords identified. To do this, the following procedure was followed. First, the WOS core collection database was chosen since choosing this will enable using the advanced search features with specific string search and download the structured text data

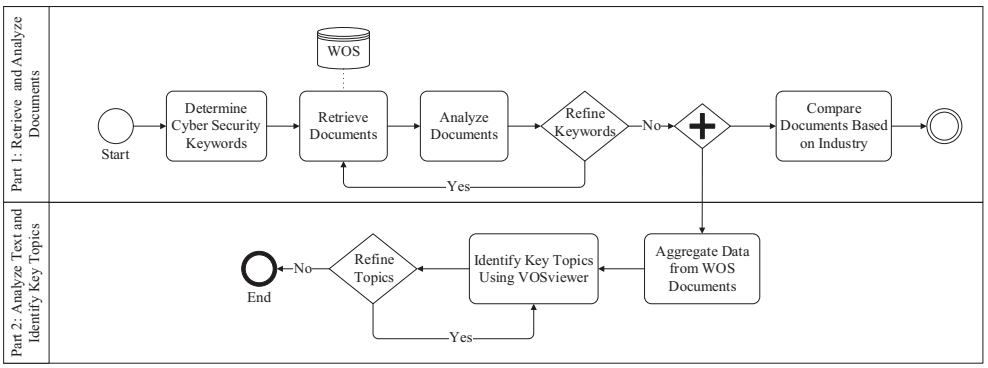

FIGURE 1 | Overview of the methodology for the text mining approach.

(e.g., title and abstract) for further analysis in VOSviewer. Second, an advanced search option is selected. Third, the timespan is selected from 1900 to 2019. The year 2020 was not selected to maintain consistency and avoid discrepancies in the number of documents observed. Fourth, to understand the documents' quantum across different languages and article types (e.g., article, book chapter, and conference proceedings), the search is not restricted to any language or article type. That is, all languages and document types are chosen. Finally, the search string criteria field tags of TI (title) or AB (i.e., abstract) were used with an OR Boolean operator. That is, the resulting document will either have the keyword in the title or the abstract. In addition, a search query using wildcards was also used, which is represented by the asterisk (*). Significantly, the wildcard search query used was to represent and identify words that begin with a group of characters. As previously indicated, all the words that began with hack were retrieved using the following expression hack*. This way, all the documents that contain words starting with "hack" will be shown in the results, such as the words including but not limited to hacking, hacker, and hacked. This is believed to be a reasonable representation of the documents under the cybersecurity category. **Table 1** summarizes the above-mentioned different characteristics of the search criteria used. The above search criteria and the variants of the keywords mentioned resulted in a total of 23,359 documents.

Analyze Documents

This step aims to analyze and identify any anomalies in the search criteria based on the documents resulting from the previous step. To achieve this, the resulting first 50 documents were analyzed for the keyword matched, and any potential anomalies were investigated accordingly. For example, one observation was that the documents which had the word "hackneyed" were also included in the search results. However, "hackneyed" is a general English term meaning "*lacking in freshness or originality*" and not relevant to this study. This could be because of several reasons, such as inconsistencies in the keywords selected and acronyms that might have interpretations and meanings in other industries. After considering the additional criteria and eliminating the anomalies, 22,909 documents were observed compared to the 23,359 retrieved initially.

TABLE 1 | Summary of WOS search criteria characteristics.

Search criteria description	Option selected
Search type	Advanced search
Languages	All languages
Document types	All document types
Timespan	1900–2019
Booleans used	OR, AND, NOT
Advanced search queries used	Wildcard (*)
Overview search logic	TI = (keywords) OR AB = (keywords)

Refine Keywords

In this step, based on the observations from the previous steps, the keywords and the search logic are refined to obtain a refined list of documents. This step is very crucial to ensure a representative number of documents are shown in the search results. If the refinement is not done cautiously, the search result could lead to a lot more documents that are not directly or indirectly relevant to the topic of interest. Therefore, based on the identified anomalies, additional search criteria such as NOT could be included in the previous search criteria fields. In this step, the NOT Boolean operator will most likely be used to eliminate the additional documents that showed up due to a rather incomprehensive search criterion. For example, to remove search results that had "hackneyed," a new logic is introduced, such as (hack* NOT hackney*). This means the search results will include word variants of hack, such as hacking and hacked, and not the variant of hackney, such as hackneyed. At the end of this step, the refined keywords and the search criteria are used to obtain a refined list of documents that should represent the topic of interest, which is cybersecurity in the context of this study.

Compare Documents Based on Industry

This step aims to segregate the cybersecurity-related documents obtained from the previous step and compare the total number of documents among different industries. That is, among the whole list of documents obtained that conducted cybersecurity research, which belongs to a specific industry. The objective is to

get a general understanding of the research in cybersecurity in different industries. Specifically, the idea is to compare the total number of documents in construction with other industries such as telecommunications, manufacturing, and energy.

So, the idea is to categorize the list of cybersecurity documents into different identified industries. To do this, an additional search constraint is added to the previous search criteria. That is, along with the same search criteria (i.e., the one used for obtaining the cybersecurity documents) as before, an additional Boolean operator AND is added along with the respective industry's keywords. For example, to obtain construction cybersecurity documents, the following logic is used: TI = (*cybersecurity keywords* AND *construction keywords*) OR AB = (*cybersecurity keywords* AND *construction keywords*). For example, to obtain construction-relevant documents, additional keyword search within the title and the abstract is performed. All the documents with both the cybersecurity and construction keywords in either the title (TI) or the abstract (AB) will be categorized as documents that have conducted cybersecurity research in the construction industry.

Some of the example keywords that can be used for construction include variants of the following words such as "construction industry," "aec industry," "aecfm" (from architecture, engineering, construction, and facility management), "aeco" (from architecture, engineering, construction, and operations), and "building information modeling." Although this might not be an exact representation or categorization of the documents, it is a reasonable assumption and should give an overview picture of the volume of documents among different industries. **Table 2** shows the keywords used for each of the considered industries and the respective number of documents obtained. It has to be noted that this is not an exhaustive search, but a search performed to corroborate the significant gap of cybersecurity research in the AEC (i.e., construction) industry. As can be observed, it is evident that the construction industry lacks a lot compared to all the other industries considered. Given the fundamental digital element within the industry, a tremendous number of documents fall under the telecommunications industry. That is, the industry deals with digital communication, which is the core of any cyber environment. This is followed by the energy industry, which can be understood given the critical nature of the industry. Any disruptions to this industry will have severe implications and detrimental consequences. Similarly, these numbers could be observed for the other industries as well.

Only 66 documents contained the AEC industry keywords mentioned in **Table 2**. Upon further refinement to eliminate some of the keywords particularly relevant to the operation and maintenance phase (i.e., if the built environment keywords such as smart homes, built environment, smart buildings, building automation systems, and building management systems were removed), only four documents were retrieved. This refinement is deliberately performed to investigate the current state of cybersecurity research within the AEC industry that focuses on the construction phase rather than on the operation and maintenance phase. The goal was to show the meager amount of attention that has been received toward the construction phase compared to the operation and maintenance phases. Upon further investigating the four documents (without considering the built environment), it was observed that two of them were focused on BIM and blockchain implementation, one of them was focused on common data environment (CDE) vulnerabilities during the operation and maintenance phase (e.g., securing the remote monitoring and maintenance of the existing facilities and the corresponding digital assets), and one of them was focused on the topic of smart grid. This means none of the studies were focused on investigating the cybersecurity aspects during the construction phase. In addition, further investigation of the 66 documents showed that the topic of smart buildings was one of the potential applications for the proposed research, and the core of the research did not correspond to the built environment. Overall, it is clear that the construction research community needs to incorporate cybersecurity into the research agenda. To facilitate this, universities, government and non-governmental funding agencies, student and professional organizations, private entities, journals, and conferences should accelerate the efforts to include cybersecurity in their grand vision rapidly. For example, journals can have special issues focusing on cybersecurity aspects.

Aggregate Data From WOS Documents

This step aims to aggregate the WOS documents data that correspond to the topic of interest, which is cybersecurity in

TABLE 2 | Categorization of cybersecurity documents among different industries.

Industry (or Sector)	#Documents	Variants of keywords used
AEC (without built environment)	4	AEC; AECO; AECFM; construction industry; construction sector; building information model.
AEC (with built environment)	66	AEC; AECO; AECFM; construction industry; construction sector; building information model; building automation systems; building management systems; smart homes; built environment; smart buildings.
Tele-communications	5,203	Telecommunications; communications; internet; wireless network.
Energy	3,379	Energy; nuclear; solar; wind; electric; coal; oil; gas.
Defense	2,014	Defense; defense; military; surveillance
Banking and Insurance	1,065	Banking; insurance; finance; e-commerce; credit unions; credit cards; credit cooperatives
Manufacturing	1,536	Manufacture; product; factory

the current context. To do this, a complete record of all the documents' data is exported into the "other formats" (i.e., tab-delimited) from WOS. Since WOS only allows exporting the records of 500 documents at once, this process is iteratively done for all the documents manually (i.e., until the 22,909 documents were extracted).

Identify Key Topics Using VOSviewer

This step aims to identify the most researched topics and trends from the title and abstract data of all the 22,909 document records downloaded from WOS in the previous step. In this study, VOSviewer was used to visualize the network of words and their link strengths. The following is the brief procedure followed to achieve this in the VOSviewer: (a) create a term co-occurrence map based on text data; (b) read data from a bibliographic database file (i.e., all the tab-delimited files consisting of 22,909 document records); (c) perform co-occurrence analysis on all the words in the title and abstract with a full counting method. Here, abstract section labels (if any) and the copyright statements (if any) are ignored for further analysis. The full counting method refers to all the word occurrences instead of the binary counting method, which means that only the presence of a word is considered. This is because the objective is to determine critical topics based on the total number of occurrences; and (d) choose a threshold number of keyword occurrences to determine the total number of keywords accordingly. For example, a trial and error method can be applied to change the number of occurrences and obtain a fixed number of keywords such as 10, 20, or 50. Since it will not be legible to visualize all the words (more than 270,000 that appeared at least once and more than 69,000 words appeared at least twice), a threshold of 772 was applied to show the top 100 keywords (**Figure 2**). Since the most appeared will have larger node size and text size, some of the most appeared words can be seen, such as system, model, data, security, technology, and framework.

A threshold occurrence of 2,775 had to be applied to obtain the top 10 keywords in the context of this study. **Figure 3** shows the top 10 keywords obtained from the VOSviewer analysis. Based on the word co-occurrence in the documents, VOSviewer segregates these keywords into distinct clusters, as shown in different colors (red and green). The size of a given node (i.e., keyword) in the network is proportional to the number of occurrences of a given keyword (i.e., node) in the documents analyzed. For example, within the red cluster, the word "system" appeared more often than "cyber-attack." Similarly, in the green cluster, the word "security" appeared more times than "internet." As shown in **Figure 3**, most of the topics obtained might not add much value to identifying cybersecurity research topics or trends. For example, it is known that the topic of interest is cybersecurity, so "security" might not add much value. Similarly, "system" might not have much significance since it is a very generic term. An additional step of refining topics is performed to address this issue is explained in the following subsection.

Refine Topics

This step aims to refine the topics obtained from the previous step for similar reasons as those for the refinement of keywords done in 2.4. Given the nature of occurrences, some of the usually used terms appear in the result, which do not add value. Therefore, some of the commonly occurred terms are removed from the search, such as "model," "algorithm," "analysis," and "design." In addition, some of the terms with slightly different formatting are clubbed together and are represented in the same term, such as "cyber-physical system," which is replaced by "cyber-physical systems" or "intrusion detection system," which is replaced by "intrusion detection." After the application of these rules and constraints, the visualization of the network is obtained. **Figure 4** shows the top 10 keywords from VOSviewer based on a threshold occurrence of 1,200. That is, these ten keywords occurred more than 1,200 times in all the abstracts combined. Similarly, 36 keywords met the threshold occurrence of 1,000.

RESULTS AND DISCUSSION

This section discusses the meaning, significance, context, and relevance with corresponding examples in the AEC industry for each of the ten key topics identified from the methodology. Since the topics identified are based on the number of occurrences from more than 22,000 cybersecurity-related documents, it is warranted to assume and argue that these are some of the significant aspects of cybersecurity investigation. Therefore, moving forward, these topics will form an essential basis in shaping the future of fundamental research in the area of cybersecurity in the AEC industry.

Several studies have suggested the use of clustering as a means to analyze and define research trends. For example, Duarte et al. (2020) mapped the existing literature in supply chain risk management (SCRM) and defined the future research agenda on decision-making models and support systems based on clustered topics. Similarly, Fagundes et al. (2020) identified the potential emerging avenues for future research based on the systematic literature review on geotourism and territorial development. The underlying principle was to conduct a thorough review of articles based on their keywords and then define future research avenues based on the clustering analysis. Some of the other studies that adopted similar approaches include (Hosseini et al., 2018; Mascarenhas et al., 2018; Sainaghi et al., 2020). Inspired by those studies, a similar approach was followed here. The clusters formed (**Figure 4**) are used as the basis for defining future research areas specific to the AEC industry.

To better understand the clustering process in VOSviewer, it is important to note the following terms and concepts. A network visualization map consists of items and links. Items refer to the objects that are of interest, whereas link refers to the connection or relation between the items. Examples of items include keywords, author names, publications, and journal names. Examples of links include co-authorship links, bibliographic coupling links, and co-occurrence. In the context of this study, items are keywords, and the links represent the co-occurrence. In addition, each link has a strength called link strength. This is essentially a numerical value that represents the strength of the link. As can be expected, the link strength value is directly proportional to the strength of the link. That

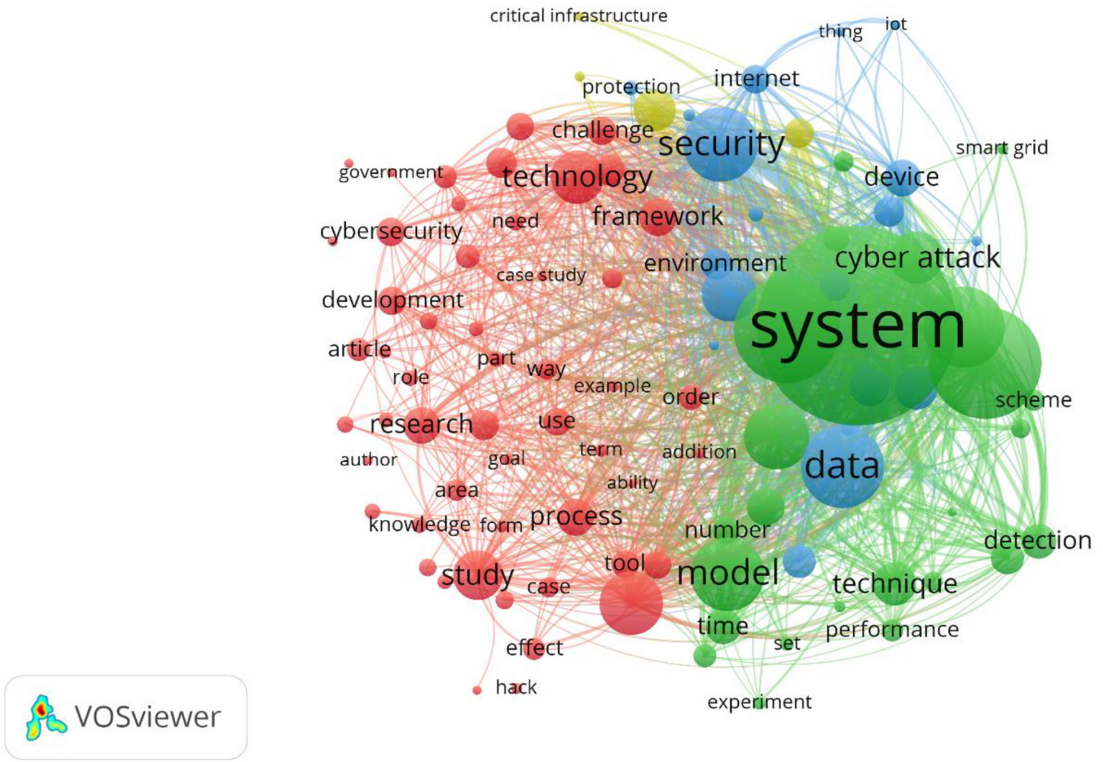

FIGURE 2 | Top 100 keywords (before refinement) obtained from VOSviewer.

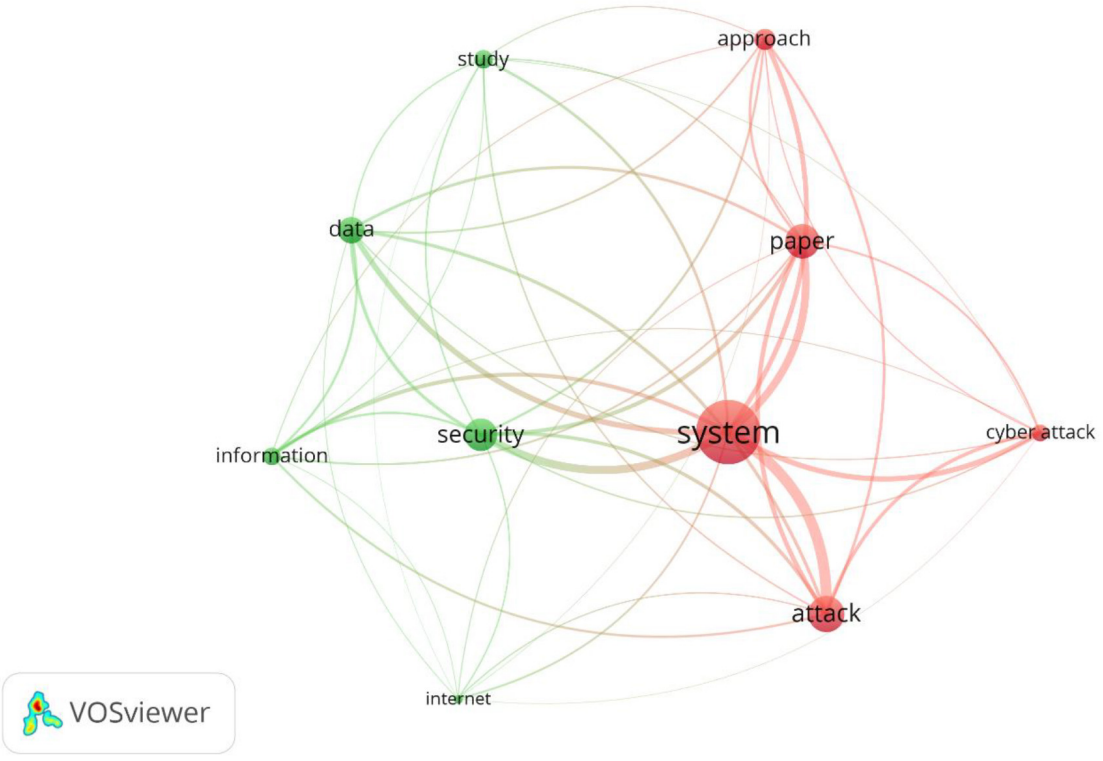

FIGURE 3 | Top 10 keywords (before refinement) obtained from VOSviewer.

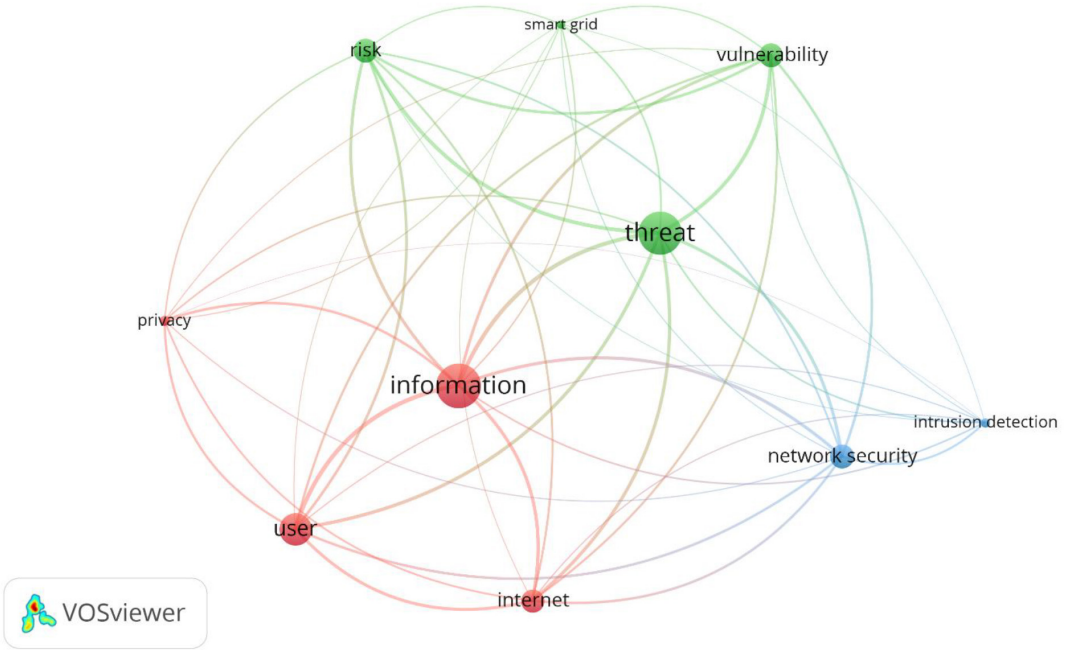

FIGURE 4 | Top 10 keywords (after refinement) obtained from VOSviewer.

is, the higher is the link strength value, the stronger the link is. For example, in the case of bibliographic coupling, the link strength may represent the number of cited references the two publications have in common. In the context of this study, the link strength represents the number of publications the two terms occur together. Based on the links, link strengths, inter- (i.e., link strengths among the items in the same clusters) and intra- (i.e., link strengths among the items in different clusters) connectivity, VOSviewer segregates the items into different clusters. These clusters are non-overlapping (i.e., one item is assigned into only one cluster). Due to the nature of cluster formation in VOSviewer, the clusters formed have a stronger connection within themselves. For further details regarding the terminology and cluster formation, readers are encouraged to refer to Van Eck and Waltman (2020).

Given the overlap some of these topics have, the authors would like to take advantage of the clustering performed by VOSviewer. As can be observed from **Figure 3**, there are three clusters of topics. The first one consists of "information," "user," "privacy," and "internet." The second cluster contains "threat," "risk," "vulnerability," and "smart grid." Finally, the third cluster contains "network security" and "intrusion detection." These clusters or research areas are discussed next.

Research Area 1 – Information and Data Privacy

The first cluster is an aggregation of keywords such as "information," "privacy," "user," and "internet." In the domain of cybersecurity, all these keywords relate to a widely researched area called information privacy for data privacy. For example, information and data privacy deal with the privacy of personal information or data, such as medical records, financial data, business-related information, consumers' information, and website data. This has received growing attention over the past decade because of the advancements in technology and increasingly complex data collection and storage mechanisms. The resulting top cluster from the analysis also aligns with the fact that most cyber-attacks focused on the data breach, as extensively discussed in the section "Introduction".

The AEC industry is no different when it comes to data or information privacy. With increasing interest and implementation of digital models and automation, this will be of great concern to the AEC industry. Although (Mantha and García de Soto, 2019) enumerated and taxonomized some of these data elements for a particular delivery method and specific construction stakeholders during the construction phase in the context of cybersecurity, a comprehensive investigation of the information and communication technologies (ICT) across different life cycle phases of the project is still missing. In addition, Parn and Edwards (2019) suggested some measures to secure the stored and managed information through the CDE. However, moving forward, more comprehensive studies need to be conducted that encompass and safeguard the information of all the different products, processes, and people involved in the AEC industry. Examples of products include highly sensitive facilities such as government buildings, nuclear facilities, general utilities and equipment, and tools such as excavators, 3D printers, tower cranes, loaders, and dump trucks. Examples of processes that include sensitive and proprietary information include surveillance systems on job sites, state-of-the-art technologies such as concrete 3D printing, drone-based monitoring and

project control, and robotic construction. People represent all the stakeholders directly or indirectly involved in the projects, such as contractors, vendors, suppliers, workers, engineers, designers, managers, investors, owners, tenants, or visitors.

It is also of paramount importance to investigate the interdependencies of information storage and exchange. Since the AEC industry is well known for its fragmented nature, several information exchanges occur through various media such as emails, hard disks, and the cloud. While such information exchange can improve collaboration and potentially productivity, it poses a significant risk of being stolen or modified along the process. More importantly, it is sometimes challenging to identify any potential modifications made during the process, which will pose a considerable risk to the following (or subsequent) activities, processes, or project phases. Therefore, it is critical to investigate the information privacy from one activity to another and from one project's lifecycle phase to another.

Research Area 2 – Risks, Threats, and Vulnerabilities

The keywords observed in the second cluster are "risk," "threat," "vulnerability," and "smart grid." Although the first three keywords can be categorized as one of the fundamental aspects of cybersecurity, "smart grid" seems to be an outlier. Upon further investigation of these documents, which consisted of "smart grid," it was observed that most of them either identified the risks, threats, and vulnerabilities of smart grids or mentioned smart grids as one of the potential applications for the frameworks and methodologies proposed. This means that smart grids have received significant attention, especially in the cybersecurity aspects. Similar to what was observed for the AEC industry, most of the cybersecurity research done so far within the AEC industry was either focused on smart homes, smart buildings, or smart building management systems (i.e., 66 vs. four documents retrieved from the WOS database with and without the built environment keywords).

Any fundamental research performed in cybersecurity will have at least one of these terms: risks, threats, and vulnerabilities. Often, even in the security community, these related terms are mixed up, used interchangeably, and confused (Muscat, 2019; TAG, 2020). Briefly defined, a threat is something likely to cause damage or disrupt operations. Vulnerability can be seen as a weakness in the protection efforts. Risk is the potential of an impact or loss to the asset caused because a threat exploited vulnerability (TAG, 2020). The fundamental nature of these terms is corroborated by the fact that several standards and codes suggest identifying any of one or many of these as a preliminary step toward cybersecurity investigation and mitigation. For example, the NIST framework suggests identifying risks as one of the preliminary steps toward improving critical infrastructure cybersecurity (NIST, 2018). In addition, the ISO standard 27,000 and 27,001 (ISO, 2018) emphasizes the identification and documentation of all the potential threats and vulnerabilities as a means of conducting a comprehensive and overall cybersecurity assessment. Furthering to that, several governmental and reputed international organizations (e.g., NIST) developed databases [e.g., National Vulnerability Databases (NVD) and Common Vulnerabilities and Exposures (CVE)] to document, periodically maintain, and update these key aspects (CVE, 2020; NVD, 2020).

Such a comprehensive list of risks, threats, and vulnerabilities does not exist within the AEC industry. A few recent studies have explored and proposed frameworks to assist in the identification of critical aspects. However, this is just a preliminary step toward conducting a more thorough and rigorous evaluation. Further investigation is required to thoroughly investigate each of the life cycle phases of a project. In addition, taking inspiration from the existing standards and databases, a common database of risks, threats, and vulnerabilities in the AEC industries can be enumerated and maintained by some of the internationally reputed organizations such as the American Society of Civil Engineers (ASCE), the Associated General Contractors of America (AGC), the Construction Industry Institute (CII), the European Network of Construction Companies for Research and Development (ENCORD), or the International Association for Automation and Robotics in Construction (IAARC).

Research Area 3 – Network Security and Intrusion Detection

The keywords observed in this cluster are network security and intrusion detection. In the context of cybersecurity research, network security and intrusion detection were primarily focused on computer networks. While intrusion detection is focused on identifying or detecting malicious activity in the networks, network security can be considered a broader concept that deals with the protection, usability, and integrity of the networks. Given the nature of the systems that exist in the field of cybersecurity, they were mostly focused on the hardware and software of these IT infrastructures. However, in the AEC industry, these will have direct and indirect consequences on the quality, productivity, safety, and health of the facility (e.g., building under construction), equipment (e.g., tower cranes on job sites), people (e.g., workers), and society (e.g., inconvenience caused due to construction site disruptions). Thus, a similar investigation in the AEC industry can be considered as a hybrid network consisting of IT software, hardware, and physical assets such as facility, equipment, and stakeholders.

Therefore, this can also be considered as a critical research topic with a slightly varying scope (i.e., additional aspects such as the consideration of hybrid networks) in the AEC industry, given its significance and implications. Several studies were conducted in the context of intrusion detection with potential applications in the smart home and built environment context (Malche and Maheshwary, 2017; Pan et al., 2019). The main objective was to monitor and control the safety of smart home-related systems and services connected through the IoT architecture. It is also worthy to note that one of the recent studies conducted by Jin et al. (2020) proposed an unauthorized IoT-based intrusion monitoring system to improve worker safety. This, however, was focused only on monitoring the location of the workers based on their access levels and did not consider the detection of unknown malicious outsiders into the construction environment. Several research questions in the area of network security and intrusion

detection are still largely unaddressed, such as (a) How does the introduction of a new technological system (e.g., a progress monitoring drone, a bricklaying robot, and a construction 3D printer) into the existing construction process impact the overall security of the construction network? What will be impacted the most? How can this be addressed? (b) What are some of the implications of an unauthorized intrusion by a malicious insider or an outsider on construction sites? Who will bear the responsibility in case of a malicious insider? How should the project progress further? (c) How will an unauthorized undetected intrusion during one activity or one phase of a project potentially impact activities in another phase of the project? Who will bear the responsibility for project completion, delays, and potential lawsuits? Thus, it is evident that there is much scope and need for future research with potential benefits to the stakeholders and the broader society.

CONCLUSION AND OUTLOOK

This study has two main contributions. The first one is the identification of a largely neglected research area of cybersecurity in the AEC industry. This is achieved by comparing and analyzing the number of cybersecurity-related documents in the AEC industry with several other industries (or sectors) such as healthcare, energy, defense, telecommunications, manufacturing, banking, and insurance (financial). After completing the document screening process, more than 22,000 documents in the area of cybersecurity were retrieved from WOS. Comparing the number of documents that belong to several different sectors revealed that the AEC industry has given little to no attention to this topic. Only 66 documents were extracted when considering the AEC industry keywords compared to thousands of documents for other domains. Upon further investigation, it was also observed that most of these 66 documents were focused on smart homes, smart buildings, building automation systems (or building management systems)—a further refinement of the 66 documents resulted in just four documents that were focused during the construction phase.

The second contribution is the identification of potential future research trends and topics for the AEC community. This was done by further analyzing the structured data (e.g., title and abstract excluding copyright information) cybersecurity-related documents (which were more than 22,000) with the help of VOSviewer (a network visualization and analysis tool). Based on the occurrences, the top ten most occurring words were retrieved. These words were automatically grouped into three clusters (research areas or trends) based on their link strengths by the VOSviewer software. The first one consisted of "information," "user," "privacy," and "internet." The second research area contained "threat," "risk," "vulnerability," and "smart grid." Finally, the third research area contained "network security" and "intrusion detection." A discussion was provided for each of these research areas and their significance, context, and relevance to the AEC industry. Taking this further, focus-group interviews or surveys could be conducted to identify the challenges of adopting these research areas in the AEC industry. Learning's from those interviews/surveys could complement this study's outcomes and ease the implementation and integration of new technologies with a cybersecurity mindset.

The results from this study show a research gap in the AEC industry and warrant future research efforts to focus on the areas of (1) information and data privacy, (2) risks, threats, and vulnerabilities, and (3) network security and intrusion detection. Therefore, this study has potential benefits to the stakeholders and the broader society, given the repercussions of cyber-attacks on the AEC industry.

DATA AVAILABILITY STATEMENT

Publicly available datasets were analyzed in this study. Interested readers can request the datasets used for this study, such as the WOS files (e.g., .txt bibliographic files), and VOSviewer files (e.g., network and cluster files with .net and .clu extension) by contacting the corresponding author.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct and intellectual contribution to the work, and approved it for publication.

ACKNOWLEDGMENTS

The authors would like to thank the Center for Cyber Security at New York University Abu Dhabi (CCS-AD) for the support provided.

REFERENCES

Ben, G. (2013). Australian Google Office Building Hacked. *The Sydney Morning Herald.* Available online at: https://www.smh.com.au/technology/australiangoogle-office-building-hacked-20130507-2j416.html (accessed April, 2021).

Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technol. Innov. Manag. Rev.* Available online at: https://timreview.ca/sites/default/files/article_PDF/Boyes_TIMReview_April2015.pdf (accessed April, 2021).

Brooks, D. J., Coole, M., and Haskell-Dowland, P. (2020). Intelligent building systems: security and facility professionals' understanding of system threats, vulnerabilities and mitigation practice. *Secur. J.* 33, 244–265. doi: 10.1057/s41284-019-00183-9

Chen, Q., García de Soto, B., and Adey, B. T. (2018). Construction automation: research areas, industry concerns and suggestions for advancement. *Autom. Constr.* 94, 22–38. doi: 10.1016/j.autcon.2018.05.028

CIS (2019). V7.1 Introduces Implementation Groups to the CIS Controls. *Center for Internet Security (CIS).* Available online at: https://www.cisecurity.org/blog/v7-1-introduces-implementation-groups-cis-controls/ (accessed April, 2021).

Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., and Herrera, F. (2011). Science mapping software tools: review, analysis, and cooperative study among tools. *J. Am. Soc. Inf. Sci. Technol.* 62, 1382–1402. doi: 10.1002/asi.21525

Collier, K. (2021). *Lye-Poisoning Attack in Florida Shows Cybersecurity Gaps in Water Systems*. New York, NY: NBC News.

CVE (2020). Common Vulnerabilities and Exposures (CVE). *The MITRE Corporation.* Available online at: https://cve.mitre.org/docs/cve-intro-handout.pdf (accessed April, 2021).

Cyware Social (2018). *Hackers Hit French Firm Ingerop Stealing 65 GB Data Relating to Nuclear Power Plants*. New York, NY: Hacker News.

Ding, Z., Li, Z., and Fan, C. (2018). Building energy savings: analysis of research trends based on text mining. *Autom. Constr.* 96, 398–410. doi: 10.1016/j.autcon.2018.10.008

Duarte, A., Braga, V., Marques, C., and Sá, A. A. (2020). Geotourism and territorial development: a systematic literature review and research agenda. *Geoheritage* 12:65. doi: 10.1007/s12371-020-00478-z

Fagundes, M. V. C., Teles, E. O., Vieira de Melo, S. A. B., and Freires, F. G. M. (2020). Decision-making models and support systems for supply chain risk: literature mapping and future research agenda. *Eur. Res. Manag. Bus. Econ.* 26, 63–70. doi: 10.1016/j.iedeen.2020.02.001

García de Soto, B., Georgescu, A., Mantha, B., Turk, Ž, and Maciel, A. (2020). *Construction Cybersecurity and Critical Infrastructure Protection: Significance, Overlaps, and Proposed Action Plan*. *Preprints* 2020050213. doi: 10.20944/preprints202005.0213.v1

Hammi, A., and Bouras, A. (2018). "Towards Safe-BIM curricula based on the integration of cybersecurity and blockchains features," in *12th International Technology, Education and Development Conference* (Valencia). doi: 10.21125/inted.2018.0453

Holst, A. (2020). *Global Cybersecurity Market Forecast 2017-2023*. Hamburg: Statista.

Hosseini, M. R., Martek, I., Zavadskas, E. K., Aibinu, A. A., Arashpour, M., and Chileshe, N. (2018). Critical evaluation of off-site construction research: a scientometric analysis. *Autom. Constr.* 87, 235–247. doi: 10.1016/j.autcon.2017.12.002

Hutchins, M. J., Bhinge, R., Micali, M. K., Robinson, S. L., Sutherland, J. W., and Dornfeld, D. (2015). Framework for identifying cybersecurity risks in manufacturing. *Procedia Manuf.* 1, 47–63. doi: 10.1016/j.promfg.2015.09.060

IET (2013). *Resilience and Cyber Security of Technology in the Built Environment, Institution of Engineering and Technology/CPNI*. Stevenage: IET Standards.

International Telecommunication Union (ITU) (2008). *Definition of Cybersecurity*. Geneva: ITU.

ISACA (2020). *State of Cybersecurity 2020 Part 2: Threat Landscape and Se*. Schaumburg, IL: ISACA.

ISO (2018). *ISO – ISO/IEC 27000:2018 – Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary*. Geneva: ISO.

ISO (2020). *ISO – ISO 19650-5:2020 – Organization and Digitization of Information About Buildings and Civil Engineering Works, Including Building Information Modelling (BIM) — Information Management Using Building Information Modelling — Part 5: Security-Minded Appro*. Geneva: ISO.

iSqFt (2016). *Data Breaches, Cyber Security and the Construction Industry*. Cincinnati, OH: iSqFt.

ITRC (2018). *2018 End of Year Data Breach Report*. Los Angeles, CA: Identity Theft Resource Center.

Jiang, H., Qiang, M., and Lin, P. (2016). A topic modeling based bibliometric exploration of hydropower research. *Renewable Sustainable Energy Rev.* 57, 226–237. doi: 10.1016/j.rser.2015.12.194

Jin, R., Zhang, H., Liu, D., and Yan, X. (2020). IoT-based detecting, locating and alarming of unauthorized intrusion on construction sites. *Autom. Constr.* 118:103278. doi: 10.1016/j.autcon.2020.103278

Krebs (2014). *Target Hackers Broke in Via HVAC Company*. Washington, DC: KrebsOnSecurity.Com.

Malche, T., and Maheshwary, P. (2017). "Internet of Things (IoT) for building smart home system," in *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017*, Palladam, 65–70. doi: 10.1109/I-SMAC.2017.8058258

Mantha, B., and García de Soto, B. (2019). "Cyber security challenges and vulnerability assessment in the construction industry," in *Proceedings of the Seventh Creative Construction Conference*, eds M. J. Skibniewski and M. Hajdu (Budapest: Budapest University of Technology and Economics), 9. doi: 10.3311/CCC2019-005

Mantha, B. R., García de Soto, B., and Karri, R. (2021). Cyber security threat modeling in the AEC industry: an example for the commissioning of the built environment. *Sustain. Cities Soc.* 66:102682. doi: 10.1016/j.scs.2020.102682

Mantha, B., Jung, Y., and García de Soto, B. (2020). "Implementation of the common vulnerability scoring system to assess the cyber vulnerability in construction projects," in *Proceedings of the Creative Construction E-Conference 2020*, eds M. J. Skibniewski and M. Hajdu (Abu Dhabi: New York University Abu Dhabi), 117–124. doi: 10.3311/CCC2020-030

Manucaster, P. (2020). *Maze Ransomware Hits Law Firms and French Giant Bouygues*. Richmond, VA: Infosecurity Magazine.

Mascarenhas, C., Ferreira, J. J., and Marques, C. (2018). University-industry cooperation: a systematic literature review and research agenda. *Sci. Public Policy* 45, 708–718. doi: 10.1093/SCIPOL/SCY003

Mohamed Shibly, M. U. R., and García de Soto, B. (2020). "Threat modeling in construction: an example of a 3D concrete printing system," in *Proceedings of the 37th International Symposium on Automation and Robotics in Construction (ISARC 2020 Online)*, Kitakyshu.

Motley, C., and Mas, I. P. (2017). *Key Issues for Lawyers as Cyber Risk Leaders*. Chicago, IL: American Bar Association Forum on Construction Law.

Muscat, I. (2019). *Cyber Threats, Vulnerabilities, and Risks*. Austin, TX: Acunetix.

Mutis, I., and Paramashivam, A. (2019). "Cybersecurity management framework for a cloud-based BIM model," in *Advances in Informatics and Computing in Civil and Construction Engineering*, (Berlin: Springer International Publishing), 325–333. doi: 10.1007/978-3-030-00220-6_39

Neff, M. W., and Corley, E. A. (2009). 35 years and 160,000 articles: a bibliometric exploration of the evolution of ecology. *Scientometrics* 80, 657–682. doi: 10.1007/s11192-008-2099-3

Nie, B., and Sun, S. (2017). Using text mining techniques to identify research trends: a case study of design research. *Appl. Sci.* 7:401. doi: 10.3390/app7040401

NIST (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. Gaithersburg, MD, National Institute of Standards and Technology.

NVD (2020). *National Vulnerability Database (NVD).* NIST Information Technology Laboratory. Available online at: https://nvd.nist.gov/vuln (accessed April, 2021).

NYDFS (2017). *Cybersecurity Filing*. Albany, NY: Department of Financial Services.

Oh, K. Y., and Lee, M. J. (2017). Research trend analysis of geospatial information in South Korea using text-mining technology. *J. Sens.* 2017:2765256. doi: 10.1155/2017/2765256

Ozturk, G. B. (2020). Interoperability in building information modeling for AECO/FM industry. *Autom. Constr.* 113:103122. doi: 10.1016/j.autcon.2020.103122

Pan, Z., Hariri, S., and Pacheco, J. (2019). Context aware intrusion detection for building automation systems. *Comput. Secur.* 85, 181–201. doi: 10.1016/j.cose.2019.04.011

Parn, E. A., and Edwards, D. (2019). Cyber threats confronting the digital built environment: common data environment vulnerabilities and block chain deterrence. *Eng. Constr. Archit. Manag.* 26, 245–266. doi: 10.1108/ECAM-03-2018-0101

Pärn, E. A., and García de Soto, B. (2020). "Cyber threats and actors confronting the construction 4.0," in *Construction 4.0*, eds A. Sawhney, M. Riley, and J. Irizarry (Oxfordshire: Routledge), 441–459. doi: 10.1201/9780429398100-22

Pash, C. (2018). *How Hackers and Spies Tried to Steal the Secrets of Australia's One-Armed Robot Bricklayer*. New York, NY: Business Insider.

Ponemon Institute and Accenture Securuty (2019). *Ninth Annual Cost Of Cybercrime Study Unlocking The Value Of Improved Cybersecurity Protection The Cost Of Cybercrime Contents*. New York, NY: Accenture Securuty.

Rezaeian, M., Montazeri, H., and Loonen, R. C. G. M. (2017). Science foresight using life-cycle analysis, text mining and clustering: a case study on natural ventilation. *Technol. Forecast. Soc. Change* 118, 270–280. doi: 10.1016/j.techfore.2017.02.027

Sainaghi, R., Köseoglu, M. A., d'Angella, F., and Mehraliyev, F. (2020). Sharing economy: a co-citation analysis. *Curr. Issues Tour.* 23, 929–937. doi: 10.1080/13683500.2019.1588233

Sawyer, T., and Rubenstone, J. (2019). *Construction Cybercrime is on the Rise*. Manhattan, NY: Engineering News-Record.

Sheikh, A., Kamuni, V., Patil, A., Wagh, S., and Singh, N. (2019). "Cyber attack and fault identification of HVAC system in building management systems," in *Proceedins of the 2019 9th International Conference on Power and Energy Systems, ICPES*, Perth.

Shemov, G., García de Soto, B., and Alkhzaimi, H. (2020). Blockchain applied to the construction supply chain: a case study with threat model. *Front. Eng. Manag.* 7, 564–577. doi: 10.1007/s42524-020-0129-x

Shu, X., Tian, K., Ciambrone, A., and Yao, D. (2017). *Breaking the Target: An Analysis of Target Data Breach and Lessons Learned*. Ithaca, NY: Cornell University. http://arxiv.org/abs/1701.04940

Song, J., Zhang, H., and Dong, W. (2016). A review of emerging trends in global PPP research: analysis and visualization. *Scientometrics* 107, 1111–1147. doi: 10.1007/s11192-016-1918-1

TAG (2020). *Threat, Vulnerability, Risk – Commonly Mixed Up Terms*. Rotorua: Independent Security Consultants.

Tang, S., Shelden, D. R., Eastman, C. M., Pishdad-Bozorgi, P., and Gao, X. (2019). A review of building information modeling (BIM) and the internet of things (IoT) devices integration: present status and future trends. *Autom. Constr.* 101, 127–139. doi: 10.1016/j.autcon.2019.01.020

Van Eck, N. J., and Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics* 84, 523–538. doi: 10.1007/s11192-009-0146-3

Van Eck, N. J., and Waltman, L. (2020). *VOSviewer Manual*. In Leiden: Univeristeit Leiden, p. 53.

VOSviewer (2020). *VOSviewer, version 1.6.15*. Leiden University, [software]. Available online at: https://www.vosviewer.com/download (accessed February, 2020).

Wang, H., Pan, Y., and Luo, X. (2019). Integration of BIM and GIS in sustainable built environment: a review and bibliometric analysis. *Autom. Constr.* 103, 41–52. doi: 10.1016/j.autcon.2019.03.005

Warrington, J. (2020). *Interserve Hit by Cyber Attack as Hackers Target Hospital Construction Firms?*. London: CityAM.

Watson, S. (2018). *Cyber-Security: What Will it Take for Construction to Act?*. London: Construction News.

Zhang, K., and Liao, P. C. (2015). Ontology of ground source heat pump. *Renewable Sustainable Energy Rev.* 49, 51–59. doi: 10.1016/j.rser.2015.04.021

Zhao, X. (2017). A scientometric review of global BIM research: analysis and visualization. *Autom. Constr.* 80, 37–47. doi: 10.1016/j.autcon.2017.04.002

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.