EPiC Series in Built Environment

Volume 3, 2022, Pages 643–651

ASC2022. 58th Annual Associated Schools of Construction International Conference

Pragmatic Development of a Cybersecurity Module for Construction Education

Kenneth S. Sands II, Ph.D.
Florida Gulf Coast University
Ft. Myers, FL

Min Jae Suh
Sam Houston State University
Huntsville, Tx

Technology use has significantly increased in the construction industry. The industry creates large amounts of confidential, sensitive, or proprietary information which is susceptible to unauthorized access by cybercriminals and access to network infrastructure can create havoc on construction companies. Construction students must apply electronic-based technology to manage the construction process, but based on various cyber incidents, construction students should also understand their responsibility regarding cybersecurity when working with the various technology. The problem is that it is already difficult to incorporate new content in an already tight construction curriculum and there is no academic literature that provides guidance on how to teach this type of topic. Therefore, the purpose of this paper is to provide the course development process undertaken to develop a module on cybersecurity for construction. Using this framework in combination with a three-phase framework, the authors have outlined the assumptions about the learner and society; the aims and objectives; content or subject matter with its selection, scope and sequence; modes of transaction; and evaluation methods for the module. The authors expect that this module will be used by educators to further cybersecurity instruction which will hopefully mitigate cybersecurity incidences in the construction industry.

Key Words: Cybersecurity, Cyber-risk, Construction, Education, Construction 4.0

Introduction & Background

The use of technology in construction, "offers the potential for revolutionary change in the effectiveness with which construction related activities are executed and the value they add to construction industry stakeholders" (Gallaher et al., 2004, p. iii) and opportunities offered by emerging technology for the construction industry should be fully exploited (Froese, 2010; Sands, Fiori, & Suh 2018). What was once known as a low-tech industry or "one that has been slow to adopt process and technology innovations" (Agarwal, Chandrasekaran & Sridhar, 2016) has in large part evolved into a highly digitalized, automated, and technologically capable industry. The industry is shifting toward Construction 4.0 which is the movement toward digitization and having connected systems at every stage in the lifecycle of a construction project (Mantha & Garcia de Soto, 2019).

This shift toward more digitization improves workflows throughout a construction company's operations.

The construction industry tends to create large amounts of highly confidential, sensitive, or proprietary information (Mantha & Garcia de Soto, 2019). There are a variety of sensitive data housed and exchanged within company databases which may include, design documents or other highly sensitive project data types. Also, data in company databases may include bidding strategies that is essential to a company's competitive advantage and other organizational information such as employees' social security numbers, home addresses and/or medical information. There are vast amounts of data that are at risk and organizations need to understand the inherent risk of working in a new digital world, especially when considering that globally, the average cost of a data breach can cost a company $3.9 million according to the Ponemon Institute (2019).

Information exchange is a key process in the construction industry and according to Blakley, McDermott & Geer (2001), securing the information we exchange is important in proportion to an organization's dependence on information technology. Information and other advanced construction technologies are becoming heavily reliant on digital environments and operating in digital environments make industries prone to technological risk such as cyberattacks (Li et al., 2017; Liu et al., 2017; Mantha & Garcia de Soto, 2019). As the construction industry gets more involved with advanced technology, the more susceptible it will become. According to the senior director of IT at Warfel Construction (with 230 employees and $235 million in revenue), the construction industry is unprepared to face such cyber-attacks (Sawyer & Rubenstone, 2019). Adding to this, according to Welsh (2018), of the 2,800+ construction professionals surveyed, roughly 14% of survey participants indicate that they or their companies have experienced a cyber-attack. This number may in fact be higher as an M-Trends report conducted by Mandiant Consulting (2019) which provides annual data on the industries targeted by cybercriminals often found that in 2019, 4% of all cyberattacks were on the construction and engineering industries and as the industry engages in more connected technology, that number is sure to rise.

Direct Impact on the Industry

There are a variety of examples of cyberattacks on the construction industry, many of which are not publicly shared as victims decline to share any details about the incident (Sawyer & Rubenstone, 2019). One such incident discussed by Sawyer and Rubenstone (2019) includes how Brothers Construction of Willoughby, Ohio had not received payment of $1.7 million from St. Ambrose Roman Catholic Church (owner). The owner had been paying; however, at some point as transactions were being made, a hacker was able to access the email system of the owner and change routing numbers for wire transfer payments so in essence, the $1.7 million disappeared. Sawyer and Rubenstone (2019) also recounts how Turner Construction Co. in 2016 had sensitive data stolen due to cybercrime.

O'Connor (2016) highlights multiple cyber-incidents related to the construction industry. A major U.S retailer known as the 'Target Corporation', had credit cards and personal data of approximately 110 million customers exposed. The breach occurred due to stolen credentials obtained by cybercriminals from Fazio Mechanical Services, an HVAC contractor. The attack appears to have been the result of a malware-embedded email phishing attack sent to employees of the contractor. Another case described by O'Connor includes the theft of plans of an Australian secret intelligence center being stolen while

the center was still under construction and it was reported to increase the time of the project while increasing the cost of the project by $132.6 million. Additionally, O'Connor points out how AECOM had current and former employee records stolen due to hackers. In addition to these examples of external cyber-incidents, it has been reported that cyber-risks also involve employees (current and former) and external contractors working on project sites. Also, a recent incident described by Medina (2019) highlights how a 'scammer' took $640,000 after sending an invoice directing payment to a fraudulent bank account that was meant for a contractor.

In addition to risk associated with information and cybersecurity, digitally connected equipment and device security poses another major threat to the construction industry. Rubenstone (2019) discusses a Trend Micro research study which highlights the vulnerability of digitally connected equipment such as cranes, to being 'hacked' or accessed without authorization. There were 17 brands of wireless controllers associated with crane operations at sites in the U.S., Europe and China that were susceptible to attacks, which included one called a replay attack to get cranes to perform actions that it has done before.

Significance of Cybersecurity Education for Construction Students

According to the American Council for Construction Education (ACCE, 2020, p.13), construction students must be able to "apply electronic-based technology to manage the construction process." Understanding that there is a growing trend toward the use of technology in construction, educational program who wish to be accredited needs to provide electronic-based technology instruction to their students; however, there's no specific requirement to educate students on the risks that use of technological innovation pose to their future employers. As educators, we have a duty to provide students with knowledge that will help them to be as efficient and as innovative as possible through the use of various technologies, but we must equip students with the tools that will allow them to be as safe as possible in their professional environments. It can be physical safety or virtually to protect themselves and their companies from cyber threats.

Educators can support students not only understand the nature of cyber threats, but they can also provide education that will improve their cyber security habits. According to McCrohan, Engel, & Harvey (2010), it was concluded that when users were educated on cyber threats and were trained about proper security practices, their behavior could be changed to enhance online security for themselves and the firms where they are employed.

Problem

Construction Students & Cybersecurity Issues

To get an understanding of undergraduate student competency with regard to cybersecurity in construction, the authors surveyed 56 junior and senior undergraduate construction students. The survey indicates that only 28% of students were aware of the dangers of information security using construction technology and 79% of students pointed out the need of training for cyber-security for construction technologies.

In addition to this initial investigation, two students who have worked for construction companies through their cooperative education program have reported that they and their companies have personally experienced a significant cyber-attack. The attacks were described as 'ransomware attacks' where a cybercriminal was able to take control over their IT systems and demand a ransom of a certain amount of Bitcoin in order to return control to the organization. A few students are already experiencing the significant impact of cybersecurity in construction.

Construction Curriculum

With the advent of the connected construction company, it is important that every construction professional using electronically connected devices has education on cybersecurity and cyber risk and construction education should be part of this effort; however, barriers to adopt and teach cybersecurity education may include squeezing another topic in an already constrained curriculum to a resistant faculty (Sinha et al. 2007; Sands, Fiori, & Suh, 2018). Also, there is very limited literature that provides guidance on how and what to teach construction students topics on cybersecurity.

Purpose

The purpose of this paper is to provide insight into how the authors have used the systematic course development framework (Mager and Beach, 1967; Ahn et al., 2009) and Graves' (1996) framework of course development processes in addition to Eash's (1991) curriculum components to develop an introductory cybersecurity module for construction students.

Curriculum Development in Construction Education

A review of ASC proceedings; in addition to electronic databases, provides insight to curriculum development in construction. Research with regard to development of curriculum elements is not a new concept in construction education. Ahn et al. (2009) focused on the systematic course development process for building a course in sustainable construction for construction students. Ahn, Cho, and Lee (2013) discusses how the systematic course development process was used for the creation of a BIM course suitable for construction and engineering students. Mostly related to this particular research is Sands, Suh and Fiori (2018) which focuses on the re-development of an IT for construction course. Review of this research guided this process and have led the authors to adopt the frameworks described and used within.

Approach to Teaching Cybersecurity

The authors suggest a modular approach to educate students about several issues related to cybersecurity in construction. It allows for content to be incorporated into any relevant construction course, such as a building information modeling (BIM) course, project management course, a construction business management course (for risk control) or a stand-alone IT for Construction course. To develop this module, the authors operationalize Eash's (1991) curriculum components as the conceptual framework for the module development which include: (a) framework of assumptions about the learner and society; (b) aims and objectives; (c) content or subject matter with its selection, scope and sequence; (d) modes of transaction, for example, methodology and learning environments; and (e) evaluation.

Additionally, the systematic course development framework focuses on three phases; preparation, development, and improvement (Mager & Beach, 1967; Ahn et al., 2009) while Graves' (1996) framework focuses on the elements of; needs assessment, course objectives, conceptualizing and organizing content, materials, and activities, evaluation techniques, and understanding available resources and constraints. Combining these frameworks allows to fully define and refine the module.

Phase I: Preparation

Needs assessment

During the preparation phase, the authors performed a needs assessment. First, external requirements were assessed. Guidance and insight were provided from professional organizations, advisors, industry councils, literature, and seminars/webinars to understand the necessary competencies of our students.

Assumptions about the learner

Assumptions about the learner should be made. The authors assumed that students will be involved in the construction industry upon graduation and they will be exposed to environments that use electronically connected technology. In addition to this assumption, it is assumed that these students do not have any significant knowledge regarding the impact of cybersecurity issues in the construction industry as evidenced by the initial survey completed.

Phase II: Development

Assessment of resources and constraints

The authors assessed the resources and constraints to the development and incorporation of a cybersecurity module. The major resource necessary to prepare the module is a significant amount of time to compile the resources into an appropriate lesson plan. Access to various professional and educational literature/articles are also a significant resource needed. The ability to download videos from online resources is also useful as a resource. A significant constraint of this module is determining where to place this module in the curriculum. For this case, an IT for construction class was observed to be the easiest way to integrate this content into the construction curriculum.

Content or subject matter and activities

The content for the module is based on a 2-hour 40-minute class session and is separated into seven topics (see Table 1.). The lesson plan is based on a slide presentation with integrated videos, cases and activities. The module begins with an introduction to cybersecurity and a brief discussion on the impact of cyber incidents on the construction related industry. Further discussion gives students a broad overview of cybersecurity and then begins to move into construction specific topics pertaining to items of 'Construction 4.0,' the internet of things (IoT), and electronically connected devices. A significant case study is reviewed and discussed. The means of prevention and reaction to a cyber issue is discussed as well and a phishing email activity is done to complete the session as it is a significant means of unauthorized access into network infrastructure by cybercriminals (see Figure 1.).

Table 1

Organization of Content Coverage for a 3-hour module

#	Topic	Significance	Resource
1	Introduction to Cybersecurity	What is cybersecurity? Noting that Construction/Engineering is the 5th most targeted industry by cybercriminals in 2019	M-Trends (2020)
2	What are we protecting?	Sensitive employee data Sensitive client data Network and infrastructural access	Goodman (2020)
3	Who are we protecting from?	White Hat vs. Black Hat Hackers	Caldwell (2011) Norton (2017)
4	Relevance to construction	Cyber risk and the industry. Radio Frequency (RF) Controllers and Hacking of Cranes	Constructible (2018) ENR (2019) Brewster (2019)
5	Case Study Review	Target & Fazio Mechanical	Krebs on Security (2014)
6	Protecting Your Company	Cyber Liability Policy Training & Education	Risk & Insurance (2018) Beyer & Brummel (2015) DHG (2016)
7	Phishing Email Activity	Identify Phishing Attack Risk	See Table 1.

Activity. Figure 1. provides a screenshot of an activity used to help students understand how to identify a spear-phishing email based on various identifiable features (Yahoo, 2020).

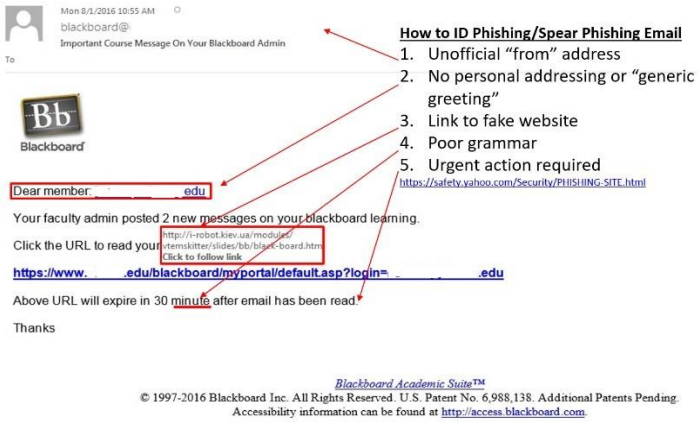

Figure 1. Student activity: review of phishing email

Modes of Transaction

The authors suggest using the structure outlined in Table 1. as a module in a construction course. The module can and has been offered in two modalities, via live face-to-face instruction and via an asynchronous online environment. In both cases, an electronic learning management system (LMS) is used and all content are made electronically available to student.

Evaluation

The authors suggest incorporating test questions pertaining to the module into an existing evaluation technique that would allow for integration into established course to observe if objectives of this course module were met. Additionally, a mini quiz with spear-phishing email activities may also be useful.

Phase III: Improvement

There is always a need to continue improving any courses, particularly with regard to a technology-based module. As iterations of the course are offered, new case studies have been added due to new cyber-attacks on construction organizations. In addition to this, new resources/sources of information and online video contents have been incorporated into the module.

Conclusion

Construction students must be able to apply electronic-based technology to manage the construction process (ACCE, 2020) and the industry is moving toward the use of more technology and electronically online devices. With this and further advancements of Construction 4.0, the construction industry is becoming more susceptible to cybersecurity risk and students need to understand the risks and the means of preventing and/or preparing for cybersecurity threats. The problem is that there is limited guidance from academic literature or otherwise as to how educators are to teach cybersecurity to construction students.

Through the use of the course development process in conjunction with the framework for course development processes, the authors have presented a pedagogical strategy for teaching cybersecurity to construction students as a module that can be incorporated into a technology-based construction course. The content covers the broad topic of cybersecurity and then moves toward a more specific review of the impact of cybersecurity in construction, the cases that support this review and ways to protect organizations from cybersecurity incidences. The module ends with a spear-phishing email activity that will give students the fundamental skills of being able to recognize an email of this nature. Therefore, this module will serve as a resource to construction educators to support them with teaching the important topic of cybersecurity in their construction classes. In the future, the authors hope to investigate construction programs that incorporate cybersecurity teaching in their curriculum in hopes to collaboratively improve on the module.

References

Ahn, Y. H., Cho, C. S., & Lee, N. (2013). Building information modeling: Systematic course development for undergraduate construction students. *Journal of professional issues in engineering education and practice*, *139*(4), 290-300.

Ahn, Y. H., Kwon, H., Pearce, A. R., and Wells, J. G. (2009). The systematic course development process: Building a course in sustainable construction for students in the U.S.A. *Journal of Green Building*, 4(1), 169-182.

American Council for Construction Education (ACCE) (2020). Standards and criteria for the accreditation of bachelor's degree construction education programs. Retrieved from https://683b8d30-e51d49ba9440a5669f44051b.usrfiles.com/ugd/683b8d_92a40873c33d4413a776063e873f52a.pdf

Agarwal, R., Chandrasekaran, S. and Sridhar, M., (2016). Imagining construction's digital future. McKinsey Productivity Sciences Center. Retrieved from https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/imagining-constructions-digital-future

Beyer, R. E., & Brummel, B. J. (2015). Implementing effective cyber security training for end users of computer networks. *SHRM-SIOP Science of HR Series: Promoting Evidence-Based HR*.

Brewster, T. (2019). Crane hacking pt. 1 [Video]. YouTube. https://www.youtube.com/watch?v=k8F7glmbCNg&feature=youtu.be

Caldwell, T. (2011). Ethical hackers: putting on the white hat. *Network Security*, *2011*(7), 10-13.

Constructible (2018). Cybersecurity in construction, what you need to know. Retrieved from https://constructible.trimble.com/construction-industry/cybersecurity-in-construction-what-you-need-to-know.

DHG (2016). A cybersecurity risk in the construction industry. Retrieved from http://www.dhg.com/Portals/0/ResourceMedia/publications/Construction_Cybersecurity_DHG-Views.pdf

Eash, M.J. (1991) *Curriculum components.* The international encyclopedia of curriculum (pp. 67-69). Elmsford, NY: Pergamon Press, 1991.

Engineering News Record (ENR) (2019). Construction cybercrime is on the rise. Retrieved from https://www.enr.com/articles/46832-construction-cybercrime-is-on-the-rise

Froese, T. M. (2010). The impact of emerging information technology on project management for construction. Automation in construction, 19(5), 531-538.

Gallaher, M. P., O'Connor, A. C., Dettbarn, J. L., and Gilday, L. T. (2004). Cost analysis of inadequate interoperability in the U.S. capital facilities industry. Retrieved from http://www.fire.nist.gov/bfrlpubs/build04/PDF/b04022.pdf

Goodman, J. (2020). Cybersecurity expert: All construction data is an asset and should be protected. Retrieved from https://www.constructiondive.com/news/cybersecurity-expert-all-construction-data-is-an-asset-and-should-be-prot/573037/

Graves, K. (1996). *Teachers as course developers*. Cambridge University Press, Cambridge.

Krebs on security (2014). Target hackers broke in via HVAC company. Retrieved from https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Mager, R.F. and Beach, K. M. (1967). *Developing Vocational Instruction*, Fearon Publishers, Palo Alto, CA.

Mantha, B.R. and Garcia de Soto, B. (2019). Cyber security challenges and vulnerability assessment in the construction industry. *Proceedings of the Creative Construction Conference*, Jun. 29 – Jul. 2 2019, Budapest, Hungary

Mandiant Services (2020). M-Trends 2020. Retrieved from https://content.fireeye.com/m-trends/rpt-m-trends-2020

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of internet Commerce*, *9*(1), 23-41.

Norton (2017). What is the difference between black, white and grey hat hackers? Retrieved from https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html

Ponemon Institute (2019) Cost of a Data Breach Report 2019. Retrieved from https://databreachcalculator.mybluemix.net/

Risk & Insurance (2018). The case for cyber coverage in the construction industry. Retrieved from https://riskandinsurance.com/case-cyber-coverage-construction-industry/

Sands, K.S., Fiori, C.M. and Suh, M.J., (2018) Beyond BIM: The Evolution of an IT for Construction Course. *Proceedings of the Construction Research Congress 2018*, 54-64.

Sinha, S. K., Thomas, H. R., and Kulka, J. R. (2007). "Integrating ethics into the engineered construction curriculum." *Journal of Professional Issues in Engineering Education and Practice*, 133(4), 291-299.

Sawyer, T. and Rubenstone, J. (2019) Construction cybercrime is on the rise. Enginereing News Record. Retrieved from https://www.enr.com/articles/46832-construction-cybercrime-is-on-the-rise

Yahoo (2020). How can I identify a phishing website or email? Retrieved from https://safety.yahoo.com/Security/PHISHING-SITE.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAADpJElzVBcpp0Iu_9YpHJ1zXy0xkc38K7W8yGImBQCP16dCNMvo6GjSgcDkk1SrCpqIJqtiCHLx18xnXHOSlwku_0YnEMyAlXiSZ7Zna-srvyfLKJa4qzBZhyGIVKzeya-tpqKEJI--Ph5U88L8HC7TC2ZjU9eNwcV6SKyTETcW6