NAC Executive Insights

Cybersecurity in Engineering and Construction

Key Points

- Attacks on the engineering and construction industry are growing as are the impacts of the attacks.
- Internal attacks may be considered to be direct attacks originating from an employee, a trusted security vendor, or an IT hosting or services supplier.
- External attacks may be considered to be indirect attacks originating upstream from the company or project environment or from any of the connected sources from which data of connected signals originates.
- External attacks may originate from the client, suppliers, or connected subcontractors.
- The paths of attack and the ability to protect and defend them will vary depending on the primary attack point.
- The scope of an attack is a function of whether the specific system component attacked results in an expansive or cascading attack beyond the initial point of vulnerability.
- First order impacts can be related to the targets of the attack in the first instance, while second order attacks are associated with the forward transmission of either the effects or actual malware.
- A range of potential defensive strategies and tactics may be viewed from an open systems perspective.
- Recommendations herein represent both initial steps and directional activities that can be undertaken to improve the cybersecurity within the industry.

Introduction

This Executive Insight looks at the cybersecurity landscape facing engineering and construction and is intended to provide a framework for discussion and action by engineering and construction leaders. This Insight will suggest paths that can lead to an improved cybersecurity environment in what is becoming an increasingly connected and networked industry (Construction 4.0). One of the key focus areas relates to the ability to quantitatively measure and understand the vulnerability of industry participants (owner, engineer, contractor, and supply chain) and the projects they undertake together.

Context for Concerns

In order to frame the discussion and considerations that follow it is important to frame the context for industry concerns. Succinctly, cyberattacks on the industry have been growing as have the impacts of the attacks. Many of these attacks go unreported to protect reputations. Table 1 provides a sampling of some of the attacks experienced within the engineering and construction industry.

Table 1 **Table of Attacks**
Stolen design files of Australian intelligence HQ
Proprietary information of robotic bricklayer
Operational facility attack through HVAC vendor-compromised customer information
1.5 TB of sensitive data stolen from Singaporean engineering firm related to NASA, air carrier, and governments
Major U.S. construction company theft of personnel data
Changed routing numbers in email for payment instructions to contractor
Energy infrastructure compromise of internet facing web server, resulting in systematic removal of all corporate data
Theft of 60 GB of data from leading Canadian construction company
Construction company cyberattack provided pathway to two dozen utility-critical control networks
U.S. construction company personnel data used to file false tax returns and healthcare claims
Concrete supply company W-2 tax information used for false returns
Supply chain provider control system accessed by malware, causing improper shutdown and physical damage to the plant
Multinational manufacturer of construction materials lost approximately €250 million in sales and €80 million in operating income as a result of nearly one month of downtime following an attack
Multinational engineering company suffered a breach of approximately 52,000 employees' names, addresses, social security numbers, and personal bank account information

Construction is experiencing more confirmed phishing attacks than any other sector; phishing attacks increased by 250 percent last year.

- ***eSentire*** **"Second Quarter Threat Intelligence," 2018, and *ENR* FutureTech Conference, 2019**

In this Executive Insight, we will refer to vulnerability, which is defined as "a weakness that can be exploited by an attacker to perform unauthorized actions." Quantifying these vulnerabilities will be essential to prioritizing and judging the effectiveness of mitigation measures and solutions.

Sources of Attack

Sources of attacks relate to the ability to exploit vulnerabilities and the defensive strategies and measures deployed. For simplicity, the sources can be viewed as either internal or external.

Internal attacks may be considered to be direct attacks originating from an employee, a trusted security vendor, or an IT hosting or services supplier. External attacks may be considered to be indirect attacks originating upstream from the company or project environment or from any of the connected sources from which data (information of connected signals) originates. External attacks could originate from clients, suppliers, or connected subcontractors.

Attack Objectives

There are a broad range of potential objectives a cyberattack may seek to accomplish. This range of objectives relates to both the path and target of attack. Some potential attack objectives may include:

- Ransom/blackmail
- Denial of service/punishment
- Destruction/theft of intellectual property
- Destruction/theft of physical property or financial assets
- Pathway to downstream system

These objectives are not ranked in terms of vulnerability. Depending on their context, they can result in extreme outcomes including potential loss of life.

Attack Pathways

Potential attack pathways need to consider and characterize both the potential access vectors and the requirements for user interaction. Access vectors consider the proximity required of the attacker in order to exploit a vulnerability. Proximity includes both physical (physically present or locally present, for example, through a malicious link that has been opened) and connectivity (local sub-network; internet) proximity.

Some potential pathways may include:

- Insider threat
- External link (direct or embedded) (email, text, video platform, social media)
- Malware (from malicious link; from corrupted trusted link)
- External system sharing the same server or common software or data (for example, a badge reader system connected to an HR database that also drives other information systems)
- Interjection into routine data flows (impersonation; client communication; banking information)

The paths of attack and the ability to protect and defend them will vary depending on the primary attack point. Considered here are attacks on:

- Corporation (characterized by a semi-permanent network)
- Project (characterized by a temporary/ad hoc/particular network)
- Corporate executives' private emails

Method of Attack

The method of attack relates to the attack complexity required. This in turn will relate to the level of privileges required to effectively exploit a vulnerability. An example would include who has access to what data in the Common Data Environment (CDE).

Some common methods of attack include:

- Routine process (regular updating of password or timesheet submission; accounts payable/receivable; banking transactions)
- Exceptional process (your password is corrupted, please update; confirm your work location or beneficiaries)
- Embedded in external email or frequently visited site
- Forced access to system (direct; through interconnected system)

Target of Attack

The target of a cyberattack will require different privilege levels depending on the selected target. Depending on system design and operation, these may be more or less than other potential targets. Potential targets in the engineering and construction industry may be considered in two different ways. The first potential targets are the "end-state" targets. The second are the targets (information) to be attacked.

"End-state" targets may include:

- Employee
- Company
- Project
- Client and the constructed facility during its operating phase
- Smart network solutions (for example, a "Smart City")

Information targets may include:

- Data corruption/ modification tool corruption (performance of analytical tool/calculation)
- Design object (Building Information Modeling - BIM object) modification (dimensions, specifications, notes)
- Component/ system set points or concept of operations
- Plant operating system software
- Smart network solution algorithms or control logic

Table 2 highlights some potential target data types.

Table 2 Potential Target Data Types	
Corporate	**Project**
Modification of bank account numbers	Modification of structural member sizing or specification
Creation of a vendor/employee and payments to them	Modification of purchase order quantities, items of supply, or delivery schedule
Unauthorized modification of standard company designs/specifications	Changed construction installation notes
Calculation tool algorithms or data sets	Removal of safety related information
Standard control logic programs	Changed set points for equipment
Artificial intelligence (AI) training and/or test data	Modified specifications for lubricants, fills, and filters
	Insertion of malware into plant operating system software
	Malware in connected site system for broader future access (drones, cameras, construction robots)

Impact of Attack (First and Second Order)

The scope of an attack is a function of whether the specific system component attacked results in an expansive or a cascading attack beyond the initial point of vulnerability. This type of impact results from a high degree of interconnectedness in the engineering/construction system, including unseen couplings within the project's complexity.

First order impacts can be thought of as those related to the targets of the attack in the first instance, while second order attacks are associated with the forward transmission of either the effects or actual malware.

Impacts of an attack include:

- Denial of service/inability to operate.
- Loss of data or data integrity (unknown errors/ changes/ modifications) with unknown or uncertain impacts.
- Deliberate modification of operating information of company including financial records.
- Theft of funds or intellectual property (IP).
- Deliberate modification of design-related data, causing errors or omissions in developed calculations, specifications, and designs.
- Corruption or manipulation of AI training and/or testing data to create misinterpretations or otherwise introduce bias into AI algorithms.

- Systemic modification/corruption of BIM models used for construction or critical point modification of BIM elements to create failure on erection or latent risks.
- Modification of controls logic and/or programs to adversely impact component and/or system operation, including potential catastrophic behavior (such as information to be included in Enterprise Asset Management systems).
- Falsification of quality, testing, inspection, or validation and verification (V&V) data and records.

Attacks may directly impact initial delivery of a capital asset (first order) or create latent defects, including nascent malicious code that will affect subsequent facility operation (second order).

Defensive Strategies and Tactics

A range of potential defensive strategies and tactics exist and may be viewed from an open systems perspective as including:

- Education
- Vulnerability measurement (for prioritization and risk treatment)
- Avoid/prevent
- Transfer
- Mitigate — Defense in depth
    - Security/barriers/two-factor authentication
    - Augmented automated checking/AI-enabled pattern recognition
    - Independent V&V and assignment of Single Value of the Truth (SVT) (utilizing Blockchain technology)
- Audit of systems/processes/outputs
- System security stress test

Recommendations

The recommendations that follow represent both initial steps and directional activities that can be undertaken to improve the cybersecurity within the engineering and construction industry.

These recommendations map to some of the defensive strategies and tactics laid out in the prior section. NAC does not have a direct and enabling role with respect to a number of these strategies, but can aid in raising industry awareness and fostering stronger foundations.

Education. Industry leaders should educate participants about cybersecurity risks[1] and encourage the development of training courses related to industry cybersecurity, such as the following:

- Cybersecurity in engineering organizations
- Cybersecurity during the engineering process

[1] Research shows that 55 percent of construction firms do not take the proper computer security measures until after there is a breach.

- Cybersecurity in a project environment (engineering, procurement, construction, startup, and commissioning)
- Cybersecurity over a facility's life cycle
- Cybersecurity in Smart network solutions

This Insight suggests some of the considerations to be addressed in each of these training courses. These courses could be developed to include modules suitable for use by academia and/or trade schools. They also could be made available to meet professional development hour (PDH) requirements for licensure.

Vulnerability Measurement. A range of vulnerability measurement tools exist with different strengths and weaknesses. The challenges of the engineering and construction environment creates special needs because of the growing emphasis on interconnectedness (Construction 4.0) and the temporary, specific nature of the projects undertaken. Some industry vulnerability protocols are shown in Table 3 (next page). Because of the customized nature of networks in engineering and construction, focus should be placed on education and actions related to vulnerability assessment utilizing the Common Vulnerability Scoring System (CVSS). Industry-wide problems will require industry-wide solutions.

Table 3 Vulnerability Scoring Systems	
Scoring System	**Primary Use**
CERT/CC[2] (Computer Emergency Response Team)	Assess whether internet infrastructure is at risk. Assess preconditions to exploit vulnerability.
System Administration, Networking and Security (SANS)[3] Vulnerability Analysis Scale	Assess weakness in default configurations or client server systems.
Microsoft™ proprietary scoring system[4]	Assess difficulty of exploitation and overall impact of vulnerability.
Common Vulnerability Scoring System (CVSS)[5]	Assess principal characteristics of a vulnerability and yield severity score.

CVSS "is actively used by many organizations, including the United States (U.S.) federal government systems and the National Institute of Standards and Technology (NIST). The U.S. federal government uses this to rate the severity of vulnerabilities within their systems. The NIST National Vulnerability Database (NVD) provides a comprehensive database of CVSS vulnerability scores validated by the U.S. government. These scores enable organizations to understand and rank the impact of the vulnerabilities of individual subsystems and participant's level. CVSS is also one of the six vulnerability management standards that comprise the Security Content Automation Protocol (SCAP). SCAP is a method to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., Federal Information Security Act[6] (FISMA) compliance.[7])."

CVSS can be applied to different participants in the engineering and construction system.

[2] US-CERT, "CERT Vulnerability Notes Database," CERT/CC Vulnerability Notes Database, 2006 (https://kb.cert.org/vuls/bypublished/desc/)
[3] S. Cima, "SANS Institute Information Security Reading Room – Vulnerability Assessment," SANS Institute, 2001. (https://www.sans.org/reading-room/whiteExecutive Insights/basics/vulnerability-assessment-421
[4] Microsoft, "Security Update Severity Rating System," Microsoft Security Response Center Security Bulletin Severity Rating System, 2007 (https://www.microsoft.com/en-us/msrc/security-update-severity-rating-system)
[5] "Common Vulnerability Scoring System version 3.1: Specification Document," 2019 (https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf)
[6] The act recognizes the importance of information security to the economic and national security interests of the United States
[7] Mantha, Bharadwaj & Jung, Yeojin & García de Soto, Borja. (2020). Implementation of the Common Vulnerability Scoring System to Assess the Cyber Vulnerability in Construction Projects

Avoid/Prevent. Corporate participants in engineering should be required to meet identified minimum CVSS scores and whether those scores should be included in the NIST National Vulnerability Database (NVD).

Transfer. The industry should consider a roundtable of industry insurers and engineering and construction firms to ensure consistent approach to required cyber insurance and coverage (form of policy)[8].

Mitigate. A performance-based standard focused on AI-enabled checking of designs and specifications to detect potential cyber manipulation or latent cyber risks is needed. Standards related to validation and verification (V&V) should include considerations related to cybersecurity.

Audit. Industry leaders should encourage development of an engineering audit standard that includes consideration of the full range of cyber risks.

References

Mantha, Bharadwaj & Jung, Yeojin & García de Soto, Borja. (2020). *Implementation of the Common Vulnerability Scoring System to Assess the Cyber Vulnerability in Construction Projects*.

US-CERT, "CERT Vulnerability Notes Database," CERT/CC Vulnerability Notes Database, 2006. (https://kb.cert.org/vuls/bypublished/desc/)

S. Cima, "SANS Institute Information Security Reading Room – Vulnerability Assessment," SANS Institute, 2001. (https://www.sans.org/reading-room/whiteExecutive Insights/basics/vulnerability-assessment-421)

Microsoft, "Security Update Severity Rating System," Microsoft Security Response Center Security Bulletin Severity Rating System, 2007. (https://www.microsoft.com/en-us/msrc/security-update-severity-rating-system)

"Common Vulnerability Scoring System version 3.1: Specification Document," 2019. (https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf)

Prieto, R., VERIFICATION & VALIDATION OF PROJECT MANAGEMENT AI; *PM World Journal*, Volume VIII, Issue 10, November 2019.

About the Author

Bob Prieto was elected to the National Academy of Construction in 2011. He is a senior executive who is effective in shaping and executing business strategy and a recognized leader within the infrastructure, engineering, and construction industries.

[8] Only about 15 percent of U.S. construction companies have cyber insurance.

Although the author and NAC have made every effort to ensure accuracy and completeness of the advice or information presented within, NAC and the authors assume no responsibility for any errors, inaccuracies, omissions or inconsistencies it may contain, or for any results obtained from the use of this information*. The information is provided on an "as is" basis with no guarantees of completeness, accuracy, usefulness or timeliness, and without any warranties of any kind whatsoever, express or implied. Reliance on any information provided by NAC or the authors is solely at your own risk.*