Cybersecurity Risks of Collaboration in the Construction Industry

By: Scott Lyon and Kathryn Richter, Sedgwick LLP

With Gartner predicting that IoT devices will top 20 billion by 2020, we become increasingly immersed in the IoT; we find our smart homes and smart cities populated with connected devices and sensors collecting, analyzing, storing and sharing our data, in the name of improved performance, reduced cost and risk, and enhanced safety. This increased functionality also comes at a cost — for example, as convenient as it may be to have Amazon’s Alexa at our digital beck and call, we also recognize that “she” may be eavesdropping on our “private” lives in our homes and workplaces. However, the tension between utility through connectivity on the one hand and privacy and security on the other is by no means a recent phenomenon — it has existed in commercial and heavy industry for decades, where Supervisory Control and Data Acquisition (SCADA) software and Industrial Control Systems (ICS) and similar software products have been utilized in industrial automation for monitoring and controlling equipment. However, attacks on these Operational Technology (OT) systems are on the rise, with Siemens and the Ponemon Institute reporting that 68 percent of oil and gas companies have suffered a digital attack, which can have potentially devastating consequences for the economy and national security, according to Dr. Larry Ponemon, chairman and founder of Ponemon Institute.

Just as OT systems are utilized in energy, utilities management and numerous commercial and industrial uses, construction projects are increasingly utilizing these technologies for remote monitoring, data analytics, and building information modeling (BIM). While increased reliance on these collaborative and device-driven technologies may increase competitive advantage, it also increases vulnerability to cyber risks and liabilities if not considered and addressed from the outset. This is especially true in the government contracting field — following the very public hacks of the OPM, FBI, DHS and IRS in 2015 and 2016, the DoD, GSA, NASA and DHS have all moved toward higher levels of government contractor security and, effective January 19, 2017, privacy training. If an organization intends to embrace these types of collaborative technologies, it must first assess its own security policies and procedures, and identify the compliance baselines necessary to remain competitive.

Architects, Engineers and Contractors Beware

With the goal of reducing building project risk in the AEC (Architect, Engineer and Contractor) industry, we have seen the collaborative use of digital information for building projects used widely to accomplish many goals, from integrated design to reduced costs in time, claims and dollars. Additional benefits of collaboration can include improved project safety, fewer design and construction errors, and perhaps environmental improvements through collaborative selection of sustainable products. In the same vein, SCADA and ICS systems are used in public and private sector organizations to manage and monitor operational aspects of critical infrastructure, i.e., HVAC systems in large commercial, industrial, healthcare and government complexes; waste water treatment facilities; transportation systems; oil and gas operations; and virtually all manufacturing facilities. The software and data collected/stored is used to manage and improve operations, and reduce cost through connected solutions that capture, manage, report, monitor, measure and share data with the enterprise (and/or vendors, regulators or other stakeholders) not only in real time, but with historical data and trends. However, with this increased interconnectivity and access to critical data — whether in the private or public sector — comes the risk of security breach and resulting loss of non-public data, which can be harmful not only for the organization, but also the community and economy as a whole.

Architects, engineers and contractors are not unique as targets for cyberattacks; however, as an industry sector, they have been slow to prioritize cybersecurity while simultaneously adopting many of these new connected technologies, thereby rendering them more vulnerable to attack. Because the AEC industry has increasingly shared access to information related to critical infrastructure, the industry is increasingly subject to cyberattack by those seeking to access and exfiltrate data, hold hostage critical infrastructure information or disrupt operations. For AEC companies working on government or infrastructure projects, insiders, competitors or foreign governments may seek access to the company’s network to obtain proprietary information or trade secrets, for competitive advantage, information warfare, extortion/ransom, protest, financial gain or revenge. Collecting inside information on suppliers, vendors and customers, and their business plans can be extremely valuable. Foreign hackers may be financially motivated, but may
also be associated with suspected political and terror-related objectives, such as gathering intelligence from
government contractors and/or plans and specifications for targeted government facilities. Verizon’s latest Data
Breach Investigations Report (DBIR, 2016) indicates that 90 percent of cyber-espionage breaches capture trade
secrets or proprietary information.iii

Some of the most prevalent forms of cyberattacks in the AEC industry involve spear phishing and ransomware.
According to a blog by security firm Wombat Security, 91 percent of cyberattacks begin with a spear phishing email,ix
where an attacker has tailored his/her attack to specifically target the company, often impersonating a key employee or known associate
(“spoofing”) in the email in order to trick the recipient into opening a malware-infected attachment or visiting a malicious website. The
FBI also reports a steep rise in ransomware attacks in 2016x where intruders attach malware that encrypts critical data
on affected systems, holding the data “hostage” until the victim pays the ransom to recover the encryption key. AEC
companies are susceptible to these attacks because holding plans, specifications and other key electronic records
hostage for an extended period of time can result in missed deadlines, breached contracts and a general paralysis of
the project.

2017 Privacy and Security Requirements in Government Contracting

As noted above, in the government contracting sector there has been increasing focus on securing private information
held by government agencies, following a series of highly publicized breaches of government networks. Recently, a
final rule issued by the DoD, GSA and NASA amended the Federal Acquisition Regulation (FAR) to require that
(federal government) contractors, whose employees have access to a system of records or handle personally
identifiable information, complete privacy training, effective January 19, 2017. xi The rule incorporates the Office of
Management and Budget’s (OMB) definitions of key terms, and provide(s) guidance to contractors regarding the
requirement to complete training that addresses the protection of privacy in accordance with the Privacy Act of 1974,
5 U.S.C. 552a, as amended, and the handling and safeguarding of “personally identifiable information” (PII). The rule
defines “personally identifiable information” as information that can be used to distinguish or trace an individual’s identity, either
alone or when combined with other information that is linked or linkable to a specific individual. The rule requires privacy training
compliance for contractors who have employees who:

1. Handle PII;
2. Have access to a system of records; or
3. Design, develop, maintain or operate a system of records

Contractors must train employees before employees handle PII or have access to a system of records, providing both
initial training and annual privacy training updates. The rule requires contractors to maintain training records and
provide evidence to the government that relevant employees completed the required training, if requested.
Significantly, the rule requires flow down to all applicable subcontracts.

There has also been government activity specifically seeking to secure critical infrastructure and protect it from the
vulnerabilities in our shared resources and the IoT. DHS defines 16 critical infrastructure sectors,xii whose assets, systems,
and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a
debilitating effect on security, national economic security, national public health or safety, or any combination thereof and establishes two
centers: one for physical infrastructure and one for cyber. Architects, engineers and contractors touch every one of
these sectors through design, engineering, procurement, construction, maintenance and operations, and may fall
within the class of “critical infrastructure owners and operators” defined in Presidential Policy Directive 21 (PPD-21),
Critical Infrastructure Security and Resilience. xiii Also in January, 2017 the Department of Homeland Security (DHS),
proposed rules to amend the Homeland Security Acquisition Regulation (HSAR), that would expand privacy and
security requirements for contractors, and protect controlled unclassified information (CUI). DHS is also proposing
to require contractors to complete training that addresses the protection of privacy, in accordance with the Privacy
Act of 1974, and the handling and safeguarding of PII and Sensitive Personally Identifiable Information (SPII).xiv

Mitigate Risk Through Implementation of a Robust Cybersecurity Program
Whether evaluating regulatory compliance or the risk of cyberattack (recognizing that no company is immune to attack), the best approach is to create a robust, enterprise-wide plan through the following approach, preferably with the assistance and guidance of experienced information security professionals.

1. **Assess** — Review the types of data (paper and digital) the company collects and stores (as well as where it is stored), identify the purpose for which the data is collected and what immediate value is gained through its collection and storage, and determine what risks are presented by its continued storage versus destruction.

2. **Prevent** — Identify necessary security controls (administrative, technical, physical) and security measures (encryption, firewalls, etc.) that will allow the organization to best defend against, mitigate and recover from a cyberattack, as well as establish regulatory and contractual compliance requirements. One such security control involves “accountability” — identifying an individual or group within the organization that will be responsible for prioritizing the security and privacy policy internally.

3. **Train and Test** — Employees often present an organization’s the greatest vulnerability. Accordingly, it is vital that they be trained on the importance of strong passwords, password protection and the risk of sharing credentials, as well as how to identify potential cyberattacks and what to do in the event of an attack (i.e. how to execute the organization’s incident response plan).

4. **Detect Intrusion** — As of 2015, an attacker will be present in a victim’s network for an average of 146 days before being discovered.\(^{1}\) Accordingly, it is important for organizations to be proactive in “hunting” attackers in their environment, expanding information security resources to more quickly identify and isolate potential threats. This can be accomplished through a combination of host-based and network-based solutions, but there is no replacement for engaging experienced and properly trained security professionals.

5. **Respond** — In order for an organization to quickly and efficiently respond to a potential security incident, it is imperative to have prepared an incidence response plan (IRP) tailored to the organization’s structure and capabilities. An effective IRP will not only describe the process for identifying, reporting and responding to potential security threats, but will also identify specific stakeholders (insurance, legal, law enforcement, public relations) who can be called in to respond to a cyber event.

**Conclusion**

As connectivity through collaborative technologies and shared risk models enhance functionality while increasing vulnerability and potential exposure to the construction industry, increased contractual and regulatory requirements add new levels of complexity to compliance. Further, as cybercriminals recognize that architects, engineers and contractors are not robustly prepared, the risk of cyberattacks escalates both for the AEC industry and for the many sectors of our critical infrastructure that it touches. Recognizing that no organization can be fully protected from mistakes or unknown security vulnerabilities, planning and preparation are the keys to an organization’s cybersecurity defense, requiring collaboration with key vendors who can assist. Organizations should ensure that adequate internal controls are in place and employees are not only trained to recognize and respond to threats, but also regularly tested to measure the organization’s security maturity and continually improve its processes and controls.

**Kathryn N. Richter, Partner, San Francisco, is a certified mediator with deep experience in construction, real estate and other commercial disputes. Scott T. Lyon, Partner, Orange County, focuses his practice on technology, cybersecurity and data privacy. Both Kathryn and Scott work for Sedgwick LLP. For their complete article, visit UCON Magazine’s webpage at unitedcontractors.org/media-center/ucon-magazine. Visit sedgwicklaw.com, or contact Kathryn at kathryn.richter@sedgwicklaw.com, (415) 781-7900; or Scott at scott.lyon@sedgwicklaw.com, (949) 852-8200.**

\(^{1}\) [http://www.gartner.com/newsroom/id/3598917](http://www.gartner.com/newsroom/id/3598917)
The Internet of Things (IoT) is the network of physical objects or “things” embedded with electronics, software, sensors and network connectivity, which enables these objects to collect and exchange data.


The State of Cybersecurity in the Oil & Gas Industry: United States


The DoD, GSA, and NASA [have issued] a final rule amending the Federal Acquisition Regulation (FAR) to require that contractors, whose employees have access to a system of records or handle personally identifiable information, complete privacy training. https://www.federalregister.gov/documents/2016/12/20/2016-30213/federal-acquisition-regulation-privacy-training

Critical Infrastructure is defined as those assets essential to the economy and society to function that we all depend upon


DHS, Critical Infrastructure Sectors:
1. Chemical Sector
2. Commercial Facilities Sector
3. Communications Sector
4. Critical Manufacturing Sector
5. Dams Sector
6. Defense Industrial Base Sector
7. Emergency Services Sector
8. Energy Sector
9. Financial Services Sector
10. Food and Agriculture Sector
11. Government Facilities Sector
12. Healthcare and Public Health Sector
13. Information Technology Sector
14. Nuclear Reactors, Materials, and Waste Sector
15. Transportation Systems Sector
16. Water and Wastewater Systems Sector


Mandiant Consulting M-Trends 2016 Report

No locale, industry or organization is bulletproof when it comes to the compromise of data. Verizon DBIR, 2016
The Australian Broadcasting Corp. reported that Chinese hackers accessed the computers of a “prime contractor” to steal floor plans, communications cable layouts, server locations and security system designs for the Australian Secret Intelligence Organization’s new headquarters, which was still under construction. Security experts feared the leak compromised the building’s physical and network security.


The PhishMe Q1 2016 Malware Review found that 92 percent of recorded all phishing emails contained a strain of cryptoransomware. By the Q3 2016 report, this figure had grown to over 97 percent.

Technology research firm Vanson Bourne pegs the average financial impact of a successful spear phishing attack at $1.6 million.

Six Tips for Staying Safe from Phishing:

1. Avoid replying to suspicious emails or engaging with senders
2. Open the site yourself — don’t click on embedded links or media
3. Look out for pretexts laced with a sense of urgency or threat
4. Verify requests and information with out-of-band communication
5. Check your browser to ensure Anti-Phishing services are enabled
6. Use a password manager; don’t use the same password across multiple sites

https://www.wombatsecurity.com/about/news/evolution-phishing