FMI

Industry Focus. Powerful Results.™

Information Security in Engineering and Construction: The Big Blind Spot

by Jay Snyder, Gaylynn Fassler and Alyssa Menard

The last thing any engineering and construction company wants is for all its data to be stolen due to a lack of understanding by employees or mismanaged network settings.

Over the last few years, many engineering and construction (E&C) firms have started to invest in new technologies that improve efficiency, productivity and safety. This increased use of technology is long overdue, and although it has been a slow process, there are now many new technology applications that are proving to be vital for the industry. Today, project managers can use mobile phone or tablet applications to update project information, report incidents and monitor sites in real time[1] —and all while digital tools and interconnected devices using IoT are streamlining the flow of information for all project stakeholders. While technology applications for E&C will continue to improve, it's important to note that the increased use of technology doesn't come without risk. As E&C companies begin to embrace technology more broadly, they also need to learn about and adopt information security.

Information security is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction to provide confidentiality, integrity and availability."[2] Ask any information security professional and he or she will say that a data or network breach is not a matter of "if," but rather a matter of "when." Corporate data breaches amounted to a total loss of $61 million in 2017,[3] and there seems to be a new major data breach every other month. Such breaches can represent a significant cost to companies, including potential litigation and government fines. Recent research shows that 29% of businesses that face a data breach end up losing revenue, and among those, 38% experience a loss of over 20% in revenue.[4] Not only that, companies that don't protect their systems (and their customer data) can lose their customers' confidence, loyalty and support, leading to a loss of business over time.

E&C companies are prime targets for data breaches because not only do they have their own project data to protect (e.g., building plans, bids and customer data), but also they must guard their employees' sensitive information. The increased use of connected devices on construction sites and within companies can also create vulnerabilities; any device that's connected to the internet can fall victim to a cyberattack at any time. Moreover, 33% of crimeware incidents across all business sectors occur within the E&C industry, according to Verizon's 2018 Data Breach Investigations Report.[5] According to Forrester, more than three-quarters of engineering, construction and infrastructure firms reported a cyber incident during the prior 12 months. More than half (60%) of attacks on construction firms are aimed at small businesses, which are easy targets.[6]

In 2013 Target made headlines when it suffered a data breach that compromised at least 40 million records, including credit card numbers. Attackers gained access to Target's internal systems after stealing login credentials from an HVAC contractor that had remote access to the servers. The point-of-sale systems were also compromised in the attack.

Outlining and enforcing an information security strategy can be intimidating and overwhelming, and often falls by the wayside. However, pretending an incident can't or won't happen to an organization is not an effective strategy. In 93% of successful data breaches, the amount of time to successfully breach a company is less than one minute; yet, for more

---

[1] Kendall Jones. "How Technology is Improving Construction Site Safety." ConstructConnect. April 26, 2017.

[2] "Small Business Information/Cybersecurity Workshop." National Institute of Standards and Technology. U.S. Department of Commerce.

[3] "2017 Internet Crime Report." FBI. Internet Crime Complaint Center.

[4] "Data Security Breach: 5 Consequences for Your Business." The AME Group. 2018.

[5] "2018 Data Breach Investigations Report." Verizon. 2018.

[6] "The Case for Cyber Coverage in the Construction Industry." Allied World. Risk and Insurance. 2018.

than 75% of companies, it takes weeks or even months to realize the breach has occurred.[7] Recent figures estimate that nearly 50,000 websites are compromised every single day.[8] The risks associated with information security continue to grow for E&C firms using construction technology both on- and off-site. Due to the growing emphasis on effective security strategies, we've identified three approaches that—when combined effectively—can set the foundation for a solid information security program: security awareness training, risk management and incident response.

> According to HUB International, "the construction industry lags behind others when investing in high-level security and keeping up with current threats, and hackers are well aware and take advantage."

Building Awareness and Educating Employees

Good information security starts with educated employees. Just as construction sites must be secured against unauthorized personnel, data also needs to be secured; employees are the first line of defense. In fact, workers need to be aware of how they should (and shouldn't) use technology. According to IBM's data breach study, nearly half of all data breaches are caused by human error and system glitches, suggesting that employee training is critical to companies' information security protocols.[9] For example, many people see free Wi-Fi as an excellent perk. However, there are numerous free tools that allow people to watch network traffic over open Wi-Fi networks, where any unencrypted data is "visible." While this practice is technically illegal, the law seldom deters motivated criminals.

Educating employees on the more common technology-oriented risks can help prevent major incidents. Because most people don't know how their technology use can negatively impact their organizations, security awareness training is a fundamental first step.

Questions to consider:

- Have you communicated and set priorities with management to encourage employees to integrate security practices every day?
- How have you defined appropriate and consistent behaviors and actions for the organization's security culture?
- Have you established a training program to keep employees motivated throughout the year? (Start by organizing small groups and by covering simple and easy to understand topics with these groups.)

[7] Melissa Stevens. "28 Data Breach Statistics That Will Inspire You (To Protect Yourself)." BitSight. June 14, 2016.

[8] John Stevens. "Internet Stats & Facts for 2018." Hosting Facts. July 10, 2018.

[9] "2018 Cost of a Data Breach Study: Global Overview." IBM and Ponemon Institute LLC. July 2018.

Learning and Protecting Your Blind Spots

Think it's safe? A Las Vegas casino once had its high-roller database stolen through a connected thermometer in a fish tank.

Risk management, or the understanding of your technology, its vulnerabilities and the devices that need to be secured, should be the second area of focus in an information security strategy. But it can be difficult to protect what you don't know you have. Having a risk management strategy means keeping a close eye on all the organization's devices and being aware of the vulnerabilities each device exposes. For example, every organization has servers that store company, employee and client information. Even if these servers are in the cloud, understanding the intricacies of your data storage system and how to properly protect that data is extremely important. A vulnerable server could lead to a major data breach. And while protecting servers should be a priority for any organization (as they contain high-value data), these pieces of equipment are just one small piece of the larger security puzzle.

Companies should also consider the devices or "endpoints" that connect to their networks. Devices include servers, desktops, laptops, tablets and smartphones. While these increase productivity and accessibility, devices can also increase the potential for a data breach. Some E&C firms have lost or fallen victim to theft of equipment with sensitive information and have been exposed to email-based phishing scams, virus/worm infestations, data deletions, ransomware attack and data breaches. These incidences resulted in the loss of customer and/or employee data, intellectual property, and research and design or trade secrets. Between 2016 and 2017, cyberattacks on construction firms increased by 13%, and in 2017, 83% of E&C firms reported some type of fraud.[10]

When companies don't use proper security strategies, the "connected" nature of today's technology tools can let a hacker access an entire network or system via a stolen phone or lost tablet. And while every single device can't be fortressed 24/7, most firms fail to implement the proper training to prepare a cyber-savvy workforce to avoid these types of breaches.

But that doesn't mean companies don't know that they could become targets of cybercrimes. In a 2017 cyber risk survey, 85% of U.S. employers rated cybersecurity as a top priority for their companies.[11]

The Kroll study[12] found that:

- 83% of E&C firms reported some type of fraud incident.
- 93% reported a cyber incident.
- 67% reported some other type of security incident.

With this severity of fraud and security breaches within the E&C industry, identifying the risks to your organization and preparing a strategy to handle these incidents as they occur are both vital. The most common types of information security breaches include information theft, loss or attack, physical theft or loss of intellectual property and regulatory/compliance breaches. By staying up-to-date on the potential threats, your organization will be better-equipped to handle these incidents as they occur.

---

[10] "Global Fraud & Risk Report: Forging New Paths in Times of Uncertainty." 10th Annual Edition – 2017/18. Kroll. 2018.

[11] "The Future of Financial Services: How Work is Impacted by the Connection and Convergence of People and Technology." Willis Towers Watson. 2017.

[12] Global Fraud & Risk Report: Forging New Paths in Times of Uncertainty." 10th Annual Edition – 2017/18. Kroll. 2018.

To prepare for the "when" (not the "if") of an information security breach, focus on improving your firm's overall cybersecurity processes by:

- Using antivirus, encryption and malware protection on all devices that are connected to your servers, such as desktops, laptops and mobile devices (i.e., phones, tablets, wearables, etc.).
- Identifying and understanding the benefits and limitations of the technical controls that your organization uses to protect your information (i.e., network monitoring, firewalls, updates and patching).
- Considering vulnerable areas like access to Wi-Fi through home and remote workers, suppliers and contractors, staff turnover, mobile devices and any other weaknesses in your network (28% of breaches are perpetrated by insiders).[13]
- Implementing staff training that's centered on safe practices and procedures regarding the protection of your organization's secure information (17% of breaches occur through human errors).[14]
- Creating formal processes for addressing breaches as they occur (and for after the breach has been identified and mitigated).

Once the security risks have been identified and mitigated to the best of an organization's ability, the next step is to develop an incident response strategy, which is another critical aspect of managing risk.[15]

Preparing for the Worst-Case Scenario

Incident response is the third security component in protecting your company from information security risks and includes methods for responding to both cyber and real-world incidents. An incident can refer to a data breach, hacking attempt on a network or even a lost device. Incident response is also vital for network security, where knowing how to respond can limit the negative effect of a breach on your organization and help recover systems more efficiently.

---

[13] "2018 Data Breach Investigations Report." Verizon. 2018.

[14] Ibid.

[15] "Small Business Information/Cybersecurity Workshop." National Institute of Standards and Technology. U.S. Department of Commerce.

COMMON CYBERATTACKS

PHISHING

Phishing emails appear to come from a legitimate institution, such as a bank, usually saying you need to update information or solve an issue. The email will include a link that takes you to a malicious website that seems legitimate, but entering your username and password on that site compromises your bank account.

If you receive such an email, do not click any links, but rather go to the institution's website in the browser yourself.

SPAM

Spam emails include links that will download malware onto your machine. They often include misspellings but may seem legitimate.

Don't open emails from senders you do not know. If you do open the email, don't click on the link in the email.

SOCIAL ENGINEERING

Social engineers use sensitive information such as birthdates, hometowns and mother's maiden name to access online accounts, like banking accounts.

Be careful with the information that you share online, and never give out personal information via email to people you don't know.

RANSOMWARE

Ransomware rewrites system files to lock users out of their devices. The malware will demand payment to "give" the device back. They will often threaten to delete data and information off the system if payment is not given promptly.

Ensure that antivirus software is updated on all devices, routers and firewalls are patched, and systems are backed up elsewhere to create restore points.

When formulating an incident response plan, start with a previously designed formal procedure. For example, if a project manager loses his or her tablet, there should be a formal response to mitigate the risks associated with losing that device (e.g., reporting the lost device to the proper personnel, wiping the device so data cannot be accessed by an unknown party, and retrieving the device's data). This way, the data is both secured and accessible. Now, let's say a computer within your organization suddenly starts sending huge amounts of data to an unknown receiver.

A prepared incident response team would handle this breach by:

1. Removing the computer from the network immediately to stop the data flow.
2. Analyzing the computer and network for the exposed or vulnerable data.
3. Determining how the incident occurred in the first place.
4. Determining whether there is malware on the device and, if so, taking measures to remove it.
5. Ensuring that the incident has been limited and resolved efficiently.

Today the average cost of an information security breach in the U.S. is $7.91 million, and the average number of exposed records is 31,465.[16] Effective response to an incident (which includes reporting the incident to authorities and clients) could make or a break a company. Severe security breaches can compromise an organization's customer base, partnering organizations and insurance costs, just to name a few.

According to IBM's data breach study, factors that may reduce the impact and cost of a security breach include:

- Having a prepared incident response team in place
- Using encryption on all devices
- Conducting employee training
- Organizing threat sharing among team members
- Getting the board involved
- Using security analytics
- Appointing a CPO and a CISO
- Using a data classification schema
- Getting proper insurance protection for your secure information

Factors that can increase the cost of a security breach are:

- Third-party involvement
- Cloud migration
- Compliance failures
- Lost or stolen devices
- Provision of ID protection
- Use of mobile devices (especially important for E&C firms)

[16] "2018 Cost of a Data Breach Study: Global Overview." IBM and Ponemon Institute LLC. July 2018.

Companies that develop and implement effective security strategies will be better-prepared for the continued adoption of technology in E&C. The last thing any E&C company wants is for its data to be stolen due to a lack of understanding by employees or mismanaged network settings. Security awareness training, risk management and incident response are three places to start when developing an informative and thorough information security strategy.

On a final note, understand that—unless it has been designated as such—your in-house IT staff is not your in-house IT security staff. While there is overlap between IT and information security, security is a job of its own. It is not feasible, however, for some businesses to have their own in-house information security staff. Managed IT services can assist in securing your business environment. Consider your company's needs carefully, follow the strategies outlined in this report, and then make the best possible decision for your individual organization.

Jay P. Snyder, MBA, CHC is the technology practice leader with FMI. Jay has been in the engineering and construction industry throughout his entire career. He has industry experience as a construction project executive; corporate director of planning, design and construction for a health care system; founder and managing partner of a risk management tech startup company; and as a valued business consultant. He can be reached via email at ***jsnyder@fminet.com***.

Gaylynn Fassler, MS, serves a key role in the day-to-day operations at FMI. She is passionate about information security education, and works with local organizations on outreach and improvement, while encouraging more professionals to pursue careers in security.

Alyssa Menard is a market research associate with FMI. Alyssa is responsible for conducting primary and secondary research around market trends within the AEC industry and built environment. Her primary objective is to ensure best practices in the collection, management, analysis and interpretation of data for content development within the organization.

FMI

Industry Focus. Powerful Results.™

About FMI

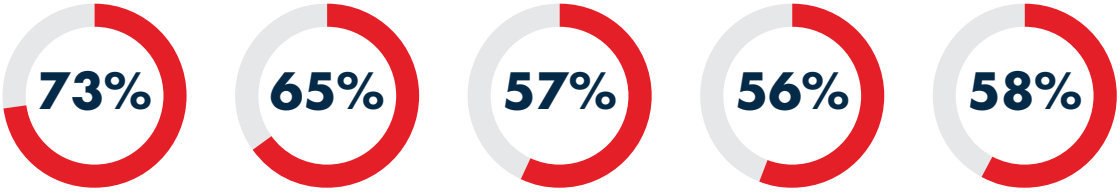
For over 65 years, FMI has been the leading **management consulting and investment banking** firm dedicated exclusively to **engineering and construction, infrastructure and the built environment**.

FMI serves all sectors of the industry as a trusted advisor. More than six decades of context, connections and insights lead to transformational outcomes for our clients and the industry.

Sector Expertise

- A/E and Environmental
- Building Products
- Construction Materials
- General Contractors/CM
- Energy Service & Equipment
- Energy Solutions & Cleantech
- Heavy Civil
- Industrial
- Owners
- Private Equity
- Specialty Trades
- Utility T&D

FMI Client Highlights



of the ENR **Top-400** **LARGEST CONTRACTORS**

of the ENR **Top-200** **SPECIALTY CONTRACTORS**

of the ENR **Top-100** **DESIGN FIRMS**

of the ENR **Top-200** **ENVIRONMENTAL FIRMS**

of the ENR **Top-100** **CM FOR FEE FIRMS**

Denver
210 University Boulevard
Suite 800
Denver, CO 80206
303.377.4740

Edmonton
Edmonton, AB
780.850.2693

Houston
1301 McKinney Street
Suite 2000
Houston, TX 77010
713.936.5400

Phoenix
7639 East Pinnacle Peak Road
Suite 100
Scottsdale, AZ 85255
602.381.8108

Raleigh (headquarters)
223 S. West Street
Suite 1200
Raleigh, NC 27603
919.787.8400

Tampa
308 South Boulevard
Tampa, FL 33606
813.636.1364