The Magazine of the Construction Association of South Florida

CONSTRUCTION ink!

Winter 2017

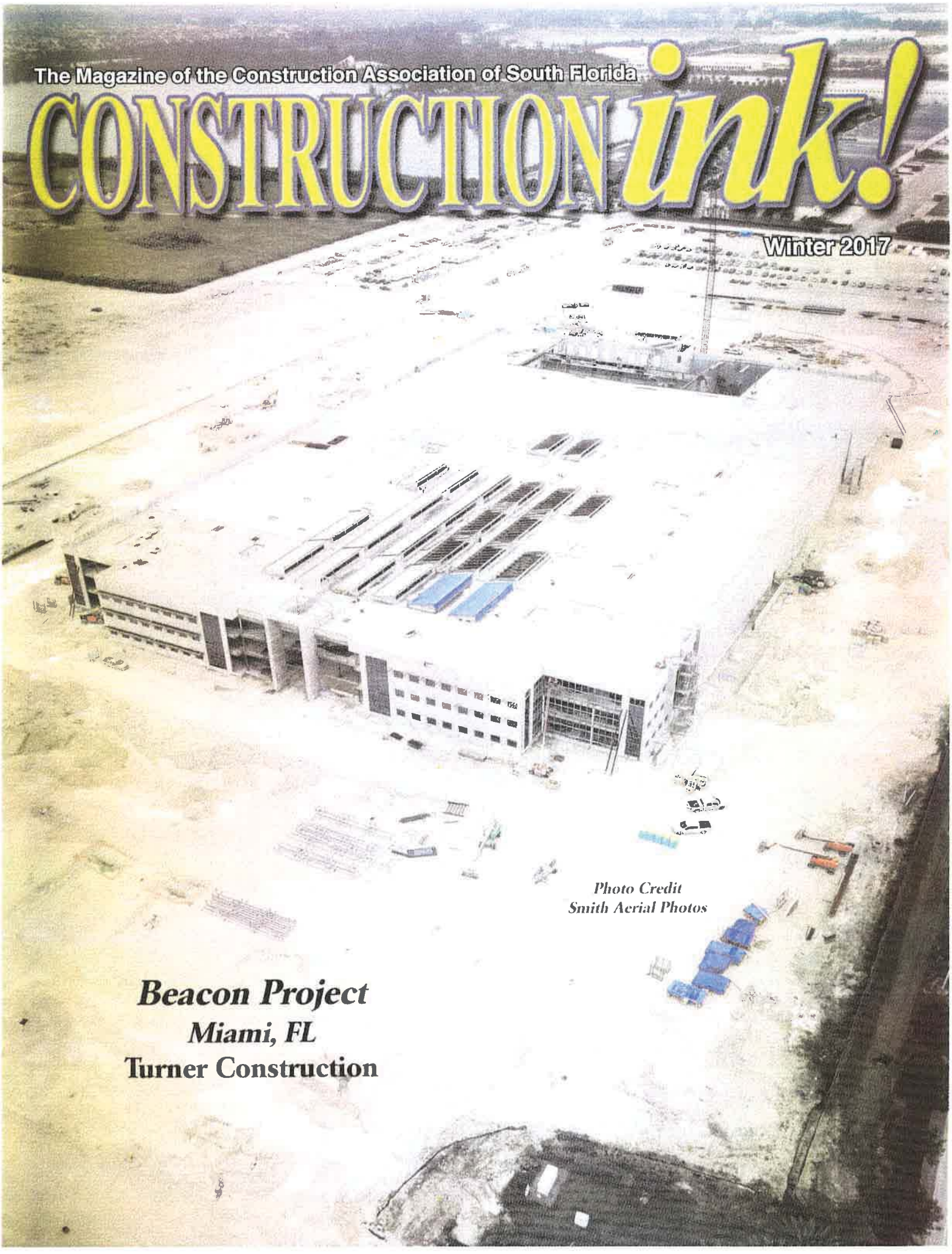

Photo Credit
Smith Aerial Photos

Beacon Project

Miami, FL

Turner Construction

A NEW YEAR'S RESOLUTION FOR YOUR CONSTRUCTION BUSINESS: PRACTICAL GUIDELINES FOR MITIGATING THE RISKS OF A CYBERATTACK

2016 was a remarkable year for many reasons. On the cybersecurity front, there was a marked increase from 2015 in reported cyberattacks and data breaches in the United States and abroad, including several high-profile hacks of large companies and organizations such as Yahoo!, Oracle, and the U.S. Department of Justice.

One notable trend in 2016 was the increase in use of ransomware to hijack a company or an organization's computer systems and the data stored within the systems. In March 2016, MedStar Health Inc. suffered a ransomware cyberattack which shut down the records systems of 10 hospitals in Maryland and Washington, D.C. with hackers demanding 45 Bitcoins (approximately $19,000) to unlock the data. In November 2016, a ransomware attack shut down ticket machines for San Francisco's light rail transit system for a day on one of the busiest shopping weekends of the year, causing the agency to let users ride for free until systems were restored.

Industry experts agree that ransomware has proven to be one of the most effective ways for a hacker to breach a company's computer systems and access sensitive data. Moreover, it appears that hackers are becoming more adept at embedding viruses and Trojan software into innocuous-looking e-mails and e-mail attachments, avoiding tell-tale linguistic errors (recall, for example, the easily detectable Nigerian lottery scam e-mails which were replete with improper spelling and grammar), and creating official-looking web pages as part of their phishing efforts.

Another form of cyberattack that saw an uptick in 2016 is the "business e-mail compromise" attack. In this type of cyberattack, hackers use fake company e-mails or other social engineering methods to assume the identity of the President, CEO, or CFO of the company, or perhaps a trusted business partner of the company, typically requesting a company employee to wire transfer company funds on an emergency or urgent basis. Once the transfer is made, the funds are directed to the hacker's account and are then laundered in order to make the funds untraceable. In April 2016, it was reported that an unnamed American company was defrauded of $98.9 million as a result of a "business e-mail compromise" cyberattack.

More sophisticated hackers using the "business e-mail compromise" attack may research employees who manage the company's finances and attempt to use targeted language specific to the victim or company and a dollar amount which appears reasonable based on the company's size and normal operations. Hackers may also study the impersonated person's travel or vacation schedule, timing the fake e-mail to a period when that person is out of the office. In addition, hackers may preempt the fake e-mail by using malware to infiltrate the company's computer systems in order to gain access to information regarding the company's billing and accounting processes, using this information in the fake e-mail to increase the appearance of legitimacy. As a result, an employee receiving such an e-mail may not be able to readily discern that the e-mail is fake.

2017 should prove no different from 2016 with respect to the need to be increasingly vigilant in defending against cyberattacks. Industry experts predict that several key trends which emerged in 2016 - including the evolution of ransomware as an effective method of cyberattack - are likely to continue in 2017. Notably for the construction industry, some industry experts also predict that small and mid-sized businesses will see a significant increase in cyberattacks.

Any construction company with access to the internet is at risk of a cyberattack. Construction companies are collecting and storing increasing amounts of personal, confidential, and proprietary information, including sensitive financial information and personal information of employees and clients. In addition, with technological advances, data sharing between participants in a construction project has increased in popularity. Given these factors, construction companies could be at increased risk of liability in the event of a data breach.

A cyberattack could result in significant first-party costs to the breached construction company, including costs associated with hardware and electronically stored information, such as IT expenses; data loss and restoration expenses; public relations costs; and extortion/ransomware costs; as well as costs associated with federal and state regulatory compliance, including fines and penalties.

In addition, a cyberattack could result in significant third-party costs to the breached construction company, such as costs arising from third-party claims for privacy breaches, including liability for breach of contract as a result of failure to comply with contractually mandated data security measures and tort liability for negligent failure to protect sensitive information.

All hope is not lost, however. A construction company can follow several practical guidelines to mitigate the risks of a cyberattack and data breach.

First, the construction company should have a qualified party perform an assessment of existing vulnerabilities of its network security systems. There are a number of companies which can provide varying levels of cybersecurity testing, diagnostics, and monitoring. Mark Agulnik, a partner at Marcum LLP and leader of its Southeast IT Risk & Assurance Services Practice Group, recommends an enterprise-wide risk assessment of the company's people, processes, and technology. To the extent feasible, the construction company should then take steps to address its known vulnerabilities.

Second, the construction company should develop, implement, and enforce a formal Written Information Security Program ("WISP") which sets forth a protocol for protecting sensitive information and complying with applicable regulatory requirements.

Like water intruding into a building, hackers most frequently take the path of least resistance. The driver of a successful company is its people but, unfortunately, those same people are often simultaneously the first line of defense and the weak link in the company's computer security systems. This is evidenced by the efficacy of ransomware and phishing attacks. Accordingly, the WISP should reflect a company "culture" of data security and should include employee training with periodic reinforcement, given that poor employee "cyber hygiene" has been the cause of the majority of network breaches.

As explained by Mr. Agulnik, there are several practical guidelines a construction company can follow to reduce the risk of a cyberattack. The construction company should:

- Implement a network security risk assessment at least annually or upon a significant change to the company, e.g., a merger/acquisition or other change in structure.
- Screen potential employees carefully, including a background check, which should reduce the risk of an internal cyberattack by unethical employees.
- Conduct an even more rigorous background check (for potential IT employees since these individuals will receive elevated or administrative network credentials.
- Have tools in place to ensure employees are and remain ethical, including an annual review of the company's data security policy and confirmation by the employee that they understand the policy.
- Require annual training of employees regarding significant cybersecurity events that have occurred and how to avoid falling victim to similar cyberattacks. Training should be tailored to the specific risks of the company. There are several companies, including Marcum LLP, which can provide such courses; in addition, there are interactive online programs available on various cybersecurity issues.
- Pay careful attention to independent contractors or third-party providers who have access to the company's network systems, but are not usually screened or background-checked, and, if possible, include robust data security requirements in their contracts.
- Implement network system controls, including restricted "need to know" employee access to data and dual controls for those who have access to banking processes, i.e., one employee would be authorized to initiate a wire transfer and another would be authorized to release the funds.
- Immediately revoke network access for any terminated employees, in order to reduce the risk of "revenge" cyberattacks.

There are also several practical guidelines a construction company's employees can follow to avoid becoming the victim of a cyberattack. The company's employees should:

- Perform periodic backups of company data, in the event the employee's laptop or other mobile devices contain data not on the company's servers, in order to mitigate the effects of loss of data in the event of a cyberattack.
- Be careful with company laptops and mobile devices - don't leave them unlocked and unattended in public places such as the airport or at a Starbucks.
- Be cautious of using unsecured Wi-Fi networks in public places.
- Ensure that home wireless network systems are secure and password-protected.
- Use strong passwords, e.g., with upper and lower case letters, numbers, and special symbols, which will make it more difficult for a hacker to guess.
- Not visit suspect websites using company computers or mobile devices.
- Be cautious of impersonated e-mail addresses, which may be very similar to legitimate e-mail addresses except for one letter or number, e.g., iam@yourceo.com versus iam@yourrceo.com.
- Not click on attachments from unknown or untrusted sources.
- Be cautious of free, web-based e-mail accounts (e.g., @yahoo.com; @hotmail.com; @gmail.com), which are more susceptible to being hacked.
- Contact the IT department after receiving an e-mail with a suspect link or attachment.
- Not provide personal or financial information in response to unsolicited e-mails without first independently verifying the source and/or checking with the IT department.
- Be cautious when posting employee and financial information to company websites or social media.
- Be cautious of e-mail-only wire transfer requests which are of an emergency, secret, or urgent nature.
- Confirm the identity of the person requesting a wire transfer by contacting that individual via another medium, e.g., telephone. Mark Agulnik also recommends questioning the individual as to the grounds for the requested wire transfer as an added security measure.
- Verify changes in third-party vendor payment locations and confirm requests for transfer of funds via another medium, e.g., telephone.

As noted above, federal and state laws and regulations may also govern how the construction company must prepare for and respond to data breaches.

There are several federal laws which address information privacy and security and which apply to the construction industry. For example, the Federal Acquisition Regulation contains provisions for the safeguarding of contractor information systems that contain nonpublic information provided by or generated for the federal government. The Federal Information Security Modernization Act of 2014 requires federal government contractors to comply with specific information security measures. Construction companies who are or will be working on healthcare projects should be aware of the

Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which includes data privacy and security provisions regarding electronically stored protected health information.

With respect to state laws, as of September 1, 2016, only Alabama, New Mexico, and South Dakota had no security breach laws. The other 47 states and the District of Columbia, as well as Guam, Puerto Rico, and the Virgin Islands, have enacted legislation requiring private, governmental, or educational entities to notify affected individuals of security breaches of personally identifiable information. Thus, the construction company should consult with outside counsel in the states in which it is operating to confirm the requirements of applicable data security laws and regulations.

Third, the construction company should prepare a preemptive Incident Response Plan ("IRP") in order to maximize the effectiveness of the company's response in the event of a cyberattack. It should be noted that a number of states have laws requiring companies to have an Incident Response Plan in place.

An effective IRP will typically include the following components:

- Allocation of a budget for cybersecurity, including costs of cyber insurance if applicable, and for follow-up measures to address specific security issues identified after a cyberattack.
- Involvement of the entire company, since the respondents to a data breach may necessarily include senior management, IT staff, and the company's legal department, among others.
- Identification of key personnel who should be notified when a breach is detected, a timeline for communications, and how information regarding the data breach is communicated internally within the company and externally to potentially affected parties and/or the public and/or regulatory agencies.
- Annual simulation of a phishing attack or data breach so employees understand their responsibilities in the event of an actual cyberattack. Several companies, including Marcum LLP, can conduct planned simulated attacks and assess the company's (and its employees') response thereto.
- Provisions for periodic review and revision of the IRP to reflect new threats or significant changes in company size, structure, or policies.

Fourth, the construction company should work with in-house and outside counsel to manage its contractual risks associated with a cyberattack and data breach. As owners and developers become more keyed into cybersecurity issues, their contracts may require construction companies to implement specific data security measures; provide notice of data breaches within specific time periods; carry cyber insurance; and/or indemnify the owner or developer for costs arising from a data breach. As such, the importance of careful

contract review and negotiation cannot be understated. The construction company should also work with its counsel to include strong hold harmless and indemnity clauses in its downstream contracts with subcontractors, sub-consultants, and third-party vendors who have access to sensitive electronic data.

Finally, the construction company may want to consider purchasing cyber insurance to cover costs of data restoration, business interruption, and extortion/ransomware payments in the event of a cyberattack, and costs of liability to third parties damaged by a data breach. Some industry experts predict that private sector demand for cyber insurance will surge in 2017 as more companies focus on managing the risks of cybersecurity.

Careful review of the cyber insurance policy is critical. The construction company should pay close attention to the 'trigger' for cyber insurance coverage. Since it may be difficult to prove unauthorized use of lost or stolen information, coverage should not depend on proof of actual access to, or misuse of, information. The construction company should also consider retroactive coverage for unknown losses that occurred prior to the policy period, since data breaches may remain undiscovered for several years.

If the construction company is purchasing cyber insurance in connection with a specific project, the cyber insurance should optimally be coordinated in order to cover any potential liability the company assumes under its contract. The cyber insurance policy will likely contain notice provisions which must be followed in the event of a data breach. Further, insurance companies may require specific data security practices of its insureds and require higher premiums - or refuse coverage - for insureds who do not comply. The construction company should ensure it fully understands the scope of coverage afforded under the cyber insurance policy, including any exclusions. For example, if a policy excludes employee-caused losses, damages resulting from an employee's download of malware may not be covered. Therefore, it is important for the construction company to understand its rights and obligations under the cyber insurance policy as well as under its contract for the project.

In sum, it is becoming increasingly important for construction companies to be vigilant in defending against cyberattacks. The practical guidelines noted above could result in real cost savings and reduced exposure to liability in the event of a cyberattack and data breach. Ultimately, inclusion of cybersecurity as part of a construction company's compliance and risk management policies, and a coordinated effort between IT, management, and in-house and outside counsel, are critical to an effective cyber-defense strategy.