Build It, and They Will Come
Data Security for the Construction Industry

ABA 2018 Annual Meeting Forum on Construction Law

Ian T. Ramsey CIPP/US, CFEI
Member, Stites & Harbison PLLC
400 West Market Street, Suite 1800
Louisville, Kentucky 40202
iramsey@stites.com

Unlike the movie Field of Dreams[1], my title is not about standing on the edge of cornfield where the possibility of creating from a dream exists—at least not for you. “They” in this quote are disrupters, criminal organizations, or even competitors fixed on the pursuit of an ideal, making money from internet crimes, or even wanting a business advantage. Because you exist, you must accept that you will have a data breach. I am not encouraging a defeatist attitude. Instead, the goal is to offer some examples showing why the construction industry is not immune from risks, identify such risks, and offer solutions.

I thought the following quote captures how technology has changed the industry: “I got into construction decades ago because you didn’t have to be a rocket scientist, only to find out that now, you have to be a rocket scientist to be in construction.”[2] I like this quote because it presents two divergent opinions at once; the industry is now complex because of technology, and technology can only be understood by a select few. I agree that the traditional paper model of construction is becoming obsolete, but disagree that the effective use of technology is reserved for only rocket scientists. Significant computer science skills are required to design, install, and maintain systems. That same level of skill is not needed by everyone in a company. Instead, a high level of trust and constant communication is the key. It is a marathon, as is said, not a sprint.

The race is much easier when the course is marked. The construction industry has chalk lines, at best, to describe its variability. The United States operates under a sectorial data security environment where rules apply to certain industry sectors. The financial industry has standards set by the Gramm-Leach Bliley Act, Bank Secrecy Act, Fair Credit Reporting Act, and Fair and Accurate Credit Transactions Act, while health care has Health Insurance Portability and

[1] For those not familiar with the film, it was released in 1989 and is about an Iowa corn famer hearing a voice in the sky telling him “build it, he will come,” which he interprets as a command to build a baseball diamond in his fields. He does and the Chicago White Sox eventually come.

[2] James M. Benham, President of JBKnowledge attributes this quote to one of his clients. JBknowledge produces an annual report and good resource titled “Construction Technology Survey” in coordination with the Construction Financial Management Association and Texas A&M’s Department of Construction Science.

Accountability Act of 1996 and Health Information Technology for Economic and Clinical Health Act. Among many, retailers would follow Payment Card Industry Data Security Standards and educators would follow the Family Educational Rights and Privacy Act of 1974.[3]

There are not, for example, federal or state laws that set data security standards to be used for construction projects. There are some guidelines as those who work with federal projects know[4], and the American Institute of Architects has workings drafts covering data management.[5] However, I suspect no construction professional will be celebrating ANSI World Standards Week 2018 this October presented by the American National Standards Institute and the National Institute of Standards and Technology.[6]

Standards after-all are critical to the industry and required at every step to insure projects are completed on time and within budget. Absent standards, the motivation to be data secure is left to fear, which is a powerful motivator and obstacle. Your employees fear having their personal information stolen, while others fear being the employee who accidentally downloads malicious software onto the company's computer system. Those responsible for information security fear they are only being reactive to hackers who are more sophisticated and more persistent. But fear at a certain point stops motivating and instead just creates anxious and distracted employees. Sadly, without training to educate employees to give them the skills to prevent data breaches, the basic human desire to be responsive or to satisfy one’s curiosity is what drives a person to click a dangerous link in an email, ultimately opening the door to a cyber-attack.

Hopefully, you have allocated resources to improve safeguards, implement policies, strengthen email systems and firewalls, and provide security awareness training—all in the name of improving your data security and protecting your valuable and sensitive information.

[3] *See generally* “Information Security and Privacy,” Andrew B. Serwin, published by Thomson Reuters, 2016 Edition.

[4] The Public Buildings Service as part of the Government Services Administration strongly encourages use of electronic project management (ePM) a web-based tool creating a collaborative environment to consolidate planning, design, procurement, and construction system under a sensitive but unclassified compliant secure workspace. *See* http://www.gsa.gov/portal/category/26745 (last visited September 15, 2016).

[5] *See* AIA Docs E201-2007 and E202-2008, effective until April 2017 and replaced thereafter by E203-2013, and G201-2013 effective until April 2017 and replaced thereafter by G202-2013.

[6] https://www.ansi.org. NIST has developed and promotes its cybersecurity framework, which was created through a collaboration between industry and government and consists of standards, guidelines, and practices to promote the protection of critical infrastructure. *See* https://www.nist.gov/cyberframework (last visited September 15, 2016).

I. You Are Not Alone.

Data Breaches for the Construction Industry

Turner Construction Company has 5,200 employees and completes $10 billion of construction on 1,500 projects each year. Turner is a leading world builder with immense resources.[7] Yet, in March of 2016, a single employee was duped by a spearphishing scam[8] when asked to supply names and social security numbers of the company's current employees and former employees, including interns and trade employees, who received a W-2 form from the company for 2015.[9] The official number of affected employees has not been made public, but, to give some perspective, Turner was required to report the breach to the Washington State's Attorney General and that office reported 566 affected Washington State residents.[10]

This was not a complex cybersecurity intrusion. Most likely, it was an email from a senior executive to someone in the human resource or accounting departments saying "I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap."[11] Even though Turner has not disclosed the details, I speak with some certainty, as I have personally seen identical language in emails related to similar scams.

The breach was newsworthy for a few reasons; Turner is a big company and the breach seemed to involve a lot people. The reality is that similar scams have resulted in the disclosure of thousands of employees' confidential information across the United States for numerous companies. I am aware of a few breaches in Kentucky alone which combined exceed Turner's breach.

To give more perspective, at the same time Turner fell victim to the scam, numerous other companies did as well. The scam was so prevalent across the United States that the Attorney General for Connecticut[12], among other attorney

[7] http://www.turnerconstruction.com/about-us (last visited September 15, 2016).

[8] A phishing scam is a general email sent to many users having the appearance of a legitimate sender. The goal is for a user to submit personal information in response to the email. A spearphishing scam is directed at specific individuals and generally involves social engineering. Social engineering is research by criminals done for a company or individuals within a company by reviewing publically available information found on a private or public websites, government filings, or through social accounts like LinkedIn, Facebook, Twitter, Instagram or any similar platforms. Criminals may pose as legitimate professionals or personal contacts by creating fake social profiles or even company websites with the aim towards collecting personal information.

[9] https://nyccbf.com/data-breach-warning-for-past-and-current-employees-of-turner-construction-company/ (last visited September 15, 2016).

[10] http://www.atg.wa.gov/data-breach-notifications (last visited September 15, 2016).

[11] http://krebsonsecurity.com/2016/02/phishers-spoof-ceo-request-w2-forms/ (last visited September 15, 2016).

[12] http://www.nbcconnecticut.com/news/local/State-Warns-Residents-of-W-2-Scam-371671101.html (last visited September 15, 2016).

generals, the F.B.I.[13], and the IRS[14] posted alerts warning companies. The scam was timed to coincide with tax season so the need for the information would not appear unusual. And, significantly, it involved clever spoofing of email senders to appear as though someone within that individual's company was actually making the request. I have actually been in a business meeting with a CEO and CFO and watched the expressions on their faces as an email making a similar request appeared on the CFO's phone. This email appeared to come directly from the CEO sitting a few inches away.

If any fault were to be given, it is that Turner did not stay current with the news and missed an opportunity to alert and train its employees on the scam.

Whiting-Turner Contracting's March 2016 breach was due to a vendor preparing W-2 and other tax forms that were infiltrated by unauthorized users. That breach became known after the vendor reported suspicious activity on its servers and employees began to report fraudulent tax returns being filed under their names. In a letter to the California Attorney General, the company's notification warned of the risk of employees' childrens' information being taken.[15]

Central Concrete Supply Company aka Right Away Redy Mix, Inc., Rock Transport, Inc. reported to the California Attorney General that it fell for the same spearphising email in February 2016 that duped Turner. Here is how they describe the breach to their employees: "[W]e became aware of a data breach by which we believe a third party obtained access to copies of your 2015 W-2 income and tax withholding statements. This information was stolen through a sophisticated social engineering scheme in which an outside party posing as another person convinced an employee of Central Concrete Supply to provide copies of the documents by email…."[16] The list of reported data breaches just for the month of August 2016 in California alone is lengthy and diverse, and some are even familiar by name.[17]

Finally, you should be reminded that the interconnectivity so common in the construction industry is precisely how the Target breach occurred. Fazio Mechanical Services Inc., a small 125 employee company, "got access to login

[13] https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams (last visited September 15, 2016).

[14] https://www.irs.gov/uac/newsroom/irs-alerts-payroll-and-hr-professionals-to-phishing-scheme-involving-w2s (last visited September 15, 2016).

[15] http://oag.ca.gov/ecrime/databreach/reports/sb24-60875 (last visited September 15, 2016).

[16] http://oag.ca.gov/ecrime/databreach/reports/sb24-60270 (last visited September 15, 2016).

[17] Noble House Hotels & Resorts, M Holdings Securities, Inc., Kimpton Hotels & Restaurants Group, LLC, Jerry's Artarama N.C. Inc., Toyota Motor Credit Corporation, County of Sacramento, Dominican Hospital, SCAN Health Plan, Schwan's Home Service, Inc., Symphonix Health, Eddie Bauer, LLC, Newkirk Products, Inc., John E. Gonzalez DDS, Valley Anesthesiology Consultants, Inc. d/b/a Valley Anesthesiology and Pain Consultants, Bon Secours Health System, Inc., HEI Hotels & Resorts, PAX Labs, Inc. NLU Products, LLC, Brian Goldman, MD A Medical Corporation, 7-Eleven, Inc., Multi-Color Corporation, Banner Health, and Disney Consumer Products and Interactive Media (DCPI).

credentials for Target's computer network from Fazio Mechanical."[18] In the official company statement, Fazio said: "Our data connection with Target was exclusively for **electronic billing**, **contract submission**, **and project management**, and Target is the only customer for whom we manage these processes on a remote basis. No other customers have been affected by the breach." [19] (Emphasis added).

A more current breach is PAR Electric Contractors, Inc., which according to its data breach disclosure had back-up tapes stolen. The disclosure suggests the tapes were stolen from a location where PAR stored the back-up tapes and other items. The tapes, unfortunately, contained all of the personal information of every employee within the company, including back account information for those that used direct deposit.[20]

The theme from all of these breaches is that companies in the industry have sensitive employee information wanted by criminals and at the same time are vulnerable to be used as a weak link in their own and their client's data systems.

Solutions

The above examples could likely have been avoided if the involved employees had simply taken the following steps:

- **Validating the sender** by verifying the sender's email address.
- **Not being fooled by graphics** which are often stolen from legitimate websites.
- **Being suspicious and checking all links and attachments** by hovering your cursor over the link.
- **Watching out for threats and warnings** which is a common trick to scare you into quick action.
- **Noticing misspelled words and poor grammar** which often signals a scam or malware.
- **Not being fooled by personal information or details** because a motivated hacker will take the time to collect this information.
- **And, most importantly, verifying the requests** by making telephone calls**.**

The U.S. Department of Homeland Security has declared October as National Cyber Security Awareness Month. Its motto is: "Stop. Think. Connect.™" This motto is simple and condenses important concepts into these short, directive

[18] http://www.wsj.com/articles/SB10001424052702304450904579367391844060778 (last visited September 15, 2016).
[19] http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ (last visited September 15, 2016).
[20] https://oag.ca.gov/ecrime/databreach/reports/sb24-133549

instructions. Most data security problems can be resolved by these simple directives.

Know Your Data. Identify, protect, and limit access to your most secure information, which should include all customer and employee personally identifiable information. Consider compartmentalization by keeping the most sensitive information on separate encrypted servers. Being transparent is important; however, distinguish those who really need access from those who merely want it.

Know Your Plan. A data security plan is just a piece of paper unless you have the right team to update, practice, and implement the plan when a breach occurs. An employee's title might be important to the chain of command, but the ability to solve problems calmly and quickly under pressure is paramount.

Data Security Minimums. Designate an employee to maintain a security program. Anticipate and limit risk by employee training, detection and prevention of system failures, imposing disciplinary measures for violations, preventing access by terminated employees, contractually requiring subcontractors and service providers to maintain security, limiting and controlling physical access, monitoring and reviewing effectiveness, and documenting all responses to incidents.

Email Education. Hackers and social engineers increasingly use "phishing" emails to get into company servers or as the first step towards a more sophisticated intrusion. A recent trend includes encryption malware known as "ransomware" that holds data hostage until a ransom is paid. It might seem obvious, but a recent Pentagon data breach was because of a single employee opening a malware infected email. Training your employees on how to recognize and avoid the bait is a simple yet important piece of your overall data security plan.

Additional security controls to consider:

Security entry requiring ID

Internal locked rooms for servers and equipment

Location specific access and control

Shredding and secure disposal

Passwords, Biometrics

Classification and Segmentation

Encryption, Digital Signatures, Keys or Tokens

Role based authentication

Logical Intrusion and Alert Solutions

II. Where to Look for Risks.

The Target breach is a good example of where to start outlining data security. It is also a good example of how contractors are used as connectors, enabling criminals to reach information-rich companies. The criminals behind the Target breach did not just happen upon Fazio Mechanical. Instead, it is more likely that the criminals heavily researched how Target does business with its vendors and attempted to gain access through multiple vendors. Fazio Mechanical did not have the only access key, just one that the criminals were able to exploit.

This raises two principles to consider as a contractor: (1) your clients rely on your data security to protect them and (2) your data security will fail unless you insure everyone having access meets your standards. This becomes complex if your company utilizes any of the many applications becoming prominent in the industry from pre-qualification and bidding to building information, modeling, project scheduling and management, time management, billing, and auditing—all of these applications envision transmission of electronic information and simultaneous multiple users.

Technology makes the process more efficient, but it has not changed that individuals are still doing the work. That is why, for example, a computer does not handle the morning tailgate safety meeting. Effectiveness in that area requires one person to say to another, “don’t do this, and if you do, I am going to remove you from the job site.” Breaches can occur in many ways. For instance, a breach can occur with an unintended disclosure like when you send an email to the wrong person. A breach can also happen when a device is lost or stolen. Additionally, your company could be hacked or, more likely, an employee could introduce malware or a virus into your systems. Your data can also be intercepted by unauthorized users because of non-secure transmissions, obsolete devices, or outdated or imperfect software. General contractors may need to coordinate access to confidential data with owners, subcontractors, design professionals or others, and these third parties are equally responsible for your data security. Finally, employee theft is on the rise because of the ease in which large amounts of data can be transferred.

Mobile and Cloud Security Risks

The ability to match data and user mobility equals efficiency and ultimately profitability. It also creates gaps in physical and virtual data security. You might recall the bag mobile telephone, which allowed field personnel to communicate in real time with administration. That heavy and awkward brick became the smart phone, which now is essentially a powerful mobile computer either kept in your pocket or its big sister, a tablet. Both can serve as a signal gateway providing wifi connections for even more powerful computer generating devices like laptops. All mobile devices are inherently unsecure because of their size. Their mobility is equivalent to a beacon for criminals. Minimizing the risk relies on each user having constant awareness of where their respective devices are located. A construction site is not ideal, certainly less so considering the daily flow of people moving in and out.

The virtual security is similar given that most sites have limited hard-lines dedicated to data communication. This plus whatever lines might exist are likely temporary and thus exposed to tampering. Therefore, the tendency is to rely on wifi with boosters around the site to provide a constant signal. Wifi itself is not secure unless protected by a firewall and the normal host of malware protections. Assuming secure wifi is used, sharing the password with vendors creates a security risk, while constant changing of the password results in more administrative work.

Cloud based storage is also an issue. There is a private cloud, where all of your information is stored on a physically separate server, which has a physical location having your own private virtual door in and out. Some cloud-based systems are less secure, are shared, and might be spread across multiple servers in multiple locations, stored together with other people's data segmented from others. This can be likened to the storage of virtual boxes, but nonetheless, still co-existing. So, concepts like data retrieval, malware and other malfunctions become more complicated in a shared cloud.

Password Security Risks

A long-standing common practice is to have policies requiring individuals to create a new password frequently, such as every 60 to 90 days. Heavily regulated industries like banking and health care are required to have password management safeguards in place that often result in such mandates.

A blanket approach to passwords, and frequent mandatory password changes may not be the right answer for every industry or every company. Credit this shift to the FTC's now past Chief Technologist, Lorrie Faith Cranor. Ms. Cranor does research at Carnegie Mellon University's CyLab Usable Privacy and Security Laboratory. She is smart and password-savvy. She and her team researched passwords and concluded that while a properly-written password policy can improve security, it may be time to rethink the standard for what a properly-written policy should require.[21] She surmises that forcing regular password changes may actually decrease security, by driving people to select weaker, easier to remember passwords, which are also easier for hackers to crack.

The response to this information is not to create short, easy to guess passwords. Nor is it to allow people to pick a password and never change it. Instead, to realize improved security from your passwords, you need to start with a

[21] Lorrie Cranor, *Time to Rethink Mandatory Password Changes* (March 2, 2016) available at, https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes (last visited August 25, 2016).

very clear policy and enforce the rules always. If you have software that helps enforce the policy for you by rejecting passwords that violate the rules you have established, the job will be even easier.

Solutions

Consider these tips for password policies derived from CyLab's research:

- Never reuse a password from a private account at work.
- Never allow pet names, birth dates, street addresses, or names of family members as a password.
- When changing a password, always pick a password unrelated to the old one and warn against obvious letter-digit substitution, i.e., the letter "o" becomes the number "0."
- Establish password length and complexity requirements. Consider a minimum of eight characters using at least three variations such as capital letter, small case letter, digit, or symbols, but suggest that 16 characters with two variations is even more secure.
- Never share your password with anyone and do not write it down or keep it somewhere accessible to others.
- Mobile devices need protection too. Biometric thumbprints are good, 12 characters with two variations are better. Because these devices auto correct spelling, do not hide the characters while typing to avoid frustration.
- Use a password limitation block so that after five wrong guesses the user needs to contact an administrator to allow access.
- Require all employees to report any data breach.
- Cultivate and reward an atmosphere of responsible data use.
- If you think your password has been stolen or compromised, change it.

If you do not have password policies and practices incorporating these tips, requiring a regular 60 to 90 day password change is still better than nothing. It is better because you are essentially in a foot race where hackers are just picking up password crumbs leading to your company. Requiring password changes gives you a chance to stay ahead, and maybe, if you use that time for training and implementing a password policy, you may even improve your distance.

Ransomware Risks

The most commonly known form of Ransomware is called Cryptolocker. Another form is called Locky, which is so sophisticated that there is no known antidote to get your data back once encrypted. You may have read in the news that this problem seems limited to hospitals. It is not. The criminal enterprises behind the malware are aiming at any company that needs a data system to be operational. This is a significant risk for those mid- and small-size companies lacking big technology budgets.

The problem starts when an employee opens an email attachment, clicks on a link within an email, or simply goes to an infected website. The malware is then transferred to your system. It is incredibly simple for malware to completely lock a company out of all items kept in its computer systems until the organization makes payment to get it back.

Solutions

Here are a few tips on how to protect your company from Ransomware:

- Always conduct regular system back-ups, store the backed-up data offline, and verify the data is intact and secure.
- Categorize and secure data based on its organizational value. Consider creating a separate system for those most valuable assets.
- Update antivirus software, operating systems and web browser.
- Install a pop-up blocker.
- Prohibit employees from downloading any software onto the company computer without proper approval.
- Warn your employees to not open attachments in unsolicited e-mails, even if they appear to come from people in your contact list, and never click on a URL contained in an unsolicited email, even if you think it looks safe.
- Warn your employees to use the same precautions on their mobile phone as they would on a computer when using the Internet.

Take the time this year to do a data audit. A company forgets, misplaces, or has lost things just like a person. Unlike a person, a company generally has more than one person holding the knowledge about what it has, where it is, and who has the keys. A map of your data will help you understand what is affected and how to get back to an operational level quickly.

Preventing Ransomware is heavily dependent on employee training. You cannot expect to protect your company's data when everyone doesn't know how. Preventing Ransomware is not just about having the right software to scan for malware or viruses, but is a continual investment in technology and the people who understand how all of it works together.

Limit the amount of data that your company carries so there is less at risk. Ask these questions before saving: (1) what data do you need to operate; and (2) how long do you need to keep it. Dispose of unnecessary data in a safe and documented manner so it cannot be retrieved or reconstructed. In other words, don't just collect data and instead create a process which is audited to insure only the information that you need is kept.