Beazley Breach Response Services Industry Insights Construction and Engineering Firms

What can go wrong?

On March 17, 2017, the United States Secret Service announced that a laptop with sensitive information related to Trump Tower's floor plans was stolen from the car of an agent. The laptop had multiple layers of protection, including full disk encryption, and could be wiped remotely.[1] While your organization probably doesn't have plans for presidential security, imagine having to explain to a customer or client that you've lost their plans or other sensitive data. Does your organization have proper controls in place for a situation like this? How many times does your organization have laptops or other electronic devices with plans or other sensitive business materials traveling to job sites?

Protecting your business from cyber threats is becoming ever more important in today's world. While healthcare or financial institutions face constant threats and industry specific regulations, construction and engineering firms may be under the impression that they just aren't targets, and that they don't have information worth stealing.

Construction and engineering firms have valuable data

Firms often don't assess the value of the data they may have. "Construction firms have … intellectual property, proprietary assets, architectural drawings and specifications … all of which are prime targets"[2] for hackers. Also, like most companies, these firms also maintain employee data. This includes full names, addresses, Social Security numbers, and often bank account information. In addition, they may have financial information about clients.

As construction and engineering firms begin taking advantage of advances in technology, such as "Building Information Modeling (BIM), telematics and project management software,"[3] they expose themselves to more cyber risks.

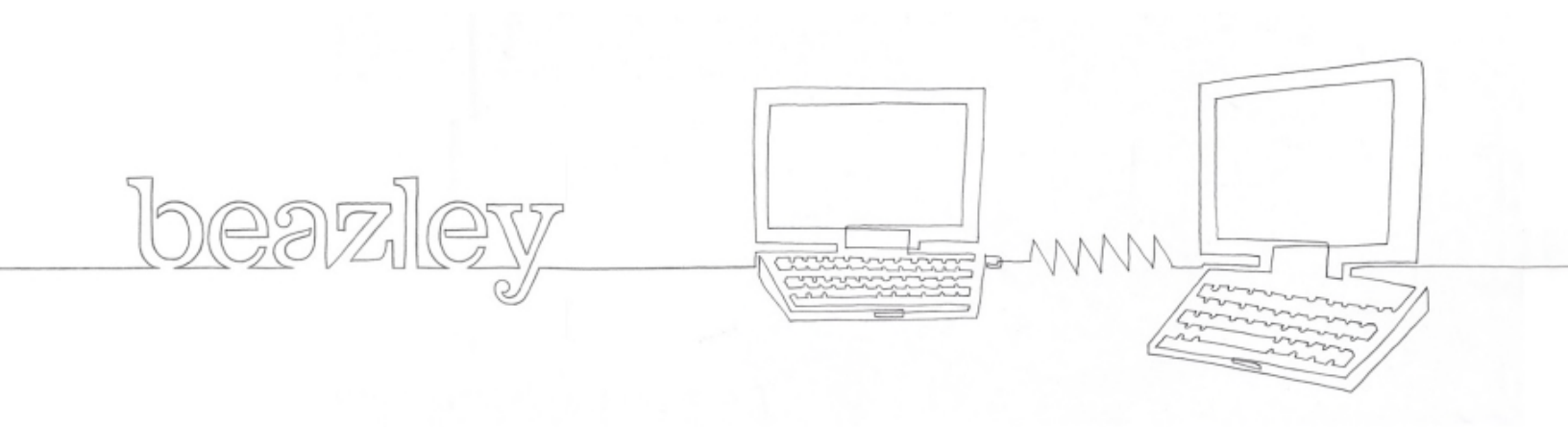
In addition, construction and engineering firms are fast becoming targets on the international scene. The engineering powerhouses in the Asian-Pacific region, for instance, are "home to innovations that are highly coveted by nations with less advanced engineering capabilities. Designs, blueprints, formulas and equipment specifications are typically prized by threat groups that steal data in support of domestic industries."[4] It's only a matter of time before such attempts become more common in the United States.

Construction and engineering firms may not think of themselves as being part of a supply chain, but firms upstream from major companies are often prime targets for attacks.[5] The premier example is the Target breach. An employee at a small HVAC firm based in Pennsylvania fell victim to a phishing attack, giving the attackers access to their system through malware. The firm was a contractor for Target Corporation, and the attackers then exploited the access to the vendor's system to connect to Target's network, through Target's hosted vendor services.[6] As a result, the attackers were able to steal information for 40 million payment cards and customer data for 70 million individuals by breaching the security of a vendor.

Attacks are often opportunistic, not targeted

But Beazley Breach Response (BBR) Services data shows that the most common source of breaches is not a targeted attack, but an opportunistic one. Phishing and ransomware often don't discriminate; they're sent out to as many people as possible in hopes of getting a result. That means that anybody could become a victim, and the lack of systems and experienced professionals in place to deal with something like this often makes the situation worse. Healthcare and financial Institutions, which are often targeted, are more likely than other sectors to be versed in privacy laws and breach response.

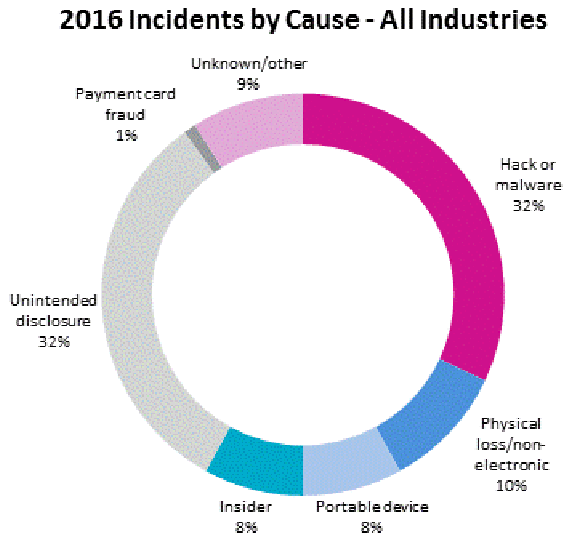
Phishing emails are sent to a broad group of people and may be written to trick the recipient into believing they're from a known organization or individual, such as an email provider or a bank. They'll ask the user to do something like change their password or confirm their banking details on a site that's designed to look legitimate, but is actually designed to capture user credentials or other information. These websites may also contain malicious code or malware, which can then infect the user's computer.



In contrast, spear phishing is targeted at a select group of people with something in common—whether they work at the same company, share the same bank, or have some other similarity. The emails are supposedly sent from organizations or individuals from whom the recipients would normally get emails. A greater effort is made to make it look like it's from a trusted party. Both phishing and spear phishing are attempting to get users to visit a site to compromise their credentials or to download a malicious payload.

Cyber extortion is becoming more and more prevalent. Ransomware, usually a variant of the Locky or CryptoLocker virus, encrypts files on a computer's hard drive and any shared drives to which the computer has access. Users' computers become infected by opening email attachments containing malware, or by clicking on a compromised website or pop-up window. Once the computer is infected, the user is directed to a page that demands a ransom payment in the form of Bitcoin within a certain amount of time and contains detailed instructions about how to purchase the Bitcoin to pay the ransom. Beazley insureds reported 203 ransomware incidents in 2016.

Not all losses are electronic. Loss of data in paper formats made up 10% of the breaches that BBR Services dealt with in 2016.



Legal and Regulatory Issues

For the types of incidents discussed above, 48 different state breach notification statutes govern legal obligations to investigate and respond. These statutes are a messy patchwork of often inconsistent requirements, with significant variations in the scope of data covered, the definition of what constitutes a "breach," and the mechanics of how impacted persons must be notified.

What's more, depending on the size of the breach, a firm may have to notify various state attorneys general and potentially be subject to fines and lengthy regulatory investigations.

Finally, upon learning of the breach, clients may file suit against the construction firm, alleging negligence or breach of contract. While suits against construction firms for data breaches are uncommon at present, all it takes is a bad breach to change that.

What can construction and engineering firms do?

Construction and engineering firms can take a number of steps to reduce their risk of a data breach:

- *Incident response planning*. Develop an incident response plan, designate your incident response team, and practice and update your plan regularly.
- *Employee training*. Train employees on security awareness throughout the year; consider phishing tests to maintain employee vigilance.
- *Risk analysis*. Conduct a risk analysis to identify what sensitive data the firm holds and where, and to evaluate your risks and the effectiveness of mitigating controls. Consider employing an experienced third-party vendor to conduct the risk assessment.
- *Encryption*. Implement full device encryption on all portable devices and consider secure email solutions.
- *Two-factor authentication*. Set up two-factor authentication for remote access and for administrator access to key resources. Provide remote access only through secure channels, such as a well-configured virtual private network (VPN) connection. Require strong passwords.
- *Backups*. Implement a data backup and recovery plan; maintain copies of sensitive or proprietary data in a separate and secure location not readily accessible from local networks.
- *Document retention policy*. Develop a document retention policy and properly dispose of sensitive data accordingly.
- *Penetration testing*. Retain a security firm to evaluate the risk that an attacker can compromise your IT assets and remediate accordingly.
- *Antivirus and patching*. Regularly update antivirus definitions for all users and ensure timely patching of operating systems and software.
- *Intrusion prevention and detection*. Deploy an intrusion detection system (IDS) and an intrusion prevention system (IPS) that aggregate logs to a Security Information and Event Management (SIEM) tool that sends real-time alerts.

- *Vendor risk management*. Ensure vendors are contractually obligated to protect sensitive data, provide timely notice of a breach, return or destroy data at termination, and maintain cyber liability insurance.

Beazley Breach Response policyholders will find a wealth of relevant resources at BeazleyBreachSolutions.com.

How BBR Services assists

As the industry leading solution for data privacy and security risk management, BBR Services helps BBR insureds successfully prepare for, investigate, and respond to privacy or security breaches.

Guided by the experience of handling more than 6,000 breaches, BBR Services is your frontline partner in data breach investigation and response, and available to your organization regardless of the size, severity, or cost of a data breach. The BBR Services team works in collaboration with your incident response team to triage and assess the severity of a data breach incident, while coordinating the range of resources and services you may need to meet legal requirements and maintain customer confidence.

By Luke Green, CIPP/US, CIPM, BBR Services manager

Luke received his J.D. from Hofstra Law School and is a Certified Information Privacy Professional (CIPP/US) and Certified Information Privacy Manager (CIPM). As part of the BBR Services team, he guides policyholders through suspected and confirmed data privacy and cyber security incidents. He works with policyholders in industries including retail, financial services, healthcare, and higher education. Before joining Beazley, Luke completed a fellowship in legal technology.

Example: Ransomware Nightmare

Ransomware attacked and encrypted all the files of a BBR policyholder engineering firm, stopping their business completely. Trying to handle the matter themselves at first, the firm discovered that every time they restored from backups, the virus would encrypt the files again. Desperate for any type of security help that could eradicate the virus, the firm called BBR Services. BBR Services coordinated a forensic team who was on site within 12 hours. The team deployed a network device that helped isolate the virus and stop it from spreading, allowing the engineering firm to get their business back up and running.

Example: Missing Hard Drive

A hard drive containing a potentially large number of sensitive records went missing from the field office of a BBR policyholder construction firm. Shortly after the company discovered the drive was missing, a state regulator somehow learned of the incident, which resulted in multiple government demands to notify a large number of individuals. The construction company called BBR Services, who immediately coordinated outside legal help and engaged a forensic firm to perform data mining on the backup of the missing hard drive. The company was able to show the government body that they were responding quickly and taking the matter seriously. Analysis showed that a large number of individuals needed to be notified, and BBR Services assisted in engaging notification, call center, and credit monitoring vendors to make a large notification in a short timeframe.

1 Eric Walsh, *Secret Service Says Laptop Stolen from Agent's Car in New York*, Reuters (Mar 17, 2017), http://www.reuters.com/article/us-usa-trump-laptop-idUSKBN16O2EH.

2 iSqFt, *Data Breaches, Cyber Security and the Construction Industry* (May 2, 2016), http://www.isqft.com/start/blog-data-breaches-cyber-security-and-the-construction-industry/.

3 *Id*.

4 Mandiant, M-Trends 2017: A View From the Front Lines (2017), *available at* https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html.

5 Nate Lord, *The Third Party Data Breach Problem*, Digital Guardian (Oct. 13, 2016), *available at* https://digitalguardian.com/blog/third-party-data-breach-problem.

6 Thor Olavsrud, *11 Steps Attackers Took to Crack Target*, CIO (Sept. 2, 2014), http://www.cio.com/article/2600345/security0/11-steps-attackers-took-to-crack-target.html.