AIA Best Practices:
6 steps to prevent a cyber attack

Contributed by Nick Maletta

Summary

The emerging risk of a cyber breach of information can severely damage a firm's reputation, productivity, and balance sheet with a single attack. This risk isn't limited to just high-profile breaches that are seen in the headlines. They can impact firms of all sizes, all with varying levels of technology adoption. Being proactive and putting in place the right steps to mitigate this risk can be a matter of survival for any firm.

There are many reasons for firms to proactively approach a cyber event, three of which will be highlighted here:

- contractual obligation
- security and public safety
- obligation to employees

Each one of the above is as pertinent and important to firms as the next. Firms that don't seek out and embrace this very real, evolving risk have placed themselves in a naive invincibility state of mind. One cyber event, or alleged cyber event, that's traced back to a firm will incur a great financial burden to the company's balance sheet. In the absence of proactive planning, the breach can seriously threaten the financial stability and longevity of the firm.

Contractual obligation

Many new lines of insurance coverage attribute their successful adoption to a firm's contractual obligation to carry said coverage. Clients and owners alike have started and will only continue to require a firm to carry cyber liability coverage due to claims in which firms were conduits to the valuable information housed within the client's walls. Reviewing these contracts to ensure the firm is in compliance is no simple task. The lack of consistency in cyber liability nomenclature can make for a confusing contractual request.

Security and public safety

The profession of architecture puts many in a unique position in that every inch of every design has been thought through and understood by its designers. As such, a firm will have an intimate level of knowledge about the security and safety of projects. How much does a firm tell vs. how much is the firm "giving away"? This is a tricky one, and one companies have to be careful about.

Take a school for example. If a firm is in the middle of a school construction project and is asked, "What securities are you building in that will help protect our children?" the firm must be very careful on how it answers.

Depending on the level of security around the project, a discussion should occur between the architect and owner regarding how these issues will be addressed—specifically in light of the Freedom of Information (FOI) laws that apply to public projects. Companies can't just give the keys to the castle to everyone.

Employee data

Every firm has an obligation to employees to maintain a high level of confidentiality with the information it's privy to. Failure to meet these expectations can cause a great deal of internal uproar, of which lack of productivity may be the least of the firm's worries.

Many firms maintain some form of employee data stored on their servers or even paper records in filing cabinets. Each firm is in charge of keeping this data secure. Items like health information, Social Security numbers (SSN), birth dates, addresses, etc., are all appetizing to a hungry criminal. Allowing a cybercriminal access to an employee's name, in combination with an SSN, birth date, address, or other financially driven information, can lead to falsified tax returns being filed, stolen identities, fraudulent credit cards being created (thereby ruining an employee's credit), etc.

An employee's personal health information has a much higher value on the black market than personally identifiable information stolen to create a credit card because health information can't be altered or deleted. Credit cards and fraudulent identities can be deleted or fought. Think of the potential consequential damages that could derive from the loss of an employee's personal information.

The six steps firm can take to prevent a cyber attack

1. Educate employees: Educating employees is key to helping thwart cyberattacks. Firms should educate employees on the risks of:

- using their own devices when working on jobs or what they should do if their device is lost or stolen
- traveling and the use of hotel lobby business centers

Also, firms should discuss with employees email protocols, including the importance of strong password usage, what phishing emails are, the definition of social engineering, and how these all can jeopardize the fate of the firm.

For example: According to the 2015 Verizon Security Report on breaches in 2014, nearly 2/3 of all breaches involved some level of a phishing scam. On average, 9 out of 10 employees will click on a phishing email scam. The most commonly used password is in fact the word "password." Developing a base level of knowledge for employees is a start. This base level of knowledge (with annual reminders) is vital to the success of a proactive cyber approach.

2. Review vendor agreements: Firms shouldn't just assume that if a vendor handles their security the vendor will be responsible for something that goes wrong. Using a third-party service to manage security is a good idea, but keeping a close eye on the contracts that are involved is crucial. Many of these agreements contain a limitation of liability that's very minimal or a strongly worded indemnity provision which pushes all responsibility back to the firm. Reviewing these contracts is a must.

3. Ensure security is kept up to date: This is often seen as the boring task. It was referred to in the Wall Street Journal as "Cyber Hygiene." But making sure the automatic updates that are pushed by the Microsoft's of the world are kept up to date is necessary. Many of these updates, which may seem annoying, are security patches and, as such, are in place to keep a firm's systems secure. Companies should maintain these updates and run them regularly. Not doing so could result in the voidance of any cyber liability insurance policy the firm has in place.

4. Develop a breach response plan: Creating a proactive plan which is tested within the firm's policies and procedures is a must. This is often a requirement from insurance carriers to get coverage in place. This is a plan of action in the event of a cyber breach. Much like a fire drill, it should designate the right people in the right positions to respond during a breach. It should have a calling tree of who will be contacted and in what order. Lastly, it should contain how to address the media in a time of second-to-second responses. Being proactive and having a well-tested breach response plan could mean the difference between a firm keeping its doors open or not.

5. Review policies and procedures with sub-consultants: All parties on a project should be subject to the same controls, policies, and procedures from a cyber liability standpoint. Firms should ensure sub-consultants address these same issues. As a reminder, the Target breach flowed through a subcontractor, so sub-consultants should take this risk as seriously as the firm they're working with. Firms should consider adding cyber liability coverage as a contractual requirement for a working relationship.

6. Protect the balance sheet with insurance: Many see insurance as a necessary evil; however, cyber insurance can protect the very livelihood firms have created. Companies should review their current insurance programs and the coverages in place. Reviewing a cyber-liability policy should include 1st and 3rd party coverages, along with adequate limits and structure. In the cyber liability world, as the cliché goes, "You get what you pay for," so be leery that the comparisons are truly apples-to-apples.

Conclusion

A cyber event can't be fully prevented. In some way, shape, or form, everyone will fall subject to a breach and have their information in the wrong hands. Being proactive, raising self-awareness, and educating employees will vastly improve the potential damages a firm might incur.

About the contributor

Nick Maletta is the Cyber Liability Practice Leader for Holmes Murphy and Associates, an independent brokerage, serving business and industry leaders across the nation in the areas of property casualty

insurance, employee benefits, captive insurance, risk management, and loss control, in West Des Moines, Iowa.

The AIA collects and disseminates Best Practices as a service to AIA members without endorsement or recommendation. Appropriate use of the information provided is the responsibility of the reader.

About AIA Best Practices

AIA Best Practices is a collection of relevant, experience-based knowledge and expert advice on firm management, project delivery, contracts and more, aligned with the *Architect's Handbook of Professional Practice, 15th edition*. See the full AIA Best Practices collection at aia.org/aia-best-practices.

This article corresponds to:

Architect's Handbook of Professional Practice, 15th edition Unit 1 - The Profession
Chapter 16 – Risk Management
Section 01 – Risk Management Strategies