XL CATLIN

**Insurance**
Design
Professional

# Protecting Your Firm from Cyber Liability Risk

The following article was written by Nick Maletta, Cyber Liability Practice Leader for Holmes Murphy and Associates, a 700-person independent brokerage headquartered in West Des Moines, Iowa. Serving the professional liability needs of architects and engineers has helped Maletta shed a unique light on the unintended consequences a cyber event could have for designers.

A single cyber breach of information can severely damage a design firm's reputation, productivity and balance sheet. This type of attack isn't limited to the high-profile breaches seen in headlines. A breach can impact firms of all sizes, with varying levels of technology adoption. Putting the right steps in place to mitigate this emerging risk could help prevent a firm's demise.

There are many reasons for design firms to proactively approach a cyber liability breach event, three of which they might not have considered:

## Contractual Obligation

Owners increasingly require by contract that design firms carry cyber liability insurance coverage. Owners are familiar with cases such as the infamous Target breach, (in which the attacker stole an HVAC contractor's credentials and gained control over Target's servers) and are concerned that design firms may unwittingly provide hackers with a point of entry into the owners' data infrastructure.

The lack of consistency in cyber liability nomenclature can make for a confusing contractual request. When reviewing an owner's minimum insurance requirements, you'll need to pay extra attention to confirm your compliance with cyber liability-related obligations.

## Security and Public Safety

Design professionals think through every inch of every project, which gives them an intimate level of knowledge about a project's security and safety. How much detail should the design professional share with the public regarding the security built into a project, and how much should the design professional share only with the owner? This is a tricky situation in view of the ease of obtaining such information, and one firms 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 the question, "What kind of security systems and features are you incorporating that will help protect our children?", the firm must be very careful about how it answers. A discussion should occur between the designer and owner regarding how these issues will be addressed—specifically in light of Freedom of Information Act (FOIA) and similar laws that apply to public projects. Firms must comply with such laws, of course, but they can't just give the keys to the castle to everyone.

## Employee Data

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

Continued

Many firms maintain some form of employee data, whether stored digitally on their servers or even as 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 to access an employee's name, in combination with an SSN, birth date, address or financial information, can lead to the filing of falsified tax returns, stealing of identities, creation of fraudulent credit cards (potentially ruining an employee's credit) and more.

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. While credit cards and fraudulent identities can be deleted or fought, health information can't be altered or deleted. Think of the potential consequential damages that could arise from the loss of an employee's personal information.

## Best Practices

There are six steps design firms can take to help prevent a cyber event and its potentially devastating consequences:

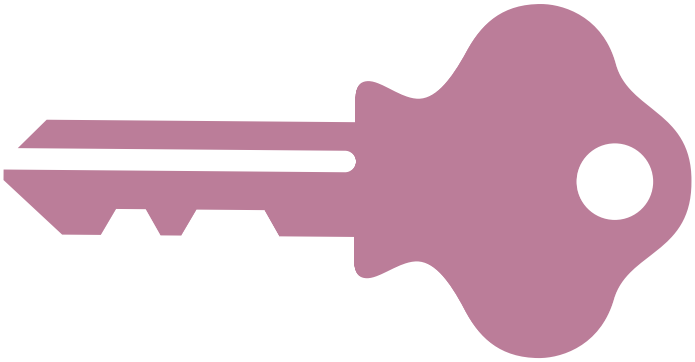
**1. Educate employees**
Educating employees is key to helping thwart cyberattacks. Firms should educate their staff on the risks of:

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

Also, firms and employees should discuss email protocols, including the importance of strong password use, phishing emails, social engineering, and how these all can jeopardize the fate of the firm. For example, according to a 2015 Verizon security report on breaches in 2014:

- Nearly two-thirds 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."

On average, 9 out of 10 employees will click on a phishing email scam.



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 involved is crucial. Many of these agreements contain a limitation of liability that's very minimal or a strongly worded indemnity clause that pushes all responsibility back to the firm. Reviewing and amending 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 updates from Microsoft, Adobe, Apple and other software vendors are installed 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 regularly check for these updates and install them. 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 and testing a proactive plan, and incorporating it into the firm's policies and procedures, is a must. This is often a requirement from insurance carriers to get coverage in place. It's 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 designating which parties will be contacted and in what order. Lastly, it should contain instructions on how to address the media in an age of 24-hour news cycles and instantaneous communication vehicles such as Twitter. Being proactive and having a well-tested breach response plan could mean the difference between a firm keeping its doors open or not.

Continued

**5. Review policies and procedures with subconsultants**
All parties on a project should be subject to the same controls, policies and procedures from a cyber liability standpoint. Firms should ensure subconsultants address these same issues. The massive Target breach flowed through a subcontractor, so subconsultants should take this risk as seriously as the firms 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 first- and third-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 sure the comparisons are truly apples-to-apples.

## Conclusion

No firm can be fully protected against every type of cyber breach. In some way, shape or form, everyone will at some point fall prey to a breach and have their information end up in the wrong hands. Being proactive, raising awareness and educating employees will vastly improve the potential damages a firm might incur. Companies shouldn't be naive about the reality of a cyber event.

**Nick Maletta may be contacted at**
**nmaletta@holmesmurphy.com or 800 247 7756.**

Owners increasingly require design firms to carry by contract cyber liability insurance coverage.

**Contact**
**Design Professional**
30 Ragsdale Drive, Suite 201, Monterey, CA 93940
Phone: 800 227 8533 x21022508
xlcatlin.com/dp

100 Yonge Street, Suite 1200, Toronto, ON M5C 2W1
Phone: 800 820 2721 x8682
xlcatlin.com/dp-ca

***MAKE YOUR WORLD GO***
**xlcatlin.com**

The information contained herein is intended for informational purposes only. Insurance coverage in any particular case will depend upon the type of policy in effect, the terms, conditions and exclusions in any such policy, and the facts of each unique situation. No representation is made that any specific insurance coverage would apply in the circumstances outlined herein. Please refer to the individual policy forms for specific coverage details.
XL Catlin, the XL Catlin logo and Make Your World Go are trademarks of XL Group plc companies. XL Catlin is the global brand used by XL Group plc's (re)insurance subsidiaries. In the US, the insurance companies of XL Group plc are: Catlin Indemnity Company, Catlin Insurance Company, Inc., Catlin Specialty Insurance Company, Greenwich Insurance Company, Indian Harbor Insurance Company, XL Insurance America, Inc., XL Insurance Company of New York, Inc., and XL Specialty Insurance Company. In Canada, coverages are underwritten by XL Specialty Insurance Company—Canadian Branch. Coverages may also be underwritten by Lloyd's Syndicate #2003. Coverages underwritten by Lloyd's Syndicate #2003 are placed on behalf of the member of Syndicate #2003 by Catlin Canada Inc. Lloyd's ratings are independent of XL Catlin. Coverage may not be available in all jurisdictions. Information accurate as of July 2016.