L'ABBATE, BALKAN, COLAVITA & CONTINI, L.L.P.

LEGAL COUNSEL

FOR THE DESIGN PROFESSIONAL

LBCC when it really matters

L'Abbate, Balkan, Colavita & Contini, L.L.P.
ATTORNEYS AT LAW

NEW YORK OFFICE
1001 Franklin Avenue
Garden City, NY 11530
Office: 516.294.8844
Fax: 516.294.8202
www.lbcclaw.com

NEW JERSEY OFFICE
100 Eagle Rock Avenue
Suite 220
East Hanover, NJ 07936
Office: 973.422.0422
Fax: 973.422.0420

Comprised of a team of experienced attorneys dedicated exclusively to representing design professionals.

Summer 2016

Cyber Attacks: A Clear and Present Danger to Architects and Engineers

BY DOUGLAS L. PINTAURO, ESQ.

Typically, a data breach, or the hacking of a company's network, is associated with identity theft or credit card theft, such as in the Target, Staples, Kmart, Home Depot, Starbucks and Five Guys restaurants breaches. Consequently, architects and engineers generally do not consider such risks to be anything more than newsworthy events. However, the breaches of Sony Pictures Entertainment, Ashley Madison, HSBC, AT&T, as well as numerous government networks, including President Obama's unclassified computer system, have underscored the fact that much more is at risk than simply social security numbers and credit card information. This is evidenced by the now well publicized concerted efforts of China, Iran, Korea and Russia to hack into the secured networks of the government and private businesses in order to steal technology, trade secrets, government secrets and even plans for certain public and private facilities. In short, hacking has gone well beyond social security numbers, credit card data, or even the occasional nude photos of celebrities. For lack of better terminology, hacking has become a multimillion dollar industry. So much so that companies have offered bounties to hackers who can breach certain secured sites, such as Apple's mobile operating system.

With the above in mind, cyber security is just as relevant to architects and engineers as it is to Sony. Specifically, since the advent of CAD, BIM, FTP sites and email, architects and engineers have become more and more reliant upon the World Wide Web. In fact, these tools have become such an accepted part of the design profession that they are used even for small projects. While there are many benefits to employing these electronic tools, as a result of today's environ-

(continued on p.4)

Ransomware: A Growing and Expensive Cyber Concern

BY DOUGLAS R. HALSTROM, ESQ.

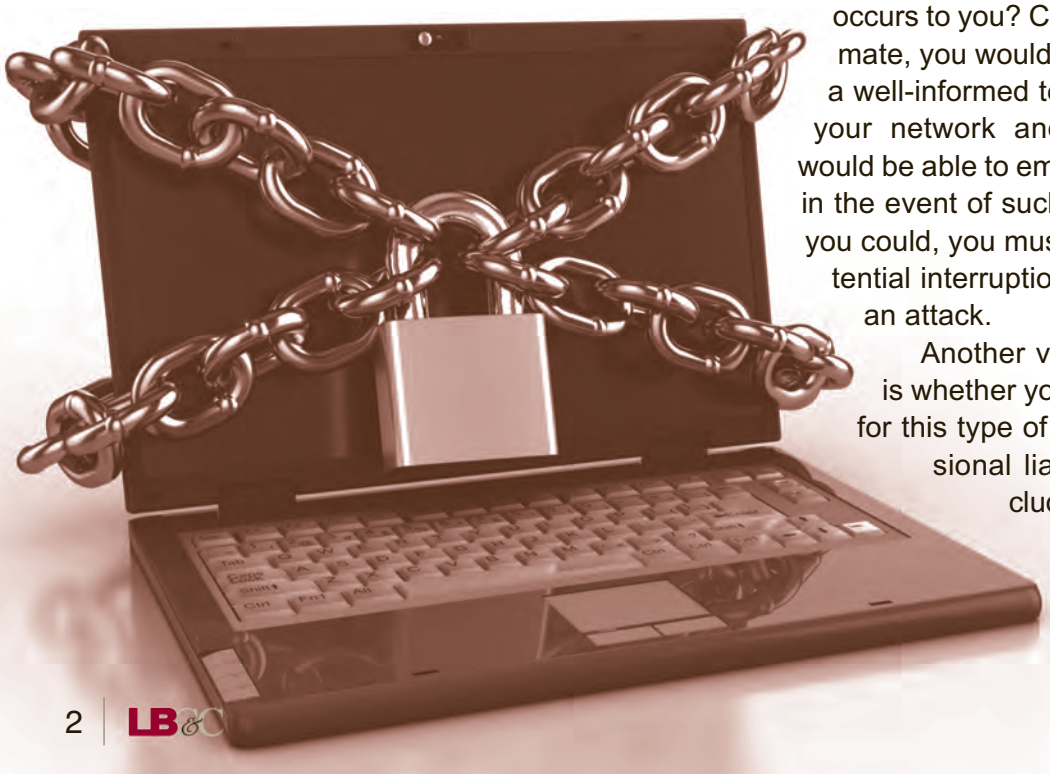
Members of the Design Profession are increasingly reporting instances of ransomware attacks. Ransomware attacks have been reported for a few years now and involve someone hacking into a computer system and essentially "taking it hostage" by disabling it and demanding a money payment or some other action (e.g., the Ashley Madison cyber attack) before the hacker will release the system.

As a design professional, you may ask: "Why should I be worried about this? I am not a Fortune 500 company with billions of dollars at risk or millions of customers' personal information stored away on our servers. And even if I am a target, is there an insurance policy available on the market that protects me from this type of risk?"

The motivation for people to hack into computer servers of small businesses is simple: In the case of ransomware, the hacker is not looking to steal personal data that might be stored on your server. Rather, they are simply looking to put a cyber gun to your head in order to extort a "ransom" payment. The more common instances involve requests for $5,000, $10,000 or $15,000 in exchange for the cyber hacker agreeing to give you back your servers without losing any data. While this is still a breach and the likelihood of the hacker stealing your clients' personal information is almost certain, the immediate concern is to insure that your computer system is not destroyed and that you are able to continue operations with little to no interruption.

The hacker is not looking to steal personal data that might be stored on your server. Rather, they are simply looking to put a cyber gun to your head in order to extort a "ransom" payment.

If this circumstance has not happened to you, just ask your friends in the profession whether it has happened to them. Very likely, you will discover a few ransomware victims. So what can you do? One firm, given the extensive automatic backup performed on their system on a daily basis, was willing to allow the attacker to delete the data from its system, as the hacker promised to do if the firm did not pay a $10,000 ransom. The firm ignored the request and the hacker promptly erased all the data on the system. As a result of the extensive backup system maintained by the firm, they were able to retrieve all the data the next day within a few hours. Is this an option in the event this occurs to you? Considering today's cyber climate, you would be well served by retaining a well-informed technology expert to assess your network and determine whether you would be able to employ the same type of tactic in the event of such an occurrence. Assuming you could, you must also be mindful of the potential interruption to your business by such an attack.



Another valid question in this regard is whether you are covered by insurance for this type of attack. Your typical professional liability policy very likely excludes coverage for any type of cyber attack or breach. Notwithstanding this shortcoming, the in- ›

(continued on p.7)

Risk Management: Contract Scope Language

BY DOUGLAS R. HALSTROM, ESQ.

A recurring theme in the litigation arena is the inadequate expression of scope of services in the design professional's contract. The scope of services description in your written contract can be the most effective risk management tool you can employ in order to avoid or successfully defend against lawsuits over issues with which you had little or no involvement.

A typical written agreement employed by design professionals often reads, under "Scope of Services" that the design professional will provide "typical architectural services" or "necessary engineering services", without specifying the precise nature of the work to be performed. As a result of this vague description, disputes generally focus upon the role of the design professional during construction inasmuch as the typical lawsuit, whether it be for personal injuries or construction defects, focuses upon the activities during the construction phase. Accordingly, if you do not plan to have any involvement in the project during the construction phase, then your proposal and contract should specifically state that in no uncertain terms. More often, however, the architect or engineer does have a limited role, whether it be "periodic site visits", as described in many of the standard AIA contract forms, attendance at certain job meetings, review of shop drawings, certifying payments, or other contract administration functions. Whatever services the professional agrees to perform, the contract should specifically identify them.

Whatever services the professional agrees to perform, the contract should specifically identify them.

A rather typical scenario, is one which may involve various construction defects in a building, none of which arise from a deficient design. Although the design is not in issue, the architect or engineer may nevertheless be faulted for having failed to detect the various defects in the construction work. In such cases, the contract may articulate, under the heading "Construction Administration", four areas of responsibility, including review of shop drawings and submittals, attendance at four job meetings during construction, review of test reports and inspection reports and monthly site visits to observe the construction in progress. The day to day construction inspections and special inspections, on the other hand, might be delegated by the owner to an outside inspection company which has no relationship to the project architect or engineer.

Based upon the above scope, being able to demonstrate that the owner retained a separate entity to perform the construction inspections, could make the difference between staying embroiled in ›

(continued on p.8)

If you would like to receive our newsletter via email, please email your address to: mmorabito@lbcclaw.com

Cyber Attacks: A Clear and Present Danger to Architects and Engineers (continued from p.1)

ment, there are also risks, many of which are not perceived by architects and engineers, especially solo practitioners or small architectural and engineering firms. The fact is that everyone is at risk, to varying degrees. Despite the risks, most architects and engineers who read this article will remain convinced that this does not apply to them. Clearly, why would anyone want to waste time hacking into an architect's or engineer's network, especially if it is a small firm? Of course, if this question is asked, it is because the threat is not perceived. If the threat is not perceived, the appropriate measures to protect the electronic data are probably not in place. If that is the case, you are a target. Significantly, at least one survey has disclosed that approximately 30% of all data breaches focus on small businesses. While this may seem implausible based upon what is disclosed in the media today, it is only because the media does not publicize small business breaches. There is a greater audience for the more sensational big breaches. In reality, however, even a small architectural or engineering firm is at risk of being hacked.

> Why would anyone want to waste time hacking into an architect's or engineer's network, especially if it is a small firm?

If an architectural or engineering firm is hacked, what is at risk? Certainly anything maintained on the company's network is at risk of being stolen, such as the firm's financial information, the personal and financial data of the firm's clients, as well as the architect's or engineer's intellectual property. Of course, not all hackers simply steal information. Some install "ransomware" which locks the users data or electronic files by encrypting them until a monetary ransom is paid. Should this occur, the architect or engineer would lose access to its ongoing projects, some of which might be in the design development stage or the construction document stage. Under any scenario, however, being locked out could have significant monetary consequences such as delaying a project. These are only generic examples of the monetary consequences from being hacked. Accordingly, the associated monetary risks, while potentially significant, are generally identifiable.

But consider this: An architect or engineer is hired to prepare designs for an annex to the UN, or for the new Tappan Zee Bridge, or a new sports center, or an airport terminal, or a celebrity's home, or a religious house of worship, or a railroad terminal/station. Certainly today, each of these facilities either is, or has been the focus of terrorists, radicals or the common thieves. As a result, securing a copy of the designs which detail, for example, the security systems, could be quite useful to people with less than honorable intentions. Should such a breach occur, how are the damages determined and what is the architect's or engineer's liability? Are the damages simply the cost to redesign and reconstruct the security systems? What if the plans are used to implement a terrorist attack? Are the damages now measured by the resulting property damage and loss of life? What is the impact of such a breach on your business and reputation? These questions only underscore the severity and dire consequences of a breach.

While some may feel safe with the purchase of a cyber liability insurance policy, such policies do not cover all damages that flow from a data breach. Some damages may be covered under the architect's and engineer's professional liability policy, a business owner's policy, or not covered at all. Accordingly, insurance is only one line of defense. Establishing appropriate data security practices is another, but critical line of defense.

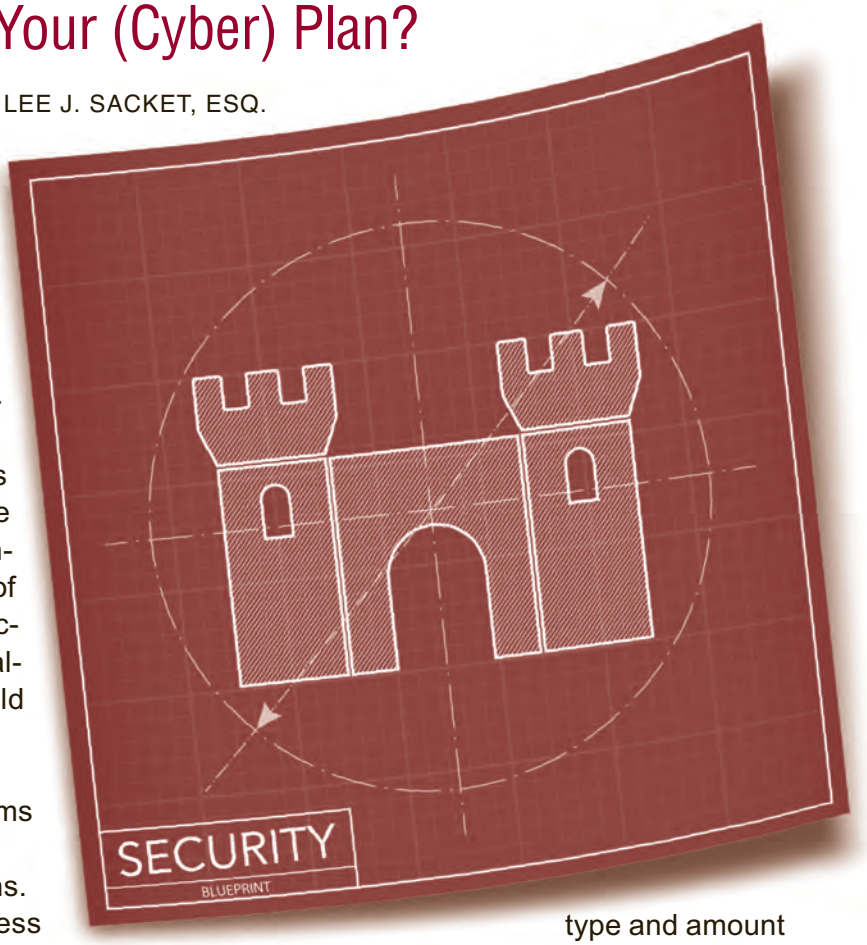
If a business does experience a network data breach and private client data is stolen, in addition to damaging its reputation, losing business information, as well as clients, the business is exposed to a potential lawsuit by the client. In such cases, a negligence claim is the most common theory of liability. Such claims are typically premised upon the theory that the client's data was negligently stored and ›

(continued on p.6)

If you would like to receive our newsletter via email, please email your address to: mmorabito@lbcclaw.com

What is Your (Cyber) Plan?

BY LEE J. SACKET, ESQ.



Every business that uses or relies upon technology faces the risk of a cyber breach or cyber-attack. The numbers suggest that the question is not if you will be breached, but when. Ignoring the probability of a breach could expose your business to unexpected and irrevocable losses. So, what is your plan?

There is an endless market of antivirus software and firewalls which companies use to protect against a cyber breach. A preventative cyber plan to mitigate the likelihood of a breach is vital to any business infrastructure and its importance should not be devalued. A preventative cyber plan should include, at a minimum:

1. Limit and restrict access rights to systems and equipment to necessary personnel.
2. Develop and test disaster recovery plans.
3. Provide information security awareness training to all personnel.
4. Configure strong access controls on firewalls.
5. Monitor system activity and all remote access.
6. Provide secure off-site storage of back up data.
7. Maintain updated virus protection.

However, even the largest and most financially able companies with preventative cyber plans in place, to varying degrees, suffered significant and well-publicized cyber breaches. The hackers seem to always be a step ahead of the preventative technology. As a result, if your plan is limited to preventative measures, you should rethink that strategy.

Companies must have a second plan focused on what to do when the inevitable breach occurs, commonly referred to as an Incident Response Plan ("IRP"). An IRP should be tailored to that business, but should consider, at a minimum, the type and amount of information maintained by the company, and who and where that information is currently available.

> The impact of a cyber-attack to an organization's brand, reputation and business operation can be catastrophic and beyond any dollar value.

Too often, a company's IRP is limited to calling its counsel, or the insurance company to file a claim. These calls should be a component of the IRP, not the full extent of it. Every second wasted allows the breach to potentially expand, which increases the company's exposure. There must be protocols in place to react immediately. Common key elements to an IRP generally include, but are not limited to:

1. Response Team: Identification of personnel, which almost always includes members of IT, HR and management, each with well-defined roles to immediately respond to the breach.
2. Stop or Mitigate the Breach: While identifying the breach is the most obvious and important el- ›

(continued on p.7)

Cyber Attacks: A Clear and Present Danger to Architects and Engineers (continued from p.4)

secured in such a fashion that permitted hackers to breach and steal the data. In order to prevail on such a claim, the client must establish that the business entity breached the standard of care in securing and/or safeguarding the client's data. Since there is no global or national standard of care, the courts will look to other criteria to make that determination. For example, some government contracts specify the security measures that the design professional is required to implement in order to safeguard the project file. Absent such a contractual provision, the courts will apply a "reasonable man" standard. In other words, what security measures would a reasonable man implement in similar circumstances.

Of course, the application of a reasonable man standard is not an exact science. Consequently, the courts will look at a number of factors, among which include: the nature and sensitivity of the stolen data; the type and cost of available security systems; the laws, rules, regulations or standards that may be applicable; what security measures are commonly employed by other architects and engineers; and the commonality of data breaches in general, as well as in the industry. While some illusory solace may be taken by assuming that all architects and engineers do what you do, that is usually not the case. Accordingly, staying current on the available security systems and periodically updating your network security, as well as routinely backing up your network, would be helpful in maintaining an appropriate standard of care. None of these precautions, however, will shield you from all potential breaches or claims. Rather, like the building code, they are merely the minimum steps you need to take in order to protect all concerned. ■

> Under any scenario, however, being locked out could have significant monetary consequences such as delaying a project.

SEMINAR BULLETIN

● LBC&C partner, Douglas R. Halstrom, presented a seminar for the American Council of Engineering Companies of New Jersey (ACEC) members at their 2015 Fall Conference entitled "Cyber Liability: Current Landscape and Managing Risk Through Insurance" which educated engineers on cyber/computer hacking risks to small businesses and those risks specific to the design profession.

● Doug also presented a seminar for the Real Estate Board of New York (REBNY) entitled "Risk Management for the Design Professional".This seminar addressed various areas of risk to the design professional and how to manage those risks by contract.

● More recently, Doug presented a seminar in conjunction with the Marquis Agency Risk Management Design Symposium entitled: "Protecting Your Practice—Trends & Challenges Facing Design Professionals Today; *Current Issues Involving Risk Management for the Design Professional: Cyber Liability Exposures + Case Studies on Contractual Terms and Conditions*. This program addressed contract preparation in order to address risk to the architect and engineer and how the design professional can identify cyber risk and prevent future exposure to cyber risk.

● LBC&C partner, Lee J. Sacket, recently presented a seminar to a land surveying company entitled "Current Issues Involving Risk Management for the Design Professional". The learning objectives in this seminar were, among other things: developing strategies for drafting design professional contracts to limit risk; accurately expressing payment methodology in order to be paid on time; hold harmless provisions, etc..

Information regarding these and other seminars may be obtained by contacting Margie Morabito at 516-294-8844 or mmorabito@lbcclaw.com.

ABOUT THE FIRM

LBC&C, founded in 1981, has offices in Garden City, New York and East Hanover, New Jersey. From these two locations, the Firm provides a wide array of legal services to design professionals throughout the New York Metropolitan area, Long Island, upstate New York and central and northern New Jersey. In addition to representing design professionals, the Firm has a recognized practice in other areas of professional liability, as well as environmental, employment practices liability, product liability, trust and estates and insurance law. As a full service law firm, LBC&C provides legal counseling, as well as litigation services, on matters affecting its clients from business issues to employment and labor practices. Always on the alert for new trends in business and changes in the law, LBC&C is continuously striving to keep its clients ahead of their competitors. Working in conjunction with each other, the Practice Groups at LBC&C provide a network of legal experience that can meet today's design professional's needs. For additional information visit our website at **www.lbcclaw.com**

Ransomware: A Growing and Expensive Cyber Concern (continued from p.2)

surance industry has for years been offering cyber liability insurance to cover various types of cyber risks. Whether your cyber liability policy covers you for this occurrence, however, requires an in-depth conversation with your insurance broker. During that conversation, you should also explore issues relating to the type of notice you would be required to provide your cyber liability carrier in the event of a ransomware attack, whether the policy permits the carrier to pay the ransom and whether the insurance carrier is equipped to respond immediately, as is typically required in these situations, in order to guard against the destruction of the data stored on your system. What if you agree to pay the ransom before notifying the insurance company? What if you agree to pay the ransom after notifying the insurance company in order to avoid the destruction of your electronic data? Will these payments be covered under your cyber liability policy?

The law on, and insurance for, these issues is evolving and many of these questions have not yet been addressed. Nevertheless, these are questions you should be considering, discussing with your insurance broker and, eventually, the insurance carrier issuing your cyber liability policy. ■

What is Your (Cyber) Plan? (continued from p.5)

ement, you must next stop or mitigate the breach. Categorizing and prioritizing confidential information may expedite the response and mitigate the breach.

3. Communication: Get out in front of the breach! Communication with IT, counsel and your insurance company is vital. In addition to communicating internally with employees and externally with clients (whose information may be subject to the breach), each state has different notice requirements for breaches, which must be addressed within generally short timeframes. Failure to do so could lead to fines and other compensatory damages.

Damages for cyber breaches can be extensive and sometimes, beyond measure. The impact of a cyber-attack to an organization's brand, reputation and business operation can be catastrophic and beyond any dollar value. Organizations need to plan proactively, but prepare for the reactive. While every company has varying resources to formulate these plans, utilize all available assets, including counsel, your insurance company and outside consultants, to navigate this ever changing landscape. You cannot afford not to. ■

If you would like to receive our newsletter via email, please email your address to: mmorabito@lbcclaw.com

Risk Management: Contract Scope Language (continued from p.3)

a lawsuit and convincing the Court to dismiss all claims asserted against the architect or engineer.

Of course, the more specific the scope of services, the better. For example, the provision "review shop drawings and contractor's submittals" should be written to indicate the purpose of the professiona's review of those documents and whether the professional's review of those documents constitutes the professional's assumption of (or not) responsibility for any errors in the shop drawings and submittals.

Typically, a shop drawing review is undertaken to assure conformance with the overall design intent, and not to confirm that the shop drawing is accurate. There are, however, those who would benefit from skewing or expanding upon the purpose of such review. In order to minimize such an occurrence, it would be prudent to identify the purpose and function of the shop drawing review so that there is a clear understanding of what obligations and responsibilities you are assuming.

In addition to specifying the precise nature of the services that you will perform, it is also advisable to describe those services that you will not perform on the project. This can be very helpful in limiting your risk on a project insofar as a list of services you are not performing provides all parties with a clearer understanding of the nature and extent of the services that you will provide.

By way of example, lawsuits involving injured construction workers typically focus on site safety issues, the contractor's means and methods of construction and supervision of the contractor. While the architect or engineer typically do not provide services that impact these issues, they often provide periodic site observations to determine if the work, when completed, will conform to the contract documents. Unfortunately, this service is often cited to imply that the architect or engineer may have somehow addressed site safety issues, directed the contractor, etc., during, or as part of, the periodic site visits. In order to avoid this expansion in responsibilities, the contract should specifically provide that the architect or engineer will not provide the following services: site safety; determining or overseeing the contractor's means and methods; and supervision of the contractor. While such exclusionary language will not always result in a quick resolution to the claim against the architect or engineer, it will establish a solid foundation for securing a dismissal. In short, be as specific as is practical in identifying those services that you will provide and those services that you will not provide. ■

By way of example, lawsuits involving injured construction workers typically focus on site safety issues, the contractor's means and methods of construction and supervision of the contractor.

ABOUT OUR NEWSLETTER

Legal Counsel for the Design Professional addresses current legal developments affecting architects and engineers. The articles contained in this publication are for your information. You are advised to consult with legal counsel to address whatever specific issues you may have. Your questions, comments and suggestions are appreciated and should be directed to the Practice Group's chairperson, Douglas L. Pintauro, Esq., at L'Abbate, Balkan, Colavita & Contini, L.L.P., 1001 Franklin Avenue, Garden City, New York 11530 516.294.8844
dpintauro@lbcclaw.com

The Law Firm for Design Professionals
LB&C
when it really matters

L'Abbate, Balkan, Colavita & Contini, L.L.P.
ATTORNEYS AT LAW

NEW YORK OFFICE
1001 Franklin Avenue, Garden City, NY 11530 [o] 516.294.8844 • [f] 516.294.8202

NEW JERSEY OFFICE
100 Eagle Rock Avenue, Suite 220 East Hanover, NJ 07936 [o] 973.422.0422 • [f] 973.422.0420

www.lbcclaw.com