2018 CLM Business Insurance & Construction
September 26-28, 2018
Chicago, IL

Cybersecurity and The Construction Industry: Relevance of Cybercrime to The Construction Industry; Why the Industry is Particularly Vulnerable and The Steps Organizations Can Take to Avoid Attacks.

I. Introduction

It is an unfortunate reality that the construction industry is increasingly vulnerable to cybercrime threats, and with additional technology platforms constantly rolling out there are no signs of the crime slowing down. Hackers are more adept at staying on the heels of these companies than the companies are of protecting themselves and preventing future security breaches. Although cybercrime is seen within all industries in today's age of cutting-edge technology, the risks associated with the construction industry are particularly prevalent, which is why it's imperative that construction companies implement effective cyber security. Small, medium, and large construction companies need to be more aware than ever about these cyberthreats. These cyberthreats exceed the basic challenges facing construction companies of making sure they are performing quality work and are paid in a timely manner.

Commercial contractors have long faced their own unique business risks - labor and material shortages, delay claims, bonding issues, and defects in workmanship. But, in today's ever-evolving cyber world, it is imperative that contractors understand they are vulnerable to risks beyond finishing a project on time and on budget. As we are seeing more and more each day, cyber threats impact all businesses, including the construction industry. The failure to protect against these threats will cost construction companies both large and small millions in damages and reputational harm.

The construction industry lags others when investing in high-level security and keeping up with current threats, and hackers are well aware thus take advantage. According to the JB Knowledge 2016 Construction Technology Report, firms indicate that the biggest challenges they face in adopting new technology are the lack of IT staff, inadequate budgets, and both employee and management resistance. In other words, they underestimate the likelihood of hackers' interest and don't invest in enough protection, which makes it easy for hackers to infiltrate their systems. Small companies are especially oblivious and assume only large corporations are targets, but they're just as vulnerable. In fact, in 2016, hacker targeting of small businesses increased from 34 percent to 43 percent.

Due to factors like a rapidly increasing number of vendors entering the construction marketplace, high turnover, and the use of mobile offices, hackers are a pervasive threat to construction companies and the sensitive information they hold. Although it might not be obvious that the construction industry is just as reliant on technology as other industries and utilizes many tools including onboard computers, sensors, telematics, GPS, Building Information Modeling, integrated project delivery, and a variety of others. Using this kind of technology construction companies electronically store their employees' and their clients' information, including social security numbers, bank accounts for payroll, and healthcare information – all of which is worth money to hackers. Even project bids and intellectual property are at stake and can compromise a company, its vendors, employees, and clients.

Many security experts agree it's a matter of when, not if, hackers target differed sized construction companies, but there's no reason to feel powerless amid the abundance of cybercrime in the industry. To start, companies should allocate more resources toward cybercrime prevention, specifically in the areas of training, establishing IT protocols, developing response and recovery plans, and reviewing their insurance coverage.

II. Cyber Threats in Construction

Traditionally, cyber threats are thought of as the theft of employee and customer information over the internet. Given the construction industry is the largest employer in the world, the need to protect this information is obvious. The release or loss of personnel or consumer data could lead to extensive liability under a variety of potential claims, including statutory fines. In addition to securing confidential information, companies must protect against outside agents accessing control of a company's security protocols, equipment or encrypting files using malicious software.

a. Examples of Breaches and Potential Threats of Future Breaches

In May 2013, Chinese hackers stole floor plans, server information, and security system designs from an Australian prime contractor. Fearing the risks of compromised physical and network security, the contractor incurred additional costs of $132.6 million in project delays and costs to rework the various components that had been stolen.

In December 2014, a German governmental office reported that a steel mill suffered massive damage when malware prevented a blast furnace from being properly shut down. Hackers gained access to key technology within the company, which eventually allowed them to control the production line.

Take, for instance, Turner Construction in Seattle. In 2016, the company fell victim to a major phishing scheme that exposed the Social Security numbers of 566 current and past employees across the state. According to the Washington State Office of the Attorney General's website, an employee mistakenly forwarded private information to a fraudulent email address, which led to a companywide breach.

In addition to the potential legal ramifications, there are other costs that are often overlooked. For example, a company's insurance premiums could go up significantly after a cyberattack. Companies may also experience a drop in new business or the loss of existing business due to poor public perception. Further, the damage to a company's reputation and trustworthiness may have unforeseen consequences.

b. Liability to Customers for Loss of Confidential Data

In today's litigious society, businesses can be assured that at some point some customer, whether an online or in-store patron, will bring suit for perceived wrongs. And in this new age of increased interconnectedness, one type of wrong is particularly likely to give rise to lawsuits – a company's failure to protect confidential customer information from theft by cybercriminal (e.g., hackers stealing credit card numbers). Companies can anticipate such suits becoming increasingly common as consumers become ever more aware of the potential risk and real-world losses associated with cyber-theft. A company's exposure is further increased by the availability of class action lawsuits and their prospect for significant damages, litigation costs, and adverse publicity.

Customers suing for theft of their confidential data, such as credit card information or customer profiles, may claim that the company breached express or implied contractual obligations by not safeguarding the data properly. Absent a preexisting contractual relationship, customers alternatively may seek to recover compensatory and punitive damages based on a tort theory of negligence. To make out a claim of negligence, customers would argue that the defendant-company owned them a duty of

care, that the company breached this duty by not safeguarding the customer data stored on its network, and that the breach proximately caused the theft and accompanying loss. Although the thief's intervening act presents a problem in proving that the business's protection systems caused the customers' harm. Plaintiff-customers might attempt to overcome this difficulty by arguing that computer hacking is foreseeable in light of high cyber-crime rates and wide-spread awareness of these rates.

Companies also may face legal liability in instances where the customer information is not stolen directly from their network, for example, liability may arise if a company shares customer data with a non-secure source from which the data is then stolen. Similarly, a company's failure to take steps to prevent wrongdoers from setting up web sites that are misleadingly similar to that company's site may give rise to liability if customers then erroneously transmit confidential data to the masquerading site. In one recent case, cyber-criminals obtained financial data from bank customers by setting up a web site with a name almost identical to the bank's name, prompting the Comptroller of the Currency to recommend safeguards that banks should adopt to prevent similar occurrences. Now that such standards have been announced, the failure of a bank, or even another, to adopt these or similar safeguards may leave a company unnecessarily vulnerable to claims by customers of, among other things, breach of contract and negligence.

c. Liability to Other Companies for Business Loss

Companies may also face liability exposure if a cyber-crime committed against them somehow causes business loss to another company. For example, companies could face contractual liability if a cyber-crime renders them unable to fulfil their contractual duties to another company, either because of lost data or temporary service stop-pages.

Additionally, companies may find themselves the subject of multiple civil suits brought by a myriad of third parties if the company's computers are compromised as part of a directed denial of service ("DDOS") attack. In such an attack, a hacker accesses the inadequately-secured computers of one company and uses them to send voluminous traffic (e.g., e-mail) to another company's computers, thereby overloading the second company's systems. The affected company may then attempt to recover its business losses by suing based on a theory of negligence against the company whose computers were used as instruments in the attack.

Fortunately for a defendant company, plaintiff companies are burdened not only with causation problems (much like those discussed earlier in relation to customer claims) but also with demonstrating that the defendant owed the plaintiff-company a duty of care and/or that the plaintiff-company was a foreseeable victim of the defendant's negligence. Nevertheless, targeted companies in the end may prove successful in undermining claims for business loss, the costs of litigation and the risk to both reputation and public image may themselves be damaging enough to render a finding for the defendant little more than a hollow victory.

Other potentially cognizable claims for a business loss include claims against a company whose computers were used to spread viruses or other malicious code as well as claims by companies to recover losses suffered from accepting seemingly good credit card numbers which, in fact, had been stolen from another company.

III. The New World of the IoT

In addition to these types of "traditional" hacking threats, cybersecurity risks continue to evolve and become more complicated every day. Some of these new threats are driven by the development of a phenomenon known as the Internet of things, or IoT. The IoT is most basically defined as the interconnection of devices with on / off switches to the Internet and each other. Many or most IoT devices

were designed for convenience, not security, and as a result can easily be hacked. They were not designed with robust protections against malicious code, or the capability to be easily patched. As Bruce Schneier, a leading technologist, has said, "the result is hundreds of millions of devices that have been sitting on the Internet, unpatched and insecure for the last five to ten years". Here are just a few recent examples of vulnerabilities. First, many home security systems are not especially secure. White hat hackers have made their way into Comcast Xfinity system the SimpliSafe alarm systems. (White hat hackers are also referred to as "ethical" hackers. They find weaknesses in systems, for fun and profit. So, when they find one, they reveal or sell it to the affected company or the government. Or, if they prefer glory, they give it to the media or reveal it at a tech conference. One of the highest profile conferences is called, incongruously, the Black Hat conference. There is a loosely affiliated group of reputable white hat hackers called We Are the Cavalry, in which it's good to have some contacts.)

Since the IoT is estimated to be 20 billion or more devices within 3 years, and can be combined with malicious software, IoT poses one of the most challenging risks for contractors to protect against. The technology included in today's commercial buildings clearly opens this avenue of risk. A centralized computer control center, typically employed in new buildings, controls and maintains the systems that are vital to the operation of the building, e.g., power, elevators, HVAC, lighting, and security. What happens if a hacker gains control to one of these systems, let alone all of them? What if a hacker simply utilizes an IoT attack to overwhelm a building's computer systems? In either scenario, at a minimum, significant disruption would occur.

Worse, the health and safety of those within the building could be jeopardized. A hacker may utilize ransomware in combination with an IoT attack to take over control of the building and hold it and possibly the occupants "hostage" until a ransom is paid. The first significant IoT attack happened in October 2016 when a major web hosting company was attacked through the IoT, causing the host site to crash. The attack did not steal information, it simply caused the site to crash. But, that crash caused world-wide disruption across the Internet. Hackers used malicious software to access a hundred thousand common household devices — web cameras, fitness trackers, DVR's, smart TVs, and even baby monitors — to flood the hosting company's servers with incredibly high internet traffic. This attack showed that everyday items can be hacked and controlled by cyber criminals and then used against anyone else. As we have all seen in recent news, the WannaCry cyber attack impacted businesses across the globe. Days after the attacks, hospitals were still left feeling its impact with continued appointment and planned operation cancellations, and delays in service. We should expect to see these types of attacks increasing in frequency.

IV. Privacy and Data Security through IoT

IoT devices most often store information in unencrypted form, which can be improperly accessed or inadvertently transmitted.

The focus of cyber liability so far has been on data breaches resulting in the loss of personally identifiable information and private health information. Most of the litigation concerns whether consumers, or banks issuing debit or credit cards, have causes of action against retailers or other hackees. There is virtually no definitive law. So far, plaintiffs have not had much success seeking recovery in claims based on breach of contract, invasion of privacy, unjust enrichment and bailment. They have had more success, at least avoiding motions to dismiss, in claims based on common law negligence and under consumer protection statutes.

The government is active in this area. The Federal Trade Commission conducts enforcement proceedings based on the position that the lack of reasonable security measures to protect consumer data constitutes an unfair or deceptive trade practice under Section 5 of the FTC Act. It has moved against companies who lose information through "inadequate" data security practices.

In 2014, the FTC extended its oversight to IoT consumer products, commencing a proceeding against, and ultimately reaching a settlement with, TRENDNet, which sells Internet-enabled surveillance cameras used for home security and baby monitors. The FTC alleged that because of software defects, hackers were able to easily access and post hundreds of live feeds, and that the feeds constituted private information. The matter was resolved by a consent order.

The FTC subsequently held workshops on the IoT and is expected to continue to play a leading role in enforcement. In January 2015, it released a staff report making non-binding recommendations for best practices, including building security into the devices at the outset.

In February 2016, the FTC (resolved another administrative complaint. This one was against ASUSTeK Computer which is a Taiwanese hardware manufacturer that sells, among other things, routers. ASUS claimed its routers had superior security. Not so. Researchers demonstrated that it was possible to commandeer consumers' Web traffic. Among other flaws, ASUS set the same default login for every router – both the username and password were "Admin", and users were not required to create a unique set of credentials. Its cloud services were also insecure. The matter was resolved by a consent order that requires, among other things, that ASUS's security program is subject to audit for the next 20 years. The Order also is worth looking at, as it operates as a useful checklist of steps that could reduce the risk of liability for other companies.

Increased vehicle connectivity may yield substantial safety benefits. Consider the example of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) (together, "V2X") communications. The Secretary of the Department of Transportation recently explained: "Vehicle-to-vehicle technology represents the next generation of auto safety improvements, building on the life-saving achievements we've already seen with safety belts and air bags. By helping drivers avoid crashes, this technology will play a key role in improving the way people get where they need to go while ensuring that the U.S. remains the leader in the global automotive industry." Additionally, with Bluetooth and Wi-Fi increasing connection to smartphones and tablets through Apple Car Play and Android Auto, cars are more connected than ever before to third-party devices and the outside world.

The issues related to connected vehicles are not going away any time soon, as the industry moves towards increasingly connected and autonomous vehicles. OEMs as well as new players in the automotive field such as Apple and Google are or are rumored to be building fully autonomous vehicles for sale to the public in the years ahead. And there will be a market for such vehicles – Uber's CEO has reportedly stated that Uber will buy all of Tesla's autonomous vehicles if Tesla meets its goal of producing half a million of them by 2020. The industry is clearly moving toward increased connectivity and automation.

Increased connectivity, however, raises the possibility of unauthorized access to a vehicle and the data it stores. Although many of the perceived risks remain, for practical purposes, largely hypothetical, security researchers' attention to these issues continues to build. There are "hackathons" where students are invited to try to hack into vehicle systems, in attempt to demonstrate vulnerabilities. Other public "white hat" hacking demonstrations, such as the "Stunt hack" of a researcher's vehicle, hacks of the OnStar app, a Tesla vehicle, and a "dongle" plugged into a Corvette's OBDII port, have increased public awareness of these issues.

Likewise, Congress is focused on vehicles cybersecurity and has been engaged in ongoing discussions with many OEMs and suppliers. From a litigation perspective, there are two pending class action lawsuits against OEMs for alleged cybersecurity issues: one against Ford, GM, and Toyota (*Cahen et al. v. Toyota Motor Corporation et al.,* case no. 3:15-cv-01104 in the U.S. District Court for the Northern District of California), and another against FCA (*Flynn et al. v. FCA US LLC et al*., case no. 3:15-cv-00855 in the U.S. District Court for the Southern District of Illinois).

Meanwhile, the headlines bombard consumers every day with the latest privacy and data security missteps in other industries. 2014 was declared the "Year of the Data Breach" by 20/20 and several other organizations, and many companies including Target, Home Depot, and Sony faced high-profile breaches. Media attention on these hacks likely has raised public awareness about cybersecurity hacks and related risks. Penalties for privacy violation can be expensive, and damage from a breach or privacy violation takes a long time to repair. According to the Ponemon Institute, it takes about twelve months for a company's reputation to recover from data breach and successful hacks may result in a loss of consumer trust.

V. Building Information Modeling

Building Information Modeling (BIM) is an important step toward total integration of Information Technology into the world of Professional Construction Management, Architectural design, and the full development of digital project delivery process. As with any emerging technology, many issues regarding liability are now beginning to unfold as this technology gains a foothold and consequently a stake in the productivity and profitability of construction firms, subcontractors and owners representatives. The obligations associated with professional practice such as accuracy, punctual decision making, timely sharing or submission of information and the collaboration requirements of various professions do not simply disappear with the implementation of BIM. What exactly is timely submission of information? What is accuracy? What is the proper and acceptable form of communicating the information contained in a BIM project? What, if any, are the obligations of the software developer other than properly functioning software?

BIM, as we now know it, is a process by which buildings and other construction projects are designed, built, operated, and maintained. Some long-term plans call for BIM to be utilized in the deconstruction of these same buildings. Within this process and certainly a large component of it is a software platform that will create or "model" the project under commission by the owner. The model is outwardly a three-dimensional (3D) representation of the project. Typically, the software has the ability for the modeler to view the model from any vantage point, including a walk-thru of the project. So far it sounds as if the only component of BIM is the software used to model the project. If this indeed were the case, the potential for BIM as an emerging technology and process would be severely restricted and its use limited to the design professional.

Two additional dimensions have been incorporated into BIM related software to represent two very important aspects of any construction project: time and cost. These are currently being referred to, respectively, as the fourth and fifth dimensions (4D & 5D). How does time affect a construction project? Time, as it is routinely stated, is money. Project owners develop project feasibility plans based on occupying a building or utilizing a project from a certain point in time, typically due to the fact that this new building, which is considered a tool, will generate a certain amount of income due to the location, size or features of the building. If this projected time frame is not realized, the owner incurs financial losses and routinely looks to the contractor for reimbursement of those losses or damages. Proper scheduling or time management of the project is vital in meeting these contractual project completion dates. The ability to look forward in time and accurately predict the status of the project, anticipate any potential schedule delays and make alternate plans has now been realized with the incorporation and development of the fourth dimension of time into the BIM process.

VI. Developing a Cyber-Security plain to Mitigate Exposure

A key strategy for managing the legal risks associated with cyber-crime is to develop an effective cyber-security plan. Such a plan must go beyond the technical measures now emphasized by industry analysts. Although technical protections such as firewalls and intrusion detection systems are critical, they should be combined with non-technical safeguards to afford companies more complete protection against the various potential losses that could result from cyber-crime. Yet, all too often companies are not taking these steps. As the Deputy Chief of the Justice Department's Computer Crime and Intellectual Property Section recently observed; "the victims…have no response plan in place; they don't involve their lawyers, and all too often, they don't involve law enforcement."

What follows is a list of considerations essential to mitigate potential legal exposure from cyber-crime. To the extent possible, these elements should be incorporated into a written cyber-security plan, which should be reviewed and updated at least annually. Developing and implementing such a plan not only encourages internal compliance, but also serves, in the event of legal action, as valuable evidence of a company's care to develop a complete cyber-security system.

Determine Cyber-Security Needs

Determining a company's precise cyber-security needs is a dynamic multi-step process in which company executives, managers, IT staff, and lawyers should be involved. First, companies should identify the cyber risks to which they are susceptible. To this end, a complete review of the network system and all potential architectural and technological vulnerabilities must be conducted. Second, companies should fully understand the applicable legal standards of care as well as any relevant regulatory standards. Third, companies should identify the costs associated with a network breach, including repair costs, business loss, and litigation expenses. Fourth, companies should assess the costs of adopting the various technical safeguards intended to plug identified system vulnerabilities.

Once companies complete these four steps, they must balance the attendant costs (including legal liability exposure) of a network security breach against the costs of adopting cyber-security safeguards. In order to perform this balancing test, companies must ensure that they have the expertise to select from among the range of applicable standards of care to which they might be subject and to evaluate whether the safeguards they intend to adopt actually comply with these standards.

In determining standards of care, companies also must consider any applicable regulatory standards. This too requires considerable expertise. For example, certain health care organizations are required to adopt measures to protect patient health information and to detect and "mitigate" damages caused by computer breaches. Likewise, financial institutions are required to protect consumer data in a manner commensurate with "the size and complexity of the bank and the nature and scope of its activities."

Assess Whether to Outsource

After a company has determined its precise cyber-security needs, the company then must decide whether it can handle its own cyber-security needs or whether it must outsource them to a third party. For many smaller companies, particularly those that lack the resources to hire in-house network security experts, outsourcing is a necessary option. Outsourcing, however, t not without risk, including loss of control over data, proprietary information, or other closely-held material.

For this reason, companies—both large and small—must not only exercise great care in selecting the contractor to whom security needs will be outsourced but also must ensure that the contractor, once hired, maintains an adequate level of security to meet the outsourcing company's cyber-security needs.

To that end, companies should negotiate a contract that provides the outsourcing company with the practical security safeguards and legal liability protections that are in its interests while also giving the contractor incentive to perform at a high level.

Adopt Technical Security Measures

Regardless of whether a company chooses to outsource network security, a comprehensive cyber-security plan should also include detailed descriptions of the technical safeguards to be adopted and the procedures for implementing those measures. Industry analysts regularly discuss the availability of various security technologies, and for this reason, these measures are not addressed in this article. Suffice it to say that common safeguards include such measures as maintain firewalls to regulate incoming traffic, using encryption software to protect the transmission of data, and monitoring and filtering of both incoming and outgoing traffic to prevent the company's computers from being used in DDOS attacks.

Monitor for New System Vulnerabilities

Technical safeguards are only adequate when they are combined with protocols for both monitoring their ongoing effectiveness and plugging identified holes. For example, computer experts can monitor current industry trends and developments in order to identify further improvements that should be made to a company's technical safeguards. Today, a significant breadth of resources exists for upgrading technical safeguards including web sites operated by government centers (such as the National InfraStructure Protection Center); private organizations, (such as the Computer Security Institute), vendors (such as Microsoft), and peer networking companies. Incorporating provisions detailing the use to be made of these resources into a cyber-security plan is critical because failure to adopt even basic safeguards like installing patches against known problems can open companies to substantial risk of liability.

In addition, depending on the nature and size of the company, the cyber-security plan may include procedures for periodically testing the security of a company's computer system. Computer experts, whether in-house or retained, may test the effectiveness of a company's security measures by attempting to infiltrate its network system. If holes in the system are identified, these same experts can take the necessary steps to reconfigure the out-of-date firewall or tweak the lagging intrusion detection system.

Manage Employee Use

Many cyber-crimes are perpetrated by current or former employees. To limit this risk, companies should adopt appropriate policies and procedures related to the hiring, training, oversight, and termination of employees. Hiring procedures should include proper background checks and in requirement that certain employees sign confidentiality agreements. Employee training should include education on company procedures and methods for promoting cyber-security-related regulations.

Oversight should include ensuring that only certain employees have access to confidential information, monitoring computer activity for wrongdoing, ensuring that employees follow proper security measures (such as maintaining confidentiality of and regularly changing passwords), and providing employee with reminders of their security obligations (such as through the use of policy banners at the point of system log-in). Termination procedures should, among other things, ensure that former employees' passwords are immediately disabled upon departure and that these employees are otherwise blocked from future access to the company's computer systems.

Use Contracts to Limit Liability

Where possible, contracts with customers and business partners should be negotiated to contain provisions that serve to limit a company's liability for cyber-crimes directed against its own network as well as cyber-crimes impacting company data residing on the network of a contactor. One popular provision limits a company's liability for stolen data to instances where the company recklessly stored the information on its own network and/or recklessly shared the data with a contractor who then failed to protect it.

Develop an Immediate Response

A key to developing an effective cyber-security plan is determining ahead of time what to do if a cyber-attack occurs. Such a protocol should consider basic elements, such as how to identify a cyber-attack, steps to be taken to contain the attack, and methods for preserving evidence of the attack. The protocol also should include guidelines on maintaining records of the breach for internal purposes (e.g., to plug the exposed vulnerability) as well as for external purposes (e.g., to provide to law enforcement if requested). To do this, companies must possess the technical means to log activity and to take basic steps to preserve evidence, as even the simple act of turning on a computer after a hack can destroy valuable evidence.

Develop a Plan to Report Hacks to Potentially Affected Parties

Companies also should have an established protocol for identifying potentially affected parties, including customers, business partners, and investors. The protocol should include a list of considerations (e.g., regulatory requirements, contractual obligations, consequent harm to party if not reported) guide the decision of whether and when to notify affected parties. Although proper notification can avoid or limit liability while at the same time maintaining goodwill, untimely or otherwise inappropriate notification can expose the company to further risk of liability.

Develop a Plan to Notify Law Enforcement

Similarly, a comprehensive cyber-security plan should contain protocols for determining whether to notify law enforcement, companies must balance competing concerns. Some companies may be reluctant to notify law enforcement of every network breach because of perceived publicity concerns, risk of liability, and the potential for delays and costs should law enforcement initiate an investigation. However, some of these concerns may be overstated and, in some instances, may fail to take into consideration the benefits of notifying law enforcement, including preventing further attacks and reducing potential tort or contract liability.

If the decision is made to notify law enforcement, then companies must know how to go about reporting the hack. For this reason, a cyber-security plan should include detailed information on the appropriate law enforcement agency to contact, how to work with that agency to limit any damaging publicity, and how to cooperate with the agency in a way that protects the company's interests, including the privacy interests of third parties.

Finally, a complete cyber-security plan should contain guidance on identifying when regulatory reporting requirements are triggered by a hack attack or other cyber-crime. Failure to comply with such reporting requirements can lead to the imposition of civil money penalties as well as unwanted regulatory oversight and negative publicity.

Asses Rights Against Other Parties

Knowing one's obligations to third parties and government agencies is only one piece of the cyber-security puzzle Companies must also be aware of their legal rights. This includes knowing the avenues available for obtaining information about the hack from other companies, such as Internet service providers, and other cyber-crime-related loses from partners, vendors, and third parties.

Secure Insurance Coverage

Far too many companies fail to evaluate whether their existing insurance policies cover most, if not all, of their cyber-crime-related exposures. Rather than simply renewing existing, possibly outdated, policies, prudent executives, in close consultation with legal counsel, should evaluate their company's insurance needs and obtain policies that address those risks. Companies should examine carefully the coverage provided by traditional policies (such as commercial general liability), and consider the benefits, if any, of specialty products, designed by insurance companies to cover risks associated with cyber-crime. The goal should be to create a seamless blanket of policies providing coverage for foreseeable cyber-crime risks.

VII. Conclusion

Contractors and related trades have a new threat that must be addressed. This threat is cybercrime. Today we live in a society where a construction project can literally stop cold with a ransome-ware attack. This threat needs to be communicated to employees of contractor's, clients, as well as claims adjusters who are handling claims for the respective construction companies.