CYBER LIABILITY INSURANCE: GROWING CONCERNS FOR GENERAL CONTRACTORS, OWNERS AND SUBCONTRACTORS

BY ROBERT F. MOGLIA, JR., CIC, LIC
PARTNER
CAPITAL INSURANCE GROUP

Cyber-attacks on individuals, corporate America and the federal government are increasing in frequency and size, and contractors are not immune. Contractors are increasingly at risk for direct cyber fraud from internal and external sources (first party liability) and while performing work at clients' premises and unknowingly creating cyber exposures to the client (third party liability). The Congressional Research Service Report surveys of 2013 estimate the losses due to cyber-attacks alone at $20 billion. This figure is now considered low in view of the Target Brands, Inc., Home Depot and federal government attacks (Office of Personnel Management with over 20 million federal employees impacted, according to Reuters and CNN in July 2015). The 2013 cyber-attack on Target Brands, Inc. was one of the largest single attacks to date.

Cyber attackers were able to access Target's systems using network credentials stolen from a Pennsylvania mechanical contractor with 120 employees. Initially, cyber analysts believed the mechanical contractor was working monitoring systems for energy efficiencies and gained access in this manner. After more analysis, it was determined the contractor was doing routine work on electronic billing and project management. Obviously, these are routine tasks for contractors but it was the performance of these services that allowed the hackers to penetrate into the Target systems.

This has become a very interesting topic in view of our global economy and interconnections via cyber space. Hence the development and need of cyber liability insurance, both first party and third party. Cyber liability and resulting property damage from a cyber-attack is a standard exclusion under all general liability policies. As stated, cyber incidents are multiplying in frequency, scope and size at an alarming pace for corporate America. In general, risk management assessments, evaluations and resources devoted to cyber protection does not remotely match the skill set, resolve and stealth of the cyber criminals. Certainly, for the small to mid-size commercial contractor, cyber security does not receive the strategic investment it deserves. In 2014 the Price, Waterhouse, Cooper, PC, "Global Economic Crime Surveys" found that 7 percent of United States organizations lost $1 million or more due to cyber-crime incidents in 2013. Furthermore, 19 percent of United States entities reported financial losses of $50,000 to $1,000,000, compared to 8 percent world-wide.

If outside cyber-attacks are not enough of a threat, attacks from the inside account for 28 percent of criminal cyber activity. This includes former employees, disgruntled employees, ethical and honest employees, let alone contractors and service providers. Typically, the economic case of an attack from the inside is greater than outside involvement. Often, the insider incidents are created from unknowing use of social media, loss of smartphones or laptops. (Stolen laptops are a common source). A thorough employee education for use of electronic devices is key to mitigating this risk (mobile security strategy). For more information and risk assessment guidelines for cyber security, please refer to the Commerce Departments "National Institute of Standards and Technology" NIST.

The basic framework of the NIST funnels into five ongoing functions:

IDENTIFY • PROTECT • DETECT

RESPOND • RECOVER

The increasing vulnerability to inside and outside cyber-attacks and the difficulty of adequate security will only lead to more litigation and expensive law suits. This again points to the important consideration of cyber liability insurance (liability limits of $1 million are common).

Another consideration for the purchase of cyber liability insurance is to remove the gray area of "tangible vs. intangible property damage." Property damage is a key component of every contractor's general liability insurance. All contractors have the exposure to property damage liability, and certainly absorb even more exposure with the contractual property damage language required by owners and general contractors, i.e. hold harmless agreements, waivers of subrogation, primary and noncontributory wording and additional insured status. Many contractors make the assumption they are insured for "all property damage" by the general liability policy. While most contractors will find the appropriate property damage coverage in their insurance policy (at least to satisfy the contractual requirements of their owner or general contractor) they have only satisfied part of their property damage exposure.

The appropriate general liability policy will respond to claims of "tangible property damage." For example: A mechanical contractor, while completing a project for a local school, installs a pressure release valve incorrectly. As a result, under pressure, water is erroneously released and floods the school gymnasium. The resulting damage to the wood floor would be insured to the policy liability limits as it is "tangible property." "Tangible property" as defined must be able to be touched, seen or have measurable economic impact such as consequential damage (loss of rental income, loss of revenue).

Now let's move on to the "intangible property damage" (the gray area). For example: An electrical contractor, while installing a commercial light fixture, inadvertently cuts a line to the file server creating an erasure or corruption of data to the client. Obviously, the client will be looking to the electrical contractor for relief for recreating the lost data. The client estimates it will take $150 per hour to restore the lost information, and 20 hours total time. A claim is submitted to the electrical contractor's insurance company. However, under some general liability policies, loss or corruption of data may be construed as "intangible property" (you cannot touch it, feel it, or see it) and could be excluded; and hence the claim denied. Case law for intangible property damage claims is inconsistent and at this juncture there is no definitive case law on the subject.

Again, the answer is that contractors should do a risk assessment and evaluate their exposure and consider the purchase of cyber liability insurance.

Increasingly, contractors need, or are required to, have cyber liability policies as part of their insurance portfolio (hospital risk management guidelines now require contractors on their premises to carry $1 million minimum of cyber liability). Examples of claims come in all forms; on a small scale an electrical contractor performing commercial work on the client's premises (rearranging the low voltage wiring for an office remodel) unplugs the firewall and neglects to re-plug before end day. As a result, hackers are able to access the system and obtain sensitive client information. This would be considered cyber breach and would be considered excluded from the general liability policy, but would be insured by third party cyber liability insurance.

Cyber third party liability policies also insure against alleged attacks and cyber theft of copyright, trademark, domain name, trade name and the consequential reputational damage and loss of customers. Cyber third party liability policies also respond to alleged patent infringement and theft of trade secrets.

The contractor, through the simple theft of a laptop or unplugging the wrong line, can expose their clients to these types of cyber damages. The typical cost of a cyber-liability policy including third party coverage is $2,000 to $2,500 for a contractor with under 50 employees, and $5,000 to $15,000 for contractors with 50 to 500 employees. Cyber liability evaluations and assessments should become an integral part of every contractor's overall risk management evaluation.

ABOUT THE AUTHOR

Bob Moglia is a certified insurance counselor based in Bloomfield Hills, Michigan and a partner with Capital Insurance Group, a leading business insurance agency in Southeast Michigan. He is a past contributor for CAM Magazine.