PENTARISK PERSPECTIVES

PentaRisk Insurance Services Newsletter - Volume 5 Issue 5 July 2018

Cyberattack - Everybody is at Risk

With online payment systems, certified payrolls and sharing of specifications and bid documents, contractors are exposed to cyber losses that are not covered by traditional insurance. Add on cyber-ransom and you really have several areas of concern. Not only do you have to contend with your own records, you have to be concerned about your clients' records too.

- If you use credit or debit cards to accept payment from customers, you are at risk.
- If you have your employee's personal information stored online or in unlocked file cabinets, you are at risk.
- If you bank online, you are at risk.
- If you have Intellectual Property of your customers, such as drawings or specifications, you are at risk.
- If you have log-in credentials in order to access customer systems, you are at risk.
- If you store other personally identifiable information, such as Social Security numbers, names, addresses and driver license numbers, you are at risk.

A new form of crime in America is cyber-ransom. It has been spreading fast and it is global. One antivirus firm reported that Internet users visited ransomware-infected sites 18 million times in a single six-week period. SentinelOne's *2018 Global Ransomware Study*, conducted by Vanson Bourne, found that Construction was the second worst hit industry (65%), behind IT, Technology and Telecoms (67%).

Ransomware is dangerous because it infects your company's system and then encrypts all of your locally stored files behind a wall of encryption. The attacked victim must pay a fee to the hackers to get their files back, or attempt to break the encryption themselves. Your company's money is involved for either task, and traditional insurance will not cover the loss.

What about your clients? Contractors have exposure for possible data breaches. This is due to the fact that they are often on the ground level of all new construction projects. Since contractors and their clients are more and more interconnected by technology, paper files are no longer a viable defense. Attacks on your system can disclose very sensitive, propriety information relating to your clients. Once you have a breach, there could be potential third party liability. Ouch! You now have to pay a settlement for someone else's hacking crime that created problems for your client's business. Again, not covered by traditional insurance.

Malicious advertisers take advantage of small-business websites using a specific type of search engine optimization known as "spamdexing." Before you know it, you are advertising for people not connected to your business.

Recent real-life incidents in the construction industry include the following scenarios:

1. It is late on a Friday, and your employees are finishing up after a long week. Eager to start the weekend, one of your trusted workers leaves behind an unlocked company laptop with instant access to hundreds of bid documents, your secured network and e-mail records from online payment systems. A third-party vendor's worker happens to stay late that day and notices the laptop and takes it home, stealing information. When you figure out what happened, you start the forensic process determining what was actually compromised, and notify all of your clients of the mistake. One of them sues you for failing to safeguard their information and the trusted reputation you worked so hard to build is destroyed in an instant.

2. One of your employees is checking business e-mail from a familiar company. It is complete with logo, message and file attachment. Curious about the file, the employee opens it. Immediately you are locked out from accessing your network, database, payroll, invoicing and other sensitive files. The seemingly authentic e-mail message is in fact a malicious ransomware attack. A ransom of $20,000 is demanded as you are left to figure out what to do. A specialist is brought in and after a few days, the cost exceeds the ransom amount. Your business loses critical revenue and you are left to fully fund the mess created from an honest mistake.

It is not a question of ***if***, but ***when*** the next cyberattack will happen. The truth is that the volume of attacks is increasing, and their speed, scale, sophistication and success in evading detection will likely keep ransomware among the top threats in 2018 and beyond.

Practical Steps to Take:

1. Meet with your IT experts to ensure you have the latest antivirus and firewall protection.
2. Use encryption software to transmit sensitive data.
3. Change employee login passwords 2-6 times per year.
4. Purchase cyber insurance.

The good news is you can protect yourself by purchasing cyber insurance coverage. Premium ranges from $2,500 to $10,000 per year, for $1,000,000 in limits with a $10,000 deductible.

First Party Cyber Insurance will deal with the following:

Costs to notify affected parties via letter, and to reissue credit/debit cards

- Credit remediation expenses (credit freeze, hold and watch)
- Crisis management expenses and public relations expenses
- Lost revenues, including business interruption
- Costs to improve or upgrade IT security systems
- Reputation damage, including loss of customers

Third Party Liability (claims against your company) Cyber Insurance will deal with the following:

Failure to prevent unauthorized access

- Error or omission in IT security practices and procedures
- Misappropriation of digital assets or personal information
- Failure to prevent a Distributed Denial of Service (DDoS) attack
- Failure to prevent transmission of malicious code/malware/viruses
- Copyright, trademark, domain name, trade name, trade dress claims

In 2017, 20% of our clients were impacted by cyber issues/attacks. None of these losses exceeded $100,000. Some of our client's bore the costs because they had not procured cyber insurance. This could be a serious financial concern to be reckoned with if you have no coverage.

NOTE: In addition, think about a Social Engineering Fraud coverage too. It addresses confidence schemes that intentionally mislead an employee to send money or divert a payment based on fraudulent information that is provided to the employee in a written or verbal communication through e-mail, fax, letter or a phone call. Over 100,000 people a day are influenced by social engineering attacks, a huge number.

Contact Jim Untiedt at 408.418.2734, juntiedt@pentarisk.com, or your PentaRisk broker or account executive for more information on cyber insurance coverage. Visit our website at http://pentarisk.com/.