akerman

Practice Update

Cybersecurity and Privacy Risks for the Construction and Real Estate Industries

September 9, 2022

By Christy S. Hawkins

In July, WCOE's Regional Director – West (Southern), Brenda Radmacher, Esq., presented an extremely timely and informative webinar regarding cybersecurity risks and best practices for construction firms. The below Practice Update highlights a few key takeaways from the presentation by Brenda, her colleague Christy Hawkins, Esq.; and industry experts, Danette Beck, Head of Industry Verticals & National Construction Practice Leader, USI Insurance Services and Michael Corcione, Partner, Global Cybersecurity & Privacy Risk Management Lead, HKA.

The construction industry has experienced an amazing evolution in recent years thanks to the rapid adoption of new technologies. While all of this new technology has the potential to make companies more productive and more efficient, it, like all new tools, also creates new risks and liabilities. The modern construction firm must be as vigilant and prepared for cyber threats as they are of jobsite dangers. The first danger to overcome, however, is the misconception that hackers are not interested in construction companies or smaller businesses. This simply is not true. Cybercriminals can now cast a very wide, indiscriminate net with their cyberattacks, entangling companies they were completely unaware of beforehand. More disturbing still is the fact that the cliché of hackers living in

Related People

Christy S. Hawkins

Related Work

Construction

Data Privacy and Security

Real Estate

Related Offices

Dallas

Los Angeles

their parents' basements has been replaced by sophisticated state-sponsored hacker teams. For example, there is evidence that hackers backed by the Russian government have infiltrated American government agencies and Fortune 500 companies as part of its war with Ukraine, as noted in a recent *New York Times* article[1]. While these attacks have mostly targeted specific agencies and companies, experts note that there is often "spillover," with the malware used in the attacks spreading beyond the original targets.

It is clear to see how a construction company working on a major infrastructure project or sensitive government installation could be a prime target for hackers. And it is just as clear to see how a company simply going through day-to-day business could become ensnared in a wide-reaching fishing expedition. But with effective planning, due diligence, and vigilance those risks can be greatly reduced.

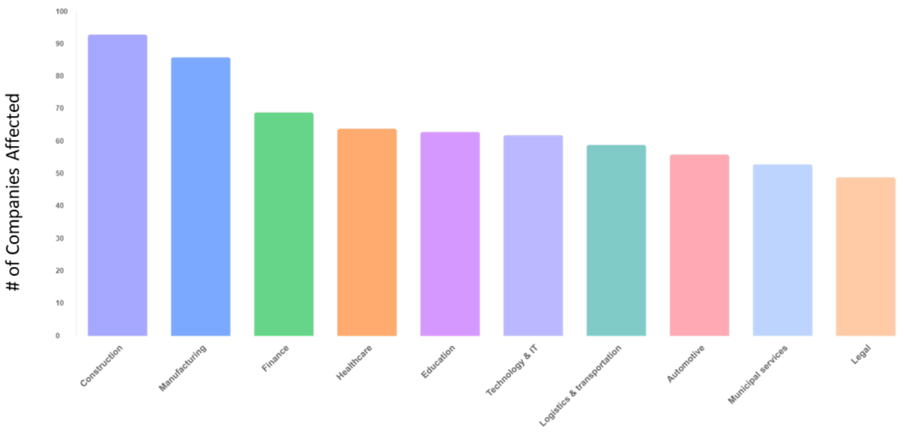
Why Cybersecurity Matters to Construction Firms

At the most basic level, cybersecurity should be a priority for any construction firm because there are laws you are likely required to comply with. For example, the California Consumer Protection Act (CCPA) became law in 2020, and applies to for-profit entities that collect personal information from California residents and meet any of the following thresholds: (i) At least $25 million in gross annual revenue, (ii) Buys, sells or receives personal information about at least 50,000 California consumers, householders, or devices for commercial purposes or; (iii) Derives more than 50% of its annual revenue from the sale of personal information.

And that is just the tip of the iceberg. Since the CCPA became law, a growing number of states are considering comprehensive privacy laws. In 2022, 29 states considered data privacy legislation.

Even if your company is not subject to data privacy laws like CCPA because of your size or where you do business, you are still vulnerable to cyberattacks. This is why the Cybersecurity & Infrastructure Security Agency recommends organizations of any size "adopt a heightened posture when it comes to cybersecurity, to protect their most critical assets."2

Earlier we mentioned indiscriminate wide-net cyberattacks, the most common of these are email phishing scams. For those not familiar, this is when cybercriminals use email messages to obtain data from individuals or gain access to your network. These email messages are most often sent by the thousands to addresses, which are often obtained through equally nefarious means. A 2019 study conducted by cybersecurity firm KnowBe4 highlighted just how vulnerable construction companies are to phishing attacks. They found "those who work in **construction are the most susceptible to phishing attacks among small-to-medium-sized businesses and the second-most likely to fall for a phish among large corporations**."3 The study, "Phishing by Industry 2019," surveyed nine million users across 18,000 organizations with simulated phishing security. Other industries found to be most vulnerable to phishing include hospitality, finance, and healthcare.



Source: Ransomware analysis | NordLocker' | NordLocker

The dangers of a phishing attack are numerous, but ransomware attacks are becoming some of the most common. A ransomware attack is most often accomplished when an employee falls victim to a phishing email, unknowingly providing malicious software access to the company's network. This malicious software then locks you out of your network or steals information, controlling either until a ransom is paid. Though rarely publicly divulged, these attacks have become very common and victim companies often have little recourse other than paying the ransom.

And just like other aspects of your business, your cyber risk extends beyond your organization as well. The interconnectedness of construction projects with the supply chain provides further areas for exposure to cybersecurity issues. Specifically, vendors, third parties, and fourth parties, can cause an exposure – you have limited insight into their controls and processes and are reliant on them.

With all this in mind, it is easy to see that as technology proliferates in the construction industry, the threat landscape and opportunities for attackers expand. There is no need to throw the baby out with the bathwater, however. With a little planning, the implementation of a few best practices, and some smart investing you can take full advantage of the latest technology available while also dramatically reducing your cyber risk.

Cybersecurity Best Practices

I. Internal Best Practices

Some practices that you can implement to manage and reduce cybersecurity and privacy risks include the following:

- Penetration Testing/Vulnerability Assessment -- Find the holes before the bad guys do.

- Increase Visibility -- Install a Security Information and Event Management system and/or enlist Security Operations Center services to monitor your systems.
- Protect Your Data -- Install Data Loss Prevention systems to prevent exfiltration or accidental data exposure.
- Patch, Remediate and Repeat -- Ensure that your patch management system can detect and remediate vulnerabilities for all applications, on all your systems.
- Multi-Factor Authentication -- Adds layers of security that protects against compromised credentials by providing additional information.

Give strong consideration to cybersecurity insurance. There are a host of issues that the insurance company will ask about, so before you invest in insurance, be prepared to explain your cybersecurity hygiene and protocols. Do you have network segmentation? What about end point detection and response? Do you have 24/7 network monitoring? What type of network backups do you have in place? What third party risk management controls do you have in place?

A myriad of coverage types exist, including general cyber-risk policies, but you may need other coverage and should consult with an experienced broker to ensure you are protected. Other, additional coverage extensions include but are not limited to: Voluntary Shutdown Coverage (coverage in the event the insured decides to shut down their computer network to prevent the proliferation of a computer attack); Bricking Coverage (coverage for the replacement costs associated with computer hardware rendered useless due to a computer attack); Reputational Harm Coverage (for income loss lost as a result of adverse publicity associated with a computer attack); Overlapping Coverage (select which policy is triggered first when more than one policy overlaps); and Computer Crime (including invoice manipulation).

II. Supply chain/Vendor Best Practices

As for risk outside of your organization, the panel had the following recommended steps for construction firms to take both before and after selecting a vendor:

During Selection Process

- Establish a programmatic approach
- Identify vendor criticality and risk rating
- Conduct due diligence based on risk rating
- Review remote access to the company's network
- Evaluate data and monetary processing
- Review vendor maturity
- Evaluate contractual requirements regarding cybersecurity

Post-selection

- Conduct "tabletop" exercises (incident scenarios) that include vendors and third parties
- Implement continuous monitoring
- Ensure clear lines of communication with your vendors
- Create a vendor contingency plan

Data privacy laws extend through your supply chain, and you may be responsible. Be sure to have experienced consultants and legal advisors to assist you and ensure you are protecting your business.

III. Attack Response

If you do become a victim of a cybersecurity attack, the panel recommended the following four-step action plan:

1. Fire up your incident response plan (if you don't have one, get one now!);

2. Use the right tool for the right job (know when to bring in third-party forensics, legal, insurance);
3. Restore to a secure site;
4. Know your rights and responsibilities (what are your reporting requirements?).

The human is the weakest link and therefore, cyber and information security training programs should be relevant and current. Give due consideration and priority to ensuring you have relevant, period, and specific role-based training. Consider email phishing tests, computer based training, and internal communications.

Final Takeaways

- Cyber risk should be part of your overall enterprise risk management and should be reviewed as a key business risk at least annually.
- Monitor and measure security and availability of systems through continuous vulnerability and risk assessments.
- Train, train, train your staff via information security training awareness and phishing campaigns.
- Work with professionals to obtain the proper cyber insurance, evaluate vendor risks, and protect your systems.

Citations

[1] "Volunteer Hackers Converge on Ukraine Conflict With No One in Charge," *New York Times*, March 4, 2022

2 *See* https://www.cisa.gov/shields-up

3 "Job Security: Certain Industries More Susceptible to Phishing," *Security Boulevard*, August 27, 2019

This information is intended to inform firm clients and friends about legal developments, including recent decisions of various courts and administrative bodies. Nothing in this Practice Update should be construed as legal advice or a legal opinion, and readers should not act upon the information contained in this Practice Update without seeking the advice of legal counsel. Prior results do not guarantee a similar outcome.