



N*~~T~~ OUT OF THE WDS:**

Lumber and Building Material Suppliers
Continue to Face Cyber Threats

By Erin Selfe

Recently, newspapers and other publications have been littered with headlines about cyber-attacks at major companies. From the oil industry to agriculture, valuable information is at risk, with hackers finding new ways to access vital company information every day.

"During the last three years, the rise in attacks, specifically ransomware attacks, has had costly impacts on nearly every industry, including the lumber industry."

During the last three years, the rise in attacks, specifically ransomware attacks, has had costly impacts on nearly every industry, including the lumber industry. Cyber criminals recognize that many business owners would rather pay a ransom than forgo money to lost business or compromise their business reputation. With the rising prices and supply shortages the industry is already experiencing, stopping or slowing down production and delivery only exacerbate an already thorny issue.

Recent attacks on the Colonial Pipeline and the JBS Beef Plant demonstrate the severity of a cyber-attack. In the incident involving the pipeline, a single compromised password led the criminals to access the company's computer network. The company was forced to shut down operations, which led to fuel shortages across the East Coast, according to Bloomberg. Colonial ended up paying a \$4.4 million ransom to the criminals. In the case of the JBS Beef Plant, cyber criminals hacked into computers systems reaching from Australia to the U.S. Ransomware was used in this incident as well, leading the victims to pay \$11 million to protect consumer data and stop disruptions to the supply chain, according to the BBC.

While these two examples involve larger companies, cyber criminals are not necessarily targeting only larger companies. Instead, they target known vulnerabilities. In fact, in many cases, they do not know who they are targeting until they've successfully found a hole and breached the company's system. Then, once they're "in," they research the company to learn how best to interrupt or threaten the business—in many cases, to ultimately get the company to pay a ransom. In other words, cyber criminals are not simply targeting financial services companies and large manufacturers with significant revenue; they are casting a wide net and reeling in whichever unsuspecting company tugs on their line.

Again, the lumber industry has been no exception. In 2019, Lumber Liquidators fell victim to malware. The attack impacted company operations, including point-of-sale transactions, according to Security Week. While their employee and customer-sensitive data was not compromised, this attack lasted several weeks.



CYBER THREATS

Cyber crime has elevated to the level of organized crime with organizations complete with offices, computer systems, and paid staff, some of whom don't even realize they are engaged in cyber crime. With cyber criminals aggressively hunting for their next catch, companies of all sizes and across all industries need to be on the lookout for cyber threats. The top cyber threats facing businesses in the wood niche include the following:

Phishing is one of the most prevalent forms of cyber-attack and often leads to ransom requests. In incidents of phishing, employees are often enticed over email to provide compromising company information or log-in credentials to an unauthorized person or to download an attachment that could plant ransomware on the computer.

Business email compromise plays on trust and relationships. An attack could occur if a vendor were hacked leading to an unauthorized person gaining access to their company email. In such a situation, the criminal could send an email requesting compromising information or changing banking information under the trusted name.

Software vulnerabilities and outdated or poorly configured systems also open the door to cyber-attacks as criminals can easily sneak into computer systems to steal information or plant ransomware. The criminals write code to automatically search thousands of systems per second and open doors for the hacker's work to begin.

While some companies have been able to put cyber protection measures in place through training and other company policies, other companies haven't. This lack of cyber preparedness can leave them open to cyber-attacks that can lead to costly damage and reputational harm.



MITIGATING MEASURES

Fortunately, there are a number of preventative steps—both in terms of human and IT firewalls—lumber and building material suppliers can take to not only reduce their risk of falling victim to a cyber-attack, but also to decrease the severity of a potential attack should one occur. The U.S. Cybersecurity and Infrastructure Security Agency provides a number of recommendations that call for, among other things:

- Updating and patching software
- Verifying email senders
- Using caution when opening links or attachments
- Staying informed on cyber activity and protections
- Installing antivirus software
- Improving password security and using multifactor authentication


In addition, companies should develop and implement cyber security best practices. If they don't have an in-house IT team, lumber and building material suppliers should consider hiring a third-party IT services firm that specializes in cyber security. They can conduct a cyber risk assessment, implement monitoring, and help execute a cyber incident management plan to be ready if a problem should occur.

On the human firewall side, management should make sure staff are adequately and regularly trained on cyber safety. Cyber safety is no longer simply the job of the IT

department; it's everyone's job. An awareness of cyber risk must be built into the company's culture. Further, just as suppliers are vetted for their ability to fulfill product demand, management should ensure that all vendors have been checked for good cyber risk management practices.

Finally, cyber insurance should be a critical part of any lumber and building material supplier's cyber safety plan. It's important for business owners to understand that cyber insurance is relatively new and isn't something that is automatically included in many insurance packages. While coverage can vary, a good cyber policy will include coverage for data breaches, computer attacks, fraud, and more.

When purchasing a policy, it can be particularly helpful to go with an insurer that understands the wood niche. A specialty insurer will know your industry and help with large and small incidents covering things like ransomware, network outages, data breaches, and financial fraud. They could also offer cyber tools or information to help educate business owners and employees.

Lumber and building material suppliers may be temporarily distracted by ever-changing pandemic protocols, dramatically fluctuating lumber prices, and supply chain shortages, but they cannot lose sight of cyber safety. Fortunately, with proper mitigation measures in place, an educated team, and a comprehensive, quality cyber insurance policy, lumber and building material suppliers can be confident they are ready should the worst happen. 

About the author: Erin Selfe is the vice president of IT at Pennsylvania Lumbermens Mutual Insurance Company. Selfe joined PLM in 2017 and has more than 20 years of experience in infrastructure, security, applications development, systems support, and quality assurance. For more information, please contact Erin at eselfe@plmins.com.

