CYBER LIABILITY: INSURANCE NOT REQUIRED, BUT IS NECESSARY

BY ROSS DRISCOLL, JR.

Business owners seem to be waking up and seeing the need for better cybersecurity. Cyber liability is still relatively new compared to the rest of the insurance marketplace. I estimate that less than 10% of the restoration industry purchases cyber liability coverage. This is far too low, as restoration contractors are highly vulnerable. You have technicians and project managers out in the field using their cell phones or laptops to send or store personally identifiable information. Likely, you may not have as many controls in place either.

In 2021, global cybercrime damage cost more than $6 trillion. Growing at an average of 15% per year, it is estimated to increase to $10.5 trillion by 2025. In 2015, the total was $3 trillion. We are all tired of talking about the adverse effects of COVID-19, but the pandemic really accelerated the volume of cyber-attacks. According to Intrusion Inc., this increase is the most significant transfer of wealth in history. It risks the incentives for innovation and investment. To paint a picture, it is considerably larger than damages caused by natural disasters in a year. It will be more profitable than the global trade of all illegal drugs combined.

Only 31% of businesses have Cyber Liability Insurance

Although Cyber Liability is not a coverage often required by TPA's, franchisors, or property managers, it is a coverage that is growing in popularity, and you need to weigh the cost. I have talked a lot about how there is a fine line between being insurance rich vs. coverage poor, but I strongly feel that you need to bring this up with your insurance agent.

When a breach occurs, cyber insurance covers the range of expenses that arise. These include identifying and solving the breach, recovering data, customer notifications, PR costs, possible credit monitoring expenses, legal expenses, potential fines from compliance regulators, extortion costs from ransomware, and general business interruption.

SMALL BUSINESS CYBER SECURITY STATS

- 43% of cyber-attacks aim at small businesses with 100 employees or less.
- 60% of small businesses that become victims of a cyber-attack are out of business within six months.
- 47% of small businesses have no awareness of how to protect themselves against cyber-attacks.
- Human error and system failure represent 52% of data security breaches.
- 63% of confirmed data breaches leverage a weak, default, or stolen password.
- 65 % of small businesses have failed to act following a cyber security incident.
- 50% of small and mid-size businesses reported suffering at least one cyber-attack in the last year.
- 54% of small businesses don't have a plan in place for reacting to cyber-attacks.
- Small businesses spend an average of $955,429 to restore normal business in the wake of successful attacks. (These are all references from NerdWallet.)

Common Cyber Insurance Claims

Data Breaches – These are the most common and have the largest total losses. Globally, for small and large businesses, the average cost per breached record is close to $8, where the average claim has nearly 700,000 records breached.

Cloud hacks – When we store data in a cloud, everything is often thought to be secure. Still, you are vulnerable if you do not have strong passwords and/or advanced authentication.

Account takeover – The best way to picture this is when a hacker "takes over" your social media or bank account. If this happens to one of your business accounts, someone can access your employees' or customers' online accounts.

Malware – We all have antivirus protection of some kind, but even the best ones out there cannot fully guard against all types of spyware, ransomware, computer worm, Trojan virus, or adware that it comes up against.

Website Vulnerabilities – No website is perfect, as they all have vulnerabilities. Antivirus may be able to prevent hackers in many cases, but nothing is guaranteed.

Phishing – Cyber Insurance does not often cover this. For most policies to respond, there needs to be a breach of security. Although these losses may look like theft, these payments are usually "authorized" by an innocent employee, which would not be covered.

Ways to Protect Your Business from Cyber-Attacks

Understanding that Cyber Liability will protect you from certain losses, we can all agree that not being a target of an attack would be even better. To protect your business from security breaches and cyber risks, here are a few tips:

- A strong antivirus should be your first investment. To help prevent cyber-attacks involving malware, you absolutely need an antivirus built for businesses.
- VPN (Virtual Private Network) is a simple and effective tool that can help you conceal your IP address and encrypt your traffic on the web. These are highly recommended when using an unsecured internet connection but should be used as often as possible. The most common VPN uses are on your laptop or cell phone, but some use a VPN directly on their own private routers.
- Encrypt! Almost all companies have remote employees or people in the field; encrypting your data can prevent unauthorized individuals from gaining access to your data.
- Construct a firewall. A good firewall can identify and prevent attacks on your company. Be sure to activate your spam filters within your company emails which to help limit phishing.
- Require strong passwords. We have all had some weak passwords at some point in our digital careers. This can be one of the easiest ways to create a way in for hackers. A strong password is 16 or more symbols with a mix of numbers, letters, and special characters. They should be unique and not used for multiple accounts. Change it if you have the same password for your bank account and social media!
- MFA, or multifactor authentication, may be one of the most essential tools to implement. A good example is when you log into your bank account, and then they text you a secondary code to type in to gain access. This can dramatically reduce your risk of a cybercriminal gaining access to your business and corrupting your systems with ransomware by requiring other ways to validate a user further than their preliminary login. Some cyber insurance carriers won't even offer coverage to a business if they do not utilize MFA. When a business applies MFA, they often have more choices of carriers and gain access to more competitive rates.

Where the Cyber Market is Headed

Looking back at 2021, it is apparent the cyber market is hardening. I do not foresee any relief coming, as there are many difficult questions concerning systematic cyber risk, how it is underwritten, and where cybercriminals will hit next. With more and more claims paid every year, Cyber rates were up 204% in Q3 2021 over the previous 12 months.

Reinsurance capacity is scarce, where reinsurance carriers tend to only provide protection for those with good track records and strong relationships. We have seen carriers enter the cyber market only to exit a few years later. With loss ratios ramping up, the market is taking steps to protect itself.

Rate increases – Premiums are increasing across the board, where even the best risks saw close to 50% rate increases. Those who did not have good controls saw rates increase 100% - 300%.

Stiffer underwriting – Nearly every underwriter is asking for more information around one's data security and controls. MFA is crucial for many carriers. To take it a step further, some carriers require a separate ransomware questionnaire to see how you will manage a threat.

Capacity – The industry did not see a mass exodus, but carriers want to limit their exposure. Some policy holders saw their policy limits cut in half,

especially those who had a primary and excess layer of cyber liability.

Coverage Limitations – For ransomware claims, many carriers have enforced sub-limits and co-insurance clauses. Sometimes, this would limit coverage to 50% of the policy limits or less. Other carriers added exclusions for specific vulnerabilities that they found. If the insured did not fix these vulnerabilities and there was a claim, the carrier could deny coverage.

I say all of this not to scare you but to give you a warning about an evolving market. If you are entering the cyber market for the first time, be proactive with the tips I have shared to protect your business.

For most restoration contractors, depending on where you are at in the country, the size of your business, and the controls you have, it is likely that the annual premium will be between $1,000 and $5,000. My recommendation would be to purchase cyber liability sooner than later. Not only should you have the protection, but the longer you carry coverage, the more data the carrier will have on your business. Over time, if you are claim free, you should be able to gain access to more carriers and more favorable rates. It is always better to "prepare and prevent; don't repair and repent." The latter can end up costing you in the long run.

Ross Driscoll Jr., MBA, CIC, is a Partner and the Vice President of National E&S Insurance Brokers and Driscoll & Driscoll Insurance Agency. Prior to joining the family business, he was a Contract Surety Underwriter at Zurich North America. He specializes in the risk management for contractors, especially those in fire/ water restoration industry. As a Certified Insurance Counselor (CIC), he has expertise in all lines of Property & Casualty Insurance. Ross has been recognized by various insurance carriers as one of the top up and coming producers in the country. He is one of the few producers who truly understands his customer's risks as well as how to manage them.