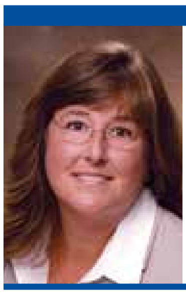
Things to know about cyber risk and insurance



Guest editorial
Becky Harding, CPCU
Director of
Work Truck Total Protect
877-924-5777
becky@worktrucktotalprotect.com

There's a lot at stake when managing your business's data and network. Cyber losses have increased exponentially in recent years, and cyber criminals are getting savvier. Companies can no longer assume they're safe from cyber attacks because they're a small business or have a third party that collects and stores their data. Not even the cloud-based services are free from threat of cyber attacks.

The most common types of cyber losses fall under two main categories: first-party and third-party claims.

First-party losses

- **Data breach.** In this scenario, a cyber criminal hacks into your system and gains access employees' and/or customers' personal data. Information can include names, addresses, social security numbers, credit card information, banking information, etc.
- **Social engineering.** Here, the criminal poses as a trusted team member to trick an employee into parting with your company's money. For example, your accounts payable personnel receive an email (which appears to be from you) asking them to send a vendor some money with bank routing information. Of course, it's not until after this transaction takes place your employee learns the email wasn't from you at all, and instead, they have fallen victim to a cyber criminal.
- **Computer fraud.** This situation involves a hacker who electronically accesses your banking information and re-routes outgoing payments.
- **Cyber extortion/ransom.** In this scenario, any employee unwittingly opens an email or clicks on an infected attachment. Then, once the cyber criminal accesses your system, they can seize your data and freeze your system, rendering it useless to you. In order to return your data and system access, they demand money (commonly in Bitcoin, since it's difficult to trace).

Third-party losses

- **Network and information security liability.** If your customers' or employees' personal data was hacked and stolen from your network, you can — and likely will — be held liable. This is true even if a third-party company administers your network because, at the end of the day, customers and employees trusted your company with their data. They have no say in your choice of network administrator, no knowledge (most of the time) of that third party, and usually don't give it much thought. You are ultimately responsible for securing the personal information of those parties.
- **Regulatory liability.** When your system is compromised, you are responsible to alert all parties whose information may have been breached. That is an expensive endeavor. You may also face regulatory action brought by state and sometimes federal authorities.

It's important to note, the previous examples are just some of the scenarios we encounter in the ever-evolving cyber world. There are many more you may have heard about on the news or even from peers.

There are insurance products for cyber risks that can include all of the above and more. The process for obtaining cyber insurance includes completing an application, including direct questions about your current security safeguards. Necessary information may include financials, network firewall and backup information, business continuity and disaster recovery plans, personnel policies and training, etc.

Multi-factor authentication (MFA) is something you will start hearing more about, if you haven't already. Many insurance companies are requiring some form of MFA from their insureds. This is a secondary form of proof that you — or your employees — are who you say you are when accessing your company's data. This could include requiring employees to enter a numerical code or pressing an authentication button on their cell phone when gaining access to your system. This is becoming more and more important, as it protects your company's data and network, and demonstrates to the insurance company that you're serious about keeping your network secure.

If interested in obtaining an insurance quote to cover cyber risks, contact your trusted insurance agent and inquire about available cyber products. The small amount of effort it takes now can save money and stress if a cyber criminal knocks at your network's door.