Understanding cyber risk and insurance protection

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 data and network. Cyber losses have increased exponentially in recent years and cyber criminals are getting more and more savvy. Business owners 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 cloud-based services are free from the threat of cyber attacks.

The most common types of cyber losses fall under two main categories: first-party claims and third-party claims. This article outlines some examples of those types of losses.

First-party losses

- **Data breach**. In this scenario, a cyber criminal hacks into your system and gains access to the personal data of your employees and/or customers. The information can include names, addresses, social security numbers, credit card information, banking information and the like.
- **Social engineering**. Here, the criminal poses as a trusted member of your team to trick a staff member into parting with your company's money. For example, your accounts payable personnel receive an email that appears to be from you. In that email, they are asked to send a vendor some money with bank routing information. Of course, employees don't learn that the email wasn't from you until after the transaction occurs.
- **Computer fraud**. This situation involves a hacker who's able to electronically access your banking information and reroute outgoing payments.
- **Cyber extortion/ransom**. In this scenario, any employee may unwittingly open an email or click on an attachment that's infected. Then, once cyber criminals access your system, they can seize your data and freeze your system, rendering it useless to you. In order to return your data to you and give you access to your system, they demand money (usually in Bitcoin since it's so difficult to trace).

Third-party losses

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

It's important to note these 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.

> "Cyber losses have increased exponentially in recent years and cyber criminals are getting more and more savvy."

There are insurance products for cyber risks that can include all of these threats and more. The process of obtaining cyber insurance will include completing an application and answering some direct questions about your current security safeguards. The needed information may include financials, network firewall and backup details, business continuity and/or 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, which is a secondary form of proof that you or your employees are who they say they are when accessing your company's data. This could include the employee needing to enter a numerical code or press 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 as well as demonstrates to the insurance company that you are serious about keeping your network secure.

If you're interested in obtaining a quote for cyber risks, contact your trusted insurance agent and inquire about the cyber products they can offer you. The small amount of effort it takes now can save a whole lot of money and stress if a cyber criminal knocks at your network's door.

JD Fulwiler & Co. Insurance developed the Work Truck Total Protect program to provide the industry with underwriting, risk assessment and loss prevention services. JD Fulwiler will shop among many top insurance carriers with which it does business to find a coverage solution that best meets your needs. Learn more at ntea.com/partnerships.