Courtesy of
RiskSOURCE Clark-Theders

CYBERRISKS&LIABILITIES_

Cyber Attacks - A Growing Business Interruption Threat

When you think about what usually causes a business interruption, natural disasters such as fires, earthquakes and floods probably come to mind first. These events can physically damage your property and equipment, making your workspace unusable for a time.

The damages from Hurricane Katrina and Superstorm Sandy are great examples of how a natural disaster can put a halt to a business's day-to-day operations. Many of those affected businesses remain closed to this day.

While natural disasters are still the main reason for an interruption, another cause is quickly moving up the ranks: cyber attacks. As businesses continue to rely on computers and digital storage of essential data, cyber attacks will continue to be a potential exposure. Read on to learn how a cyber attack could lead to a business interruption and what you can do to mitigate the risk.

How Cyber Attacks Cause Business Interruptions

Hackers, thieves and other unauthorized individuals have become adept at exploiting weaknesses in a business's computer system, whether through traditional hacking methods or social engineering. There are several types of attacks that could completely cripple your ability to perform normal business activities, including:

- Malicious code that renders your website unusable
- Distributed denial of service (DDoS) attacks that make your website inaccessible to employees and customers alike
- Viruses, worms or other code that deletes critical information on a business's hard drives and other hardware

It is quite easy to see how any of these events might leave your company scrambling to do business.

Unfortunately, many smaller businesses don't have the manpower available to detect the problem and work on fixing it, which only increases the length of an interruption.

Third-party Interruptions

You can still be affected even if it isn't your business that experiences a cyber attack. Imagine what would happen if one of your vendors suffered an attack, resulting in a complete shutdown of its warehouse or website.

Unfortunately, attacks on third parties are often out of your control. Such an event could have a profound effect on how much business you are able to do, and that would trickle down to your customers, who may rely on your products or services.

Ways to Prevent a Cyber Attack

A common saying in the cyber security world is, "It's not *if* you'll be a victim of a data breach, but *when*." While 100% protection is impossible, you can help lower your chance of business interruption due to a cyber attack by following these tips:

- Create a formal, documented risk management plan that addresses the scope, roles, responsibilities, compliance criteria and methodology for performing cyber risk assessments.
  - This plan should include a characterization of all systems used at the organization based on their functions, the data they store and process and their importance to the organization.
- Make sure all firewalls and routers are secure and kept up to date.
- Implement a cyber security policy that educates

RISKSOURCE®
CLARK-THEDERS

employees about the dangers of computer intrusions and how to prevent them. RiskSOURCE Clark-Theders can help you draft a cyber security policy specifically tailored to your company.

- Download and install software updates for your operating systems and applications as they become available.
- Implement a strict password policy and have employees change system passwords every 90 days.
- Limit employee access to company data and information, and limit authority to install software.
- Make sure you are covered by a cyber liability insurance policy.

How Cyber Liability Coverage Can Help

Most traditional commercial general liability (CGL) policies will not cover business interruption losses due to a cyber event. Luckily, cyber liability coverage can fill that void.

Should your business be unable to perform normal business operations, a cyber liability policy can help pay for expenses related to an interruption. The coverage pays for:

- Lost income due to the event
- Profits that would have been earned had the event not occurred
- Operating expenses, such as utilities, that must be paid even though business temporarily ceased
- Rented or leased equipment

Cyber liability coverage also helps protect your business from the following events:

- **Data breaches,** including costs for customer notification, some legal costs and credit monitoring for those affected
- **Damages to third-party systems**, if, for example, an infected email from your servers crashes the system of a customer or vendor
- **Data or code loss** due to a natural disaster or malicious activity (physical losses are covered on a different type of policy)
- **Cyber extortion**, including ransomware, which is malicious code installed into a computer on your network that prevents you from accessing it until a ransom is paid

Even though business interruptions due to cyber attacks are relatively uncommon, being unprepared for one could prohibit you from doing business as usual. Contact RiskSOURCE Clark-Theders today to find out how we can help you avoid a business interruption.