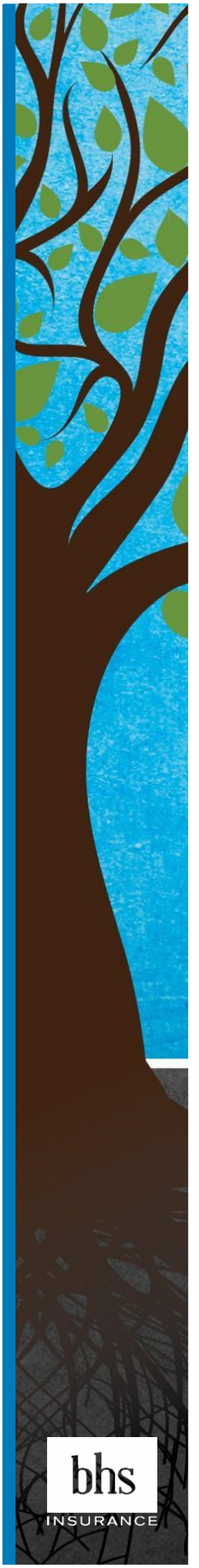
Cyber Attacks: A Growing Threat

Brought to you by BHS Insurance

August 2020



Cyber attacks are on the rise, in the first half of 2020 over 8 billion records were exposed. Ransomware has increased by 41% in 2020 and it is estimated ransomware costs will reach $6 trillion by 2021. Furthermore additional legislation has been enacted including BIPA (Biometric Information Privacy Act), GDPR (General Data Protection Regulation), & CCPA (California Consumer Privacy Act) resulting in tighter cyber security reporting rules along with penalties and fines.

With all these converging forces, there is a greater need for a strong cyber security plan and a robust cyber insurance policy.

Impact of Cyber Attacks

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
- Ransomware such as Cobolt Strike and other popular "off the shelf" products can lock up your system in demand for compensation or risk of the bad actors releasing the data they secured.

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

Third-party Vendors

You can still be affected even if it is not your system that experiences a cyber-attack. Vendor attacks can also impact your institution with the inability to process credit cards, breach of donor information or employee data.

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 risk 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 your institution 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 cyber security training that educates employees about the dangers of computer intrusions and how to prevent them.
- Download and install software updates for your operating systems and applications as they become available. This best practice can also be a requirement of your cyber insurance policy to purchase and maintain coverage.

- Implement a strict password policy and have employees change system passwords every 90 days. Passwords should be at least 12 characters.
- Limit employee access to company data and information, and limit authority to install software or other devices such as flash drives.
- Implement two factor authentication and VPN access to protect your environment when employees are working remotely.
- Be sure your vendors (cloud providers, IT providers, software, database) have strong cyber security policies and procedures including cyber insurance. Keep in mind many vendor contracts include a limitation of liability and/or indemnification protecting them. Furthermore, federal and state laws require the originator of the information to be responsible for the notification.
- Know exactly where Personal Identifiable Information (PII) is stored on your system or with third parties so a prompt assessment can be made if a breach were to occur. Know what states those constituents are located because the reporting requirements vary by state and internationally.
- Maintain strong data hygiene. Purge data that is no longer needed to reduce the number of potential files at risk. Do not store PII in fields that are not encrypted, only in appropriate designated areas of the system.
- Make sure your institution has a cyber insurance policy.

How Cyber Insurance Coverage Can Help

The prompt assistance of a cyber breach coach can help you in the early stages to identify next steps.

- **A breach coach** is generally included in a cyber insurance policy and they, along with legal counsel, can provide initial free consultation to understand the event & help determine if legal notifications need to be made to third parties.

If next steps are required, the cyber insurance can pay for the following:

- **Data breach costs,** including costs for legal, public relations, forensic investigation, customer notification 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 malicious activity
- **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. If the ransom payment is the only way to mitigate the loss or secure stolen data, the ransom payment may the only option. These payments are included in the insurance as well.
- **Lost income** and additional expenses if a temporary shutdown of operations occurs due to the cyber attack

Cyber-attacks are on the rise, being prepared with strong procedures, a business continuity plan, employee training and insurance can protect your institution from a cyber event.

MORE INFORMATION

For more information, please contact a member of the BHS Insurance Public Garden team at (800) 350-7676.