Employee Owned

SCOTT

Est. 1864

Protect Your Business from Cyber Extortion

When a technology company was hit by a Distributed Denial of Service (DDoS) attack by a hacker who had gained control of one of its critical control panels, it was asked to be paid in exchange for returning control to its operations. The company chose not to comply with the extortionists and instead worked to recover its account by changing passwords. Unfortunately, the hackers had created backup logins to the panel and started randomly deleting files once they saw the company’s actions. This example of cyber extortion, unfortunately, put the company out of business.

Extortion as a result of a cyber attack is becoming more and more common for all business types and sizes. One reason for the increase in incidents is that end-user software like Cryptolocker has commoditized the malware industry, making it accessible to a wider variety of criminals and less-skilled hackers.

Cyber criminals, for the purposes of extortion, can threaten to shut down computer systems or erase data, infect a company with a virus, publish private information or personally identifiable information on customers or employees, institute a denial-of-service attack or take over social media accounts.

Businesses can take the following steps to help protect against cyber extortion:

1. **Know your data.** A company cannot fully know how much is at risk until they understand the nature and the amount of data they have.

2. **Create file back-ups, data back-ups and backup bandwidth capabilities**. These actions will help a company to retain its information in the event that extortion occurs.

3. **Train employees to recognize spear phishing.** All employees should learn the importance of protecting the information they regularly handle to help reduce exposure to the business.

4. **Do background checks on employees.** Background checking employees can help identify whether they have criminal pasts.

5. **Limit administrative capabilities for systems and social footprint.** The fewer employees with access to sensitive information, the better.

6. **Ensure systems have appropriate firewall and antivirus technologies.** After the appropriate software is in place, evaluate the security settings on software, browser and email programs. In doing so, select system options that will meet your business needs without increasing risk.

7. **Implement data breach prevention tools, including intrusion detection.** Ensure employees are actually monitoring the detection tools. It is important to not only try to prevent a breach, but to make sure that if a breach occurs, the company is aware as soon as possible. Time is of the essence.

8. **Update security software patches in a timely manner.** Regularly maintaining security protections on your operating system is vital to them being effective over time.

9. **Include DDoS security capabilities.** It is important to have the ability to avoid or absorb attacks meant to overwhelm or degrade your systems.

10. **Put a plan in place to manage a data breach.** If a breach occurs, there should be a clear protocol outlining which employees are part of the incident response team and their specific roles and responsibilities.

11. **Protect your business with insurance coverage designed to address cyber risks.** Cyber insurance coverage typically provides protection for costs associated with data breaches and cyber extortion events. Insurance programs can also provide access to skilled professionals to manage the event from start to finish.

To learn more about cyber risks and how you can protect your business, contact a Scott Risk Advisor today.
