What is Ransomware and How Do You Prevent It From Harming Your Business?

Ransomware is a kind of malicious software that blocks or restricts your access to your computer systems and data until you pay a fee to the attacker. If you refuse to pay or can't find a way to fix the problem, your data may be lost forever. Because small businesses generally have less to spend on cybersecurity than larger companies, they are often the target of a ransomware attack. Remote desktop protocol, email phishing and software weakness were the top three access points hackers used to take control of small business networks, and the average ransom demand was $112,000, according to a 2020 Coveware report.

How do I detect a ransomware attack?

Most businesses purchase security software that includes ransomware protection. Without this, you will usually only find out that you have been attacked when you no longer have access to some or all of your data. Typical ransomware attacks come in two forms — encryption and lock screens. Encryption locks up data on your system. You will only be able to use the data if you have an encryption key, which the attacker claims they will provide once the ransom is paid.

Lock screens are as they sound. You screen will inform you that you are blocked from your own system. Typically, the lock screen will also provide you with instructions on how you are to pay the ransom. In each case, the hacker claims they will provide an encryption key once the ransom is paid, but there is no guarantee that they will or that the key will work if given.

How can I prevent a ransomware attack?

Once ransomware is in your system, your options become severely limited. The best way to prevent ransomware from harming your business is to take steps to reduce the chances an attack will be successful.

As mentioned above, you can purchase software that contains ransomware protection. Software is available to protect your server, email, web surfing and mobile devices. Make sure you regularly update your software with the most up-to-date patches.

In addition to software, train your employees how to spot potential cyber attacks. Regular cybersecurity training can lower your risk. Teach employees to never open attachments that look suspicious and to never give out personal information when answering an email, text, instant message or phone call.

Backing up your data is essential. If a ransomware attack is successful, a good backup can get your business up and running quickly and you won’t have to worry about paying the ransom.

However, you *will* have to worry about data exposure and the liability that goes along with it. You'll also have to deal with potentially angry hackers who know how to exploit the weak points in your network security. Even if you pay the ransom and your data is returned, you should assume they viewed or copied your data, which means it's been compromised.

If you experience a ransomware attack, you will have more to handle than just changing passwords – you are going to need some serious assistance.

Cyber (or data breach) insurance

You are responsible for the personally identifiable information (PII) that you store on your business network. Credit cards, social security numbers, birthdates, tax returns, social media accounts, contacts and client data history are a few examples of PII.

You could be sued by your clients and endure steep fines imposed by government regulations (if your state has them). You'll need to start damage control as soon as possible, which should include a call to your insurance company.

A general liability policy may completely exclude cyber coverage or offer very little protection. A cyber insurance policy can help you with data recovery and response (like ransomware), credit monitoring for affected clients, repair of damaged systems and public relations. Cyber policies differ quite a bit, so reach out to your insurance professional for more information about what is best for your business.

Ransomware – it's not a matter of *if*, but *when*

The number of ransomware attacks increases each year. It's not a matter of *if* your business will be targeted, it is *when*. Take steps to lower your risk by installing reputable antivirus software, regularly updating that software, training your employees on cyber threats and periodically backing up all of your data.

Work with your IT department to make sure you understand your weak spots and come up with a plan to strengthen them. Doing so can lower your risk of an attack and help your business recover as quickly as possible.

Acumen Solutions Group, LLC

(516) 986-3425
insurance@acumenins.com

Acumen Solutions Group, LLC
600 Broadhollow Road
Suite 200
Melville, NY 11550
acumenins.com/

This content is for informational purposes only and not for the purpose of providing professional, financial, medical or legal advice. You should contact your licensed professional to obtain advice with respect to any particular issue or problem.