PBMares℠
Your Future. Our Focus.

How to Protect Your Company From Ransomware

Ransomware is a significant threat for business owners of any size, and the damages can be catastrophic. Losses are in the trillions of dollars each year from the damage they cause and the ransoms paid out.

In early 2022, ransomware attacks in Bernalillo County, New Mexico, caused several government buildings to close, most government systems to stop functioning, and Albuquerque Public Schools to cancel classes. It even caused the security cameras and cell door locks to stop working at the county's Metropolitan Detention Center. Weeks later, the county was still trying to fully recover.

Attacks such as this are occurring with greater frequency, partly because ransomware is easier for a cybercriminal to obtain or construct. Cybercriminals can acquire malware kits through online marketplaces and easily launch new attacks.

Businesses must protect themselves from ransomware and other cybercrimes because an attack can quickly force companies into dire financial situations.

What is ransomware and how does it work?

Ransomware is malware that encrypts your files and holds them hostage until you pay a ransom, usually in the form of Bitcoin or another cryptocurrency. Upon payment, the attacker is supposed to send a private key that enables you to decrypt your files.

Ransomware can spread through email, infected documents, infected websites, or vulnerabilities in a network. With ransomware, a binary file containing malicious code is typically dropped onto a computer. The binary scans the computer for important files and encrypts each one, if not the entire hard drive. The ransomware will often attempt to spread to other computers and devices, encrypting their files too.

Once the ransomware has encrypted a computer's files, it will typically display a message demanding a ransom in return for the private key to decrypt the files. If the ransomware is not paid, then the files remain encrypted forever.

Fortunately, there are several things you can do to protect your company from ransomware.

How to Defend Against Ransomware Attacks

Backup your data

One of the most important ways to protect against ransomware is performing and storing backups of your data regularly. It's important to keep backups either in the cloud or on an external hard drive not connected to your network. This will prevent a ransomware infection from accessing and encrypting your backup files.

Install the latest updates

Cybercriminals constantly look for software and network vulnerabilities to exploit. Keep all software on your computers and servers updated with the latest version. Don't forget about your website - if you use a CMS like WordPress, keep all files, themes, and plugins updated. Additionally, make sure that any firmware running on computers or other hardware connected to your network is fully updated.

Use security software

When selecting a security software package, ensure it includes protection against ransomware. Different software packages use different techniques to detect and defend against ransomware, none of which is full proof. However, security software can certainly help to reduce the risk of a ransomware infection.

Use secure passwords and multi-factor authentication

While they may seem like a basic cybersecurity feature, strong passwords go a long way toward preventing ransomware threats. If an attacker can guess or steal your credentials, they may be able to gain access to your computer, network, or a connected system. Three strategies to secure credentials are strong passwords, difficult security answers, and multi-factor authentication.

Use strong passwords

To create a strong password, keep the following guidelines in mind:

- Longer is better (at least 8-10 characters)
- Use both letters and numbers
- Use uppercase and lowercase letters
- Use special characters
- Don't use words you can find in a dictionary (e.g., boat, library)
- Don't use personal information (e.g., your pet's name or your birthdate)

Use an encrypted password manager to help create, store and manage passwords.

Make security answers difficult

Most sites have security questions you can answer if you forget your password, such as "What's your mother's maiden name?". Because this information is pretty easy to find with a simple Google search, it's best to choose difficult questions or use fake answers when you set up your account. If the answers are too simple, hackers can use this workaround to access your account.

Use multi-factor authentication

Multi-factor authentication (MFA) requires multiple steps to access your account. The most common type is two-factor authentication (2FA), which, as the name suggests, requires two steps - the first step is to enter your login credentials, and the second step is to enter a code from a secondary device. So even if an attacker steals your login credentials, they won't have access to the secondary device such as your phone.

Use a VPN when in public

When using public wifi, use a virtual private network ("VPN") to protect your internet connection and privacy online. A VPN encrypts your traffic over the internet, enabling you to browse securely and privately. While a VPN is not meant to protect your computer from ransomware attacks, it can help minimize the risk of cybercriminals acquiring your login credentials or other sensitive information that could lead to an attack.

Train your employees

Just as it's important for you to learn about ransomware threats, you should train your employees on ransomware. Consider creating a cybersecurity handbook that outlines best practices for defending against ransomware and other cyberattacks. Show your employees how to recognize malicious attacks and explain the proper protocols if they believe they've been the victim of an attack.

Test your defenses

Once you have your protections in place, it's time to test them. There are many ways to test your systems to ensure you're adequately protected. Common cybersecurity tests include Penetration testing, Cybersecurity audits, Cybersecurity risk assessments, and Bug bounties. If these terms seem unfamiliar, it's because security experts usually conduct these tests. They're typically not a "DIY" task. You can ask your in-house cybersecurity team for assistance or hire a third party to conduct the testing for you.

Create a disaster recovery plan

A disaster recovery plan is another critical step to protecting your company from ransomware threats. Time is often vital to mitigating a significant problem and minimizing damages. All too often, employees lose time figuring out whom to contact and what to do. A disaster recovery plan helps solve this by outlining all the steps and procedures employees should take when a disaster occurs. It is usually part of a larger business continuity plan.

Final Thoughts

While ransomware attacks are always a looming threat, there are ways to protect yourself and your company. We hope you find these tips and strategies helpful. If you would like to discuss how to protect you and your company from cybersecurity threats, please contact our office.

About PBMares, LLP

PBMares, LLP is an accounting and business consulting firm serving U.S. and international clients, with offices in the Mid-Atlantic. The firm unlocks opportunity for clients using the right balance of industry, specialty and general business services in the areas of audit and accounting, tax planning and preparation, pension plan design/administration, and owner-managed/corporate financial consulting. In addition, the firm provides additional services through its affiliates: Artifice Forensic Financial Services, LLC, a financial consulting division specializing in fraud investigations and forensic accounting; PBMares Wealth Management, LLC, a registered investment advisor; and TMDG, LLC, a national healthcare consulting firm specializing in medical claims audits. More information is available online at www.pbmares.com.community-based initiatives.

PBMares, Headquarters
701 Town Center Dr.
Suite 900
Newport News, VA 23606

(757) 873-1587

pbmares@pbmares.com

www.pbmares.com

Baltimore | (443) 451-9010 Fairfax (Metro DC) | (703) 385-8577 Fredericksburg | (540) 371-3566
Harrisonburg | (540) 434-5975 Newport News | (757) 873-1587 Norfolk | (757) 627-4644
Richmond | (804) 323-0022 Rockville | (240) 499-2040 Warrenton | (540) 347-4970
Williamsburg | (757) 229-7180