UP TO SPEED
ON THE LATEST
EXPOSURES

Waldorfwire

05.21

Ransomware: A Trending Cyber Exposure for Churches and Nonprofits

Ransomware attacks have spiked. Infosecurity says ransomware attacks increased 485% in 2020 compared to the previous year. Some industries are especially common targets, but no one is immune, not even churches and nonprofits.

How Ransomware Works

Cybercriminals exploit both human vulnerabilities and technical vulnerabilities to infect computer systems with ransomware.

Some ransomware attacks exploit Remote Desktop Protocol and software vulnerabilities. Ransomware attacks may also be delivered through phishing attacks that dupe the recipients into downloading malicious files. Because many people have learned to avoid obvious phishing attacks, modern attacks tend to be targeted and sophisticated.

Once a system is infected, the malware encrypts files, making them inaccessible to the owners. A message will demand payment, often in the form of cryptocurrency. If the ransom is paid, a decryption key may be provided so the files can be restored, but this is not always guaranteed. The hackers may also steal the data and sell it on the dark web.

Frequently Targeted Industries

Some industries are common targets, frequently because of the data they hold. According to TechRepublic, a 2020 report found that 5.7% of ransomware attacks target healthcare organizations and 5% target educational organizations. More recently, attacks on the educational sector have increased, and the FBI warned of increase in PYSA ransomware attacks against education institutions in March. If your nonprofit fits into a frequently targeted category, your risk may be especially great.

Nonprofits organizations may also be targeted indirectly when hackers attack vendors. This is what happened to several nonprofits when Blackbaud, a cloud service provider, was hit with ransomware in 2020. According to CPO Magazine, the attack impacted multiple nonprofits that had their donor lists raided.

How to Protect Your Organization

Don't assume that your religious or charity organization is not a target. Ransomware attacks are on the rise, and no one is safe. A ransomware attack could cause financial, operational and reputational damage, so you must be proactive.

• **Train your workers and volunteers.** Many ransomware attacks begin with an innocent click. Anyone who has access to your computer system should be trained on how to spot phishing attempts and avoid malicious links.

• **Strengthen your computer systems.** Basic precautions include running up-to-date programs, using anti-malware software and following Remote Desktop Protocol best practices. Have a computer security expert review your system for vulnerabilities.

• **Take extra precautions to keep sensitive data secure.** This may include encryption and network segregation.

• **Use strong passwords with two-factor authentication.** Avoid using the same passwords in multiple accounts. If one is hacked, the others may be at risk as well.

• **Back up data.** This will let you restore data after an attack. However, modern attacks sometimes threaten to publish or sell personal data, so backups may not prevent all possible problems.

• **Vet your partners.** Ensure that vendors with access to your data are also using strong security practices and address cyber liability in your contracts.

• **Develop a ransomware response plan in case you are attacked.** Consider how you will assess the threat, notify those affected, and pay the ransom, if you decide to do so.

• **Check your insurance coverage.** Do not assume that you are covered against a ransomware attack. Make sure your insurance policies provide coverage for this type of attack.

Read your policies carefully and consult with your broker to understand the exclusions and consider additional coverage as needed.

Need Help with Cyber Coverage?

Waldorf Risk Solutions is connected with many leading insurers specializing in coverage for religious institutions and nonprofit organizations. We will shop the market on your behalf and help you compare the options available. Please reach out well ahead of your renewal date. With the hardening insurance market, rates are higher, and coverage can be hard to source in some cases. Contact us to learn more.

Stephen Waldorf