WIPFLi LLP
CPAs and Consultants

Improve Your Ransomware Awareness and Defense

By Paul Johnson, Senior Manager

March 2016

There've been a recent spate of ransomware attacks on organizations both small and midsized. One particularly high-profile case in February involved the Hollywood Presbyterian Medical Center in California. See our blog post.

Attackers essentially shut down the hospital's computer systems. The "Locky" malware encrypted the hospital's electronic medical records, thereby blocking access to patient information unless a ransom was paid. The hospital's ability to provide a normal level of care was greatly affected. The organization lost more than a week of productivity because of the crisis before paying the attackers nearly $17,000 for the decryption key to unlock its data.

Ransomware is a very real threat to organizations of all sizes, and the threat continues to grow. By some reports, incidents increased 113% last year compared to the year before.

Computers are infected when users are fooled into opening an infected attachment from a seemingly legitimate email. By opening the attached file and allowing macro to run, the malware is downloaded and begins to encrypt files. It's designed to go unnoticed until it's completed the process of encrypting files. Thereafter, a ransom message is displayed onscreen, demanding payment should you ever want to see your files again.

How well is your organization prepared to handle a ransomware threat, and how well do you know the facts surrounding this malicious attack? Test your basic ransomware understanding with a few true-or-false questions.

True or False?

- *It's always best to pay the ransom quickly and move on to recovery mode.*

  False. The FBI, industry officials, and Wipfli do not recommend paying the ransom. Remember, you are dealing with criminals. There is no guarantee you'll get the key to access your files, and paying the ransom only emboldens and finances the criminals to attack the next organization.

- *Responding to a ransomware attack is the same as responding to other kinds of data breaches.*

  False. Ransomware essentially locks your data to keep it from you; it doesn't steal it.

- *Ransomware attacks are random and not typically perpetrated by vengeful ex-employees or disgruntled patients.*

  True. No organization is immune, and the great majority of ransomware attacks are random.

What Can You Do?

Plenty. Ransomware is a serious form of extortion and a serious crisis. Defend yourself with the following tips.

- Back up, back up, back up. This is truly the single most important measure and the fastest way to regain access to your critical files. All data should be regularly backed up and kept in a separate and secure location. Your backup system should provide the ability to recover from multiple backup sets and recovery points.
- Train, train, train. Every employee should be trained to spot suspicious messages and know that if they weren't expecting an email attachment, they should never open it. Training must start as part of new-hire orientation and include regular refresher sessions throughout the year. Just a small portion of the money Hollywood Presbyterian ultimately paid to the extortionists could have otherwise gone a long way in training for prevention.
- Patch and update software. Malware often looks for security bugs in popular outdated software applications. Enable automated patches for your operating system and Web browser. Keep software up to date. Patch the holes and close the opportunities.
- Keep antivirus software up to date. Hundreds of new malware variations are introduced each day, and all are trying to find your vulnerabilities. Keep your security software up to date.
- Use Web, email virus/spam filters. Use a third-party email filtering service that blocks spam and virus-laden messages before they arrive at your server. And use pop-up blockers.
- Maintain a strong firewall. Enable automatic updates, test for leaks, and check ports.
- Develop an incident response plan that includes malware attacks. Practice it and continue to modify it as needed. Having trained staff to address an aftermath can significantly reduce downtime and the accompanying expenses.

- Conduct a network review. A reliable third party can help spot weaknesses both in systems and processes and help you shore them up. Contact Wipfli for information about review and risk assessment services.

About the Author

Paul Johnson helps clients determine their compliance with the Payment Card Industry Data Security Standard (PCI DSS) and health care security compliance including HIPAA and HITECH. He also works with clients to assess, improve, and test the security of their information systems. For more information, contact Paul at 651.766.2895 or pjohnson@wipfli.com.

About Wipfli LLP

With associates and offices across the United States, Wipfli ranks among the top accounting and consulting firms in the nation. The firm's associates have the expertise, skills, and experience to advise in areas from assurance and accounting to tax and consulting services. In addition, through the firm's membership in Allinial Global, Wipfli can draw upon the resources of firms in over 100 countries from around the world. For more information, visit www.wipfli.com.