Steps to Prevent Ransomware Shared by Top-Ranked Retail MSP

The new business in town is cybercrime. No longer dominated by quirky individuals in poorly lit basements, cybercrime gangs now run like sophisticated corporations. Well-funded, sometimes by governments, these organizations use ransomware as a weapon of choice. Their victims lose billions annually. But a comprehensive approach to cybersecurity can help prevent ransomware.

Every Organization a Target

Every eleven seconds, ransomware hits a target. Attacks against big names like Colonial Pipeline, JBS Foods and the NBA made the news in 2021. But threat actors increasingly turn their attention to small businesses, in part because they often lack adequate cybersecurity controls.

Additionally, thousands of businesses have migrated to the cloud in recent years, in part to share the security burden with cloud providers. However, while reputable cloud providers prioritize security, a successful attack on a single provider can impact dozens of businesses.

Finally, the adage that lightening never strikes twice in the same place does not necessarily hold true with ransomware attacks. The FBI and many cybersecurity experts continue to warn against paying ransoms. Not only does a ransom payment not guarantee safety, but it also encourages more attacks.

To prevent ransomware, proactive organizations need to take a layered approach to cybersecurity, starting with a few key practices.

Conduct Penetration Testing

One of the best defenses against bad actors involves thinking like one. Cybercriminals search for cracks in your defenses, vulnerabilities in the system. You should, too. For instance, proactive organizations conduct penetration tests to simulate cyber attacks and uncover weaknesses.

During a penetration test, a skilled tester uses the same means a hacker would use to attempt to exploit weaknesses in the system. The organization can then use the information gathered to outline a security strategy. In fact, some regulations require regular penetration testing and vulnerability scans.

Strengthen Email Fortifications

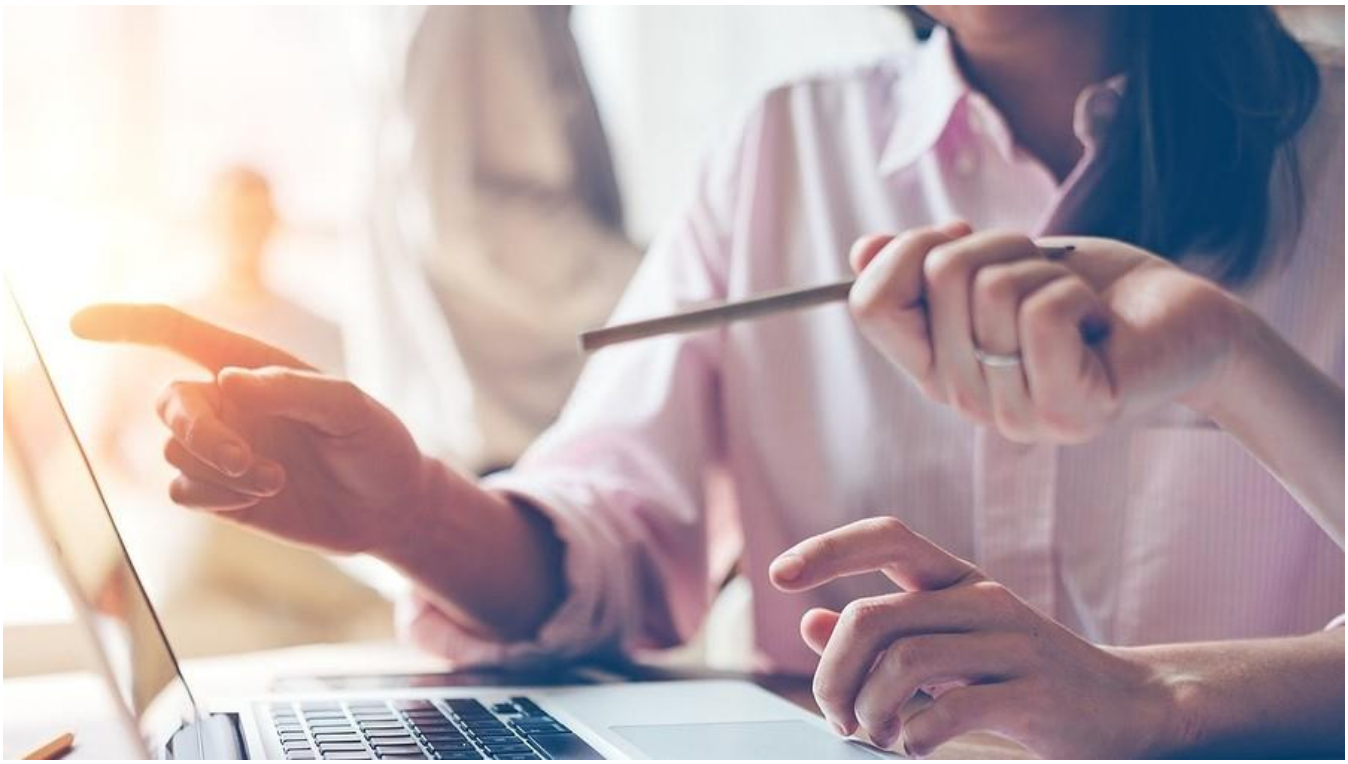
With all the communication methods at our fingertips, email still dominates business communication. Consequently, email remains the primary attack method for cyber criminals. Build essential cybersecurity awareness with regular security training for employees. Supplement employee training with automated encryption and email filtering.

Restrict Access with Geo Blocking

Geo blocking allows organizations to block access from specific countries, thus helping to prevent foreign hackers from accessing business systems. For instance, if a company has no customers in Russia, it may choose to block internet connections from Russian sources. Firewall settings or geo-based policies in Microsoft 365 make this possible.

Automate Threat Protection

To counter automated hacking efforts, organizations need to automate key tasks related to cybersecurity. This includes basic tasks such as backups, email filtering and patching updates. Additionally, companies should automate threat detection and response. For instance, big data analytics and machine learning can detect and contain attacks before they cause damage.



Regularly Review and Adjust

Attackers continually up their game, resulting in a constantly changing threat landscape. At the same time, network changes or the introduction of new software, new vendors, or additional devices can introduce unexpected vulnerabilities. To guard against ransomware and other threats, conduct regular risk assessments and adjust strategy accordingly.

Prevent Ransomware with Multi-layered Cybersecurity

While essential, none of these steps alone will provide adequate protection against ransomware attacks. In combination, however, they form the base of a solid cybersecurity strategy. Additional layers will include items such as regulating access controls, securing the supply chain and maintaining thorough incident response plans.

For best results, partner with cybersecurity professionals. eMazzanti, once again the top-ranked retail-focused MSP on the ChannelE2E Top 100 Vertical MSPs list, has built a sterling reputation for delivering comprehensive cybersecurity solutions. From 24/7 network monitoring to web and email filtering, eMazzanti delivers peace of mind.