5 Steps to Prevent Ransomware from Destroying Your Business

The message reads, "Your network has been penetrated. All files have been encrypted. We exclusively hold decryption software for your situation." Those dreaded words indicate the presence of ransomware and the stuff of nightmares. However, with advance preparation, you can prevent ransomware from crippling your organization.

Thousands of organizations, from hospitals to schools, city governments to corporations, have fallen victim to ransomware. Attacks continue to increase in frequency and sophistication. But your organization does not need to become a statistic. The key lies in minimizing the risk of attack, detecting attacks early and responding effectively.

5 Steps to Prevent Ransomware Damage

Organizations can significantly reduce ransomware damage and resulting costs by making wise IT investments before an attack occurs. Surprisingly, despite the billions of dollars lost to cyber-attacks, too many companies fail to implement some basic security measures such as the following.

1. **Regular backups stored externally** – In the event of a ransomware attack, your single most important asset lies in having clean, recent backups available. Implement a system of frequent

backups and store multiple copies, including a copy on a remote server or in the cloud. Test backups regularly.

2. **Defense in depth** – Any military leader will extol the virtues of building multiple layers of security around critical assets. For information, this includes firewalls, antivirus and anti-malware programs, email filters, and advanced threat detection. In addition, keep all software up-to-date to minimize vulnerabilities.

3. **Limited system access** – Limit employee access to only the systems they need to complete their assigned tasks. Also, where possible, segment your network into separate zones, each with its own access credentials. Hackers cannot encrypt what they cannot access, and this will limit the spread of infection.

4. **Employee training** – Hackers most often gain system access through email or social media. Teach employees to recognize phishing attempts, use strong passwords, avoid public wi-fi, recognize warning signs and adopt email best practices.

5. **Disaster recovery plan** – Assume an attack will occur and develop a comprehensive plan for recovery. Create a prioritized list of critical data sets, systems and operations. Have a communication plan in place to report threats, contact disaster recovery resources and deal with media. Know the location of backups and have a plan for backup hardware.

Early Warning Signs of an Attack

In the case of cancer or a heart attack, early detection significantly increases the chances for a positive outcome. The same wisdom holds true in cases of ransomware. Ideally, anti-malware will discover and halt ransomware before it causes damage. In addition, teach employees to recognize early indications of an infection and alert IT.

For example, a sudden influx of popups, files that refuse to open or programs that fail to work as expected may all represent a possible attack. Users should also periodically check their Sent folders for emails they do not recognize. Finally, employees who encounter encrypted files, locked drives or ransomware notes should immediately notify security personnel.

Ransomware First Aid

Any 12-year old scout can recite the basics of first aid procedures for a broken arm or a snake bite. Likewise, a few early remediation measures can help to prevent ransomware from spreading.

Once a device has been infected, isolate the device and contact your security team. Immediately disconnect the device from the network and remove any external hard drives, USB drives or other devices. Disable Wi-fi and Bluetooth. Next, take a photo or screenshot of the ransomware note. Then power down compromised machines and label them as infected.

When you have isolated infected devices, limit access to the rest of the network. Force password changes across the board so that hackers cannot use previously obtained credentials to gain access.

With stop gap measures in place, you can begin to determine exactly what type of ransomware you are dealing with and develop an appropriate response. The FBI can assist with this process and will usually respond within a day. Do not rush to restore from backups until you know you have removed the hackers from your system. And, do not pay the ransom.

Security Experts to the Rescue

As you work to prevent ransomware, ensure early detection and respond to attacks, enlist the help of qualified security experts. eMazzanti can help you implement comprehensive, multi-layer security and, if needed, walk you through crisis control. For organizations with limited IT resources, we provide reliable managed services to keep your valuable information safe.