MEDITAB™

Ransomware Protection Guide

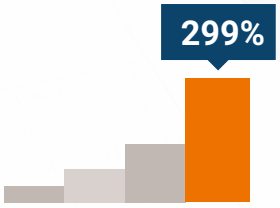
How to Protect Your Practice from the Rising Risk of Ransomware

TABLE OF CONTENTS

What is Ransomware?

Ransomware, as the name suggests, is a type of malicious software (malware) that infects your system and encrypts your data. Once affected, you are denied access to your data until you pay a “Ransom” to buy the decryption key. However, even if you pay the ransom, there is no way to guarantee that the attacker will provide you with the decryption key.

Source: Solutionary



Source: SonicWall

Ransomware has become one of the most dangerous threats facing the healthcare industry, and a shocking **88% of all ransomware attacks** in the U.S are targeted towards healthcare organizations.

And the risks of ransomware are increasing exponentially. In 2018, **Ransomware Attacks increased by 299%**

How Does Ransomware Infect Your System

A ransomware virus is commonly disguised as an email attachment or a hyperlink. However, it can also access your system when you click on an unsafe website or application that contains malicious content.

Once the ransomware has access to your system, it encrypts/locks all of your data files behind a password key held by the attacker.

Ransomware can spread quickly through your system if you're using software that enables you to control computers remotely. Make sure to check your RDP (Remote Desktop Protocol). Never provide direct RDP connections over public IP addresses. We recommend using a remote gateway with 2FA on a Cloud-Hosted server.

Top Tips for Preventing a Ransomware Attack

Prevention is always better than the cure.
Below are the top 9 tips you can use to prevent a ransomware attack:

1. Avoid Phishing Emails: Install email spam filters and train your employees to avoid downloading email attachments from unknown sources. Conducting mock scam drills can help your employees understand the strategies used by cybercriminals.

2. Provide Selective Access: Provide your employees with access to only the systems needed to get their jobs done. Access should be revoked when the user is no longer active.

3. Regularly Update Your Software: To maintain your system's security, make sure that your software is regularly updated and maintained. Download and install all the latest patches to fix your system's vulnerabilities.

4. Change Passwords Often: Set up a strong password criteria. Set passwords to expire after a certain period of time. Create a locking mechanism that prevents access to the system after several failed login attempts.

5. Closely monitor network traffic: By monitoring your network traffic, you can track unusual activity and identify patterns associated with malware or ransomware. Early detection of ransomware is key to prevention.

6. Create a disaster recovery plan: Having a contingency response plan in place for ransomware attacks will help minimize impact. The response plan can be done by prioritizing a list of systems that can be shut down due to the attack and for how long.

7. Limit the Use of Microsoft Office Macros: Many ransomware distributors now use Microsoft Office Macros to deliver their ransomware virus. A macro is a series of commands and instructions that you group together as a single command to accomplish a task automatically. If macros aren't required for any workflows, they should be completely disable. If your workflow doesn't allow you to disable, administrators should block macros Microsoft Office files (Word, Excel, PowerPoint) that have been downloaded from the Internet and macros should be blocked from automatically running.

8. Backup Your Data: Create backup copies of your data on a regular basis. Storing your backup data in an "offsite" location is highly recommended, because local "onsite" backups can often become infected as well. Meditab and IMS resellers can help keep your data safe by performing daily backups and storing your data in a secure, offsite location.

9. Switch to Cloud Hosted Servers: As opposed to traditional onsite servers, cloud hosted servers offer advanced anti-malware protection, daily offsite backups, and automatic software updates. Meditab and IMS resellers provide cloud hosting services that can help protect your data against ransomware by hosting your data on our cloud servers.

According to RapidScale, 94% of the surveyed companies claimed that they saw security improvements after switching to Cloud Hosting.

Ways to Detect a Ransomware Attack

Early detection is key to preventing a ransomware attack. The faster you can detect ransomware, the faster you can react. Below are 3 ways to detect a ransomware attack in progress:

1. Monitor File Renaming

The most reliable method for detecting ransomware on your network is to monitor changes in the rate that files are renamed. This is one of the biggest red flag warnings of a ransomware attack in progress. When Ransomware is installed, there usually is a huge increase in file renames as data gets encrypted.

This change in activity can be used to trigger an alert. The alert can be triggered whenever file renames exceeds a pre-set threshold. Setting the threshold to 4 file renames per second is recommended. You will know that you are being attacked as soon as the threshold is exceeded.

2. Create a Sacrificial Network Share

Ransomware file encryption usually starts with the encryption of files on the local machine. Once local files have been encrypted, the ransomware searches for network shares.Most ransomware progress through each network share in alphabetical order such as such as the A: drive, followed by the B: drive etc.

By creating a sacrificial network share, you can set up an early warning system. This will delay the encryption giving you more time to act before critical data is encrypted. This could give you the valuable minutes you need to shut down client machines before the infection spreads.

Use an early drive letter such as E: or a drive that precedes your actual drive mappings. Ideally, the network share should be setup on old, slow disks and the drive should be full of thousands of small files.

3. Update Your IDS Systems with Exploit Kit Detection Rules

Many intrusion detection systems (IDS) and firewalls have exploit kit detection features. Exploit kits are hacking toolkits loaded onto websites that search for vulnerabilities in web browsers and plugins. When a user visits a website hosting an exploit kit, any vulnerabilities are identified and leveraged to download ransomware. Exploit kits probe for multiple vulnerabilities and are updated frequently when new vulnerabilities are discovered and new exploits created.

Steps to Take if Infected by Ransomware

Even the most secure databases can have ransomware vulnerabilities.
Here are the 4 steps you can take if your data becomes infected by ransomware:

1. Isolate

If you are on any active network, disconnect yourself. This will prevent the virus from spreading and infecting any other device or system. Go offline, disconnect from any wireless capabilities like Bluetooth or WiFi.

2. Identify the Scope

Find out exactly how much of your files/data is compromised due to the infection. Also, determine if the first infected machine had access to any Shared drives, external hard drives, cloud-based storages (Dropbox, google drive, etc).

3. Determine the Strain of Ransomware

It is always beneficial to know your enemy, so it is important to determine the class of ransomware that has infected your system. Each ransomware has it's unique way of infecting your files. Sometimes, though in very rare cases, there is a chance that the particular strain of ransomware already has a decryption tool built by an IT security company. This will allow you to decrypt your files without having to pay the ransom. If you cannot determine the strain of ransomware you are dealing with, you can try online tools like CryptoSheriff or ID Ransomware. These tools allow you to upload encrypted files and let you know if a decryption key is available.

4. Evaluate your options

When you know the type/strain of ransomware you are dealing with, you can make an action plan. The first thing that crosses your mind is should you pay the ransom or not? Most law enforcement agencies, security experts, and even Microsoft advises against paying the ransom. Paying the ransom does not always ensure the security and the retrieval of your data. Moreover, paying ransom to the criminals might incentivise them to continue attacking you!

Here are the 3 Options if Attacked

Restore Data
from a recent backup
(highly recommended)

Decrypt your files using
an available decryptor
(Which is rarely possible; because the malware continues to evolve)

Do nothing
(lose your data)

If you Choose option 1: Restore Data from a recent backup

First, verify the files you need, and check if you are able to recover them from a backup. Once you ensure that your files are backed up, you can now take action on the infected computer and remove the ransomware. Some people run multiple antivirus scans to ensure the malicious software is removed. If you want to be 100% sure that there are no traces left of any kind of malware, completely wipe and rebuild the server. Once you are confident that all traces of the ransomware have been removed, you can now restore your files onto your server.

Cloud Hosting is one of the safest and most effective ways to protect your data from ransomware attacks. Meditab and IMS resellers can provide Cloud Hosting Services to help protect your data from ransomware.

*Always consult an IT professional to advise you on what security measures are best for your practice.

Want to Protect Your Data with Cloud Hosting?
Contact Your **Account Manager** or **Reseller**