RANSOMWARE: DON'T BE THE NEXT VICTIM

By Health Tech Access Alliance

RANSOMWARE ATTACKS WERE UP 400% IN 2018:

And Criminals are Targeting Healthcare

Ransomware: Prevent your computer from being infected

RANSOMWARE: WHAT YOUR CHC, FQHC, HCCN OR HIE NEEDS TO KNOW

By Robert Zimmerman, HTAA Founder

What is ransomware?

And what can you do to prevent your organization from becoming the next ransomware victim? 60 Minutes recently did yet another story on ransomware and healthcare.

In a nutshell, ransomware locks up critical organization data in a digital safe that only the attacker has the electronic key for. Then the attacker ransoms the combination to open the lock. This is the new "easy to commit" and "hard to get caught" crime that will impact all healthcare entities.

Ransomware is malicious software that encrypts a user's files, usually through phishing emails, un-patched programs, visits to compromised websites or free software downloads.

YES, YOUR SMALL HEALTHCARE ORGANIZATION IS VULNERABLE

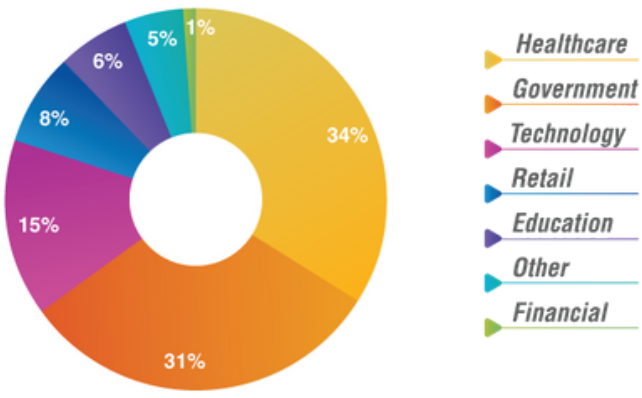
Not only can ransomware encrypt files on the workstation or or device but it can travel through your network and encrypt data and files throughout your organization. Once your critical data files are encrypted, workstations will display how to pay to unlock the files.

Ransoms are generally small. They can range from $500 - $10,000. Once the ransom is paid in Bitcoin (to keep the attackers identity secret), a software key is provided which should start the decryption process and unlock your data. Most of the time the key works but not always.

Most of us envision a lone wolf hacker or a clandestine crew of hacker dudes hiding in a basement, hacking into databases of Fortune 500 companies. That may have been true in the past, but now hacking is often an automated process with machines doing the work, scanning for any vulnerabilities across all and any organizations on the grid. If your organization's software is out of date, or your employees open suspicious emails without protection, then your organization gets flagged as vulnerable and considered fair game for criminals.

For too long smaller healthcare providers ignored this risk. It's human nature to assume the worst won't happen to us.

NUMBER OF RECORDS BREACHED BY INDUSTRY



"Data Breaches Compromised 3.3 Billion Records in First Half of 2018*" Gemalto

Prevention Checklist

Users:
☐ Implement effective security training for all staff
☐ Conduct simulated phishing attacks
☐ Provide users the minimum needed access to applications and data
☐ Limit & monitor Internet access
☐ Prevent users from downloading unauthorized software

Applications and Networks:
Make sure you have--
☐ An effective firewall
☐ Anti-spam & anti-phishing software
☐ Advanced endpoint products like whitelisting or real-time executable software blocking
☐ Current patches & software updates
☐ Segregate your applications and networks

Back-up and Recovery:
Make sure you--
☐ Perform on-going data backups. Think resiliency.
☐ Maintain data backups in a safe location whether in the Cloud or at offsite secure storage. If you can't get to them, they are of little use
☐ Test your data back-ups to make sure they work & include all critical data. Make sure you back-up data you need today & in the future. Not what you needed last year or before an upgrade or new system.
☐ Develop a business contingency plan that includes critical business and IT functions.
☐ Train & Test--Make sure your contingency plan works & management, clinicians and staff know what to do in case of an emergency or business disruption.

INVEST IN PREVENTION:

Reducing the risk of a ransomware attack takes an investment in planning and allocating the resources to prevent attacks. But it is critical.

Have a plan to reduce risks. If you do get hit, you can limit the damage. Be prepared, instead of being forced to negotiate with criminals.

GIVE US A CALL BEFORE YOU GET A RANSOM CALL.

WHY WOULD ANYONE ATTACK MY SMALL CLINIC THAT CAN'T PAY MUCH ANYWAY?

Because the game has changed...

Now there are more automated attacks on big and small organizations with many smaller ransoms. It's a volume business with many more small scores that add up to a lot of money and create a lot of mayhem.

It is much more cost effective to play defense, instead of paying ransoms and losing revenue. Can you afford to be shut down for days, or even weeks because your files are locked up? Your biggest vulnerability is every staff member including yourself, and what is most dangerous is not knowing what you don't know. A combination of software solutions and risk management techniques—including anti-virus and anti-spam software, vulnerability monitoring, regular data backups and redundant data—are critical defenses. Other key strategies include alternative processing sites that contain all critical applications, as well as segregating the network and application to limit the damage one attack can cause.

None of these strategies helps if they aren't actually implemented, or are implemented incorrectly. But how do you know if your IT provider is on top of this? That's where a formal Security Risk Assessment comes in. Third party assessment and verification can give you the peace of mind you need to focus on running your organization without unnecessary risks.

Having a plan, complete and usable data backups, alternate processing locations, a well-trained staff, and management that knows what to do greatly reduces the risk of a successful ransomware attack. And if you get attacked, you will be ready to negotiate from a position of strength, not be at their mercy.

HEALTH TECH ACCESS ALLIANCE

security@htaalliance.org

301-200-9776

www.htaalliance.org