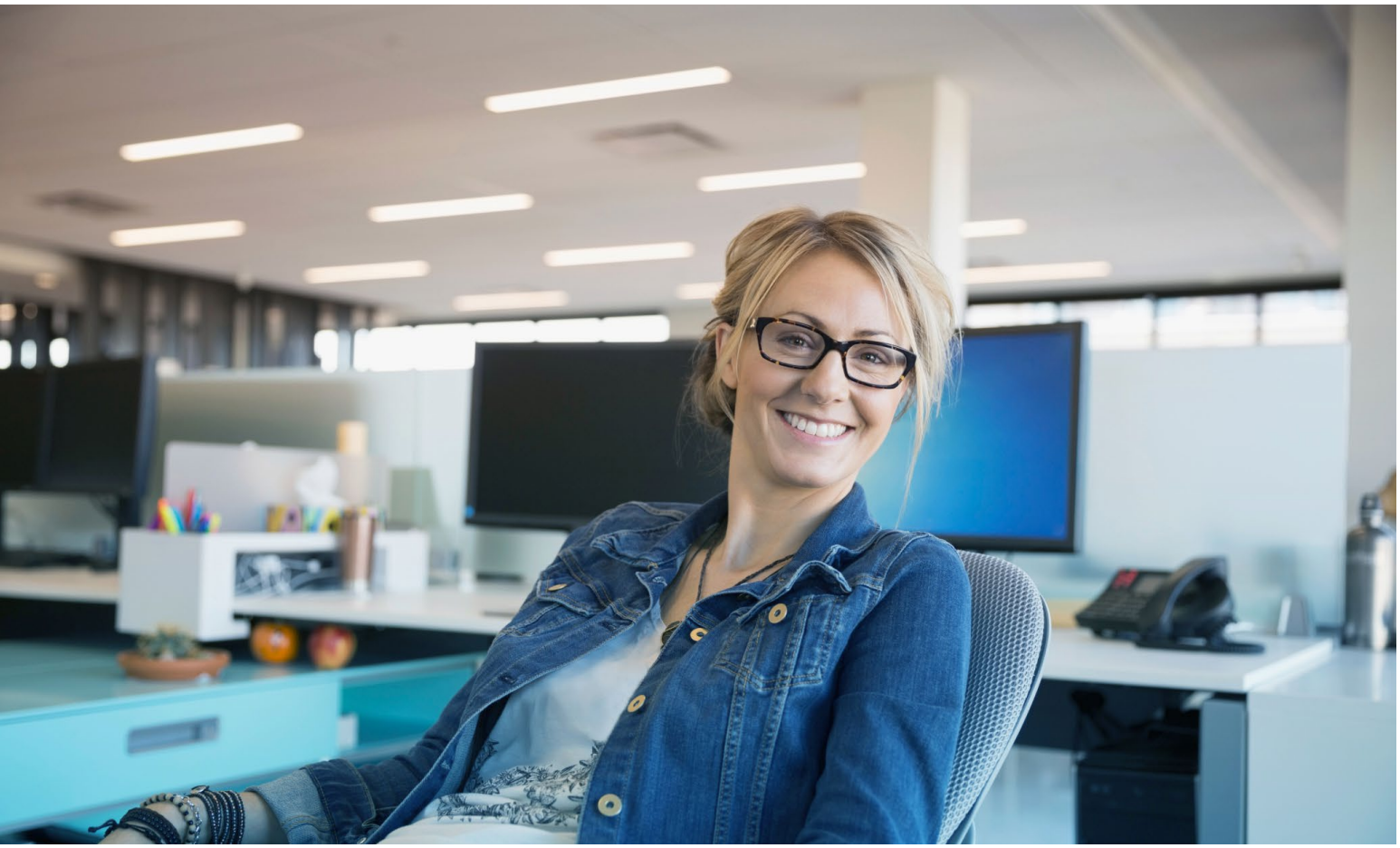
COMMVAULT®

4 Ways to Protect and Recover from Ransomware Attacks

MAINTAIN ACCESS TO CLINICAL DATA TO ENSURE QUALITY CARE

The number of ransomware incidents targeting healthcare is on the rise. It's become an easy source of revenue for cyber criminals, and as such the number of attacks continues to grow every year. When a successful attack occurs, healthcare organizations lose access to critical electronic files, putting patient care in question. To restore access, organizations are faced with the decision to pay the ransom – with the hope that the files are actually released – or attempt an ad hoc recovery, with no guarantee that current data can be reliably reproduced. To maintain necessary access to clinical data to ensure quality care, consider these four best practices to protect and recover from ransomware attacks with confidence.



4 BEST PRACTICES TO GUARD AGAINST RANSOMWARE ATTACKS

Implementing a multi-layer security strategy – including anti malware, personal firewall, hard disk and file encryption, DLP and more – is critical to protecting against growing cybersecurity threats. However, even with all of these endpoint protection solutions, there's still a modest chance of breach. According to the Gartner Magic Quadrant for Endpoint Protection Platforms[6], "When 44% of reference customers for EPP (Endpoint Protection Platforms) solutions have been successfully compromised, it is clear that the industry is failing in its primary goal: blocking malicious infections."

To protect the healthcare environment from ransomware, consider the following best practices:

ONE: HAVE AN EFFECTIVE INFORMATION SECURITY PROGRAM

If your organization is new to information security, or you have only a partially implemented information security capability, consider taking the following steps outlined in Table 2 to put an effective security program in place.

STEPS	ACTIONS
KNOW WHERE CRITICAL DATA IS STORED	Maintain awareness of data location • Data center • Remote facilities • Cloud • Service Provider
INVENTORY SYSTEMS	• Know which systems handle sensitive data: store, process and transmit • Understand the data flow • Determine which systems present the highest risk to your operations
ASSESS RISK	• Include electronic records, physical media, and the availability of critical systems, services, or devices
APPLY SECURITY CONTROLS	• Select, apply and manage security controls based on risk
MONITOR EFFECTIVENESS	Prepare for the evolving threat landscape • Proactively evaluate the effectiveness of risk-based information security strategy, the security controls applied, and the proper implementation of security technologies • Apply corrective actions, remediation, and lessons learned
EDUCATE USERS	• Make sure employees are educated on what to do when they receive emails from unknown senders with suspicious attachments or links (see Appendix for recommended steps)

Table 2) Components of an effective security program.

6 Gartner, Magic Quadrant for Endpoint Protection Platforms, February 1, 2016

TWO: PROTECT DATA WITH TECHNOLOGY BEST PRACTICES

With the growing number of threats, coupled with the evolving sophistication of attacks, healthcare organization need to clearly understand the cost tradeoffs of investing in cybersecurity and employee education, against loss of access to critical data and the resulting impact on patient care.

Network security is a good first line of defense in guarding against ransomware attacks. And by implementing effective technology best practices, healthcare organizations can further protect their critical data and IT infrastructure. Table 3 outlines key technology strategies to help eliminate the potential for infection by ransomware attacks.

STEPS	ACTIONS
DETECT AND PREVENT	Employ a multi-faceted security solution • Protect against file-based threats (traditional AV), download protection, browser protection, heuristic technologies, firewall and a community sourced file reputation scoring system • Keep systems and software updated with relevant patches
USE EXTERNAL CERT GROUPS (COMPUTER EMERGENCY RESPONSE TEAMS)	• Often identify a problem before the virus software companies • Can make recommendations on immediate steps for manual filtering (software companies may require hours or days to release a patch)
IDENTIFY AND STOP INFECTION	Define a comprehensive prevention policy • Includes endpoint and network policies and protection products, such as antivirus, antispyware, and firewall-type products • Limits execution of unapproved programs on workstations • Limits the write capabilities of end users so that, even if they download and run a ransomware application, it is unable to encrypt files beyond the user's specific files • Include electronic records, physical media, and the availability of critical systems, services, or devices
KEEP A "GOLD" IMAGE OF SYSTEMS AND CONFIGURATIONS	• A fundamental element of data management policies • Easily clone infected system with master
MAINTAIN A COMPREHENSIVE BACKUP STRATEGY	• The fastest way to regain access to your critical files • Take volume level snapshots more often (every 15 minutes) and store them for a longer period of time. • Remove the impacted system from the network and remove the threat. • Restore any impacted files from a known good backup
MONITOR EFFECTIVENESS	Prepare for the evolving threat landscape • Proactively evaluate the effectiveness of risk-based information security strategy, the security controls applied, and the proper implementation of security technologies • Apply corrective actions, remediation, and lessons learned
EDUCATE USERS	• Make sure employees are educated on what to do when they receive emails from unknown senders with suspicious attachments or links (see Appendix for recommended steps)

Table 3) Technology best practices.

THREE: EMPLOY EFFECTIVE BACKUP STRATEGIES

Recognize that a ransomware event is a progressive hack. It works over time, and can run in the background for a week or more, and learn the behavior of your backup routines. As such, it is important to maintain a persistent copy of the data in other locations as part of your disaster recovery procedures.

Many who only rely on snapshots as backup are at a higher risk. When the snapshot or the other instance is replicated, the source is corrupted too, as it follows the replication. Have a preserved version of the data from prior recovery points in protected locations is the ticket.

STEPS	ACTION
EMPLOY BACKUP AND DR PROCESSES	• Directly call out a backup copy rather than versions stored on the same system. • Have external backup copies of the data beyond simple snapshots that are maintained on the source system.

Table 4) Data protection best practices.

Using a cloud library is another alternative for a good external collection. Since the cloud backup is not visible to the local administrator operating system account, it would require additional sophistication to gain access to your cloud user credentials. And while no one loves tape in the day of "disk only," it may prove to be a better alternative in some cases, as the online nature of disk is what exposes the persistent risk.

FOUR: EDUCATE EMPLOYEES TO SECURE THE ENDPOINT

Finally, educating clinicians on good security habits is essential to keeping healthcare systems and PHI secure. Remind then to use common sense. As described by the Internet Security Threat Report[7], educate your users on the best practices outlined in Table 5.

STEPS	ACTION
TRAIN USERS TO PRACTICE SECURITY BEST PRACTICES	• Do not open attachments unless they are expected and come from a known and trusted source. • Do not execute software that is downloaded from the Internet (if such actions are permitted) unless from a trusted source or the download has been scanned for malware. • Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends. • Employ safe social media conduct. Hot topics are prime bait for scams, not all links lead to real login pages. • Encourage employees to raise the alarm if they see anything suspicious. • If Windows users see a warning indicating that they are "infected" after clicking on a URL or using a search engine (indicative of fake antivirus infections), educate users to close or quit the browser using Alt-F4, CTRL+W or to use the task manager, and then notify the helpdesk.

75 percent of U.S. hospitals responding to a recent poll could have been hit with ransomware in the last year.

HEALTHCARE IT NEWS
April 7, 2016

7 Symantec, "Internet Security Threat Report," Volume 21, April 2016

EMPLOY ENDPOINT PROTECTION BEST PRACTICES	• Deploy web browser URL reputation plugin solutions that display the reputation of websites from searches. • Restrict software to corporate-approved applications, and avoid downloading software from file sharing sites. Only download packages directly from trusted vendors' websites. • Deploy two-step authentication on any website or app that offers it. • Ensure clinicians have different passwords for every email account, applications and login - especially for work-related sites and services.

Table 5) Employee and endpoint best practices.

CONCLUSION

Securing PHI and other critical information is a necessity for healthcare organizations in order to provide patients the best possible care, and maintain compliance with industry regulations. And guarding information from ransomware attacks should be a top priority for healthcare organizations to avoid the loss of availability to critical information and systems. Protect clinical data by paying close attention to security, technology, backup and employee best practices. As a result, your critical data will be secure and you'll improve business continuity while mitigating ransomware risk.

RESOURCES

1 commvau.lt/2agPXQ7

To learn more about how Commvault® will help you intelligently manage your healthcare data, visit commvault.com/healthcare.

COMMVAULT®

PROTECT. ACCESS. COMPLY. SHARE.

COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM