Ransomware in the Healthcare Cloud

cloud security alliance®

The permanent and official location for Health Information Management Working Group is https://cloudsecurityalliance.org/research/working-groups/health-information-management/

Acknowledgments

Lead Authors:

Dr. James Angle

Contributors:

Michael Roza

CSA Global Staff:

Vince Campitelli
Alex Kaluza
AnnMarie Ulskey

Table of Contents

Abstract

Ransomware is the fastest-growing malware threat today. Over the last few years, it has risen to epidemic proportions, quickly becoming a significant revenue stream for criminal enterprises. Ransomware directly affects the ability of the Healthcare Delivery Organization (HDO) to access their data. Ransomware attacks, to complicate matters, cause more than a simple outage. They can attack the backup infrastructure. So, it's not just about restoring from a backup; HDOs need to ensure that they recover from an uninfected backup. To add to the problem, healthcare data in cloud storage is not immune to ransomware. However, cloud storage can offer a significant advantage with data protection due to the number of flexible recovery options.

Introduction

Ransomware is a form of malware used by an attacker to encrypt a victim's data and demand a ransom for the encryption key, which allows the victim access to their data. Ransomware is a rapidly growing problem that has increased 715% year-over-year, according to the latest Threat Landscape Report 2020 by Bitdefender (Bitfinder, 2020). Ransomware is highly profitable, which has made it the fastest growing malware threat. The average ransomware payment is $233,817, and many high-profile payments cost companies millions. For Healthcare Delivery Organizations (HDOs), the cost of recovery from a ransomware attack can be especially grave; the average incident costs $8.1 million, takes 287 days for full system recovery, and can jeopardize the quality of patient care for even longer than that (Digital Hands, 2021). In addition to all the financial and reputational damage caused by ransomware, it is a reportable breach under the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule, 45 CFR § 164.400-414. HIPAA is just one of the regulations an HDO may be required to adhere to. Most countries also have data protection laws that govern the processing of health data. This paper mentions only HIPAA, which is not the only law an HDO needs to be aware of; it is essential to understand the national and local laws governing where data is collected, processed, and stored. The criticality of healthcare data makes HDOs a prime target of ransomware attacks. The expansion of telehealth and the increased use of big data during the COVID-19 pandemic have increased the number of such attacks on HDOs.

During the height of the COVID-19 pandemic, healthcare found itself in another type of epidemic, ransomware. In 2020 the healthcare industry had 560 healthcare provider facilities suffer from ransomware attacks. According to the Emsisoft The State of Ransomware in the US: Report and Statistics 2020, "The attacks caused significant, and sometimes life-threatening, disruption: ambulances carrying emergency patients had to be redirected, cancer treatments were delayed, lab test results were inaccessible, hospital employees were furloughed, and 911 services were interrupted" (EMSISOFT, 2021). Ransomware attacks have taken on a new dimension. The attacker first exfiltrates the data and uses it for extortion. If the Healthcare Delivery Organization does not pay the ransom, the attackers will release the stolen data on the Internet. To increase the effectiveness of their extortion, the Darkside ransomware group is expanding its tactics with a new technique aimed at companies that are listed on NASDAQ or other stock markets. The attackers posted a message on their dark web portal that they are willing to notify crooked market traders in advance so they can short a company's stock price before they list its name on their website as a victim (Cimpanu, 2012).

Cloud storage is used to back up data that could then be restored after a ransomware attack. However, the increased use of cloud computing in healthcare for backups has escalated the number of attacks on cloud storage. This paper addresses how attackers use ransomware to attack both the HDO and the cloud service provider, and looks at ways to detect ransomware and protect the HDO's data. The paper follows the National Institute of Standards and Technology (NIST) Cybersecurity Framework structure to present this information.

Figure 1 NIST Cybersecurity Framework Core Functions

Ransomware

Ransomware is a type of malware that targets victims as a form of digital extortion. The attacker encrypts the victim's data, denying them access to the data until a ransom is paid. There are two general classes of ransomware: those that encrypt files and deny access to them, and those that incapacitate the device.

Ransomware is typically delivered through exploits, associated with website advertisements containing malware, or through phishing campaigns. After delivery, ransomware identifies the files and data to be encrypted through an embedded file extension list. Files that match one of the listed file extensions are then encrypted, and other file types are left alone. After encryption, the ransomware leaves a notification for the user, with instructions on paying the ransom.

A ransomware attack has a very familiar pattern. There are seven stages to the attack.

1. The first stage is reconnaissance. The main goal of this stage is to pinpoint the weaknesses in the target system.
2. The second stage is delivery and execution. This is when the malware is delivered and the execution begins. Persistence is also established in this stage.
3. The third stage is exploitation and infection. In this stage, the attacker finalizes an attack plan and infects the target machine after the preliminary survey. The target is infected with the ransomware, but the files are not yet encrypted.
4. The fourth stage is scanning and backup spoliation. The ransomware scans the system for important files to encrypt and removes the backup files and folders or waits until the backup synchronization infects the backups.
5. The fifth stage is file encryption. The ransomware encrypts the selected files.
6. The sixth stage is user notification and cleanup. The ransomware cleans up the system to eliminate evidence. Victims are notified and given a few days to pay before the price goes up.
7. The seventh stage is the payment process. If done right, the ransomware attack is timed for maximum impact on the business to force payment. Payment is made with Bitcoin to make tracking difficult (Kumar & Ramlie, 2021).

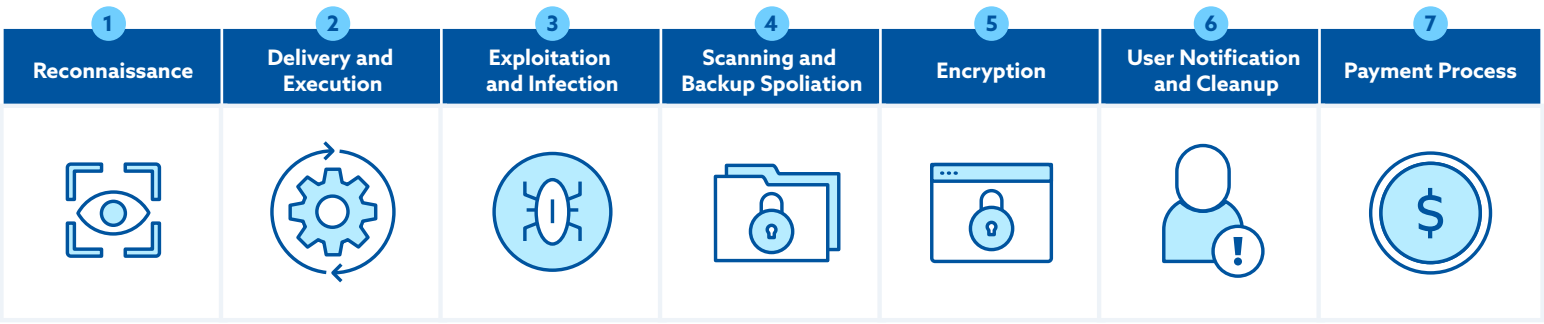

Figure 2 Ransomware Attack Stages

Gone are the days when quickly restoring a backup tape will solve a ransomware infection. A problem with the traditional backup is that the backup server can be rapidly infected by time-delayed ransomware due to the cyclical nature of backup processes. A ransomware cyberattack can be delayed, thus ensuring that all backup systems are also infected. Sometimes it can take a significant period for companies to recognize that they were hacked. During that time, backups are overwritten with malware or ransomware, infecting the backups. After a predetermined period, the hacker triggers the ransomware, and the company has no way to repair the files. At the same time, the ransomware starts looking for additional areas it can infect with the intent of infecting associated public cloud repositories while also deleting all backups (Tolson, 2020).

With the increased use of public clouds over recent years, many enterprise organizations have started adding cloud computing as a crucial part of their IT strategies. Due to the nature of public cloud, where the underlying infrastructure is secured and managed by the cloud service provider, many customers incorrectly assume that the threat of ransomware in the cloud is less than in a private data center (Netapp, 2020). However, cloud services rely on the synchronization of data, and if ransomware encrypted data enters the synchronization process, data will run the risk of being propagated in the cloud. At this point, cloud applications become complicit in spreading the malware.

To inhibit the user from choosing not to pay, attackers are now exfiltrating data before encrypting it. If the victim doesn't pay, the attacker then threatens to post the data on the Internet. Additionally, in a recent twist, attackers have started calling customers to pressure the business to pay quickly. Remember there is no honor among thieves. An attacker will usually provide the decryption key for the files if the victim pays the ransom; however, there have been incidents in which the attacker never could decrypt the files.

Ransomware continues to evolve and become more sophisticated, offering better encryption and new features (Metivier, 2019). Ransomware has become so profitable that there is now ransomware as a service (RaaS). RaaS is a platform designed so that anyone can conduct a ransomware attack. It is a user-friendly platform that enables an attacker to simply pick a victim, set the ransom, select a payment deadline, bitcoin wallet, and deploy the attack.

A ransomware attack can be devastating for an HDO. Valuable and irreplaceable files can be lost, and tens or even hundreds of hours of effort can be required to remove the infection and get systems working again. It is imperative HDOs understand how ransomware gets into the system so security professionals can put controls in place to mitigate the risk. The attack vectors are either social or physical engineering and will usually include one of the following:

1. Phishing: Phishing uses email to get users to click on a link or open an attachment that carries the malicious code.
2. SMSishing: SMSishing uses text messages to prompt the users to go to a website. Some SMSishing ransomware attempts to propagate themselves by sending themselves to all contacts in the device's contacts list.
3. Vishing: Vishing uses voicemail to deceive the user. The voicemail recipient is instructed to call a number. The voicemail takes the user through several steps to correct a fictitious problem, including entering credentials and downloading malware.
4. Social Media: Social media can be used to get the user to download an image containing malware.
5. Instant Messaging: Instant messaging can be hacked and used to distribute malware to the user's contact list.

In addition to the social engineering aspect there are also the physical attack vectors. Physical attacks are normally machine to machine and require very little user intervention. Physical attacks include the following types:

1. Drive-by: The only requirement is for the user to open a webpage that contains malicious code.
2. System Vulnerabilities: These can be exploited to break into the system and install malware.
3. Malvertising: In this type of attack, malware is inserted into ads that the user clicks on and downloads malware (Singh, 2019).

Identify

According to NIST, the Identify Function aims to "develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities" (NIST, 2018). Identifying assets, the business environment, HDO governance, risk management, and supply chain provides the foundation that the HDO's cybersecurity program is built on. This centers around pinpointing all HDO systems and platforms included in its infrastructure. Proper execution of the Identify systems will ensure that the HDO has information on all their systems. This includes all data.

The first step for the HDO is to identify and classify all IT systems (including third-party and cloud), all software (operating systems and application), and all data (collected, processed, stored, and transmitted). This entails a complete inventory of everything, people, IT systems (hardware and software), data, and facilities. Identifying and classifying these will aid in knowing what to protect and prioritizing these for a disaster recovery plan. Using this information, the HDO can identify risks and adverse impacts on the HDO. This will ensure the HDO leadership has the information they need to properly prioritize assets for protection, detection, response, and recovery. NIST stated, "Understanding the business context, the resources that support critical functions, and the related

cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs." (NIST, 2018).

The HDO should ensure that all policies, procedures, and processes are documented, readily available, and communicated. Placing data in the cloud means that the HDO must know where the data is stored and what regulations govern the jurisdiction where the data resides. Failure to identify where all the data is located can result in missing data during the recovery and reinfection of systems.

Protect

The Protect Function entails developing and implementing appropriate controls to ensure the delivery of services. This function provides the ability to limit or contain the impact of cybersecurity events which includes ransomware (NIST, 2018). Prevention is the best defense against ransomware, and it is essential to implement controls for protection. To protect an organization's cloud from ransomware, the place to start is with protecting the computer. There are some basic things the HDO can do to protect their computer systems. The first thing is to install endpoint protection. Standard antivirus software works by using signatures for malware and blocking those signatures. This approach does not work well for ransomware. Ransomware protection can be installed that will help identify potential attacks. Early unified threat management programs can find intrusions as they happen and prevent them.

The HDO should scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users. Strong spam filters should be enabled to prevent phishing emails from reaching the end users, and inbound email should be authenticated using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing. Macro scripts from office files transmitted via email should be disabled. Office Viewer software can be used to open Microsoft Office files transmitted via email instead of full office suite applications.

The HDO should employ logical or physical means of network segmentation and isolation to separate various departmental IT resources within the organization as well as to maintain separation between IT and medical devices. This will help contain the impact and prevent or limit lateral movement. Network activity should be baselined and analyzed over a period of time to determine behavioral patterns so that normal, legitimate activity can be distinguished from abnormal network activity (Multi-State ISAC, 2020).

Windows systems can use a Group Policy that allows the HDO to define how users can use the system. It can block the execution of files from local folders. Such folders include temporary folders and the download folder. This stops attacks that begin by placing malware in a local folder that then opens and infects the computer system (Dobran, 2019). Additionally, Group Policy can be set up to show hidden file extensions so users can see the double file extensions (such as filename.doc.exe) that attackers use to hide malicious software.

Identity and Access Management (IAM) is critical in preventing all types of malware but especially ransomware. IAM constitutes the HDO's perimeter for cloud computing. The HDO should manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts

should use them only when necessary. Additionally, Multi-Factor Authentication should be required for all remote access. Access controls, including file, directory, and network share permissions, should be configured with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

The HDO should implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered. Everyone must be trained to increase IT security awareness and to not fall for phishing emails, spam emails, and other social engineering attacks. Other things to train users on are never to click on unverified links, to not open untrusted email attachments and to not download from untrusted sites.

Another method of protecting data from ransomware is versioning. Versioning means that the data is immutable, and any modification results in a new version. This makes versioning effective against ransomware because encryption attacks result in a new version. Not all providers offer versioning, so availability must be verified with the provider.

Regular backups to the cloud can be an effective way to recover from a ransomware attack. The problem is if the attack is delayed, the malware may get into the synchronization cycle and be copied to the cloud. So how do we protect from this type of attack on the backups?

To defend against ransomware threats, a combination of data encryption with the use of homomorphic encryption to enable ongoing data management while encrypted and stored in the cloud, and cloud immutable/ WORM storage is the only sure way to address the new risks from ransomware. Immutable storage can be implemented in a variety of ways; the key point is that once data has been written, it can be deleted only under special circumstances. Immutability is combined with a retention period. During the retention period the backup set cannot be deleted, modified or overwritten, even by a privileged backup account.

Homomorphic encryption is different from standard encryption technology in that it allows computation to be performed directly on encrypted data without requiring access to a decryption key. Homomorphic encryption of backups and files before their move to a cloud repository guarantees data security in transit, at rest, and while in use.

Homomorphic encryption enables ongoing management of encrypted data, dramatically reducing the issues associated with standard encryption methodologies while ensuring continuous data indexing, search, and overall management and governance processes. Writing data to immutable/ WORM storage does stop the infection/encryption of backups so that they can be used to restore an infected enterprise (Tolson, 2020).

Detect

The Detect Function provides the HDO with the ability to detect events as they happen. This can be achieved through a combination of mechanisms, depending on the needs of the HDO. Malware detection, behavior-based anomaly detection, and intrusion detection are all used for event detection. The goal is to detect events as they happen, to trigger the appropriate responses, and to

provide information about the attack to the security team. Detection is implementing the controls and activities to identify a cybersecurity event while it is happening. HDOs cannot assume that having the latest antivirus software will protect their systems against ransomware. The endpoint security should consist of antivirus, anti-malware, and anti-ransomware protection. Protection from all three is necessary to ensure that the endpoints are fully protected. Advanced endpoint protection solutions can "learn" to identify malicious files and activity based on the attributes of known malware. Continuous monitoring of user and endpoint activity helps protect against malicious behavior by matching a stream of activity records against a set of dynamically updated attack activity patterns. Then, when a threat is identified, it can be immediately isolated at the endpoint to stop a ransomware outbreak.

Integrity monitoring tools provide the ability to test, understand, and measure attacks that occur on files and components within the enterprise. The value of integrity monitoring becomes clear both during and after an attack. Alerts can be set to notify the security team to act when abnormal changes are detected to a file or system, such as changes made at abnormal times or by users who typically do not make changes to these assets. The information produced by integrity monitoring systems can be used to inform a recovery process; they provide information about what changes happened, when changes began to take place, as well as what programs were involved in the changes. File integrity monitoring tools establish a baseline for integrity activity within the enterprise. This baseline is used in the event of an attack, to detect and alert on changes within the enterprise.

It is crucial that HDOs use next-generation firewalls that block unauthorized access to the computer or network. Additionally, firewalls should be augmented with web filtering specifically focused on sites that may introduce malware. SSL decryption capabilities must also be included. When the user/personnel runs the malware and virus checker frequently with updated virus and malware definitions, the security software can detect the ransomware and alert the user/personnel to its presence. Once detected, the ransomware can be quarantined and deleted, or once the ransomware is detected, administrators can opt to quarantine and delete it. Unfortunately, the first sign might be an encrypted or locked drive and a ransom note. Other detection techniques include monitoring for known ransomware file extension and/or an increase in file renames.

It is essential for HDOs to employ an all-out, multi-pronged approach of endpoint, network, server, and backup-level detection in order to protect data. Predictive analytics can be used to determine the probability that ransomware is operating in the environment. This can alert administrators if ransomware conditions are discovered. Early ransomware detection means faster recovery.

Respond

The goals of the response phase are mitigation and containment, which provide the ability to limit a destructive event's effect on the HDO. A response can involve stopping the execution of associated programs, disabling user accounts, isolating systems, and more, depending on the threat. Actions may include removing software from a system, restarting services, or copying the threat to a safe environment for analysis and forensics.

The Respond Function is developing and implementing the activities to respond to detected incidents. This is where the incident response plan comes into play. Once an HDO has been hit with a ransomware

attack, what must be done? There are several steps that should be taken that the HDO should take to deal with the attack. The first step is to determine which systems were impacted and immediately isolate them. If several systems or subnets appear affected, the network must be taken offline at the switch level. It may not be feasible to disconnect individual systems during an incident. If taking the network temporarily offline is not immediately possible, it is necessary to locate the network cable and unplug affected devices from the network or remove them from Wi-Fi. If the device cannot be isolated by disconnecting it, it will have to be powered down/the system should be powered down. Isolation will prevent the devices from spreading the ransomware infection.

Once the infected systems are isolated, the security response needs to identify the source of the ransomware. Identifying the source will make it easier to track the infection and remediate the systems. Security personnel should look for alerts from all the tools and monitoring that is in place. Log files should be checked for any anomalies that can identify the source. Additionally, security personnel should look for suspicious traffic and any increase in file renames on local and network file shares, and should not forget to check the cloud storage.

Tracking the infection allows the HDO to assess the extent of the damage. The assessment must include all assets, all devices, storage, and cloud. Security personnel must know where the infection has infiltrated in order to effectively contain and remediate it. Additionally, the specific strain of ransomware needs to be identified. The options for dealing with the infection may change based on the strain infecting the systems and will allow the HDO to take appropriate remediation actions.

The next steps are to triage impacted systems for restoration and recovery and to identify and prioritize critical systems for restoration and confirm the nature of data housed on impacted systems. Restoration and recovery should be prioritized based on a predefined critical asset list that includes information systems critical for healthcare and safety as well as systems they depend on.

At this point security personnel can start to remediate the systems. There are several possible solutions. 1) The first is to restore from a clean backup. Hopefully all the necessary steps to ensure that there is a clean backup. 2) If there isn't a good backup/If a good backup is not available, the HDO officials can accept the loss and try to recreate the data lost. 3) The HDO can pay the ransom and hope they provide the key to decrypt the data.

Once the systems are restored and before they are put back online, the personnel should make sure they are free of any hidden malware the attacker may have left there. It must also be verified the system is up to date with all patches and that all vulnerabilities have been remediated. Since the systems must be redone, it is a perfect time to make sure they are as secure as they can be. The goal is to make sure a ransomware attack does not happen again. The Department of Health and Human Services, Office for Civil Rights published a document that provides guidance for HDO's that have been the victim of a cyber attack. This document is included as "Appendix A".

Recover

The Recover Function refers to a timely recovery to normal operation, reducing the impact of a cybersecurity incident. In response to a ransomware attack, the HDO's next consideration is how to recover. If data is stored in the cloud, both the on-site systems and the cloud-based system may have to be recovered. If the disaster recovery plan calls for restoring the data from the cloud, what needs to be done if the cloud is infected? There are two possible scenarios: first, the backup plan uses immutable/ WORM storage and data can be restored from the backup. Second, the backup just used replication to a geographically separated location. Unfortunately if that is the case, it must be assumed that the cloud data is also infected. According to Gartner, there are three reasons that data cannot just be restored from a backup. 1) The data/ system may have been compromised weeks before anyone realizes there was an attack. 2) Backups from data that is weeks old are of questionable value. What happens if two weeks of data from the electronic medical records data are lost? 3) Scanning of backups when they are created doesn't always work.

The second scenario requires the HDO to build out an Isolated Recovery Environment (IRE) to ensure the data is clean before putting it back in a production environment. Cleaning data and applications via the IRE involves several steps:

1. The data is restored into the IRE, where it is completely isolated.
2. Scan 1: The restored data is scanned with conventional malware detection tools.
3. Scan 2: The next step is to start the application in the IRE then scan with malware scanning tools based on AI/ML to look for anomalous activity, such as attempts to contact external command-and-control servers.
4. Once the data has been scanned and determined to be free of malware, it can be moved into the production environment (Gartner, 2021).

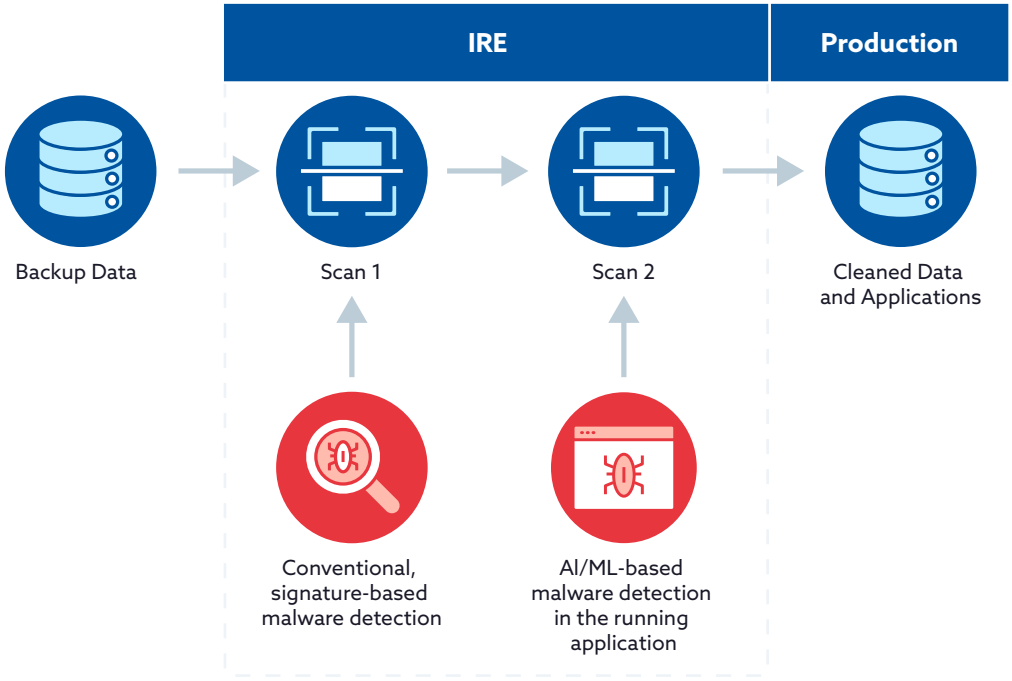

Figure 3 Cleaning Backup Data and Applications in an IRE

It must be remembered that disaster recovery is as essential in the cloud as it is for any other technology. Disaster recovery should be designed using a risk-based approach. The HDO must architect their cloud for failure. While some of these options are costly, they may be necessary due to the criticality of the data. It is essential/crucial to protect the patient's data.

Conclusion

Managing cybersecurity risks requires a clear understanding of the HDO's business and security considerations specific to the technology they use. The HDO, based on their business and technology, can apply the appropriate security controls. Several control frameworks, such as the CSA CCM and NIST SP 800-53, can all be used to support the NIST Cybersecurity Framework. Looking at the process through the lens of the cybersecurity framework core functions of identify, protect, detect, respond, and recover provides a structured, measurable approach to defending against ransomware.

With the year-to-year increase in ransomware attacks and the devastating effects and cost, HDOs are under a significant strain to prevent these attacks. A ransomware attack can significantly impact the HDO's operation, patient safety, and reputation. Ransomware can cause a complete shutdown of healthcare organizations, putting patients at risk. This makes it imperative they do all they can to prevent ransomware.

Fortunately, there are several resources to help fight the spread of ransomware. The Cybersecurity & Infrastructure Security Agency, NIST, has several Special Publication 1800 series that deal with ransomware. Also, MITRE has just unveiled its Ransomware Resource for Hospitals, and Healthcare Providers, a new ransomware resource center designed to help hospitals and other healthcare providers develop and maintain resilient security processes and policies.

References

Belding, G., 2020. NIST CSF core functions: Identify, Infosec Institute, Retrieved from https://resources.infosecinstitute.com/topic/nist-csf-core-functions-identify/

Bitfinder, 2020. Mid-Year Threat Landscape Report 2020, Retrieved from https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

Cimpanu, C., 2021. *Ransomware gang wants to short the stock price of their victims*, Retrieved from https://therecord.media/ransomware-gang-wants-to-short-the-stock-price-of-their-victims/

Dobran B., 2019.27 *Terrifying Ransomware Statistics & Facts You Need To Read*, Retrieved from https://phoenixnap.com/blog/ransomware-statistics-facts

Digital Hands, 2021. *How to Prevent & Respond to Ransomware Attacks: A Cybersecurity Playbook for Hospitals*, Retrieved from Whitepaper: How To Prevent & Respond to Ransomware Attacks | Digital Hands

EMSISOFT Malware lab, 2021. The State of Ransomware in the US: Report and Statistics 2020, Retrieved from https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/

Gartner, 2021. *Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware*, Retrieved from https://www.gartner.com/doc/reprints?id=1-25ATIQU6&ct=210222&st=sb

Kumar P.R., Ramlie, H.R.E.B.H. (2021) Anatomy of Ransomware: Attack Stages, Patterns and Handling Techniques. In: Suhaili W.S.H., Siau N.Z., Omar S., Phon-Amnuaisuk, S. (eds) Computational Intelligence in Information Systems. CIIS 2021. Advances in Intelligent Systems and Computing, vol 1321. Springer, Cham. https://doi.org/10.1007/978-3-030-68133-3_20

McGee, M.K., 2019. *Medical Practice to Close in Wake of Ransomware Attack*, Bank Info Security, Retrieved from https://www.bankinfosecurity.com/medical-practice-to-close-in-wake-ransomware-attack-a-12321

Metivier B., 2019. *Anatomy of a Ransomware Attack and How to Detect the Threat*, Tyler Cybersecurity, Retrieved from https://www.tylercybersecurity.com/blog/anatomy-of-a-ransomware-attack-and-how-to-detect-the-threat

Multi-State Information Sharing & Analysis Center, 2020. *Ransomware Guide*, Cybersecurity & Infrastructure Agency, Retrieved from https://www.cisa.gov/publication/ransomware-guide

National Institute of Standards and Technology, 2018 *Framework for Improving Critical Infrastructure Cybersecurity*, Retrieved from https://doi.org/10.6028/NIST.CSWP.04162018

Netapp, 2020. *Ransomware in the Cloud*, Netapp, Retrieved from https://cloud.netapp.com/hubfs/Ransomware%20in%20the%20Cloud%20Prevention%20and%20Remediation%20with%20NetApp%20Cloud%20Volumes%20ONTAP-V4.2-big.pdf

Singh A., 2019. *Ransomware: How to Prevent or Recover from an Attack*, Backblaze, Retrieved from https://www.backblaze.com/blog/complete-guide-ransomware/

Tolson B., 2020. *How to ransomware-proof your cloud-based data archiving and information management repositories*, Archive360, Retrieved from https://www.archive360.com/blog/how-to-ransomware-proof-your-cloud-based-data-archiving-and-information-management-repositories

US CERT, 2020. *How to Protect Your Network from Ransomware*, Cybersecurity & Infrastructure Agency, Retrieved from https://us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf

Appendix A

What should an entity do when it has just experienced a cyber attack?

A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR)

When an HDO has just experienced a ransomware attack or other cyber-related security incident, they wonder what to do. This guide briefly explains the steps for a HIPAA-covered entity or its business associate (the entity) to take in response to a cyber-related security incident. In the event of a cyber attack or similar emergency an entity should undertake the following actions.

The entity/organization must execute its response and mitigation procedures and contingency plans.ii For example, the entity should immediately fix any technical or other problems to stop the incident. The entity should also take steps to mitigate any impermissible disclosure of protected health information (iii), which may be done by the entity's own information technology staff, or by an outside organization brought in to help (which would be a business associate (iv) if it has access to protected health information for that purpose).

The crime should then be reported to other law enforcement agencies, which may include state or local law enforcement, the Federal Bureau of Investigation (FBI), and/or the Secret Service. Any such reports should not include protected health information, unless otherwise permitted by the HIPAA Privacy Rule. (v) If a law enforcement official tells the entity that any potential breach report would impede a criminal investigation or harm national security, the entity must delay reporting a breach (see below) for the time the law enforcement official requests in writing, or for 30 days, if the request is made orally. (vi)

The affected organization/entity should report all cyber threat indicators (vii) to federal and information-sharing and analysis organizations (ISAOs), including the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs. Any such reports should not include protected health information. OCR does not receive such reports from its federal or HHS partners. (viii)

The entity must report the breach (ix) to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals, and notify affected individuals and the media unless a law enforcement official has requested a delay in the reporting. OCR presumes all cyber-related security incidents where protected health information was accessed, acquired, used, or disclosed are reportable breaches unless the information was encrypted by the entity at the time of the incident or the entity determines, through a written risk assessment, that there was a low probability that the information was compromised during the breach. An entity that discovers a breach affecting fewer than 500 individuals has an obligation to notify individuals without unreasonable delay, but no later than 60 days after discovery; and OCR within 60 days after the end of the calendar year in which the breach was discovered.

OCR considers all mitigation efforts taken by the entity during any particular breach investigation. (x) Such efforts include voluntary sharing of breach-related information with law enforcement agencies and other federal and analysis organizations as described above. (xi)

Footnotes:

i. The HIPAA Security Rule defines a "security incident" as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See 45 C.F.R. § 164.304. For additional details on OCR's recommendations for preventing and responding to a ransomware attack, please refer to OCR's ransomware guidance. See https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

ii. The HIPAA Security Rule requires HIPAA covered entities and business associates to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. See 45 C.F.R. § 164.308(a)(6). The HIPAA Security Rule also requires HIPAA covered entities and business associates to establish and implement contingency plans, including data backup plans, disaster recovery plans, and emergency mode operation plans. See 45 C.F.R. § 164.308(a)(7). See also https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf?language=es.

iii. Protected health information or PHI includes all individually-identifiable health information held by HIPAA covered entities and business associates, except for employment records, records covered by FERPA, or information about individuals deceased more than 50 years. PHI includes any health information that relates to the care or payment for care for an individual, and includes, for example, treatment information, billing information, insurance information, contact information, and social security numbers. See also https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

iv. A business associate includes any vendor that creates, receives, maintains, or transmits protected health information (PHI) for or on behalf of a HIPAA-covered entity. This includes vendors that have access to PHI to provide IT-related services to the covered entity. See 45 C.F.R. § 164.103, § 164.308, and § 164.502. See also https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.

v. The HIPAA Privacy Rule permits the disclosure to law enforcement agencies under certain circumstances. See 45 C.F.R. § 164.512(f). See also https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html.

vi. See the HIPAA Breach Notification Rule at 45 C.F.R. § 164.412.

vii. The Cybersecurity Information Sharing Act of 2015 (CISA) describes cyber threat indicators as information that is necessary to describe or identify: malicious reconnaissance; methods of defeating a security control or exploitation of a security vulnerability; a security vulnerability; methods of causing a user with legitimate access to defeat of a security control or exploitation of a security vulnerability; malicious cyber command and control; a description of actual or potential harm caused by an incident; any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or any combination thereof. See also https://www.hhs.gov/hipaa/for-professionals/faq/2072/covered-entity-disclose-protected-health-information-purposes-cybersecurity-information-sharing/index.html.

viii. The Cybersecurity Information Sharing Act of 2015 (CISA) in Sec. 106 provides that "liability protections are provided to entities acting in accordance with this title that: (1) monitor information systems; or (2) share or receive indicators or defensive measures, provided that the manner in which an entity shares such indicators or measures with the federal government is consistent with specified procedures and exceptions set forth under the DHS sharing process."

ix. Breaches affecting fewer than 500 individuals should be reported to affected individuals as soon as possible, but within no later than 60 days, and reported to OCR within 60 days of the end of the calendar year in which the breach was discovered. See the HIPAA Breach Notification Rule at 45 C.F.R. § 164.404 and 164.408.

See the HIPAA Breach Notification Rule at 45 C.F.R. § 164.402-414.

x. The HIPAA Enforcement Rule provides that in determining the amount of any applicable civil money penalty, OCR may consider mitigating factors, including matters that justice may require. See 45 C.F.R. § 160.408(e). See also https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html.

xi. The HIPAA Privacy Rule permits the disclosure to law enforcement agencies under certain circumstances. See 45 C.F.R. § 164.512(f). See also https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html.