Cybersecurity White Paper HealthCare Security Best Practices

Contents

1 Information Security Overview

1.1 Purpose of White Paper

This white paper will help LeadingAge members and other aging services organizations to understand cybersecurity threats, how to mitigate them, and how to respond if attacked. In addition, the white paper includes an evaluation tool that will help providers identify where they may be at risk, so that they can work to plug those vulnerabilities.

1.2 Executive Summary

Health care providers are among the most frequently pursued cyberattack targets for two reasons: the data stored in their systems is lucrative, and security is often weak compared to other industries; this is especially true for aging services providers handling personal, financial, and health data of their residents and clients. The situation is urgent enough that in 2014, the Federal Bureau of Investigation formally warned health care that the industry is under attack.

Today, the threat continues to evolve and is highly complex. Cyberattacks are also very expensive, with the average cost of a breach pegged at over $2.4 million in notification, forensics, legal fees, and fines. This white paper will help you understand what the specific threats to your organization are, how to mitigate them, and what to do if you are attacked.

HIPAA: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) covers and regulates most health care organizations. Many LeadingAge organizations are subject to HIPAA rules. However, even if HIPAA does not cover your organization, you still have a responsibility to protect sensitive information and are subject to state regulations. Be aware that breaches and other incidents may lead to an investigation by the Office for Civil Rights (OCR), the division of the United States Department of Health and Human Services that enforces HIPAA.

Threats, Vulnerabilities, and Risks: Knowing what to look for is key to preventing cyberattacks. The top 10 most common threats for organizations are phishing attacks, negligent and malicious insiders, advanced persistent threats, cyberattacks, zero day attacks,

known software vulnerabilities, social engineering, denial of service attacks, and brute force attacks.

The good news is that you can mitigate these vulnerabilities through a variety of actions and technologies. These include external and internal network analysis, software and patch management, policies and procedures, end-user training, backups and contingencies, and having cyber liability insurance. Knowing the impact of various threats can help you prioritize your organization's action plan.

Management Techniques: Solid management techniques can also mitigate your organization's risk. These include an effective security posture, which includes systems, processes such as policies and procedures, education, and ongoing monitoring. You'll want training that raises your employees' awareness of threats, a defense in depth strategy, and careful vendor vetting and management.

As with everything that's critical to your organization's success, you'll need an adequate budget and investment in cybersecurity, including funds for staffing and tools.

Assessment, Planning, Prevention, and Response: An honest assessment of your information security program can also help you to better manage threats, as can involving your organization's senior leadership in the process. Developing strong reference architectures, reviewing your infrastructure architecture, and training employees to spot and avoid threats are also important pieces of the puzzle.

Planning your response to a threat before one happens can be invaluable. The Office of Civil Rights, part of the United States Department of Health & Human Services, has prepared a checklist so that you will know which agencies, law enforcement, and individuals your organization must notify.

Technology Infrastructure: When it comes to technology infrastructure, an array of hardware devices, software applications, security appliances, strategies, and techniques can help your organization combat modern cyber threats. Valuable infrastructure includes next-generation firewalls, network access controls, state-of-the-art e-mail filtering systems, cloud anti-virus software applications, updated endpoint management systems, and a sound backup and disaster recovery (BDR) solution.

1.3 Disclaimer

The information in this white paper provides general information about cybersecurity and guidance; it is not intended as legal advice nor should you consider it as such.

1.4 Information Security

News of a health care security breach or ransomware incident has become almost commonplace, as hackers are becoming increasingly proficient in detecting and exploiting security vulnerabilities in IT security in health care and other organizations. In response,

many health care organizations are preemptively working to identify and eliminate security vulnerabilities in operating systems, applications, and configurations as well as relevant policies and procedures.

Information security is about protecting the confidentiality, integrity, and availability (CIA) of information.

What Is Information Security?

In its purest sense, however, information security is about protecting the confidentiality, integrity, and availability (CIA) of information:

- Confidentiality: The most obvious information security component requires keeping sensitive information accessible only to those authorized to access it. Example threats to confidentiality are stolen laptops, hacked user accounts, unencrypted transmission of data, etc.
- Integrity: Information integrity involves ensuring the information is real, accurate, and unchanged from its original form. Example threats to integrity include the intentional or accidental modification of a medication list or pass, diagnosis, or directives that could lead to resident harm, billing transactions, etc.
- Availability: Information availability concerns keeping the information accessible to authorized users. Some threats to availability involve down servers, natural disasters, inaccessibility to the internet, access to cloud-based information, etc.
- What Threatens Information Security?

Threats to information security can be categorized in four general areas:

- **Malicious or Adversarial Outsiders:** These are actors outside of your organization with malicious intent. Actors could be individuals, groups, organizations, or nation-states. Examples include criminals attempting to encrypt your data for ransom.
- **Malicious or Adversarial Insiders:** These are malicious actors that are part of your workforce with access to information and with bad intent. Examples include a disgruntled employee, or a clinical worker that steals information to sell on the black market.
- **Structural or Environmental:** These threats involve failure of equipment or natural or man-made disasters that damage critical infrastructure and are outside of the organization's control. Examples are a water pipe break that floods a data center, a tornado or hurricane that damages critical IT equipment, or a telecommunications failure by a vendor.

- **Unintentional/Accidental:** These include unintentional acts by individuals in the normal course of business. Examples are accidently sending personal health information (PHI) to the wrong party, losing an unencrypted thumb drive, or accidently exposing personal or electronically protected personal health information to the internet without protection of a properly configured firewall.

What Is Cybersecurity?

Cybersecurity is a subset of information security. It generally focuses on the measures to protect information from malicious threat sources that affect confidentially, integrity, and availability of information. Following are a few examples of cyberthreats to CIA in a health care environment:

- **Confidentiality**
    - Hacker stealing personal or health information.
    - Employee downloading/exporting resident or employee information and selling it on the black market.
    - Employee accessing information about a fellow employee or resident for malicious purposes.
    - Losing an unencrypted thumb drive with resident or employee personal or health information.
- **Integrity**
    - Hacker or employee maliciously modifying, creating, or deleting billing or clinical information.
    - Employee or vendor modifying health information.
- **Availability**
    - Ransomware attack rendering data unusable until backups are accessed or encryption key obtained.
    - Malicious denial of service (DoS) attack degrading network performance and affecting operations.

- Server failure at your organization or a vendor.

1.5 Cybersecurity in Health Care

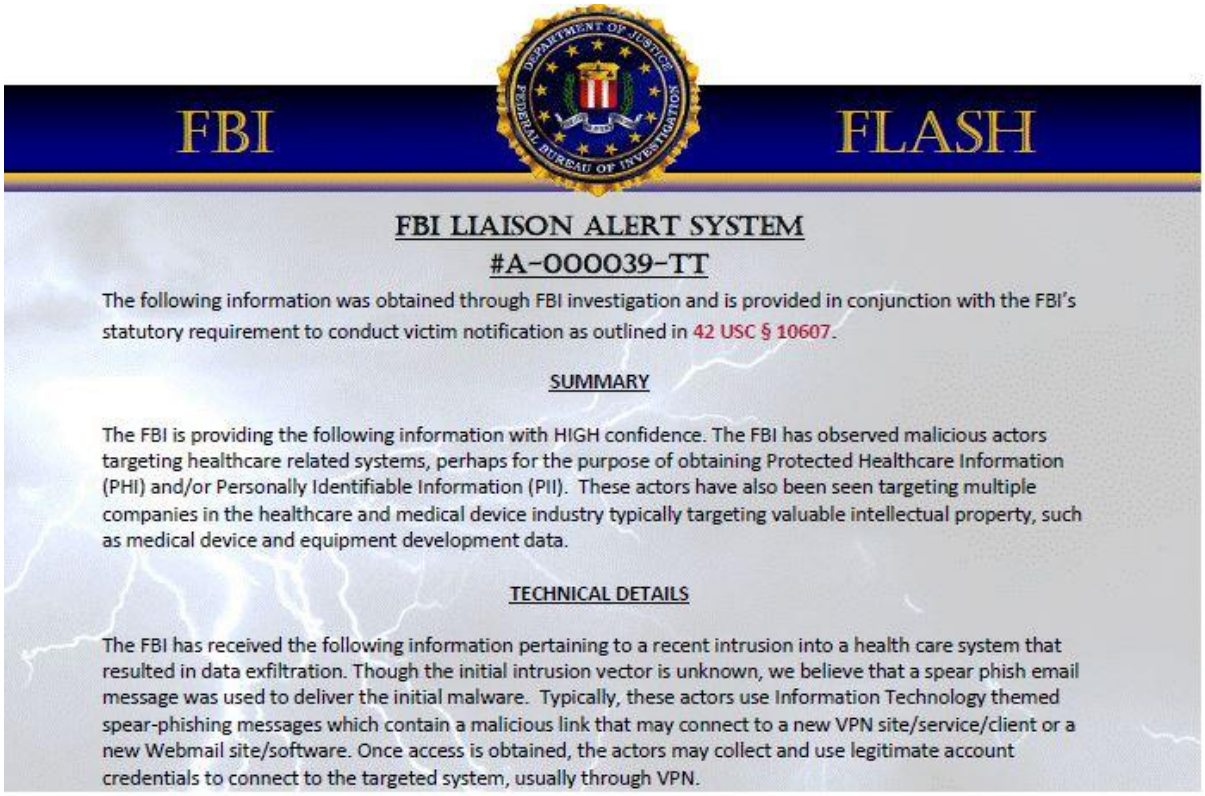
Nearly every day, organizations and individuals face new cyberthreats, and the topic can be complex and ever-evolving. For example, in 2015, the top 10 largest cyberattacks against health care organizations personally affected more than 35% of the United States population.

Health care providers are among the most frequently pursued cyberattack targets, largely because the data stored in their systems has become lucrative. The combination of value of information and weak security defenses, compared to other industries, makes health care a popular hunting ground for cybercriminals. In mid-2014, the Federal Bureau of Investigation formally warned health care that the industry is under attack.

Long-term and post-acute care is often at even greater risk than other health care providers.

In fact, electronic health records (EHRs) contain the trifecta of hacker currency: PHI, including electronic PHI (EPHI), personal identifiable information (PII), and financial information. The value of health information on the black market can be even more profitable when you consider additional nefarious uses such as medical billing fraud.

Hackers are zeroing in on health care organizations that don't have the proper technical, physical, and administrative safeguards in place. Long-term and post-acute care is often at an even greater risk, because this sector's information security is less mature than acute care's.



FBI FLASH

FBI LIAISON ALERT SYSTEM

#A-000039-TT

The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607.

SUMMARY

The FBI is providing the following information with HIGH confidence. The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII). These actors have also been seen targeting multiple companies in the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data.

TECHNICAL DETAILS

The FBI has received the following information pertaining to a recent intrusion into a health care system that resulted in data exfiltration. Though the initial intrusion vector is unknown, we believe that a spear phish email message was used to deliver the initial malware. Typically, these actors use Information Technology themed spear-phishing messages which contain a malicious link that may connect to a new VPN site/service/client or a new Webmail site/software. Once access is obtained, the actors may collect and use legitimate account credentials to connect to the targeted system, usually through VPN.

Some recent statistics about health care data breaches are as follows:

- For the second year in a row, criminal attacks are the leading cause of data breaches in health care.
- Of health care organizations, 89% had at least one data breach involving the loss or theft of patient data in the past 24 months, and 45% had more than five breaches[i].
- The average number of days before a breach is detected is 201.

2 Information Security and HIPAA

Summary: HIPAA, which establishes national security standards and requires certain safeguards, covers ar care organizations. Many LeadingAge organizations are subject to HIPAA rules. However, even if HIPAA do organization, you still have a responsibility to protect sensitive information and are subject to state regula

Breaches and other incidents may lead to an investigation by the Office for Civil Rights (OCR), the division Department of Health and Human Services that enforces HIPAA.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), which establishes national securi certain safeguards, covers and regulates most health care organizations. However, even if HIPAA does not you still have a responsibility to protect sensitive information and are subject to state regulations.

Even if HIPAA does not cover your organization, you still must protect sensitive information and meet state regulations.

Does HIPAA Cover Your Organization?

Determining if HIPAA covers your organization can be complicated, based on your organization's businesses and relationships. A basic test is that if your residents are 100% private pay, then HIPAA does not cover your organization.

Most LeadingAge organizations and Life Plan communities (formerly known as Continuing Care Retirement Communities or CCRCs) have both HIPAA-covered and non-covered components. Independent living and assisted living (in most states) are considered not covered, while HIPAA usually covers skilled nursing, some home health, hospice, therapy, memory care, etc. If any part of your organization is covered, please pay close attention to the HIPAA portions of this white paper.

Relevant laws address three parts of HIPAA:

- **HIPAA Security Rule:** Regulations pertaining to the protection of EPHI.
- **HIPAA Privacy Rule:** Regulations affecting resident/patient rights and an organization's responsibility to protect PHI.
- **HIPAA Breach Notification Rule:** Regulations related to an organization's responsibility to detect, assess, and mitigate breaches and to notify appropriate parties in a timely manner.

The relation of HIPAA to cybersecurity lies mostly in the HIPAA Security Rule. However, breaches, applicable incidents, etc. may lead to an investigation by the Office for Civil Rights (OCR), the division of the United States Department of Health & Human Services that enforces HIPAA. An investigation may examine compliance to all components of HIPAA. In addition to OCR, several other government agencies play a role in HIPAA enforcement, including state Attorney Generals, the Office of the Inspector General, and the Department of Justice.

3 Cyberthreats, Vulnerabilities, and Risk

Summary: The top 10 most common threats for organizations are phishing attacks, negligent and malicio persistent threats, cyberattacks, zero day attacks, known software vulnerabilities, social engineering, deni brute force attacks.

Attacks often follow a process, from information gathering to intrusion and infiltration, malware deployment, data extraction, and cleanup.

Through certain actions and technologies, you can reduce your organization's risk. This section describes how to carry out external and internal network analysis, software and patch management, policies and procedures, end-user training, backups and contingencies, and the importance of having cyber liability insurance. It also discusses the impact of specific risks, to help you prioritize your cybersecurity actions.

3.1 Top Threats

While many types of cyberthreats exist, the top 10 most common threats for organizations are as follows:

Threat	Description
Phishing Attacks	Phishing is an attempt to glean sensitive information (such as usernames / passwords / personally identifiable information / etc.), often for malicious reasons, by disguising as a trustworthy entity in some form of electronic communication.
Negligent Insiders	A negligent insider can be defined as a current, former, or contract employee who inadvertently exploits information or exceeds his or her authorized level of network, system, or data access in a way that affects the security of the organization's data, systems, or daily business operations.
Malicious Insiders	A malicious insider can be defined as a current, former, or contract employee who deliberately exploits information or exceeds his or her authorized level of network, system, or data access in a way that affects the security of the organization's data, systems, or daily business operations.
Advanced Persistent Threats	An advanced persistent threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific organization or entity. APT processes require a high degree of covertness over a sustained period of time. They will often use multiple cyber techniques orchestrated to extract sensitive information over time.
Cyberattacks	Typical cyberattacks can be classified as malware or ransomware. This umbrella term refers to a variety of hostile or intrusive software applications including computer viruses, worms, Trojan horses, spyware, adware, and scareware. It can take the form of executable code, scripts, active content, and other software.
Zero Day Attacks	A zero day attack refers to a hole in a software application or operating system that is unknown by the software vendor. Hackers exploit the security hole before the vendor becomes aware and can issue a patch or release to fix it.
Known Software Vulnerabilities	Very similar to a zero day attack, a known software vulnerability is a hole in a software application or operating system that the vendor is aware of but has not fixed or patched yet.
Social Engineering	Social engineering refers to psychologically manipulating people into performing actions or divulging confidential information. It is a type of confidence trick for the purposes of information gathering, fraud, or system access.
Denial of Service Attacks	A denial-of-service (DoS) attack occurs when a malicious perpetrator seeks to render a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the internet.
Brute Force Attacks	A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automation software is used to generate a large number of consecutive guesses in a short amount of time to guess at the value of desired data.

While these threats constitute a large number of information breaches in the United States, there are literally hundreds of other types of cyberattacks to which organizations can be susceptible. Despite there being so many types of cyberthreats, they have a pretty routine anatomy.

Anatomy of a Cyberattack

- **Information Gathering:** Hackers will attempt to glean any information that they can in attempt to identify users within an organization who may have privileged access or information. These activities may happen through social engineering or through targeted research on individuals through web searches, job postings, websites, and

social media. Targets may even receive a phone call from the perpetrator attempting to glean information that would allow the perpetrator to gain unwarranted access.

- **Intrusion and Infiltration:** Using the information that the offender has gleaned, the perpetrator may employ any number of cyberthreats to gain access to network or systems. This may be through phishing attempts, theft, negligent or malicious users, known software vulnerabilities, zero day attacks, or even brute force attacks. The hacker will use any means to gain access to network or system resources to begin stealing protected information.
- **Malware Deployment:** Once in, the hacker may install some sort of malicious software (such as malware or ransomware) to begin manipulating the network's or system's information. The malware may be either controlling or destructive in nature, but the intent is to either steal information or use the malware as ransom for payment before business systems become usable again.
- **Data Extraction:** Also known as advanced persistent threats, this phase of the cyberattack can continue until the perpetrator is discovered. The average duration for most cyberattacks is 280 days, meaning that hackers can continue to extract information for weeks or months until their activities are discovered.
- **Cleanup:** Some cyberattacks go completely undetected. A hacker may gain access to a network or system and steal information for long periods of time. After the damage is done, the hacker may take steps to cover up or hide any evidence that the network or system was hacked at all. Sophisticated cyberattacks may use zombie botnets (a network of compromised computers running malicious code repetitively), or other viruses and worms, to destroy digital fingerprints and other forensic evidence of infiltration.

3.2 Vulnerabilities

Organizations that seek to mitigate cyberattacks should consider a host of vulnerabilities. While organizations can systematically prevent many cyberthreats, human elements can also greatly impact an organization's vulnerability.

It is important to evaluate your firewalls and how your organization segments internal LAN traffic.

External Network Analysis

It is very important to critically evaluate how your organization connects to the internet and how it filters traffic that passes from the internet into your organization and vice-versa. This is typically done through a networking appliance called a firewall.

Over the past couple of years, firewall technologies have significantly evolved, and many industry experts are referring to these modern hardware appliances as “next-gen firewalls.” A typical next-gen firewall will have Application Layer (Layer 7) networking capabilities including mail, file, and webpage protocols[1], as well as cyberthreat subscription services. That way, the firewall can routinely receive definition update files on current cyberthreats and seek to actively monitor or block that malicious content and/or sites from passing through the firewall. Examples of next-gen firewall appliances include Cisco’s Firepower devices[2].

Because of the advanced capabilities of modern next-gen firewalls, many organizations are choosing to also implement security incident and event management (SIEM) logging systems. With so much information passing through firewalls, it is impossible for humans to review the massive amount of information contained in very dynamic log files. SIEMs are able to synthesize incredible amounts of log file information and present critical information to security experts or network administrators who can then review and intervene as necessary. Examples of SIEMs include LogRhythm[3].

Internal Network Analysis

Equally important is evaluating how your organization segments internal local area network (LAN) traffic. For many senior living and LTPAC providers, the modern LAN is used for much more than business-related information-sharing or connectivity. Many providers are allowing residents, guests, visitors, and contractors onto their network, whether physically connected or connected through Wi-Fi. With the advent of IoT devices, which heavily rely on a wireless network, extra care needs to be taken to design the network properly so as to provide a secure connection for critical devices. Higher Priority Quality of Service (QoS) can be applied to business-critical devices across the network than regular devices.

It is very important to create virtual segmentation of the LAN so that sensitive information traffic such as PII or PHI cannot be transmitted outside of the intended LAN. Additionally, it is very important to ensure that organizations have a way of only allowing intended users to access networking resources. Implementing a network access control (NAC) solution is vitally important.

It is vitally important to stay up to date with current software operating systems, patches, and releases.

Software and Patch Management

It is vitally important that computers, servers, and any other network-connected devices (also known as Internet of Things (IoT) devices) such as security cameras or appliances stay up to date with current software operating systems, patches, and releases.

Many of the major cyberattacks that have made headline news have been a direct result of zero day attacks or known software vulnerabilities. These cyberattacks can be easily prevented by routine maintenance of devices. IT administrators need to ensure that all devices are running supported operating systems and have routine updates applied to things like operating systems, commercial software applications, appliances (Java, Flash, and the likes), and anti-virus applications.

Device management software utilities can help organizations maintain inventories of hardware devices, configuration statuses, and deployment of available releases, patches, and updates. Examples include Oracle Utilities Operational Device Management solution[4].

Policies and Procedures

Organizations need to carefully craft and institute policies and procedures that enforce the way users access information and interact with network or system resources. Some policies and procedures, such as password policies, can be systematically enforced. Other policies will exclusively govern the way that information is stored, accessed, or shared.

For senior living and LTPAC, these policies must address HIPAA and HITECH governance. They should also consider the administrative, physical, and technical safeguards needed to keep organizations in compliance. Additionally, policies and procedures can assist organizations if or when a data breach occurs.

Having a well-thought-out, executable plan can dramatically reduce an organization's risk or exposure to data breaches or cyberattacks. It can also help the organization's defense in case of a breach or cyberattack. Check out **relevant resources from LeadingAge partners**[5].

Humans are probably the weakest link in cybersecurity. Organizations should train employees on the types of cybersecurity threats to which they may be exposed.

End-User Training

Humans are probably the weakest link in cybersecurity. Hence, organizations should invest in their workforce and train employees on the types of cybersecurity threats to which they may be exposed. As workforce members are more cognizant of current threats, they can hopefully avoid being conned into sharing information that otherwise isn't intended to be shared. A great example here is phishing attempts. If all of the end-users are aware of what a phishing attempt is and are trained on ways that they can identify potential phishing attempts, they will be far less likely to be duped into sharing information through a phishing scam than if they had no idea what to look for.

Backups and Contingencies

Should an organization be affected by a cyberthreat, or face some sort of data breach, it is vitally important to have contingencies in place to restore breached information or rely on data backups and disaster recovery systems to maintain ongoing operations. A ransomware attacks is a great example where up-to-date backups would come in handy.

Cyber Liability Insurance

Given the increased reliance on technology and data in everyday operations, and the evolving nature of cyberthreats, it is highly recommended that organizations have cyber liability insurance to provide some financial means of remedying attacks or breaches if/when they happen.

Depending on the severity of the cyberattack, an organization may need to hire technology forensic experts to determine the nature of the cyberattack. There may be attorney's fees to litigate any potential lawsuits or fines that an organization may face. There may be additional costs to provide enhanced data protection for those impacted by the data breach for which the organization would be liable.

These costs can quickly add up to hundreds of thousands or even millions of dollars, depending on the impact. Make sure you read the fine print of your cyber liability insurance. Know the types of attacks or breaches covered, the specific expenses covered and their limits, the types of events not covered, and the conditions that would result in revocation of the policy. LeadingAge Gold Partner **AON** has a **LeadingAge Recognized Program** that offers cyber liability insurance.

3.3 Risk/ Impact

3.3.1 Downtime

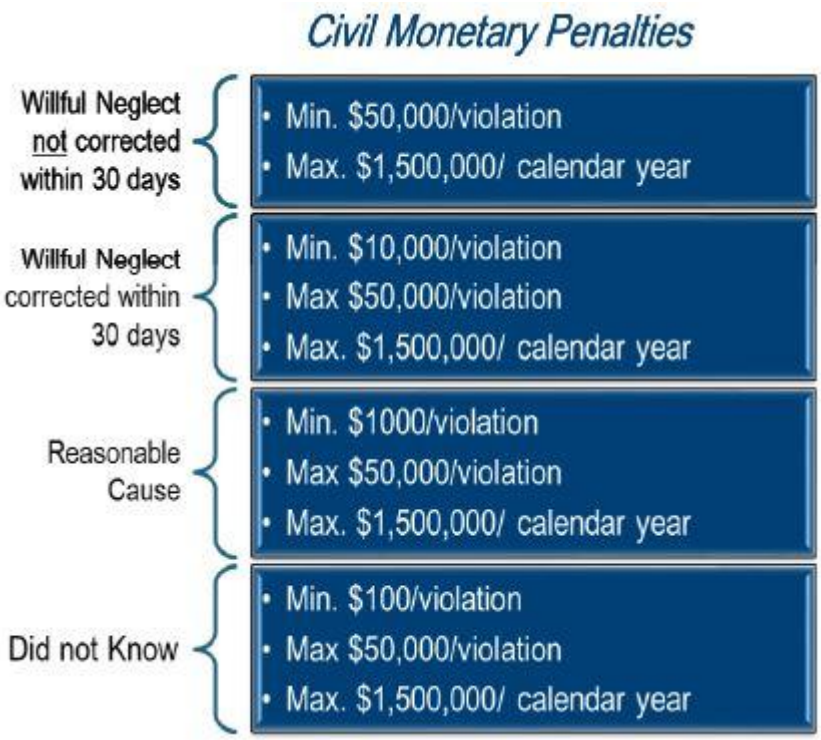
Downtime as it relates to cybersecurity results in a computing or network device being unavailable to users. Events that result in downtime create a vulnerability that is exposed due to lack of system patching, or lack of adequate monitoring, or security controls both internally and externally. For example, ransomware can create considerable downtime until a good backup is restored or files are unlocked. Downtime often results in significant financial loss and an unproductive workforce. It may even threaten the lives of high-risk patients or residents.

The average cost of a breach is over $2.4 million in notification, forensics, legal fees, and fines.

3.3.2 Financial

3.3.2.1 *Fines/Penalties*

Companies that process or maintain personal information have a responsibility to protect that information. There are standards for credit card processing, medical records, and privacy that could result in large legal fees, credit protection service costs, and implications on the organization's reputation if that data is lost or stolen. Encrypting that data both in motion and at rest is mandatory under many of these standards.



The average cost of a breach is over $2.4 million in notification, forensics, legal fees, and fines. For example, CardioNet recently agreed to settle a breach for $2.5 million, underscoring the need for protecting data[6].

3.3.2.2 *Ransom*

Ransom is a payment to a malicious actor to restore a working environment. Malware that is typically associated with some form of payment demands is called ransomware. Anti-virus that is signature-based may not be a good defense to protect against ransomware. As this malware is typically unknowingly downloaded when a user visits an infected site or clicks on a link within an e-mail, good URL filtering tools and behavioral-based anti-virus may be more effective.

OCR considers ransomware a breach.

It is important to note that OCR considers ransomware a breach. A breach risk assessment process will determine if the breach is reportable. Please see **section 5.4** for more information on response to a breach or a cyberattack, including reporting requirements.

3.3.3 Rapid Forensic/Remediation

Many experts say it's not when you will be infected by malware or when you will be compromised, it's when you will be aware that you have been compromised. The reality is there is big money in compromising a system, and there are endless resources on the internet that walk hackers through an attack step by step, with tools and scripts freely available.

Cyberwarfare is organized, and simply blocking an IP address or a block of IP addresses, or restricting access to a specific TCP or UDP port in your firewall, is simply no longer enough. To survive, you need adequate defenses to actively monitor and be able to constantly mine and correlate events that occur in your computing environment. Having and testing an incident response program is important.

Forensics is a highly technical activity that often requires more technical depth than you might have in-house. Computing operating systems are becoming increasingly more powerful and more complex. They will always contain flaws that individuals or groups chipping away at the system will expose. It might be worthwhile to build a relationship with a reputable third party that has forensic expertise.

Government regulations often require system audits, vulnerability scans, and application penetration testing. These activities conclude with a report of potential vulnerabilities that could be exposed.

Remediation is the process of fixing those vulnerabilities and may include patching to the latest patch release, updating software to the latest version, segmenting servers from the general network, and restricting access to data. Sometimes the cost to remediate those issues outweighs a company's risk tolerance. In other cases, remediation of the vulnerability might not be feasible—for example, the developer has not released a patch yet. In these cases, organizations should look for mitigating controls to help prevent that vulnerability from being exposed.

It takes a lifetime to build a good reputation, but just an instant to destroy it.

3.3.4 Reputation

It takes a lifetime to build a good reputation, but just an instant to destroy it. Strong organizations have good reputations when they maintain good practices and provide exceptional products and services.

Consumers expect organizations to protect their data. When a company or an organization is compromised, it is highly likely that sensitive data is exposed. When this happens, the organization's reputation is also compromised. Reputation can also be compromised when

an organization's website is attacked and the site's content is changed, or a denial of service prevents consumers from accessing the website.

3.3.5 Data Loss / Data Theft

Data is located many places. It can be located on printed documents, mobile devices, backup media, databases, flat files, file stores, websites, and any number of other places. Organizations should have a data classification policy that identifies how critical the data is. The more sensitive the data, the more valuable they are, and the higher access controls should be in place.

Data Loss: It is important to know where data is in your environment, so that you can ensure appropriate access. Data loss is when data is not where it is supposed to be. Say you store your backup tapes at a specified location, and all backups are supposed to be there. One day you need to perform a restore of the data and realize the backup is not there. This is data loss. If that data contains personal identifiable information (PII), payment card industry (PCI), personal health information (PHI) or HIPAA-protected data, you might be subject to fines, penalties, and other financial losses.

Data Theft: Data theft, on the other hand, is when your environment is breached and that data is taken. Technologies such as data loss prevention (DLP) provide some protection against data theft. Data theft could also occur internally when an employee transfers sensitive data to cloud storage or portable storage, like a USB stick. Your organization's policy should indicate who has access to sensitive data and how it should be handled.

3.3.6 Breach

A breach is said to occur when unauthorized access to a network, system, application, or data occurs. A breach can occur with or without the knowledge that it occurred by the owner or custodian of the network, system, application, or data.

3.3.7 Corrective Action Plan (CAP)

In addition to levying fines if a breach occurs and violations are found, OCR can enforce the implementation of a corrective action plan, which can span years and impose remediation goals under specific timeframes with regular updates to the United States Department of Health & Human Services. Please see the examples listed below and **section 5.4** for the quick response to a breach or cybersecurity attack.

3.3.8 Bad Audit

OCR also conducts random audits utilizing the OCR HIPAA Audit protocol. An unfavorable audit can result in an investigation leading to fines and potential corrective action plan.

3.3.9 Examples/Vignettes

This **OCR webpage** lists examples of violations and resolution agreements.

4 Management Techniques

Summary: Management techniques that can reduce your organization's risk include an effective security p and investment in staffing, tools, training that raises your employees' awareness of threats. They also incl strategy, plus careful vendor vetting and management.

4.1 Effective Security Posture

It is not enough to go through the motions of an assessment, purchasing a few cybersecurity tools and believing you are well-protected against cyberthreats that can damage your organization's reputation or, worse, result in an adverse health care outcome.

Cyber Resilience: Cyber resilience refers to an organization's ability to continuously deliver its intended outcome despite adverse cyber events[7]. The concept of cyber resilience acknowledges that hackers may have innovative tools and approaches plus the element of surprise, but it aims to maintain the organization´s ability to deliver the intended outcome at all times despite those disadvantages.

Cybersecurity: Cybersecurity consists of technologies, processes, and measures that are designed to protect systems, networks, and data from cybercrimes. Effective cybersecurity reduces the risk of a cyberattack and protects entities, organizations, and individuals from the deliberate exploitation of systems, networks, and technologies.

An effective security posture will include systems, processes (policies and procedures), training, education, and ongoing monitoring.

Consider investing in a chief information security officer (CISO), plus tools to help you detect events.

4.2 Budget and Investment in Cybersecurity

It is no longer adequate to appoint a HIPAA Security Officer and install anti-virus software on your network and think you are adequately protected against cyberthreats. Modern organizations have very complex networks, and they require many layers of human and technology solutions to successfully combat the threat of cyberattacks.

Organizations should consider investing in a chief information security officer (CISO), either as a staffed position or outsourced to a managed security service provider (MSSP). This position is responsible for developing and maintaining an appropriate security program for the organization, developing and communicating policies and procedures, offering training, managing systems and tools, and monitoring. The CISO also investigates potential breaches and manages the incident response process.

Investment in tools such as a log and event monitoring system (LEM) and/or a security information and event management system (SIEM) will help you detect events on your network early, and log and correlate them to identify potential abnormal behavior on the network. SIEM solutions can be a big investment both in terms of management as well the necessary security personnel to manage and understand the SIEM logs. Organizations are opting for Managed Security Service Providers to immediately deploy and managed Rreal-time threats, thus concentrating on their core business.

4.3 Training and Awareness

According to the **2015 Cost of Data Breach Study by the Ponemon Institute**[8], 49% of data breaches are caused by malicious or criminal attacks, and 19% are related to employee negligence.
Your employees are an important line of defense against a data breach or cyberattack that could lead to financial or reputation loss for your company. Increased investment in employee training can reduce the risk of a cyberattack 45% to 70%, according to a 2015 study by Wombat Security Technologies and the Aberdeen Group[9].

To be successful, follow these recommendations:

- Start at the top. A successful training program starts with support from senior leadership. Get buy-in by clarifying the business risks and consequences of a data breach.
- Increase employee awareness and train staff and consultants on how to handle confidential information and e-mail safely, and spot and report potential phishing attacks and other social engineering schemes.
- Test the security savvy of employees by simulations, testing, and ongoing education.
- Develop a comprehensive onboarding and off-boarding process, stressing role audit and minimum necessary access to all systems and databases.

Defense in depth impedes intruders from attaining their goals while monitoring their progress and developing responses to repel them.

4.4 Defense in Depth

By regularly reviewing your security posture and risk management program, you will enable your organization to develop a defense in depth and breadth program. An anti-virus program is no longer sufficient to protect an organization against cyberattacks.
Defense in depth as a concept originated in military strategy. It intended to provide barriers to impede intruders from attaining their goals while monitoring their progress and developing and implementing responses to the incident in order to repel them. In the cybersecurity paradigm, defense in depth correlates to detective and protective measures designed to impede the progress of a cyber intruder while enabling an organization to detect

and respond to the intrusion, reducing and mitigating the consequences of a breach. Defense in depth is not one thing, but a combination of people, technology, operations, and adversarial awareness. Thinking and doing solves problems, and technology enables problem-solving by providing a set of tools that can reduce risks. The best technology in the world will not prevent humans from making intentional or unintentional mistakes. Organizations must constantly adjust and refine security countermeasures to protect against known and emerging threats[10].

Defense in depth strategy elements include the following:

- Developing a risk management program to identify threats, characterize risk, and maintain an asset inventory.
- A cybersecurity architecture with standards, recommendations, policies, and procedures.
- Physical security guidelines such as equipment lockdown, access controls, and barriers.
- Network architecture design such as demilitarized zones (DMZ) and virtual LAN (VLAN).
- Network perimeter security, including firewalls and remote access authorization systems.
- Monitoring tools to correlate and identify abnormalities and events.
- Mobile device management systems with corresponding policies and procedures.
- Segregation of IT administrative access from day-to-day access.
- Development, review, and testing of an incident response plan.

During contracting and background checks, vet the vendor's cybersecurity issues.

4.5 Vendor Management

It is unusual nowadays to have an organization provide all of the IT services and supports in-house without relying on external vendors and/or consultants. This includes Managed Service Providers (MSP), Managed Security Service Provider (MSSP), vendors providing application software and services, hosting vendors, and IT consultants. Each one of these vendor or consultant relationships can open the door for accidental or malicious cybersecurity risks and events.

To best protect your organization, during vendor contracting and background checking, vet not only the business issues with the agreement, but also the cybersecurity issues, which include the following:

- Require a Business Associate Agreement (BAA) where appropriate.
- Require cyber liability insurance.
- Perform exclusion checking for Medicaid and Medicare databases.
- Request SSAE [ii]16 SOC 2 Type 1 and/or Type 2 reports. SOC 2 measures controls specifically related to IT and data center service providers in areas of security, availability, processing integrity, confidentiality, and privacy. Type 2 includes a data center's system and suitability of its design of controls.

5 Assessment, Planning/Preparation, Prevention, and Response Management

Summary: Assessing your information security program to better manage threats is an important first ste organization's senior leadership in the process. Also critical are developing strong reference architectures, infrastructure architecture, and training employees on how to spot and avoid threats.

If an attack happens, having a copy of the Office of Civil Rights checklist will help you know which agencie individuals your organization must notify.

5.1 Assessment

There is an old management saying: What you cannot measure, you cannot manage. Most people do not like assessments of any kind, but without assessing your information security program, you will surely not be able to manage the barrage of potential threats that will target your environment. In addition, HIPAA, PCI, Sarbanes-Oxley Act of 2002 (SOX), and other federal, state, or local regulations require a third party assess the organization's security.

You should create a team made up of key technology and business leaders to review the state and effectiveness of your information security program. If you have a compliance program in place, these leaders should be invited to participate, as your information system compliance should be part of the organization's overall compliance program. It is better to understand your current security state and to put in place corrective action plans before government assessment. A number of guides and frameworks can help with this assessment.

SANs[11], NIST[12], and Carnegie Mellon's OCTAVE[13] have developed frameworks that help you better understand, classify, assess, prioritize, and manage cybersecurity risks. Assessments are typically performed starting with your policies and procedures and architectural

documentation. Vulnerability scans and penetration tests are commonly completed to check for well-known vulnerabilities.

These scans and tests can produce pages of information. Many times these results are too overwhelming, and nothing gets completed. Teams will argue that remediation costs too much and/or is too complex, or that risks are unlikely to occur.

It is important to have support from senior leadership, a sense of leaders' risk tolerance, and their commitments to making resources available to address risks. It is often better to identify the top risks that should be remediated first, and work on them. Risk management is an ongoing process that is about making continuous improvement, rather than reaching a destination, and requires long-term commitment.

5.2 Planning/Preparation

Information security only works well when all levels of management participate. To be successful, senior management should support a policy around information security that defines management's risk tolerance and reporting requirements.

Performance Indicators

Information security needs to form relationships with all the IT silos as well as key business leaders and to develop performance indicators around security. Examples of performance indicators should include level of patching by criticality of system, number of attacks against those systems by threat, top threats across the organization (threat modeling), percentage of devices without the latest anti-virus definitions or older anti-virus clients, historical trends on threats identified/stopped by firewalls, intrusion detection/prevention systems, and anti-virus systems.

Too much of a seemingly good thing can increase complexity, costs, and frustration levels among staff—or your users.

Reference Architectures

Reference architectures should be developed using resources across IT silos. These reference architectures should include security configurations of the devices involved and describe user access, data flows, sensitivity of data, and infrastructure protection controls.

Too much of a seemingly good thing can increase complexity, costs, and frustration levels among staff or, worse, your users. It is imperative to do the right thing and not overburden the process in the name of security. A publicly accessible website with only publically available or general information does not need the same security controls or architecture as do sensitive business processes, such as the secret ingredient in Coke.

Importance of Planning

Security needs to be well thought-out and planned. It might not be feasible to implement the right level of security with some business processes that have been around for way too many years, and you might not be able to patch every server for one reason or another.

Information security has many weapons in its arsenal. In situations where the approach you want is not feasible, you might be able to build out an isolation network/sub-network also known as de-militarized zone (DMZ), which is isolated physically or logically from the rest of the organization's network. Some firewalls also look at the source user and can be configured with user groups.

The point is that planning needs to occur, and that plan needs to be completed within the guidelines of senior management. Reflect back to risk tolerance and the ability of information security to articulate the real risks to the organization, in terms that management understands. Otherwise, the list of required mitigation can blow up quickly if not controlled, and without strong relationships with your peers and a well thought-out program, you will fail, or at the very least no one will pay much attention to you.

If you understand the risks, have an agreeable reference architecture that makes good sense, built with the input of your peers, and you can articulate real risks to management in a matter-of-fact way, maybe with a little humor mixed in, you will be a hero.

5.3 Prevention Techniques

5.3.1 Infrastructure

Infrastructure is the foundation that all your computer resources are built on. Infrastructure includes the rooms; environmental controls; racks; wiring; routers; switches and servers that provide identity management, logging and reporting; IP address allocations and domain name resolution; Wi-Fi; printing, scanning and imaging; backup devices; etc. Applications that the business uses require the infrastructure to work.

Every component in the infrastructure is subject to vulnerabilities. The malicious actor spends the day hacking away at the software looking for these vulnerabilities. It is not as simple as making sure that you are patched. It is highly recommended that you create cross-silo teams to look at the infrastructure architecture, understanding your organization's risk tolerance, knowing the sensitivity of your data, and creating reference architectures to build or configure your infrastructure so that it gives users access when they need it, in a least privileged way. The team should also monitor access to sensitive information and enforce stronger policy for more sensitive data access.

It is imperative to have regular training for your users.

5.3.2 Training

Our users are the weakest links. The malicious actor understands this and feeds on it. People are inherently helpful, especially to sincere, nice people. All people want to feel important and for others to take interest in the wonderful things they do. This is referred to as social engineering and is a tactic that hackers use effectively today.

Information is freely available to malicious actors. With the widespread use of social media, the daily access to e-mail, and the power that mobile devices brings to the user, there is no lack of potential attack vectors. As a result, it is imperative to have regular training for your users. They need to be constantly aware of the potential threats, what to look for, and who to contact when something does not seem right. They also need to develop good behaviors. Vendors like wombat or knowbe4 implement game theory to help train end-users and educate them about potential malicious intent.

5.3.3 Policies/Procedures

It is important to have policies and procedures governing the way you do business—and for your users to understand and follow them. It is equally important that you review and update them periodically, typically every year.

Such policies should cover HIPAA, which governs the way an organization processes and stores medical information about an individual when applicable. As discussed earlier, HIPAA has three parts:

- **Security:** Protecting EPHI.
- **Privacy:** Regulations surrounding privacy rights and organization responsibilities to protect PHI.
- **Breach:** Rules and processes for detecting, assessing, mitigating, and reporting a breach.

5.3.3.1 Password Policies and Best Practices

Another important area is for organizations to consider is having policies that implement best practices in network and email passwords. It is worth mentioning that the National Institute for Standards and Technology (NIST) has recently published updated recommendations on password best practices. NIST's new recommendations reverse many of recommendations that were thought to be best practices, including forcing users to change their passwords regularly at least every 90 days and using irregular capitalization, special characters, and at least one numeral, which make passwords harder for users to remember. These recommendations led users to write down their passwords, or create a system for passwords that keeps one part of the password and changes the other to generate seemingly strong passwords, which were in fact easy for computer algorithms to crack and predict[14].

The new recommendations suggest that memorized secrets, commonly referred to as passwords, need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value. Generally these shall be at least eight characters in length if chosen by the subscriber. Passwords should be checked against the blacklist of compromised past passwords and should be verifier disallowed in such cases. No other complexity requirements for memorized secrets should be imposed. A rationale for this is presented in Appendix A: Strength of Memorized Secrets of **NIST's Digital Identity Guidelines: Authentication and Lifecycle Management**.

Generally, one should avoid using dictionary words as well using identifiers such as their name, email address, login name, phone number, date of birth, or social security number as part of the password, as these are easy to predict even with letter substitution or reversed spelling. Pass phrases—or first letters of a reasonably long pass phrase that is easy to remember— make good strong passwords.

An OCR checklist shows steps that a HIPAA-covered entity should take after a cybersecurity incident.

5.4 Response

In the wake of several recent international cyberattacks focusing on the health care sector, OCR has developed a checklist and a corresponding infographic that explains the steps for a HIPAA-covered entity or its business associate (collectively, the "entity") to take in response to a cyber-related security incident. In the event of a cyberattack or similar emergency, an entity must follow these steps:

- Execute its response and mitigation procedures and contingency plans.
- Report the crime to other law enforcement agencies, which may include state or local law enforcement, the Federal Bureau of Investigation (FBI), and/or the Secret Service. These reports should not include PHI, unless otherwise permitted by the HIPAA Privacy Rule.
- Report all cyberthreat indicators to the appropriate 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 cyberthreat ISAOs.
- Report the breach 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.

- An entity that discovers a breach affecting fewer than 500 individuals has an obligation to notify the 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.

For more information and nuances, please check out the following **LeadingAge article**.

Include modern infrastructure components in an overarching defense strategy.

---

6 Infrastructure Role

Summary: As technology infrastructure evolves, an array of hardware devices, software applications, secu and techniques is available to help your organization combat cyberthreats.

Valuable infrastructure includes next-generation firewalls, network access control, state-of-the-art e-mail virus software applications, updated endpoint management systems, and a sound backup and disaster rec

While organizations seek to mitigate cyberthreats through IT governance and preparedness, it is equally i critical role that technology infrastructure plays. There has been an evolution of infrastructure hardware c applications, security appliances, strategies, and techniques that can aid organizations in combating mode organization plans for future hardware refreshes or networking overhauls, factor in some of these modern as part of an overarching defense strategy.

6.1 Next-Generation Firewalls

Not all firewalls are created equally. As you consider the device that is the literal gatekeeper between your organization and the global internet, it is critical to select a firewall that has some strong defense capabilities.

Modern enterprise grade firewalls have evolved to include layer 7 networking features and deep packet inspection capabilities. These carefully evaluate every bit and byte that passes through the firewall to ensure that it does not contain harmful data. Deep packet inspection can be likened to the Transportation Security Administration's (TSA) inspection of luggage. While many firewalls have capabilities similar to that of the United States Customs and Border Protection Department—looking at declarations and gross product crossing our borders—next-gen firewalls with deep packet inspection go further and act more like the TSA, using advanced technologies to scan every packet that passes through.

Additionally, next-gen firewalls frequently have monthly security subscriptions services that allow the firewall to remain in real-time communication with an authoritative source to receive routine virus definitions. This service allows the firewall to remain current with new cyberthreats and offers continuous protection of networks.

You should begin to leverage your organization's firewall to inspect local area network traffic and should consider segmenting networking infrastructure into logical groupings based on location or groups of people. Then, as traffic needs to pass between networks, you can route the traffic through the firewall so that the information can be inspected and secured.

Finally, with the firewall playing such a critical role in connectivity, traffic routing, security, and gateway security services, your organization should strongly consider having two or more primary firewall devices set up in a high-availability fashion to mitigate downtime or outages.

NAC solutions bring added peace of mind that only intended users and devices are connected to a network.

6.2 Network Access Control

Another major vulnerability that many organizations face is controlling who is able to connect to a network. Many Wi-Fi networks have an intended purpose of allowing guests to connect to the internet, but other networks have an intended purpose of only allowing staff, residents, or other authenticated users to connect. Additionally, many organizations have unsecured wired ports that intruders or unintended guests could connect to and use to exploit information from the network.

Many organizations are finding an incredible benefit in network access control (NAC) solutions. NACs provide a path for intended users to onboard trusted devices to the appropriate network, using a host of authentication methods. Modern NAC solutions not only look for appropriate authentication from directory services, but also consider the devices connecting to the networking using media access control (MAC) address, which are hardware specific lookups. This powerful combination allows network administrators to control and segment networks based on the types of users and the devices.

In a senior living environment, this combination means there could be separate onboarding and networking segmentation for a resident's laptop that is capable of 802.1x authentication vs. an entertainment device like an AppleTV or Roku streaming media player. NAC solutions also allow true guests (visitors, family members, etc.) to have to authenticate their hardware devices to the wireless network for a set duration of time, similar to the way that hotels' guests authenticate to Wi-Fi. Again, network administrators can determine how long guests and visitors should be allowed to connect to a network based on the type of user and the types of device.

Finally, NACs have the ability to also control connectivity on wired network ports, forcing users to authenticate to the network even if they plug into a port within an organization. The

NAC solutions bring added peace of mind that only intended users and devices are connected to a network.

6.3 E-mail Filtering

One of the most susceptible paths to a data breach can be through phishing e-mail attempts, or even more targeted spear phishing attempts. Having a sound e-mail gateway security platform in place is essential to preventing these phishing e-mails from entering users' inboxes.

For many years, organizations have relied on spam filtering software applications or even spam filtering appliances. These platforms used a series of complex algorithms and filters to weigh each e-mail and assign it a score. Administrators could set a tolerance for the score that they wished to see e-mails be blocked or quarantined and e-mails that they allowed to pass through to the user.

Some advanced e-mail filters had the capability to do per-user e-mail quarantines, which allowed administrators to set a higher score and put the responsibility on the user to monitor the quarantine. Regardless of the capabilities, many of these spam filtering solutions lacked the capabilities to prohibit or even prevent phishing e-mails from ending up in user inboxes.

Modern e-mail gateway security appliances are often deployed as a cloud service to protect against malware and threats that don't involve malware, including impostor e-mail, or business e-mail compromise (phishing). Granular filtering controls spam, bulk "graymail," and other unwanted e-mail. Additional e-mail gateway security features allow administrators to turn on "opt-inboxes" for high-profile spear phishing candidates. Only outside senders with permission have the capability to e-mail these opt-inbox users, and they must request permission through the platform to do so.

6.4 Cloud Anti-Virus

Like next-generation firewalls and modern email gateway security platforms, anti-virus software applications have also started to leverage the capabilities that the cloud offers. Cloud-connected platforms allow for near-real-time communication with virus definition services and can prevent workstations, servers, and other devices from being susceptible to zero day attacks. The cloud has also eased the burden on administrators, seamlessly giving a single pane of glass for all endpoint administration and management.

To supplement cloud anti-virus solutions, which protect endpoints like Workstations & Servers, premises-based firewall solutions can be your next line of defense. Nowadays, edge routers with full unified threat management (UTM) functions have embedded anti-virus along with intrusion detection system (IDS) even routing and intrusion prevention (IPS) functionalities to provide a robust on-premises network.

It is critical to use endpoint management applications to assist you in updating and patching workstation and other endpoint devices on a regular basis.

6.5 Endpoint Management

For larger organizations, sometimes just maintaining an active inventory of endpoint devices can be a monumental task, let alone maintaining consistency in operating systems, software applications, utility programs, and, most critically, updates and patches. Fortunately, several excellent endpoint management software applications have emerged to market. These applications assist administrators in maintaining consistency in their endpoint fleet and can quickly and easily deploy updates and patches to workstations connected to the management software.

Organizations like Microsoft, Adobe, Java, and others release updates and patches on a weekly basis, and many of these updates are patches for known software vulnerabilities in their applications. It is critical that workstations using these applications be updated and patched on a regular basis.

Using one of these endpoint management software suites, administrators can quickly get an inventory of all endpoints on their network and determine which workstations need to be patched or updated. Many of the endpoint management suites also give administrators the ability to push updates to the endpoint through the software, saving time and resources.

It is also important that your organization stay current with commercially supported operating systems. When the WannaCry ransomware attack affected more than 400,000 workstations across the globe in the 2017, more than 98% of the workstations affected were Windows 7 operating systems. Microsoft had ended mainstream support for Windows 7 much earlier, but because of the widely known operating system vulnerability, it had taken the unprecedented step of releasing a security patch 59 days prior to the WannaCry attack.

Now, with Microsoft moving to a more dynamic release schedule for Windows 10, it has shortened the amount of time that it will continue mainstream support for versions of Windows 10. Many of the workstations still running earlier versions of the first Windows 10 release will be falling out of support just two years after the operating system was released, meaning that they will no longer receive security updates and patches from Microsoft.

Along with endpoint management, internal scanning of these edge devices provides a holistic overview of the status of the end devices in terms of vulnerabilities.

It is vital that your organization have a sound backup and disaster recovery solution in place.

6.6 Backup and Disaster Recovery

Last, but certainly not least, it is vital that your organization have a sound backup and disaster recovery (BDR) solution in place. Of course, BDR is important for a host of reasons, but in light of cybersecurity attacks like ransomware, good backups can ensure that organizations can recover to a prior point in time without having to pay for recovery efforts or ransomed file access if a cyberattack does occur.

Additionally, having a sound disaster recovery solution in place can mean that organizations won't have to face downtime or be without technology platforms for an extended period of time should an information breach or cyberattack threaten an organization. It is also important for organizations to test their BDR solution to ensure it works as expected. Please see the **Backup and Recovery section** of CAST's Strategic IT Planning Workbook[15] for more information.

On the surface, many of these infrastructure components may seem routine or even standard for many organizations. However, the capabilities of many of these platforms and services has evolved quickly even in the last 12-24 months, largely on account of some of the cybersecurity breaches that have occurred. It can quickly mean disaster for your organization if you're not carefully considering the impact of these critical infrastructure components.

7 Contributors

7.1 Contributing Writers

Carl Goodfriend, ProviNET Solutions
David Finkelstein, RiverSpring Health
Joe Velderman, ProviNET Solutions
John DiMaggio, BlueOrange Compliance
Kurt Rahner, The Kendal Corporation
Majd Alwan, LeadingAge CAST
Scott Code, LeadingAge CAST

7.2 Workgroup Members

Bill Rabe, Covenant Retirement Communities
Carl Goodfriend, ProviNET Solutions
David Finkelstein, RiverSpring Health
Diana Barlamas, Villa St. Joseph
Ed Stone, BlueOrange Compliance
Joe Velderman, ProviNET Solutions
Joseph Kulnis, The Asbury Group
John DiMaggio, BlueOrange Compliance
Kurt Rahner, The Kendal Corporation

Larry Jorgenson, Ecumen
Majd Alwan, LeadingAge CAST
Michael Freedman, BlueOrange Compliance
Scott Code, LeadingAge CAST
Travis Gleinig, United Methodist Communities

8 LeadingAge and CAST Cybersecurity Help

These LeadingAge Partners and Associates with CAST Focus may be able to help your organization with cybersecurity:

- **BlueOrange Compliance**
- **CDW Healthcare**
- **CLA (CliftonLarsonAllen LLP)**
- **Karpel Solutions**
- **Prelude Services**
- **ProviNET Solutions**
- **ThriveWell Tech**

9 Benchmarking Questionnaire

- **Assessments**
    - Have you performed a cybersecurity risk analysis, or HIPAA risk analysis (if applicable) in the past year or two?
    - Was the assessment performed using a specific methodology (like ISO, COBIT, NIST)?
    - Was the assessment performed by a third party?
- **Plan/Management**
    - Do you have an active security plan containing items identified in the risk analysis report that you actively implement and regularly review?
    - Does your security plan include staff training?
- **Policies and Procedures**

- Do you have written security policies and procedures, including an enforced network password policy and a mobile device policy?

- Do they meet all the requirements of the HIPAA Security Rule regulations (if applicable)?

- Is your appropriate staff trained on the security policies and procedures?

- Do you have documentation demonstrating implementation of the policies and procedures?

- **Infrastructure**
  - Do you have up to date firewalls, including next-generation firewall appliances, protecting your network?

  - Do you have network access control to create separate secure networks and virtual local area networks (VLANs) for staff and businesses, residents, and guests?

  - Does access to your network require authentication?

  - Do you regularly monitor your network traffic and analyze threats?

  - Do you use modern e-mail gateway security monitoring and filtering services?

  - Do you have up to date anti-virus and anti-malware, including cloud anti-virus detection?

  - Do you keep all devices' operating systems and all applications running on your network, including mobile devices and Internet of Things (IoT) appliances, patched and up to date?

- Do you have tools to manage mobile devices and other endpoint devices?

- Do you perform data backup regularly?

- Do you have a disaster recovery plan?

- Have you tested your disaster recovery plan?

- **Organization/Management**
  - Do you have a security officer?

  - Do you have a privacy officer?

- **Training**
  - Do you have training for staff on privacy, data security, and your applicable policies and procedures?

  - Do you offer training upon onboarding?

  - Do you offer regular refresher training on the topic?

- **Governance/Communication**
  - Do you have a compliance committee?

  - Is IT/cybersecurity part of the regular compliance committee?

  - Is IT security addressed regularly at compliance committee meetings?

  - Is compliance a topic in your management meetings?

  - Do you report compliance status to the Board of Directors?

- Does IT security fit within your organization's broader risk management program?

- Does your organization understand the action and communication plan in case of a security breach?

- **Cyber Liability**
  - Do you have cyber liability insurance?

  - Did you read the fine print of your cyber liability insurance?

  - Do you know the types of attacks or breaches covered, the specific expenses covered and their limits, the types of events not covered, and the conditions that would result in revocation of the policy?

  - Do you know who in your organization knows the insurance carrier's breach team and attorneys in case of a security breach?

10 References

i Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2016.
ii SSAE 16, also called Statement on Standards for Attestation Engagements 16, is a regulation created by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) for redefining and updating how service companies report on compliance controls.

1. **http://whatis.techtarget.com/definition/Layer-4-7-Layer-4-through-Layer-7-services**
2. **https://www.cisco.com/c/en/us/products/security/firewalls/index.html**
3. **https://logrhythm.com/products/siem/**
4. **https://www.oracle.com/industries/utilities/products/operational-device-management/index.html**
5. **http://www.leadingage.org/corporatepartners/cybercrime-holds-health-care-organizations-hostage**
6. **http://www.leadingage.org/regulation/hipaa-settlements-underscore-need-protect-data**
7. **https://en.wikipedia.org/wiki/Cyber_Resilience**
8. **https://www.ibm.com/security/data-breach**

9. https://www.wombatsecurity.com/press/press-releases/research-confirms-security-awareness-and-training-reduces-cyber-security-risk
10. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
11. https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76
12. http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
13. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf
14. https://www.theverge.com/2017/8/7/16107966/password-tips-bill-burr-regrets-advice-nits-cybersecurity
15. http://www.leadingage.org/case-studies/strategic-planning-and-strategic-it-planning-long-term-and-post-acute-care-ltpac