Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations

Table of Contents

List of Tables

Introduction

This volume will help answer the question, “How do I mitigate the five threats that were outlined in the Main document?” The practices outlined in this volume are most appropriate for medium-sized and large organizations.

This volume is for the technical practitioner; it contains technical details for implementing cybersecurity practices. It provides an overview of cybersecurity practices that have been outlined by the industry as highly effective at mitigating risks to the health care industry.

This volume is an index of existing industry practices, with guidance on how to start your journey implementing these practices. Details and explanations of the cybersecurity practices are included for additional context where needed.

Please consider these simple instructions when reading this volume:

1) If you are a medium-sized organization, start with the sub-practices labeled with the heading “Sub-Practices for Medium-Sized Organizations.” Feel free to consider the additional sub-practices as well.
2) If you are a large organization, consider implementing all the sub-practices listed in the document, including both those under the heading “Sub-Practices for Medium-Sized Organizations” and those labeled “Sub-Practices for Large Organizations.”

Cybersecurity Practices at Medium-Sized Health Care Organizations

Medium-sized health care organizations perform critical functions for the health care and public health (HPH) sector. These organizations include critical access hospitals in rural areas, practice management organizations that support physician practices, revenue cycle or billing organizations, mid-sized device manufacturers, and group practices. Medium-sized health care organizations generally employ hundreds of personnel, maintain between hundreds and a few thousand information technology (IT) assets, and may be primary partners with and liaisons between small and large health care organizations. It is typical for a medium-sized organization to have several critical systems that are interconnected to enable work activities in support of the organization's mission/

These organizations tend to have a diverse inventory of assets that support multiple revenue streams. They also tend to have narrow profit margins, limited resources, and limited flexibility to implement robust cybersecurity practices. For example, it is rare for a medium-sized organization to have its own dedicated 24x7x365 security operations center (SOC)

Medium-sized organizations tend to focus on preventing cybersecurity events, implementing rigid security policies, with few exceptions permitted. This rigidity is often due to insufficient resources to support more open and flexible cybersecurity models, such as those larger organizations can often afford. Medium-sized organizations usually struggle to obtain cybersecurity funding that is distinct from their standard IT budgets. The top security professional in an organization of this size might often feel overwhelmed by compliance and cybersecurity duties, wear multiple hats, and experience constraints around execution plans.

Medium-sized organizations operate in complex legal and regulatory environments that include but are not limited to the following:

- The Office of the National Coordinator for Health Information Technology (ONC) regulations for interoperability of Certified Electronic Health Information Technology
- The Medicare Access and Children's Health Insurance Program Reauthorization Act of 2015 (MACRA)/Meaningful Use
- Multiple enforcement obligations under the Food and Drug Administration (FDA)
- The Joint Commission accreditation processes
- The Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology Economic and Clinical Health Act (HITECH) requirements
- The Payment Card Industry Data Security Standard (PCI-DSS)
- Substance Abuse and Mental Health Services Administration (SAMHSA) requirements
- The Gramm-Leach-Bliley Act for financial processing
- The Stark Law as it relates to providing services to affiliated organizations
- The Family Educational Rights and Privacy Act (FERPA) for those institutions participating within Higher Education

- The Genetic Information Nondiscrimination Act (GINA)
- The new General Data Protection Regulation (GDPR) in the European Union

IT Assets Used by Medium-Sized Organizations

Medium-sized organizations may have up to a few thousand IT assets, with a mix of dozens to a hundred information systems. All assets may have cybersecurity vulnerabilities and are susceptible to cyber threats. There are three important factors in securing assets: (1) understanding their relationship within the organization's IT ecosystem; (2) understanding how the workforce leverages and uses the assets; and (3) understanding the data that are generated, stored, and processed within those assets.

Not all assets are equally important; some are mission critical and must always be fully operational, while others are less critical, and might even be offline for days or weeks without harming the organization's mission. Some assets have large repositories of sensitive data that represent significant risk, but are not as critical to the enterprise's business. In all cases, the organization uses IT assets for business reasons and should protect those assets with proper cyber hygiene controls.

Examples of assets found in medium-sized organizations include but are not limited to the following:

- Static devices used by the workforce, such as shared workstations, and clinical workstations used strictly for patient care with select mobile devices, such as laptops and smartphones. Medium-sized organizations may not maintain many mobile devices, owing to budget restrictions.
- Internet of things (IoT) devices, such as smart televisions and medical devices, printers, copiers, and security cameras.
- Data that includes sensitive health information stored and processed on devices, servers, applications, and the cloud. These data include names, medical record numbers, birth dates, social security numbers (SSNs), diagnostic conditions, prescriptions, and mental health, substance abuse, or sexually transmitted infection information. These sensitive data are referred to as *protected health information (PHI)* under HIPAA.
- Assets related to the IT infrastructure, such as firewalls, network switches and routers, Wi-Fi networks (both corporate and guest), servers supporting IT management systems, and file storage systems (cloud-based or onsite).
- Applications or information systems that support the business processes. These may include human resource (HR) or enterprise resource planning (ERP) systems, pathology lab systems, blood bank systems, medical imaging systems, pharmacy systems, revenue cycle systems, supply chain or materials management systems, specialized oncology therapy systems, radiation oncology treatment systems, and data warehouses (e.g., clinical, financial).

Personal devices, often referred to as *bring your own device (BYOD)*, are generally not permitted in medium-sized organizations due to the organizations' inability to implement dedicated security controls required to secure such devices.

Cybersecurity Practices

Medium-sized organizations should consider, at minimum, implementing the *Sub-Practices for Medium-Sized Organizations* discussed in each cybersecurity practice presented in this volume. However, medium-sized organizations may additionally adopt the cybersecurity practices used by large

organizations. Indeed, organizations should consider adopting any cybersecurity practice determined to be relevant.

Cybersecurity Practices at Large Health Care Organizations

Large health care organizations perform a range of different functions. These organizations may be integrated with other health care delivery organizations, academic medical centers, insurers that provide health care coverage, clearinghouses, pharmaceuticals, or medical device manufacturers. In most cases, large organizations employ thousands of employees, maintain tens of thousands to hundreds of thousands of IT assets, and have intricate and complex digital ecosystems. Whereas smaller organizations operate using only a few critical systems, large organizations can have hundreds or thousands of interconnected systems with complex functionality.

The missions of large organizations are diverse and varied. They include providing standard general practice care, providing specialty or subspecialty care for complicated medical cases, conducting innovative medical research, providing insurance coverage to large populations of patients, supporting the health care delivery ecosystem, and supplying and researching new therapeutic treatments (such as drugs or medical devices).

Large organizations have missions that are broad in scope, and large volumes of assets may be necessary to fulfill such missions. Even so, they often struggle to obtain funding to maintain security programs and to control their assets (potentially resulting in shadow IT, rogue devices, and unmanaged/unpatched devices). Therefore, it is essential for large organizations to understand how sensitive data flow in and out of the organization, and to understand the boundaries and segments that determine where one entity's responsibilities end and another's start/

Large organizations operate in a legal and regulatory environment that is as complicated as their digital ecosystems. It includes but not limited to the following:

- ONC Certified Electronic Health Information Technology interoperability standards
- MACRA/Meaningful Use
- Multiple obligations under the FDA
- The Joint Commission accreditation processes
- HIPAA/HITECH requirements
- Minimum Acceptable Risk Standards for payers
- State privacy and security rules
- Federal Information Security Modernization Act requirements as incorporated into federal contracts and research grants through agencies such as the National Institutes of Health
- Payment Card Industry Data Security Standard (PCI-DSS)
- SAMHSA requirements
- The Gramm-Leach-Bliley Act for financial processing
- The Stark Law as it relates to providing services to affiliated organizations

- FERPA for institutions that participate in higher education
- GINA
- The new GDPR in the European Union.

IT Assets Used by Large Organizations

Large organizations support their operations with complicated ecosystems of IT assets. All assets may have cybersecurity vulnerabilities and are susceptible to cyber threats. There are three important factors in securing assets: (1) understanding their relationship within the organization's IT ecosystem; (2) understanding how the workforce leverages and uses the assets; and (3) understanding the data generated, stored, and processed within those assets.

Not all assets are equally important; some are mission critical and must always be fully operational, while others are less critical, and might even be offline for days or weeks without harming the organization's mission. Some assets have large repositories of sensitive data that represent significant risk, but are not necessarily critical to the enterprise's business. In all cases, the organization uses IT assets for business reasons and should protect those assets with proper cyber hygiene controls.

Examples of assets found in large organizations include but are not limited to the following:

- Devices used by the workforce, such as mobile phones, tablets, voice recorders, and laptop computers for dictation (all with internet connectivity).
- Personal devices, often referred to as *BYOD*.
- Large deployments of IoT assets, including smart televisions and networked medical devices, printers, copiers, security cameras, refrigeration sensors, blood bank monitoring systems, building management sensors, and more.
- Data that includes sensitive health information stored and processed on devices, servers, applications, and the cloud. These data could include names, medical record numbers, birth dates, SSNs, diagnostic conditions, prescriptions, and mental health, substance abuse, or sexually transmitted infection information. These sensitive data are referred to as *PHI*.
- Assets related to the IT infrastructure, such as firewalls, network switches and routers, Wi-Fi networks (corporate and guest), servers supporting IT management systems, and file storage systems (cloud-based or onsite).
- Applications or information systems that support business processes. These can include ERPs, pathology lab systems, blood bank systems, medical imaging systems, pharmacy systems (retail and specialized), revenue cycle systems, supply chain or materials management systems, specialized oncology therapy systems, radiation oncology treatment systems, data warehouses (clinical, financial, research), vendor management systems, and more.

Document Guide: Cybersecurity Practices

This volume provides medium and large organizations with cybersecurity practices to reduce the impact of these five prevailing threats:

- E-mail phishing attacks
- Ransomware attacks
- Loss or theft of equipment or data
- Insider, accidental or intentional data loss
- Attacks against medical devices that can affect patient safety

Each cybersecurity practice is broken up into three core segments: **Sub-Practices for Medium-Sized Organizations** (or *medium sub-practices*), **Sub-Practices for Large Organizations** (or *large sub-practices*) and the **Threats Mitigated** by the practice. Additionally, each section contains a series of suggested metrics to measure the effectiveness of the cybersecurity practice.

Medium sub-practices apply to both medium-sized and large organizations. Large sub-practices apply primarily to large organizations, but could also benefit any other organization that interested in adopting them.

The following 10 charts present summaries of each of the cybersecurity practices described herein.

Cybersecurity Practice 1: E-mail Protection Systems		
Data that may be affected	Passwords, PHI	
Medium Sub-Practices	1.M.A 1.M.B 1.M.C 1.M.D	Basic E-mail Protection Controls Multifactor Authentication for Remote Access E-mail Encryption Workforce Education
Large Sub-Practices	1.L.A 1.L.B 1.L.C	Advanced and Next-Generation Tooling Digital Signatures Analytics Driven Education
Key Mitigated Risks	• E-mail Phishing Attacks • Ransomware Attacks • Insider, Accidental or Intentional Data Loss	

Cybersecurity Practice 2: Endpoint Protection Systems		
Data that may be affected	Passwords, PHI	
Medium Sub- Practices	2.M.A	Basic Endpoint Protection Controls
Large Sub-Practices	2.L.A 2.L.B 2.L.C 2.L.D 2.L.E 2.L.F	Automate the Provisioning of Endpoints Mobile Device Management Host Based Intrusion Detection/Prevention Systems Endpoint Detection Response Application Whitelisting Micro-Segmentation/Virtualization Strategies
Key Mitigated Risks	• Ransomware Attacks • Theft or Loss of Equipment or Data	

Cybersecurity Practice 3: Identity and Access Management		
Data that may be affected	Passwords	
Medium Sub-Practices	3.M.A 3.M.B 3.M.C 3.M.D	Identity Provisioning, Transfers, and Deprovisioning Procedures Authentication Multi-Factor Authentication for Remote Access
Large Sub-Practices	3.L.A 3.L.B 3.L.C 3.L.D	Federated Identity Management Authorization Access Governance Single-Sign On
Key Mitigated Risks	• Ransomware Attacks • Insider, Accidental or Intentional Data Loss • Attacks Against Connected Medical Devices that May Affect Patient Safety	

Cybersecurity Practice 4: Data Protection and Loss Prevention		
Data that may be affected	Passwords, PHI	
Medium Sub-Practices	4.M.A 4.M.B 4.M.C 4.M.D 4.M.E	Classification of Data Data Use Procedures Data Security Backup Strategies Data Loss Prevention
Large Sub-Practices	4.L.A 4.L.B	Advanced Data Loss Prevention Mapping of Data Flows
Key Mitigated Risks	• Ransomware Attacks • Loss of Theft of Equipment or Data • Insider, Accidental or Intentional Data Loss	

Cybersecurity Practice 5: IT Asset Management		
Data that may be affected	Passwords, PHI	
Medium Sub-Practices	5.M.A 5.M.B 5.M.C 5.M.D	Inventory of Endpoints and Servers Procurement Secure Storage for Inactive Devices Decommissioning Assets
Large Sub-Practices	5.L.A 5.L.B	Automated Discovery and Maintenance Integration with Network Access Control
Key Mitigated Risks	• Ransomware Attacks • Loss of Theft of Equipment or Data • Insider, Accidental or Intentional Data Loss • Attacks Against Connected Medical Devices that May Affect Patient Safety	

Cybersecurity Practice 6: Network Management		
Data that may be affected	PHI	
Medium Sub-Practices	6.M.A 6.M.B 6.M.C 6.M.D 6.M.E	Network Profiles and Firewalls Network Segmentation Intrusion Prevention Systems Web Proxy Protection Physical Security of Network Devices
Large Sub-Practices	6.L.A 6.L.B 6.L.C 6.L.D 6.L.E	Additional Network Segmentation Command and Control Monitoring of Perimeter Anomalous Network Monitoring and Analytics Network Based Sandboxing/Malware Execution Network Access Control
Key Mitigated Risks	• Ransomware Attacks • Loss of Theft of Equipment or Data • Insider, Accidental or Intentional Data Loss • Medical Devices and Patient Safety	

Cybersecurity Practice 7: Vulnerability Management		
Data that may be affected	PHI	
Medium Sub-Practices	7.M.A 7.M.B 7.M.C 7.M.D	Host/Server Based Scanning Web Application Scanning System Placement and Data Classification Patch Management, Configuration Management, Change Management
Large Sub-Practices	7.L.A 7.L.B	Penetration Testing Remediation Planning
Key Mitigated Risks	• Ransomware Attacks • Insider, Accidental or Intentional Data Loss • Attacks Against Connected Medical Devices that May Affect Patient Safety	

Cybersecurity Practice 8: Security Operations Center and Incident Response		
Data that may be affected	PHI	
Medium Sub-Practices	8.M.A 8.M.B 8.M.C	Security Operations Center Incident Response Information Sharing and ISACs/ISAOs
Large Sub-Practices	8.L.A 8.L.B 8.L.C 8.L.D 8.L.E 8.L.F	Advanced Security Operations Center Advanced Information Sharing Incident Response Orchestration Baseline Network Traffic User Behavior Analytics Deception Technologies
Key Mitigated Risks	• Phishing Attacks • Ransomware Attacks • Loss or Theft of Equipment • Insider, Accidental or Intentional Data Loss • Attacks Against Connected Medical Devices that May Affect Patient Safety	

Cybersecurity Practice 9: Medical Device Security		
Data that may be affected	PHI	
Medium Sub-Practices	9.M.A 9.M.B 9.M.C 9.M.D 9.M.E	Medical Device Management Endpoint Protections Identity and Access Management Asset Management Network Management
Large Sub-Practices	9.L.A 9.L.B 9.L.C 9.L.D	Vulnerability Management Security Operations and Incident Response Procurement and Security Evaluations Contacting the FDA
Key Mitigated Risks	• Attacks Against Connected Medical Devices that May Affect Patient Safety	

Cybersecurity Practice 10: Cybersecurity Policies		
Data that may be affected	N/A	
Medium Sub-Practices	10.M.A	Policies
Large Sub-Practices	N/A	
Key Mitigated Risks	• E-mail Phishing Attacks • Ransomware Attacks • Loss or Theft of Equipment or Data with Sensitive Information • Insider, Accidental or Intentional Data Loss • Attacks Against Connected Medical Devices that May Affect Patient Safety	

Cybersecurity Practice #1: E-mail Protection Systems

Cybersecurity Practice 1: E-mail Protection Systems	
Data that may be affected	Passwords, PHI
Medium Sub-Practices	1.M.A Basic E-mail Protection Controls 1.M.B MFA for Remote Access 1.M.C E-mail Encryption 1.M.D Workforce Education
Large Sub-Practices	1.L.A Advanced and Next Generation Tooling 1.L.B Digital Signatures 1.L.C Analytics Driven Education
Key Mitigated Risks	• E-mail Phishing Attacks • Ransomware Attacks • Insider, Accidental or Intentional Data Loss

According to the 2017 Verizon Data Breach Report, "Weak or stolen passwords were responsible for 80% of the hacking related breaches".[1] The report further identifies phishing attacks (a type of hacking attack) as the most common first point of unauthorized entry into an organization. After monitoring 1,400 customers and 40 million simulated phishing campaigns, the *PhishMe 2017 Enterprise Resiliency and Defense Report* concluded that the average susceptibility of users within an organization falling prey to a phishing attack is 10.8 percent.[2] Though other areas of significant threat exist, including in the web application space, the effectiveness of phishing attacks allows attackers to bypass most perimeter detections by "piggy backing" on legitimate workforce users. If an attacker obtains an employee's password via phishing, and if that employee has remote access to the organization's IT assets, the attacker has made significant progress toward penetrating the organization.

The two most common phishing methods are credential theft (leveraging e-mail to conduct a credential harvesting attack on the organization) and malware dropper attacks (e-mail delivery of malware that can compromise endpoints). An organization's cybersecurity practices must address these two attack vectors. Because both attack types leverage e-mail, e-mail systems should be the focus for additional security controls.

1. Tin Zaw, "2017 Verizon Data Breach Investigations Report (DBIR) from the Perspective of Exterior Security Perimeter," Verizon Digital Media Service, last modified July 26, 2017, https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/.

2. Ian Murphy, "How Susceptible Are You to Enterprise Phishing?" Enterprise Times, last modified December 1, 2017, https://www.enterprisetimes.co.uk/2017/12/01/susceptible-enterprise-phishing/.

Sub-Practices for Medium-Sized Organizations

1.M.A	***Basic E-mail Protection Controls***	***NIST FRAMEWKORK REF:*** PR.DS-2, ID.RA-2, PR.PT-3, DE.CM-4, PR.AC-4, PR.AC-1, PR.AC-7

Standard antispam and antivirus (AV) filtering controls are basic protections that should be implemented in any e-mail system. Both are implemented directly on the e-mail platform. These controls assess inbound and outbound e-mails from known malicious senders or patterns of malicious content. Table 1 provides a list of suggested security implementations for e-mail protection controls.

Table 1. E-mail Protection Controls

Control	Description
Real-time blackhole list[3]	Community-based lists of IP addresses and host names of known or potential spam originators. Consider Spamhaus, Spamcop, DNSRBL, or lists provided by your e-mail vendor.
Distributed checksum clearinghouse (DCC)	The DCC is a distributed database that contains a checksum of messages. E-mail messages go through a checksum algorithm and then checked against the database. Depending upon the threshold of checksum matches, these can be determined to be spam or malicious messages.
Removal of open relays	Open relays are Simple Mail Transfer Protocol (SMTP) servers that enable the relay of third-party messages. SMTP is critical for the delivery of messages, but you must configure it to allow messages only from trusted sources. Failure to do this may permit a spammer or hacker to exploit the "trust" of your mail server to transmit malicious content.
Spam/virus check on outbound messages	Spam/virus checks on outbound e-mails can detect malicious content, revealing compromised accounts and potential security incidents. Review e-mail spam/virus rules as part of **Cybersecurity Practice #8: Security Operations Center and Incident Response**.
AV check	Scan all e-mail content against an AV engine with up-to-date signatures. If possible, this control should unpack compressed files (such as zip files) to check for embedded malware.

3. Murthy Raju, "Using RBL and DCC for Spam Protection," Linux/com, last modified June 14, 2007, https://www.linux.com/news/using-rbl-and-dcc-spam-protection.

Control	Description
Restrict the "Send !s" permi ssion for distribution lists	Limit distribution lists to essential members. Distribution lists can enable attackers to disseminate malicious content from a compromised account. Therefore, they and should not be accessible to large numbers of users.
Implement sender policy framework (SPF) records	A Sender Policy Framework (SPF) record identifies which mail servers may send e-mail on behalf of your domain. This enables the receiving mail server to verify the authenticity of the sending mail server.
Implement domain key identified mail (DKIM)	DKIM is a method of e-mail authentication that uses cryptography to ensure that e-mail messages come from authorized e-mail servers. A public key is stored within the organization's DNS as a text (txt) record. All messages sent from that domain are digitally signed with a DKIM signature that can be validated through the DNS public key txt record.
Implement domain-based message authentication reporting and conformance (DMARC)[4]	DMARC is an authentication technology that leverages both SPF and DKIM to validate an e-mail's *From:* address (i.e., the sender). DMARC enables the receiving mail system to check SPF and DKIM records, ensuring conformance to the sending host as well as the *From:* address. It instills trust that the sending party's e-mail address is not spoofed; spoofing is a common attack type used to trick users into opening malicious e-mails.

In most cases, e-mail protection controls do not operate alone. When combined to evaluate an organization's e-mails, they contribute information that provides a more complete assessment of each message. Modern systems score e-mail content on each pass through the protection controls.

Implement this scoring technique and set at least three thresholds: OK for Delivery, Quarantine, or Block/Drop. Score each e-mail to determine which of the three thresholds applies. Based on that threshold, automated actions should be executed. E-mails cleared for delivery automatically pass through for additional processing. The e-mail protection system discards Block/Drop e-mails, and the user never sees them. Quarantine actions allow the user to evaluate the message in a secured environment, not the user's regular e-mail box, for final verification. In most cases, the system delivers quarantined messages to the user daily in a single e-mail digest for verification.

Adding X-Headers to the delivery of e-mail messages is a good way to flag potential spam or malicious e-mail before sending it to the user. There are two common methods for doing this: [5]

---

4. KC Cross, Denise Vangel, and Meera Krishna, "Use DMARC to Validate E-Mail in Office 365," Microsoft TechNet, last modified October 8, 2017, https://technet.microsoft.com/en-us/library/mt734386(v=exchg.150).aspx.

5. KC Cross and Denise Vangel, "Configure Your Spam Filter Policies," Microsoft TechnNet, last modified December 13, 2017, https://technet.microsoft.com/en-us/library/jj200684(v=exchg.150).aspx.

- *Spam X-Header*: If a message receives a score that prevents the system from definitely classifying it as spam/malicious, the system can tag the message with an X-Header. The system modifies the *Subject* or the top of the *Body* of the message to include a [POSSIBLE SPAM] tag. This advises the user to verify the legitimacy of the message before opening it.
- *External Sender X-Header*: Another common practice is to add an [EXTERNAL] tag to inbound messages from external senders. The tag can be configured to be highly visible, such as "**WARNING: Stop. Think. Read. This is an external e-mail.**" This method is effective at catching messages that might be spoofed or pretend to come from within the organization. It also informs the e-mail recipient to be cautious when clicking links or opening attachments from these sources.

  NOTE: If you leverage DMARC, you might consider exempting the External Sender X-header tag for messages that pass DMARC authentication. This may help e-mail users understand the trust environment and identify when it is necessary to be extra vigilant.

In addition to tagging messages that fail DMARC authentication, messages can be tagged, or digitally signed, when they originate from approved hosting or cloud-based services with a legitimate need to spoof an internal address. This is common for communications platforms, such as marketing systems, emergency management communications systems, or alert management systems.

1.M.B	***Multifactor Authentication for Remote E-mail Access***	***NIST FRAMEWKORK REF:*** PR.AC-7

It is common and expected to share sensitive information through e-mail systems. E-mail is the primary mechanism used by most organizations to communicate electronically. It is also common to access e-mail remotely, as the workforce has become increasingly mobile.

Given the prevalence of credential harvesting attacks, if remote e-mail systems are available, passwords are the only controls prohibiting malicious users from accessing sensitive information within transmitted e-mails/ This is a critical exposure that increases organizations' susceptibility to phishing attacks.

As discussed in **Cybersecurity Practice #3: Identity and Access Management**, two-factor authentication, or multifactor authentication (MFA), is the process of verifying a user's identity using more than one credential. The most common method is to leverage a soft token in addition to a password. The soft token is a second credential that can be delivered through a mobile phone or tablet, devices that most people have nearby. The soft token could consist, for example, of a text message containing a code, or of an application installed on the phone that provides the code and/or asks for independent verification after a successful password entry.

Implementing MFA on your remote-access e-mail platform mitigates the risk of a compromised credential, such as a user password. With MFA, a hacker requires both the phone and the user's password, which significantly reduces the likelihood of a successful attack. This is one of the most effective controls to protect your organization's data/

1.M.C	*E-mail Encryption*	***NIST FRAMEWKORK REF***: PR.DS-2

E-mail is the most common method of communicating content, including sensitive information, among members of an organization. Although e-mail might not be the preferred communication method, one must assume that users will leverage this common and easy-to-use communication channel.

E-mail encryption is an important security protection. Multiple encryption techniques exist, though the most common use third-party applications to conduct encryption, invoking them by tagging outbound messages in some form. Tagging can occur, for example, by putting a trigger in the subject line (e.g., #encrypt, #confidential), or the e-mail client itself can invoke the third-party application. The techniques used depend upon the technology solution deployed.

When organizations have established partnerships with third parties, they can provision fully encrypted, transparent e-mail delivery between the two entities' e-mail systems. In this model, each system can be configured to require transport layer security (TLS) encryption when sending or receiving messages from the other. This ensures that the messages are delivered over the internet in a manner that prevents their being intercepted.

Whichever encryption technique you implement, you must train your workforce to use the technique when transmitting sensitive information. You may integrate this cybersecurity practice into the data protection cybersecurity practices discussed in **Cybersecurity Practice #4: Data Protection and Loss Prevention**. Messages that users fail to encrypt can be automatically encrypted or simply blocked.

1.M.D	*Workforce Education*	***NIST FRAMEWKORK REF:*** PR.AT-1

A study released in 2017 determined that the average measured susceptibility of users within an organization to fall victim to phishing attacks is 10.8 percent.[6] Therefore, it is important to maintain a workforce that is vigilant and aware of cyberattacks. Whatever your organization's actual susceptibility to phishing attacks, it is unlikely to reach zero. Given that phishing is one of the most common methods of attack and initial compromise, a layered defense strategy is important.

Organizations should implement security awareness programs that provide context around e-mail-based attacks. The challenge presented to security departments is how to deliver a concise education on spotting technical attacks when the workforce's knowledge level does not match the hacker's level of sophistication. For example, it is easy to make a phishing e-mail appear to originate from the company itself, incorporating logos, department names, and management names, but it is difficult to train your entire workforce to detect that fake message.

When implementing information security and cybersecurity training programs, consider the key techniques outlined in a 2015 HBR article by Keith Ferrazzi:[7]

---

6. Murphy.

7. Keith Ferrazzi, "7 Ways to Improve Employee Development Programs," Harvard Business Revew, last modified July 31, 2015, https://hbr.org/2015/07/7-ways-to-improve-employee-development-programs.

- *Ignite each manager's passion to coach their employees*: Engage and train your management team. Leverage them to communicate security practices and information to staff in all areas of the organization.
- *Deal with the short shelf life of learning and development needs*: Security information changes continuously. Implement continuous and ongoing campaigns to maintain awareness of current trends, issues, and events.
- *Teach employees to own their career development*: Customize cybersecurity training to the needs of employees in different positions or units in the organization. Develop training that is clearly relevant to the user's job/
- *Provide flexible learning options*: Provide options, including on-demand and mobile training solutions that allow the workforce to schedule and complete training independently.
- *Serve the learning needs of virtual teams*: Recognize that many employees work remotely and virtually. Training solutions should fit within the work environment of virtual employees.
- *Build trust in organizational leadership*: Leaders must be open and transparent and lead by example. Managers must demonstrate to the workforce that they are fully engaged in security strategy and committed to successful execution of security controls and techniques.
- *Match different learning options to different learning styles*: Effective training accommodates the different learning styles and requirements of employees who function in diverse work environments within a single organization. Consider multiple options for conducting each training course to maximize training effectiveness and efficiency.

Organizations should implement multifaceted training campaigns that engage users to catch phishing through multiple channels. Points to include in your training campaign include the following:

- *Sender verification:* Users should look very carefully at the sender of the e-mail message. It is common to spoof the organization's name by changing a simple character, for example, "google/c0m" rather than "google/com." Be on the lookout for e-mails where the organization's name appears with a separate e-mail domain, such as "ACME/google/com" rather than "acme/com."
- *Follow the links:* Every link in an e-mail message is suspect. Organizations should limit the use of links in corporate messages to those that are necessary. Users should hover the cursor over each link to check the corresponding URL and determine whether it is credible. Specifically, mismatched URLs (i.e., those where the name of the link in the e-mail does not match the corresponding URL) are highly suspect.
- *Beware of attachments:* Though it can be difficult to determine whether an attachment is malicious based on the content of an e-mail message, there are often clues. Be wary of messages that require immediate action, for example, "You must read this right away." Be cautious when receiving attachments from senders with whom you do not regularly correspond. It is important to detect malicious attachments, which may contain malware or exploit scripts that permanently compromise your computer.
- *Suspect content:* In most cases, hackers entice you to follow a link or open an attachment. They will use messages to play with your curiosity and emotions. These messages vary widely, from urgent messages such as, "Your account will be deactivated unless you re-register," to scary messages such as, "The IRS is suing you and you must fill out the attached form." Hackers also

prey on hopes and desires. Examples of these messages include, “You have won a $100 !maz on gift card!” and the well-known Nigerian Prince messages.

As you establish your awareness campaigns, keep this simple goal in mind: you want your workforce to be “human sensors” detecting malicious activity and reporting these incidents to your cybersecurity department. !s they say in the New York subway systems, “If you see something, say something.” The earlier security personnel become aware of a phishing attack, the faster they can execute **Cybersecurity Practice #8: Security Operations Center and Incident Response**.

The following are recommended channels for cybersecurity awareness campaigns:

- *Monthly phishing campaigns:* The most effective means of training your workforce to detect a phishing attack is to conduct simulated phishing campaigns. Your authorized security personnel or third-party provider crafts and sends phishing e-mails to your employees. These e-mails have embedded tracking components (e.g., to track link clicks). Tracking enables the organization to identify employees who detect the e-mail as a phishing attack and those who fail to detect the attack, opening the e-mail or clicking the e-mailed links. Then, the organization can provide the appropriate training and feedback as soon as possible after the event. Simulated phishing attacks provide a cause-and-effect training opportunity and are incredibly effective. Consider conducting phishing simulations on at least a monthly basis for the entire workforce. Develop specialized simulations for higher-risk areas within your organization. These could be based on the department (such as finance and human resources [HR]) or on data identifying your highest-risk users.
- *Ongoing and targeted training:* Although training is not the most effective means of raising phishing awareness, you should include phishing content in your organization’s ongoing privacy and security training.
- *Departmental meetings:* Hold departmental meetings to disseminate information on information security and cybersecurity events and trends. Brief presentations or informal conversations provide face-to-face context and build relationships between security personnel and the organization’s workforce/ These relationships encourage a continuous dialogue that elevates the visibility of cybersecurity across the organization.
- *E-mail campaigns:* Deliver a pointed e-mail message or alert about specific attacks. Provide Secure Multipurpose Internet Mail Extensions (S/MIME) or other digital certificates as evidence that these messages are authentic. Remember that attackers will attempt to do the same thing!
- *Newsletters:* Working independently or with your marketing department, develop and distribute your own cybersecurity newsletter. Write articles that explain how to catch a phishing attack. Better yet, provide an example of an actual phishing attack, highlighting the warning signs that might have prevented the attack.

Sub-Practices for Large Organizations

1.L.A	***Advanced and Next-Generation Tooling***	***NIST FRAMEWKORK REF:*** PR.DS-2, DE.CM-5, DE.CM-7

Many sophisticated solutions exist to help combat the phishing and malware problem. These solutions are called *advanced threat protection services*. They use threat analytics and real-time response capabilities to provide protection against phishing attacks and malware.

The following list describes some of these tools:

- *URL click protection via analytics:* In a modern phishing attack, the hacker will create a web page on the internet for harvesting credentials or delivering malware. Next, the hacker will conduct an e-mail campaign, sending e-mails with a link to a web page that does not have malicious content. Because the linked page is not malicious, traditional spam and AV protections clear the e-mail for delivery to the user. As soon as the e-mails are delivered, the hacker changes the linked web page to the newly created malicious web page. This allows the hacker to bypass many traditional e-mail protections and leaves the organization to rely on the user's vigilance and awareness.

  Protection technologies that rely on analytics leverage the ability to re-write links embedded in an e-mail message. The rewritten URLs point to secure portals that apply analytics to determine the maliciousness of the request at the time of the click. The message is thus protected no matter where or when the user clicks the link. Such technologies use the cloud and numerous sensors throughout the install base to check linked sites in real time. They can also block discovered malicious sites ahead of time to inoculate the organization.

- *Attachment sandboxing:* Another common attack technique is to send attachments with embedded malware, malicious scripts, or other local execution capabilities that compromise vulnerabilities on the endpoint where the attachment is launched. These attachments bypass traditional signature-based malware blocking by using multiple obfuscation techniques that alter the attachment's content to provide a different hashing signature.

  Sandboxing technologies open attachments proactively in virtual environments to determine what behaviors occur after the user opens the attachment. The protection system determines whether a file is malicious based on these behaviors, such as system calls, registry entry creation, file downloading, and others.

- *Automatic response:* Another useful technique is to implement mechanisms that automatically rescind or remove e-mail messages categorized as malicious after delivery to a user's mailbox. After using the analytics approach described earlier in this section to identify malicious e-mails, cybersecurity response teams remove these messages from the user's mailbox/ This manual process requires identifying the characteristics of the malicious e-mail message, searching the organization's e-mail environments, and deleting messages that match the identified characteristics. This time-consuming process is difficult to run in a 24x7 operation and can be dangerous.

  As an alternative to costly manual removal, automatic response technologies can identify the signature of a delivered e-mail. When advanced threat tools determine that a previously clean message has become malicious, it can automatically delete that e-mail message from all user mailboxes in the organization. This reduces the labor involved compared with the manual processes and provides the consistency of automation.

1.L.B	***Digital Signatures***	***NIST FRAMEWKORK REF:*** PR.DS-2, PR.DS-6, PR.DS-8

Digital signatures allow a sender to leverage public/public key cryptography to cryptographically sign an e-mail message. This does not encrypt the message itself. Rather, it validates that a received message is from a verified sender and has not changed in transit.

As long as trusted root certificates are used to create the S/MIME certificate used in digital signatures, most modern e-mail clients will check and provide verification automatically by presenting an icon on the message itself. This icon is useful when training your workforce to determine the validity of an e-mail.

A word of caution: many e-mail protection technologies change the content of e-mail messages (e.g., by tagging subject lines, re-writing URLs). Digital signature technology that maintains the integrity of an e-mail will fail when you use these other protection techniques. Currently, there is no method to resolve this problem.

1.L.C	***Analytics-Driven Education***	***NIST FRAMEWKORK REF:*** PR.AT-1

Cybersecurity departments use data and analytics from both regular e-mail protection platforms and advanced threat protection systems to identify the most frequently targeted users in an organization. These users might not be the ones you think are highly susceptible, such as the CEO or the finance workforce. With the systems discussed in this section, SOCs can identify targets, implement increased protections (e.g., lower thresholds for spam/malware checking, delayed processing time for attachments), and provide on-the-spot and targeted education. Informing these individuals of their high risk profile instills a heightened sense of awareness and increased vigilance.

Threats Mitigated

1. E-mail phishing attacks
2. Ransomware attacks
3. Insider, Accidental or intentional data loss

Suggested Metrics

- Number of malicious phishing attacks prevented on a weekly basis. The goal is to ensure that systems are working. A reduction in attacks prevented indicates system misconfiguration. Sudden changes in the rate of phishing attacks should trigger operational checks of to ensure that systems are still operating as intended.
- Number of malicious URLs and e-mail attachments discovered and prevented on a weekly basis. The goal is to measure the effectiveness of advanced tools, like click protection or attachment protection.
- Number of account resets on a weekly basis. This is based on users who accessed a malicious website. It assumes that a registered click indicates compromised credentials, so be sure to change the credential before further compromised can occur. Implement education to keep this number as low as possible.
- Number of malicious websites visited on a weekly basis. The goal is to establish a baseline understanding, then strive for improved awareness through education activities that train employees to avoid malicious websites.
- Percentage of users in the organization who are susceptible to phishing attacks based on results of internal phishing campaigns. This provides a benchmark to measure improvements to the workforce's level of awareness. The goal is to reduce the percentage as much as possible,

realizing that it is nearly impossible to stop all users from opening phishing e-mails. A secondary goal is to correlate the percentage of susceptible users with the number of malicious websites visited or the number of malicious URLs opened.

- List of the top 10 targeted users each week, with corresponding activity. For example, how many phishing e-mails do the top three users receive compared with the rest of the workforce? What positions do these users hold in the organization? Are there correlations among the user, the user's position, and the number of phishing e-mails received? What inferences and conclusions are possible? The goal is to conduct targeted awareness training to these individuals, advising them that they are targets more often than other users, and increasing their vigilance as well as their ability to detect and report phishing attacks.
- Average time to detect and time to respond statistics for phishing attacks on a weekly basis. Time to detect measures how long the phishing attack was in progress before the cybersecurity department was aware of it. Response times measure of how quickly the cybersecurity department neutralized the messages to end the attacks. The goal is that both metrics should be as low as possible; establish a baseline to understand the current state and set goals to improve performance.

Cybersecurity Practice #2: Endpoint Protection Systems

Cybersecurity Practice 2: Endpoint Protection Systems		
Data that may be affected	Passwords, PHI	
Medium Sub-Practices	2.M.A	Basic Endpoint Protection Controls
Large Sub-Practices	2.L.A	Automate the Provisioning of Endpoints
	2.L.B	Mobile Device Management
	2.L.C	Host Based Intrusion Detection/Prevention Systems
	2.L.D	Endpoint Detection Response
	2.L.E	Application Whitelisting
	2.L.F	Micro-segmentation/virtualization strategies
Key Mitigated Risks	• Ransomware Attacks • Theft or Loss of Equipment or Data	

Endpoints are the assets the workforce uses to interface with an organization's digital ecosystem. Endpoints include desktops, laptops, workstations, and mobile devices. Current cyberattacks target endpoints as frequently as networks. Implementing baseline security measures on these assets provides a critical layer of threat management. As the modern workforce becomes increasingly mobile, it is essential for these assets to interface and function securely.

The endpoints of which our computing environments largely consist are no longer static devices that exist in the health care organization's main network. Organizations commonly leverage virtual teams, mobility, and other remote access methods to complete work. In some cases, endpoints rarely make it to the corporate network. It is important to build cybersecurity hygiene practices with these characteristics in mind.[8]

Sub-Practices for Medium-Sized Organizations

2.M.A	***Basic Endpoint Protection Controls***	***NIST FRAMEWKORK REF:*** PR.IP-1, DE.CM-4, PR.DS-1, PR.IP-12, PR.AC-4

Table 2 describes basic endpoint controls with practices to implement and maintain them.

8. "CIS Control 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers," Center for Information Security Controls, accessed September 24, 2018, https://www.cisecurity.org/controls/secure-configuration-for-hardware-and-software-on-mobile-devices-laptops-workstations-and-servers/.

Table 2. Basic Endpoint Controls to Mitigate Risk at Endpoints

Control	Description	Implementation Specification
Antivirus (AV)	Technology capable of detecting known malicious malware using signatures, heuristics, and other techniques	• Push AV packages out using endpoint management systems that interface with Windows and Apple operating systems (OS). • Develop metrics to monitor the status of AV engines, signature updates and health. • Dispatch field services/desktop support for malware that is detected but not automatically mitigated. • Leverage network access control (NAC) to conduct a validation check prior to enabling network access.
Full disk encryption	Technology capable of encrypting an entire disk to make it unreadable for unauthorized individuals	• Ensure that encryption is enabled on new endpoints acquired by the organization. • Connect encryption management to endpoint management systems that interface with both Windows and Apple OS. • Develop metrics to monitor the status of encryption. • Dispatch field services/desktop support teams to resolve encryption errors. • Use anti-theft cable locks to lock down any device that cannot support encryption. • Leverage NAC to conduct a validation check prior to enabling network access.
Hardened baseline images	Configure the endpoint operating system in the most secure manner possible	• Limit usage of local administrator accounts. Enable only local administrative rights required by the user. Use a separate account dedicated to this purpose. • Enable local firewalls and limit inbound access to the endpoint to only required ports. • Disable weak authentication hashes (e.g., LANMAN, NTML Version 1.0). • Prevent software from auto-running/starting, especially when using thumb drives. • Disable unnecessary services and programs. • Permit usage only of known hardware encrypted thumb drives for writing data. • Review and consider the implementation of Security

Control	Description	Implementation Specification
		Technical Implementation Guides.[9]
Patching	A process ensuring regular patching of endpoint OS and third-party applications	• Establish an endpoint management system and distribute OS patches during regular maintenance times. • Automatically update and distribute patches to third-party applications that are known to be vulnerable, such as internet browsers, Adobe Flash, Acrobat Reader, and Java. • Develop metrics to monitor patch status. Review on a weekly basis. • Dispatch field services/desktop support for endpoints that fail to patch.
Local administrative rights	The provisioning of privileged access to users for installing or updating application and OS software	• Limit local administrative rights deployed to endpoints. Use endpoint management systems to install new programs and patch systems. • For users that require administrative rights, deploy a local account with administrative privileges that is separate from the general user account. Never allow a general user account to operate with administrative privileges, because doing so increases vulnerability to malware and client-side attacks.

Organizations should reference **Cybersecurity Practice #5: IT Asset Management** to determine whether their endpoints meet IT asset management (ITAM) requirements. Examples include maintaining a proper inventory of endpoints, reimaging endpoints as they are redeployed, and securely removing endpoints from circulation when decommissioned.

Lastly, ensure that you train your workforce on the need to report any lost or stolen endpoints to your cybersecurity department. Reporting should occur promptly so cybersecurity departments can execute the proper incident response procedures, outlined in **Cybersecurity Practice #8: Security Operations Center and Incident Response**.

9. "Security Technical Implementation Guides (STIGs)," Information Assurance Support Environment (IASE), accessed September 24, 2018, https://iase.disa.mil/stigs/Pages/index.aspx.

Sub-Practices for Large Organizations

2.L.A	*Automate the Provisioning of Endpoints*	***NIST FRAMEWKORK REF:*** PR.DS-5

It is challenging to manage thousands of endpoints consistently, especially when endpoint provisioning processes are manually executed. Most organizations do not have the necessary resources to run such an operation.

Value-added resellers (VARs) that sell endpoints through your supply chain can preconfigure endpoints before delivering them to your enterprise. To implement preconfiguring, the organization must build a "gold image," with a series of checklists and configuration procedures, and provide it to the V!R/ This approach helps to ensure a consistent and resilient deployment of endpoints.

In some cases, vendors provide the ability for an organization to provision devices centrally. For example, Apple provides this service for its devices through its Device Enrollment Program (DEP). The DEP enables an organization to simplify enrollment and endpoint security management. The organization enters the serial number or order number of the new device in the DEP, initiating a series of device configuration tasks that are specific to your organization's requirements. Further information is available in !ppl e's *DEP Guide*.[10]

2.L.B	*Mobile Device Management*	***NIST FRAMEWKORK REF:*** PR.AC-3

Mobile devices, such as smartphones and tablets, present their own management challenges. Multiple security configuration options exist for these devices, and organizations should configure the devices consistently to comply with organizational security policies.[11]

Mobile device management (MDM) technologies manage the configuration of devices connected to the MDM system. In addition to configuration management, they may offer application management and containerization. All three are important to consider, especially for organizations that allow the use of personal devices in business operations.

Because most mobile devices travel on and off the organization's network, it is important to consider cloud-based MDM systems to enable consistent check-in. If cloud-based systems are not available, then the onsite MDM systems must be accessible over the internet through virtual private network (VPN) connectivity or in the organization's demilitarized zone (DMZ). The following paragraphs further describe the capabilities of MDM systems.

- *Configuration management:* At minimum, ensure that passcodes are in place and encryption is enabled. Ensure that each device locks automatically after a predefined duration (perhaps 1 minute). Implement device wipe functions after a series of unsuccessful logins (consider 10

10. *DEP Guide*, Apple.com, last modified October 2015, https://www.apple.com/business/site/docs/DEP_Guide.pdf

11. "CIS Benchmarks," Center for Information Security, accessed September 24, 2018, https://www.cisecurity.org/cis-benchmarks/.

unsuccessful logins). Limit the amount of time that an e-mail can reside on the mobile device (consider 30 days maximum). Consider leveraging an "! lways on VPN" to protect the device when users connect to unsecured wireless networks. Consider prohibiting the installation of unsigned applications.

- *Application management:* Malicious applications reside in app stores and may appear to be legitimate, such as PDF readers or Netflix apps, when they really contain malicious code that provides access to data elsewhere on the mobile device. MDM solutions use whitelisting or blacklisting techniques to limit the installation of these malicious applications. Consider both, especially for devices that run on the Android platform, which is an open platform that accepts a wide range of applications.
- *Containerization:* Organizations with BYOD policies should consider containerization technologies. These technologies segment and process business data on a mobile device separately from personal data. Containerized business applications exist only in a hardened container on the mobile device. Examples of such business applications include e-mail, calendaring, and data repositories. Containerization allows the organization to wipe the container and clear business data from the device when the workforce member leaves or changes position in the organization. It also limits the risk that personally downloaded malicious applications will access business data.

2.L.C	***Host-Based Intrusion Detection and Prevention Systems***	***NIST FRAMEWKORK REF:*** PR.DS-5

Host-based intrusion detection systems (HIDS) and host-based prevention systems (HIPS) use an intrusion protection method like that used by network-based intrusion detection and prevention systems. Deploy these technologies on endpoints to detect patterns of attacks launched against those endpoints. These attacks can originate at the endpoint's network, or through client-side attacks that occur when using e-mail or browsing the web.

HIDS and HIPS technologies are usually deployed and managed through central endpoint management systems used to manage endpoint software and patching. Configure them to auto-update against their command servers. The command servers should be configured to regularly download fresh signatures of attack indicators.

2.L.D	***Endpoint Detection and Response***	***NIST FRAMEWKORK REF:*** PR.DS-5, RS.AN-1

Endpoint detection and response (EDR) technologies bridge the gap between execution and processing that occurs in an organization's fleet of endpoints. These agent-based technologies allow cybersecurity departments to query large fleets of endpoints for suspicious running processes, file actions, and other irregular activities.

EDR enables large-scale response to malware outbreaks. If malware is installed in the organization's environment, cybersecurity professionals can "reach in and remove" the malware from thousands of devices using a single action. Finally, EDR technologies provide cybersecurity departments with forensic capabilities that supplement incident response (IR) processes.

2.L.E	Application Whitelisting	NIST FRAMEWKORK REF: ID.AM-2, PR.DS-6

Application whitelisting technologies permit only applications that are known and authorized to run, rather than identifying applications that not permitted to run. They are based on the assumption that it is impossible to identify and blacklist, or block, every malicious application.

Organizations should maintain a current inventory of all software on endpoints to facilitate complete and consistent maintenance and patching to protect against client-side attacks.[12]

Configuration of application whitelisting is complex and outside of the scope of this guide. Interested organizations should read *NIST Special Publication 800-167: Guide to Application Whitelisting*.[13]

2.L.F	Micro-Segmentation/Virtualization Strategies	NIST FRAMEWKORK REF: PR.AC-5

Technologies called *micro-virtualization* or *micro-segmentation* assume that the endpoint will function in a hostile environment. These technologies work by preventing malicious code from operating outside of its own operating environment. The concept is that every task executed on an endpoint (e.g., click on a URL, open a file) can run in its own sandboxed environment, thus prohibiting the task from interoperating between multiple sandboxed environments.

Since most malware is installed by launching incremental processes after gaining an initial foothold, this strategy can be effective at eliminating that second launch. Additionally, once the malicious task has completed, the microenvironment is torn down and reset. Further configuration advice is specific to the microenvironment technology deployed.

Threats Mitigated

1. Ransomware attacks
2. Loss or theft of equipment or data

Suggested Metrics

- Percentage of endpoints encrypted based on a full fleet of known assets, measured weekly. The first goal is to achieve a high percentage of encryption, somewhere around 99 percent. Achieving 100 percent encryption is nearly impossible, because defects always exist. Additionally, the percentage of endpoints encrypted will vary as you discover new assets, which is why you should measure it weekly.

---

12. "CIS Control 2: Inventory of Authorized and Unauthorized Software," Center for Internet Security Controls, accessed Sember 24, 2018, https://www.cisecurity.org/controls/inventory-of-authorized-and-unauthorized-software/.

13. Adam Sedgewick, Murugiah Souppaya, and Karen Scarfone, *Guide to Application Whitelisting*, (NIST Special Publication 800-167, October 2015, Gaithersburg, MD), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

- Percentage of endpoints that meet all patch requirements each month. The first goal is to achieve a high percentage of success. Secondary goals are to ensure that there are practices to patch endpoints for third-party and OS-level application vulnerabilities, and to be able to determine the effectiveness of those patches. Without the metric, there might not be checks and balances in place to ensure satisfactory compliance with expectations.
- Percentage of endpoints with active threats each week. The goal is to ensure that practices are in place to respond to AV alerts that are not automatically quarantined or protected. Such alerts indicate that there could be active malicious action on an endpoint. An endpoint with an active threat should be reimaged using general IT practices and managed using a ticketing system.
- Percentage of endpoints that run nonhardened images each month. The goal is to check assets for compliance with the full set of IT management practices, identifying assets that do not comply. To do this, place a key or token on the asset indicating that it is managed through a corporate image. Separate practices are necessary for assets that are not managed this way to ensure that they are properly hardened.
- Percentage of local user accounts with administrative access each week. The goal would be to keep this number as low as possible, granting exceptions only to local user accounts that require such access.

Cybersecurity Practice #3: Identity and Access Management

Identity and access management (IAM) is a program that encompasses the processes, people, technologies, and practices relating to granting, revoking, and managing user access. Given the complexities associated with health care environments, IAM models are critical for limiting the security vulnerabilities that can expose organizations. A common phrase used to describe these programs is *"enabling the right individuals to access the right resources at the right time."*

Cybersecurity Practice 3: Identity and Access Management	
Data that may be affected	Passwords
Medium Sub-Practices	3.M.A Identity 3.M.B Provisioning, Transfers, and Deprovisioning Procedures 3.M.C Authentication 3.M.D Multi-Factor Authentication for Remote Access
Large Sub-Practices	3.L.A Federated Identity Management 3.L.B Authorization Access Governance 3.L.C Single Sign On
Key Mitigated Risks	• Ransomware Attacks • Insider, Accidental or Intentional Data Loss • Attacks Against Connected Medical Devices that May Affect Patient Safety

Most access authentication methods rely on usernames and passwords, a model proven by the success of phishing and hacking attacks to be weak. Establishing IAM controls requires a distinct and dedicated program to accommodate its high level of complexity and numerous points of integration. You can find a toolkit for establishing an IAM program on the EDUCAUSE website.[14]

This section will focus on the critical elements of an IAM program required to manage threats relevant to the HPH sector.

Sub-Practices for Medium-Sized Organizations

3.M.A	***Identity***	***NIST FRAMEWKORK REF:*** PR.AC-1

As defined in NIST Special Publication 800-63-3, "Digital identity is the unique representation of a subject engaged in an online transaction."[15] A common principle to follow is "One person, one identity, multiple contexts/" In health care, a person can have the context of a patient, payor, or even employee of the health system. For clinical staff, one person can have one identity, but that person's ability to

14. David Sherry et al/, "Toolkit for Developing and Identity and Access Management (IAM) Program," EDUCAUSE, last modified May 7, 2013, https://library.educause.edu/resources/2013/5/toolkit-for-developing-an-identity-and-access-management-iam-program.

15. Paul A. Grassi, Michael E. Garcia, and James L. Fenton, *Digital Identity Guidelines* (NIST Special Publication 800-63, June 2017, Gaithersburg, MD), https://pages.nist.gov/800-63-3/sp800-63-3.html.

practice specialties will depend on context, including the country, practice area, or hospitals where the person has a business or employee relationship.

Within the United States, each citizen is provided with a unique SSN. Similarly, a person who joins an organization should be given a unique identifier. That unique identifier should not be used as a secret authenticator, the way a person's SSN is often used/The unique identifier is not the authenticator.

Establish each person's identity through onboarding systems of record. The most common of these systems is the ERP or HR system. When onboarding new employees in the organization, HR business processes identify and establish the new employee in the organization. Onboarding involves many processes, such as background checks, employment verification, and preparation for payroll. They provide solid identity proofing that you can use to verify the employee's identity in the future/ They trigger for generating the employee's new digital identity. These identity-proofing practices respond to the need to understand a person's relationship and context within the organization. Therefore, it is imperative that IAM programs and functions align with HR practices and business processes in general.

Identities maintain a series of attributes that describe common user elements. The series of attributes comes from the system of record, whether that is an HR system, contingent workforce system, medical staffing office, or other system in the organization's ecosystem/ Examples of common elements include a person's name, location, telephone number, e-mail address, job title/job code, and specialization/practice data.

The system of record transmits attributes to the IAM system, enriching the identity data and facilitating the flow of information to systems for login, access management, and other cybersecurity- and business-related functions. In addition to common descriptive attributes, there may be other system-defined attributes (e.g., roles or affiliations used to describe populations of individuals, such as clinician, staff, staff nurse, visitor, student). Organizations can leverage both types of attributes for future authorization components. For example, you can use attributes to authorize eligibility for various systems (using a technique called attribute-based access control [ABAC]).

Users defined under proper identity management processes will include more than your employees. These processes should account for volunteers, locums, contractors, students, visiting scholars, visiting nurses, physician groups staff, billing vendors, visiting residents, organ procurement organizations, special statuses (such as emeritus professors), and third-party vendors that require access to provide services to your organization. Each of these identity types must have an approved channel to serve as the system of record, where the identity proofing activities will occur.

You can store all this identity information in a single repository, enabling its consumption for other purposes. IAM systems, in principle, are an aggregate of system of record data. IAM systems should be a system of last resort when none exists (e.g., contingent workforce if HR/business does not have a solution). At a minimum, follow these basic principles:

- Enumerate all authorized sources of identity within the organization. These sources are often referred to as the systems of record. Examples include HR systems, vendor management systems, contingent workforce systems, medical staffing offices or practice offices, and student information systems.
- Ensure that all users receive a unique identity and identifier. Smaller organizations without multiple constituents may consider using the employee ID number from the system of record. Larger organizations with many constituents should establish a unique identifier for each user

and reconcile. Do not use SSNs as unique identifiers! An individual with multiple contexts should have one user record with one unique identifier that ties to all contexts.

- Maintain the integrity and uniqueness of digital identities. Never reuse identities for different people. People come and go throughout the life of an organization. Maintain their records perpetually.
- Proper identity management enables the automation of functions such as system access and authentication. Enumerate and establish attributes, which are critical to provide context to the identity and required for access and authentication controls. For complex and large organizations, this is an important principle to ensure the consistent application of attributes, which in turn enables automated authentication and authorization, for example through automated provisioning and deprovisioning.
- Store identity information in a database or directory capable of registering identity information and associated attributes. Such databases aggregate systems of record data. Consider specialized tools for organizations with multiple constituent types.
- Use a single namespace to establish user accounts within the organization. Tie these user accounts back to the identity so that you can always trace individuals to their digital identities.

3.M.B	***Provisioning, Transfers and Deprovisioning Procedures***	***NIST FRAMEWKORK REF:*** PR.AC-4

After you establish digital identities and user accounts, you must provision users with access to information systems prior to using them. It is important to ensure that provisioning processes follow organizational policies and principles, especially in the healthcare environment.

HIPAA describes key principle of *minimum necessary*, which states that organizations should take reasonable steps to limit uses, disclosures, or requests of PHI to the minimum required to accomplish the intended purpose. This same principle applies to reducing the attack surface of potentially compromised user accounts. By limiting access, you can limit the scope of a ransomware outbreak or data attack.

Follow these principles for provisioning:

- Identify common systems that all users will need to access and the most basic access rights required for each of those systems. These common systems are referred to as *birthright entitlements*.
- Define birthright entitlements in organizational policies, procedures, or standards. There should be documentation that describes the access rights that all users receive.
- Establish procedures and workflows that ensure consistent provisioning of birthright entitlements. Consider employing specialized tools to automate this process for accuracy and reliability. Do not automate bad or unknown workflows.
- Establish procedures and workflows that enable provisioning of required access in addition to birthright entitlements, such as access to auxiliary or ancillary systems. Pay special attention to cloud-based systems. Consider leveraging federated access management tools that automatically provision access in the cloud.

- Consider a two-part process that allows users to request access but requires a second individual to approve the request prior to granting access. A common approach is to designate an employee's supervisor as the approving party.

Leverage IT ticketing systems by building the provisioning workflow into the ticketing system. This establishes consistency in the approval processes, automates the requesting and granting of approval, and documents the granting of access. It is important to ensure that access provisioning processes are auditable.

In addition to establishing a robust process to grant access to users, it is equally important to establish a process to remove access at the right time. Failure to remove access promptly after an employee's relationship with the organization terminates may result in unauthorized or malicious access to systems.

Follow these principles for deprovisioning:

- Establish procedures to terminate access to user accounts. Execute these procedures promptly at the time of termination. Consider leveraging tools that automate this process after receiving notification of termination from the system of record. The system of record is usually the HR system, although other systems may trigger access termination.
- Ensure that your termination process, whether manual or automated, includes session termination steps to prevent active sessions (e.g., e-mail logins on mobile phones) from remaining active after the employee leaves the organization.
- Establish an "urgent termination" process outside of the normal termination procedures. Use urgent termination in cases of sensitive termination, such as an involuntary termination.
- Ensure that termination procedures include both critical business systems and ancillary or auxiliary systems. Pay special attention to cloud-based systems that are accessible outside of the organization's standard network. These assets will remain accessible to the user if the deprovisioning process is not completed. Consider using federated access management tools to deprovision access to cloud-based systems automatically.
- Build automatic timeouts for nonuse in critical systems. These timeouts can catch edge cases where deprovisioning procedures are not executed, ultimately reducing the exposure to unauthorized access.

Removal of access should occur when users terminate their relationships with the organization and when users transfer to new functions in the organization. For example, if a patient care services (PCS) manager transfers to the nursing department, access granted when the user was a PCS manager should be removed prior to granting access required by the user as a nurse. This helps to prevent users from accumulating unnecessary access rights.

3.M.C	***Authentication***	***NIST FRAMEWKORK REF:*** PR.AC-7

User accounts must engage in authentication to properly assert the user's identity in the digital ecosystem. The most common and, unfortunately, the weakest method for authentication relies on password credentials. Nevertheless, password-based authentication systems will continue to exist for the foreseeable future, and organizations should develop solid password authentication practices.

- *Centralized authentication:* Use central authentication systems, such as Lightweight Directory Access Protocol directories or Active Directory, to the greatest extent possible. Tying authentication mechanisms back to these central systems enables enterprise management of credentials. You can manage the access rights of your user base from a single location. This is incredibly important when access needs to be deprovisioned in a timely and automated manner.

  Passwords are the most common credential used to authenticate users. The strength and management of passwords are paramount. Strong passwords combat brute force or password guessing attacks. Assuming you can limit the exposure to brute force and guessing attacks, NIST recommends the following techniques as part of NIST Special Publication 800-63:[16]

  - Limit the rate at which authentication attempts can occur. Spacing out each password attempt by a second or two severely limits the ability of automated systems to brute force the password.
  - Ensure the use of cryptographically strong hashing and salting for password storage.
  - Use passphrases in place of passwords. Require a minimum of 8 characters and permit up to 64 characters, as well all printable ASCII characters and spaces.
  - Implement dictionary-based password checking and compromised password blacklists. Prohibit users from establishing risky passwords, such as those used in previous breaches, repetitive or sequential characters, or context-specific words (such as a name of a service, username, or derivatives thereof).

- *Privileged account management:* Centralized authentication should be used for both general user access and privileged administrative accounts. You must additionally separate privileged administrative accounts from general user accounts. For example, provision an IT administrator at least two accounts: one account for use completing day-to-day activities and a separate administrative account with access only to systems required by the IT administration function. This second step is critical; the use of privileged accounts during normal day-to-day business may expose these accounts to malware attacks, giving an attacker elevated access to the organization's environment. Limit this exposure as much as possible. Consider the following controls for managing your privileged accounts:

  - Ensure that the passwords set for service accounts are large and complex (at least 32 characters, preferably 64).
  - Rotate these passwords on a frequency you define, but certainly if the password is ever compromised.
  - Escrow privileged systems credentials, making them unique for each system or device.
  - Link privileged access to problem, change, or service tickets in the organization's ticketing system.

16. Paul A. Grassi et al., *Digital Identity Guidelines: Authentication and Lifecycle Management* (NIST Special Publication 800-63B, June 2017, Gaithersburg, MD), https://pages.nist.gov/800-63-3/sp800-63b.html#appA.

- Require the use of a jump server when elevating privileges. Ensure full recording and auditing of the jump server.
- Require brokered access to a privileged account that registers which user is using the privileged account and records all actions taken.
- Require MFA for all privileged accounts used interactively.
- Conduct regular reviews of privileged access.
- Limit actions that privileged accounts can take by using access control lists. Check for the use of sensitive commands and alert the IT or Information Security departments if there is misuse.

- For further details on how to securely configure privileged access, consider the following resources:
  - For Windows, see Microsoft's article "Implementing Least-Privilege Administrative Models/"[17]
  - For Linux, see Redhat's article "Controlling Root !c cess/"[18]
- *Local application authentication*: There may be cases where applications do not support a centralized authentication model. Although there are increasingly fewer onsite systems that cannot bind to centralized authentication systems, these systems are still prevalent in the health care environment. As organizations migrate applications to the cloud, it is easy to accidentally instantiate a cloud-based service that lacks robust authentication and focuses on local user accounts.

  Whenever you use systems with local authentication, you must maintain solid access control procedures to manage user accounts. This requires designating a responsible IT owner who will manage and regularly review these accounts. Failure to do this allows users access to systems for longer than necessary and is especially risky when an employee leaves the organization and continues to have access to these systems. Consider the following extra controls:
  - Designate an IT owner for each legacy/cloud-based system.
  - Establish a distribution list in your organization which includes your IT owners as members. Submit terminations out to these IT owners as they occur.
  - Ensure that IT owners comply with standard operating procedures for the onboarding, review and, most importantly, termination of users.

---

17. Bill Mathers et al/, "Implementing Least-Privilege Administrative Models," Microsoft Windows IT Pro Center, last modified May 31, 2017, https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models.

18. "Controlling Root Access," Redhat Customer Portal, accessed September 24, 2018, https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-controlling_root_access.

- Regularly audit compliance with these manual processes. Ensure compliance with regular account review and termination procedures.

- *Monitor authentication attempts*: Monitor both regular and privileged user accounts for security and compliance purposes. Details are discussed further in **Cybersecurity Practice #8: Security Operations Center and Incident Response**. Details on methods to monitor authentication logs can be found in the SANS white paper, *Keys to the Kingdom: Monitoring Privileged User Actions for Security and Compliance*.[19]

3.M.D	***Multifactor Authentication for Remote Access***	***NIST FRAMEWKORK REF:*** PR.AC-3, PR.AC-7

MFA systems require the use of several authentication methods to verify a user's identity. According to the common description, MFA systems use at least two of the following: something you know, something you have, and something you are. Users must correctly address at least two of these three categories before the system will verify their identities and allow access.

The most common MFA techniques use of passwords and one-time codes that are delivered to the user out-of-band from the authentication technique. For example, most banks have MFA capabilities, which require the customer to enter a password (something you know) followed by a verification code that is texted to the customer's smart phone (something you have).

MFA should be implemented on remote-access technologies to limit the exposure of password credentials that could be compromised through phishing or malware attacks. MFA is an incredibly impactful method at limiting an attacker's ability to compromise the organization's environment. Consider implementing MFA on the following types of technologies:

- *VPNs:* These allow remote network access to your environment. VPNs should be configured to limit user access based on role-based access control (RBAC) or ABAC rules and to enable MFA.
- *Virtual desktop environments:* These are environments where virtual terminal sessions can be exposed to remote access, allowing your employees to work remotely. Although highly useful for workforce flexibility, virtual desktop environments systems can be compromised easily if they lack MFA authentication.
- *Remote e-mail access:* If your organization permits remote e-mail access, MFA should be enabled to limit the risk of compromised credential access in the e-mail system. It is common for health care environments to store PHI with these systems, and this exposure could result in a breach of sensitive information, especially if MFA is not used.

19. Dave Shackleford, "Keys to the Kingdom: Monitoring Privileged User Actions for Security and Compliance," last modified May 2, 2010, https://www.sans.org/reading-room/whitepapers/analyst/keys-kingdom-monitoring-privileged-user-actions-security-compliance-34890.

Sub-Practices for Large Organizations

3.L.A	*Federated Identity Management*	*NIST FRAMEWKORK REF:* PR.AC-6

Federated identity management enables identity information to be shared between organizations in a trusted manner. This allows identities from home institutions (e.g., individual clinics) to be used across a greater ecosystem (e.g., the entire health network). In health care organizations, it is common for providers, payors, and other affiliates to work together in an integrated manner. In complex, large environments, multiple organizations operate jointly, with different HR practices inside each organization.

Rather than creating identities in each organization involved in such a joint operation, federated identity management tools and processes allow the identity assertions of the home institutions to be used throughout the federation.

Consider the following example: a clinician is part of a practice group that is credentialed within a regional hospital. From the hospital's perspective, this clinician is not an employee but must be credentialed with access to the electronic medical record (EMR). From the practice group's perspective, this clinician has been onboarded through standard HR background checks and processes. If the practice group and the hospital were operating within a federation, the clinician's "home" identity could be established from the practice group and asserted to the hospital as part of the clearance processes. If the clinician's relationship with the practice group were to change, this identity information would be revoked within the hospital based upon assertions from the federation. These processes would be completely automated.

The same model can be leveraged when working with third-party vendors that provide workforce support or staff-augmentation capabilities. In this case, the third party is the "home institution" that requires access to resources in the organization. To monitor the activities of each of those workforce members would involve a highly complicated and largely manual process unlikely to be effective. A federation can solve this problem.

In complex environments such as large integrated delivery networks, federations are almost a requirement to properly manage the temporal aspects of the identities within.

3.L.B	*Authorization*	*NIST FRAMEWKORK REF:* PR.AC-6, PR.AC-4

After authentication has occurred, the mechanism to obtain specific access to an information resource, such as an application system, is referred to as *authorization*. Authorization processes check the level of access that has been granted to a user credential and ensures that the credential can access only preauthorized areas. Consider the analogy of traveling at the airport. When you pass through the security lines, your identity is authenticated using your ID card or passport, and you are then authorized to access the terminals based on a ticket for a flight. You are not permitted to access any other flight than the one authorized on your ticket.

Authorization limitations are required by the HIPAA privacy rule under the minimum necessary principle. In addition to HIPAA compliance, minimum necessary is a leading practice to limit malicious use of credentials. In most cases, when hackers break into systems, they are trying to access the "keys to the

kingdom," or privileged access credentials that permit access to the most sensitive resources. Do not risk unauthorized access by granting more access than necessary to your users!

Consider the following techniques to limit authorization to only those components required by the user:

- *RBAC:* Conduct a high-level role-mining exercise to map out the role types that exist within your organization and the access they require. For example, identify access requirements for clinicians, support staff, unit secretaries, switchboard operators, case managers, and others. For example, the clinician may need access to the medical record (though not necessarily the entire medical record), whereas the support staff may not need access at all. By defining the unique requirements for these two roles, you have started on the path toward differentiating access models.

  It can be difficult to provision granular authorization models based on users' roles. In healthcare, two individuals might have the same job title and role, yet completely different tasks within the organization. Relying solely on a person's role to grant access could thus limit the ability for users to fulfill other authorized responsibilities.

- *ABAC:* Attribute-based authentication models consider the attributes associated with a user's identity, the attributes of the information system being accessed, and the context associated with the access request. In this model, a user may, for example, be granted an attribute that enables the user to access a specialized function within an information system, but only during business hours or only while onsite. When the user requests access, ABAC systems check the actual context against the access requirements to determine whether access should be granted.[20]

  This highly effective model limits access based on user-specific rules established in the ABAC systems that define access parameters. As an example, a request is made to grant all nurses with access to all patients on a specific floor in a specific hospital to support flexible care requirements. You might be concerned that this access is excessive, since a nurse might not be part of a care team for a particular patient. To minimize this impact, you can leverage ABAC, limiting access to times when the nurse is physically present at a specific hospital and ensuring that access is granted only after the nurse has been authenticated using both a password and MFA. The ABAC access credentials cannot be used to grant remote access to the same patients or to grant access anywhere else within the health care system. In this model, even a hacker with access to the password and the MFA answer would be unable to access patients using those credentials.

3.L.C	***Access Governance***	***NIST FRAMEWKORK REF:*** PR.AC-4

When a user joins the organization the onboarding processes generate a lot of access request activities. Once access is established for a user, it can be a challenge to determine, at a given future time, whether that access continues to be required. Consider an employee who has worked for an organization for

20. "Attribute Based Access Control," NIST Computer Security Resource Center, last updated Feburary 13, 2013, https://csrc.nist.gov/Projects/Attribute-Based-Access-Control.

many years, serving in multiple capacities, and has been placed on special projects and worked throughout the organization. Over time, this employee might accumulate more access than was ever intended.

Conducting a manual review of each employee's access to each of an organization's critical application systems would be nearly impossible. Fortunately, specialized tools are available that enable an organization's leadership to review system access in an automated, self-service capacity. These tools are generally referred to as access governance tools. Below are the relevant components:

Tooling: Specialized tools bind to identity management systems and connect to critical business systems to understand the access in place for all users in these systems. These tools require the ability to connect with and parse through specific aspects of the applications in question, such as EMR systems, revenue cycle systems, imaging systems, lab systems, and more.

- *Access rules:* Within access governance tools, specialized rules can be defined based on roles or user attributes. For example, a financial system must define the role differences between accounts payable and accounts receivable. No employee should be capable of access with both roles. Otherwise, a fraudulent purchase order could be generated and the invoice paid by the same person, resulting in a fraud loss to the organization. Understanding the characteristics and requirements of these critical roles enables you to create automated alerts that control user access.

In addition to the standard segregation of duties checks, some specialized tools compare access profiles of certain users in a role to identify outliers. For example, these tools can assess the usual pattern of access granted to nurses across multiple systems. This pattern can then be set as a baseline of access, and the tool can compare each user against that baseline. If a specific nurse is determined to have excessive access, the user can be reviewed for appropriate adjustments.

- *Access review*: Through workflows established with these advanced tools, supervisors within the organization can review the access that their employees currently have in critical environments. This can be done on a regular schedule established by policy. In the case where an employee has retained access that is no longer necessary, the manager can use self-service portals to identify these access violations and flag them for removal. In some systems, once a manager flags an access for removal, it will be automatically stripped.

  At the end of an access review, the manager can certify that the review is accurate. This documentation is useful for audit practices and to demonstrate effective reviews.

3.L.D	***Single Sign On***	***NIST FRAMEWKORK REF:*** PR.AC-7

Federated single sign on (SSO) is an effective method to authenticate users against centralized credential repositories. SSO techniques abstract authentication principles away from the general Microsoft- or Linux-based methods into a generalized standard that can be implemented across platforms. SSO involves securely conducting a general authentication process and passing additional identity attribute information to the specific authorization processes in the resources being accessed. It also has the benefit of requiring only one login while an active SSO session is enabled, eliminating annoying password prompts.

Several federated SSO standards exist, including OpenID, Security Assertion Markup Language, OAuth, and Active Directory Federation Services. When implementing cloud-based systems, such as software-as-a-service systems, the use of SSO should be a security requirement.

A health care-specific SSO model leverages a second authentication factor at clinical workstations for easy access within a health care provider space. These systems can be configured to require a user to authenticate once per day or per shift at a clinical workstation, after accessing the larger clinical setting, using a password and key card. Subsequent authentications are conducted by tapping the key card to provide secure, easy access to the clinical workstations. These systems provide MFA within the clinical environment while easing the password authentication processes.

Threats Mitigated

1. Ransomware attacks
2. Insider, accidental or intentional data loss
3. Attacks against connected medical devices that can affect patient Ssafety

Suggested Metrics

- Number of alerts generated for excessive access to common systems. For example, “allow any” permissions to core applications, SharePoint, file systems, etc.
- Number of users with privileged access, trended over time. The primary goal is to establish a baseline of the normal number of privileged accounts and monitor variances from the baseline.
- Number of automated terminations, trended over time. The goal is to establish a baseline for normal terminations and monitor variances from that baseline. A decrease in the number of terminations can indicate that the automated systems are not terminating access properly.
- Number of elevated privileged access requests, trended over time. The goal is to establish a baseline to determine how much privileged access is granted over a one-week period and monitor variances from that baseline.

Cybersecurity Practice #4: Data Protection and Loss Prevention

Cybersecurity Practice 4: Data Protection and Loss Prevention		
Data that may be affected	Passwords, PHI	
Medium Sub-Practices	4.M.A 4.M.B 4.M.C 4.M.D 4.M.E	Classification of Data Data Use Procedures Data Security Backup Strategies Data Loss Prevention
Large Sub-Practices	4.L.A 4.L.B	Advanced Data Loss Prevention Mapping of Data Flows
Key Mitigated Risks	• Ransomware Attacks • Loss of Theft of Equipment or Data • Insider, Accidental or Intentional Data Loss	

All organizations within the HPH sector access, process, and transmit sensitive information, such as health information or PII. The fundamental data used in operations are highly sensitive, representing a unique challenge to the HPH sector. Most of the health care workforce must leverage these data to carry out their respective missions.

In that context, healthcare faces a growing challenge of understanding where data assets exist, how they are used, and how they are transmitted. PHI is discussed, processed, and transmitted between information systems daily. Protecting these data requires robust policies, processes, and technologies.[21]

As your organization starts shoring up its data protection and prevention controls, it is best to begin by understanding the types of data that exist in the organization, setting a classification schema for these data, and then determining how the data are processed. Establish a set of policies and procedures for normal data use and then build in "guardrail" systems to guide your user base toward these business processes.

Sub-Practices for Medium-Sized Organizations

4.M.A	***Classification of Data***	***NIST FRAMEWKORK REF:*** (ID.AM-5)

There is a vast proliferation of data in healthcare environments. Data can range from records, including treatment information, social security numbers, insurance numbers and billing information to research information. Health care data also includes nonobvious, but still important, information such as

21. Erika McCallister, Tim Grance, and Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, (NIST Special Publication 800-122, April, 2010, Gaithersburg, MD), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

business strategies and development plans, business finances, employee records, and corporate board materials.

Before establishing policies describing how these varied data types should be used and disclosed, it is best to classify them into high-level categories that provide a consistent framework when developing policies and procedures. Table 3 provides a sample classification schema, with examples of the types of documents that the classification comprises.

Table 3. Example of a Data Classification Schema

Classification	Description	Examples
Highly Sensitive Data	Data that could easily be used for financial fraud, or could cause significant reputational damage.	SSN, credit card number, mental health information, substance abuse information, sexually transmitted infections.
Sensitive Data	Regulated data, or data that could cause embarrassment to patients or organizations.	Health information, clinical research data, insurance information, human/employee data, board materials.
Internal Data	Data that are not considered sensitive, but should not be exposed publicly.	Policies and procedures, contracts, business plans, corporate strategy and business development plans, internal business communications.
Public Data	All data that have been sanitized and approved for distribution to the public with no restrictions on use.	Materials published on websites, presentations, and research publications.

4.M.B	***Data Use Procedures***	***NIST FRAMEWKORK REF:*** ID.GV-1

After data have been classified, procedures can be written that describe how to use these data based on their classification. Such procedures describe the processes of setting usage expectations and of labeling the information properly. These two functions are described further in the following paragraphs.

- *Usage and disclosure:* Based on the classification type, data use should be limited appropriately and disclosed using specific methods. Consider the procedures in Table 4.

Table 4. Suggested Procedures for Data Disclosure

Classification	Use	Disclosure
Highly Sensitive	1. Must be restricted to only individuals who have a need to know. 2. Must use extreme caution when handling data.	Only share information internally *and* only when expressly permitted *and* when directed by the data owner.
Sensitive	3. Must be restricted to only individuals who have a need to know.	Only share information internally *and* only when expressly permitted.
Internal Use	4. Data can be generally used, but care should be considered in its consumption.	Only share information internally within the organization.
Public	5. No restrictions.	Share freely with no restrictions.

Be careful when sending information through e-mail. Ensure that sending PHI via e-mail is consistent with ONC guidance. Do not send unencrypted PHI through regular e-mail or text message. However, patients can request and receive access to their PHI via unencrypted electronic communications following a brief warning to the patient that unencrypted communications could be accessed by a third-party in transit and the patient confirms that they still want to receive the unencrypted communication.

- *Labeling*: It is important to label information properly to facilitate implementation of restrictions related to its usage and disclosure. Labeling helps keep data secure in two ways. First, users will understand how to handle information that is properly labeled. Second, specialized security tools, such as data loss prevention (DLP) systems, can be configured to discover and control information when it is properly labeled.

  At minimum, the labeling process should ensure that labels are readily apparent when users view information. Use techniques like placing the classification in the footer of the document. Collaborate with your marketing and communication departments to create document templates based on data classification levels. Organization-wide document templates enable specialized tokens or signatures to be embedded in the documents and tracked by DLP systems.

4.M.C	***Data Security***	***NIST FRAMEWKORK REF:*** PR.DS, PR.DS-1, PR.DS-2, PR.IP-6, PR.DS-5

After policies and procedures have been defined, you can establish additional data security methods. Consider the security methods described in Table 5.

Table 5. Security Methods to Protect Data

Security Method	Description	Considerations
Encrypt data at rest	Ensure data are encrypted when resident on file systems.	• When using the cloud-based services, enable native encryption capabilities to prevent exposures if the cloud provider is hacked. • Ensure that full disk encryption is enabled on all workstations and laptops.
Encrypt data in transit	Ensure that secure transport methods are used for both internal and external movement.	• Ensure that websites containing sensitive data use encrypted transport methods, such as Hypertext Transfer Protocol Secure (HTTPS). • Enable internal encryption methods when moving data in the organization. • Never send unencrypted sensitive data outside of the organization.
Data retention and destruction	Ensure that retention policies are set. Contractually bind third parties to destroy data when terminating contracts.	• Use standard destruction forms and require vendors to attest that data have been destroyed pursuant to those forms. • Set retention policies and quotas on e-mail systems to reduce the amount of data that can be exposed. Ensure that legal retention requirements are met. • Establish a purge strategy that includes purge mechanisms.
Scrub production data from test and development environments	Ensure that identifiable information is removed when replicating production environments for testing.	• Leverage specialized tools to deidentify data elements within large systems (such as EMRs). • Regularly audit data elements within test and production environments to ensure that they are clean.
Mask sensitive data within applications	Restrict users from accessing highly sensitive information, such as SSNs, by masking it unless authorized.	• Permit SSN access only to members who require it (e.g., registration desks, admitting desks, payor processing).

Security Method	Description	Considerations
Limit the ability to print, save, or export data based on function	Restrict the workforce's ability to export data out of systems that contain sensitive data, unless they have proper authorization.	• Encourage users to work within applications. Minimize data exporting by providing the required capabilities to manipulate data within the application. • Implement restrictions on data exports, especially in reporting or database systems that can query and return large datasets. • Consider removing the ability to print and copy/paste from EMR applications or web mail accessed from home.

4.M.D	***Backup Strategies***	***NIST FRAMEWKORK REF:*** PR.IP-4

A robust backup strategy for enterprise assets is critical to daily IT operations. It is equally important to have such a backup strategy in the event of cybersecurity incidents. There will be events that cause an asset, or multiple assets, to be thoroughly compromised. During these events, routine backups can be the only way to ensure proper execution of the recovery phase of your IR process. Fully decommissioning affected assets and restoring them to a time before the compromise occurred is the best method to neutralize the compromise.

At minimum, each mission-critical asset in your environment should have a backup plan. Backups can be executed using a variety of methods, the most common being disk-to-tape, disk-to-disk, or disk-to-cloud backups. The integrity of these backups is paramount; these copies are your last line of defense, and you want to make sure they are complete and accurate when you need them.

No matter what backup strategy you choose, it is very important to make sure these backup locations are not accessible from the general network or from the general user populations. These backups are can be the last line of defense against a ransomware attack, as such access to them should be severely limited. This includes access from the servers and systems themselves that are being backed up; considering letting systems only write new data rather than overwriting existing data. This can thwart the attempts of encryption attacks against these backup files.

- *Disk-to-tape*: This method makes backups by accessing designated systems and files and writing all content to a tape drive, or a tape library. Specialized software, hardware, and inventory controls are required. To conduct backups efficiently, you will need the tape robots and a tape library appropriate to the number and size of systems being backed up. These backups can be very large. Configure the tapes to use a "write once and read many" option. It is of utmost importance that encryption is enabled in writing to these tapes. If a tape is lost or stolen, unencrypted data could be breached.

There are great advantages to maintaining offline backups. You can rely on these copies to be available when you need them, and tape backups prevent attacks against the backup medium itself, because they are offline.

- *Disk-to-disk*: This method involves taking backup copies from a disk and replicating them to a separate disk or storage array that is dedicated to maintaining backup copies. This option generally costs less than disk-to-tape strategies, and disk-to-disk backups usually execute more quickly than disk-to-tape. It is important to use encryption on backup files, in case the files are copied outside of the organization.

It is important to consider controlling access to the disk storage system as part of a disk-to-disk approach. With cyberattacks like ransomware, attackers intend to disrupt both production and backup files. Attackers that launch ransomware attacks are aware that an organization's first response will be to contain the ransomware and then restore the uncorrupted files from a backup source. If they can compromise the backup and production files, there is a much higher likelihood that the organization will pay a ransom to get its files back. Access control mechanisms should prevent the system being backed up from accessing the disk array, except via required access channels. Do not permit other access to the array from other accounts, including administrative accounts. Remember, everyone is a potential target of a ransomware attack, especially administrators.

- *Disk-to-cloud:* This method is very similar to disk-to-disk backup. Cloud backup offers multiple added values, however. With a disk-to-cloud backup, you automatically get the resiliency and flexibility of the cloud environment, as well as the benefits from investments made by the cloud providers, to maintain 100 percent data availability. Rather than a single-point-of-failure model, as seen in disk-to-disk and disk-to-tape backups, cloud providers replicate data backups, leveraging cloud infrastructure with multi-fault–tolerant capabilities.

  As with the disk-to-disk model, it is important to limit access to cloud-based backup storage to only the systems and disks that are backed up and the data repository. Never implement a drive that maps to the backup repository. That mapped drive could be the vehicle that delivers the ransomware encryption. Always encrypt backup files to protect your organization if the cloud provider is breached.

Lastly, whatever method of backup is used, it is important to test the recovery of these backups on a periodic basis to ensure data availability. Again, your backup process is the last line of defense and must be demonstrated to be trustworthy in a time of need.

4.M.E	***Data Loss Prevention***	***NIST FRAMEWKORK REF:*** PR.DS-5

Once standard data policies and procedures are established and the workforce is trained to use them, DLP systems should be implemented to ensure that sensitive data are used in compliance with these policies.

Multiple DLP solutions exist and can be applicable depending on the types of data access channels that need to be monitored. Traditionally, DLP systems monitor e-mail, file storage, endpoint usage, web usage, and network transmission. All these channels should be considered.

A challenge with DLP systems is to determine which methods will be used to positively identify sensitive information. Within a health care environment, that can be tricky. Generally, there are two approaches, and both have limitations:

- Identify sensitive data based on dictionary words that may trigger the inclusion of sensitive data. These dictionaries include robust language repositories that identify health information. The challenge with this technique is related to the terminology. Medical terms are often used in the regular course of business, outside the context of sensitive information. This can lead to a high rate of false positives, forcing the workforce to apply prevention practices that are not necessary.
- Identify sensitive data based on identifiers that are known to be sensitive, a process known as *matching*. There are two popular methods of matching: (a) leveraging tokens embedded in documents classified as sensitive (document matching) and (b) leveraging actual patient identifiers from your EMR (exact data matching). Document matching dramatically reduces the number of false positives. However, the workforce must be trained on proper data classification. With exact data matching, the false positive rate will be lower than with the dictionary approach, since it involves positive confirmation. Exact data matching requires regularly extracting information from the EMR to load these identifiers into the system. Extra precautions must be taken so that the resulting large datasets are not exposed.

Once your identification methodology is established, DLP systems can be configured to monitor data access channels of interest and make policy decisions based on the data types and the access channels. It is best to provide direct feedback to users when the data policy has been violated, to avoid recurrent violations. Real-time feedback helps users adjust their data usage behaviors. Data channels are presented in Table 6 for your consideration.

Table 6. Data Channels for Enforcing Data Policies

Data Channel	Implementation Specification	Considerations
E-mail	Implement inline through SMTP routing for e-mail messages delivered outside the organization.	• Define thresholds of risky behavior. Implement a DLP block for these thresholds (e.g., > 100 records of PHI in the e-mail). • Define thresholds of risky behavior. Implement a DLP encrypt action for these thresholds, forcing the message to be encrypted before delivered.
Endpoint	Install DLP agents on managed endpoints that can apply data policies.	• Standardize and deploy encrypted thumb drives to users who require mobile storage options. • Prevent the copying of data to unencrypted thumb drives, or force encryption when copying data. • Control the use of noncontrolled peripherals and/or storage devices (e.g., backups of iPhones on devices). Permit only when specifically authorized. • Conduct data discovery scans of data residing on endpoints, exposing data on the endpoint so the user can make data destruction decisions.

Data Channel	Implementation Specification	Considerations
Network	Implement through Switched Port Analyzer ports from egress network points or through Internet Content Application Protocol on web proxies.	• If online, prevent the leakage of unencrypted sensitive data based upon predefined thresholds (e.g., files that contain > 100 records of PHI). • If out of band, activate IR procedures to contain data leakages that occur through the network.

Sub-Practices for Large Organizations

4.L.A	***Advanced Data Loss Prevention***	***NIST FRAMEWKORK REF:*** PR.DS-5

After implementing basic DLP controls, you should consider expanding your DLP capabilities to monitor other common data access channels. Table 7 recommends methods for your consideration.

Table 7. Expanding DLP to Other Data Channels

Data Channel	Implementation Specification	Considerations
Cloud storage	Use cloud access security broker systems to monitor data flows into cloud systems.	• Label data identified as sensitive. Implement digital rights and encryption to limit access to sensitive data. • Ensure that cloud-based file storage and sharing systems do not expose sensitive data in an “open sharing” construct without authentication (i.e., do not permit the use of sharing data through a simple URL link).

Data Channel	Implementation Specification	Considerations
Onsite file storage	Point discovery scanning systems at known file servers or other large data repositories.	• Conduct regular DLP scans against the file systems to scan and identify sensitive data. • Query security access permissions for each file that contains sensitive data. Define thresholds for excessive access and set alerts if these are crossed. Forward alerts to the SOC for response, as described in **Cybersecurity Practice #8: Security Operations Center and Incident Response**. • Determine staleness of records with sensitive data. Consider executing data destruction practices for records that have not been opened or viewed for an extended duration. • Determine data ownership of sensitive files identified in file storage systems, leveraging automated tools. Establish workflow options that allow data owners to provide input into access permission reviews of their sensitive files.
Web-based scanning	Configure DLP systems to crawl known public websites for sensitive information.	• Conduct a "spearing" exercise, which is similar to methods deployed by search engines. Compare files and results posted on websites against DLP matching policies and respond quickly to any sensitive data that are exposed. • Conduct manual searching activities on a periodic basis over exposed websites. Look for files that may contain large amounts of sensitive data (e.g., xls(x), csv, txt and pdf).

4.L.B	***Mapping Data Flows***	***NIST FRAMEWKORK REF:*** ID.AM-3, DE.AE-1

After data business practices are defined, it is advisable to describe these processes in a data map. Data maps should include the following components:

- Applications that house sensitive data
- Standard direction movement of data
- Users of applications and data
- Methods used to store and transmit data

Conducting this type of mapping, and potentially adding it to a larger enterprise architecture reference, enables an organization to identify data protection and monitoring requirements.

Threats Mitigated

1. Ransomware attacks
2. Loss or theft of equipment or data
3. Insider, accidental or intentional data loss

Suggested Metrics

- Number of encrypted e-mail messages, trended by week. The goal is to establish a baseline of encrypted messages sent. Be on the lookout for spikes of encryption (which could indicate data exfiltration) and no encryption (which could indicate that encryption is not working properly).
- Number of blocked e-mail messages, trended by week. The goal is to detect large numbers of blocked messages, which could indicate potential malicious data exfiltration or user training.
- Number of files with excessive access on the file systems, trended by week. The goal is to enact actions that limit access on the file storage systems to sensitive data, create tickets, and deliver to access management
- Number of unencrypted devices with access attempts, trended by week. The goal is to use this information to educate the workforce on the risks of removable media.

Cybersecurity Practice #5: IT Asset Management

Cybersecurity Practice 5: IT Asset Management		
Data that may be affected	Passwords, PHI	
Medium Sub-Practices	5.M.A 5.M.B 5.M.C 5.M.D	Inventory of Endpoints and Servers Procurement Secure Storage for Inactive Devices Decommissioning Assets
Large Sub-Practices	5.L.A 5.L.B	Automated Discovery and Maintenance Integration with Network Access Control
Key Mitigated Risks	• Ransomware Attacks • Loss of Theft of Equipment or Data • Insider, Accidental or Intentional Data Loss • Attacks Against Connected Medical Devices that May Affect Patient Safety	

The process by which organizations manage IT assets is generally referred to as *IT asset management* (ITAM). ITAM is critical to ensuring that proper cyber hygiene controls are in place across all assets in the organization. ITAM increases the visibility of cybersecurity professionals in the organization and reduces unknowns.

ITAM processes should be implemented for endpoints, servers, and networking equipment. The cybersecurity practices in this section assist and support every other cybersecurity practice identified in this publication. ITAM cybersecurity practices can be difficult to implement and sustain, but they should be incorporated into every lifecycle stage of IT operations to maintain data accuracy and integrity. For each asset, the lifecycle includes procurement, deployment, maintenance, and decommissioning. Though each type of asset is used differently during its lifecycle, the lifecycle itself is consistent.

The financial sector, as part of its public–private partnership with NIST National Cybersecurity Center of Excellence (NCCOE), has written a detailed ITAM practice guide: *IT Asset Management*.[22] Though specific to the financial sector, the methods discussed in the guide are easily applied to the HPH sector.

Sub-Practices for Medium-Sized Organizations

5.M.A	***Inventory of Endpoints and Servers***	***NIST FRAMEWKORK REF:*** ID.AM-1

The first ITAM component that should be implemented is a buildout of the inventory repository. This critical technology component provides a normalized, consistent approach that organizations can use to store inventory data.

Important data elements should be captured for each asset in the ITAM, including the following:

- AssetID (primary key)

22. Michael Stone et al., *IT Asset Management*, (NIST Special Publication 1800-5b, October 2015, Rockville, MD), https://nccoe.nist.gov/sites/default/files/library/sp1800/fs-itam-nist-sp1800-5b-draft.pdf.

- Hostname
- Purchase Order
- Operating System
- MAC Address
- IP Address
- Deployed to (User)
- Last Logged on User
- Purchase Date
- Cost
- Physical Location

A robust ITAM repository becomes your single source of truth for all IT assets in your organization. This repository will be maintained and trusted to be highly accurate and actionable.

Special consideration should be given to the differences between ITAM systems and device management systems. Device management systems, which connect to IT devices such as endpoints and servers, can automate the management and maintenance of these assets. They are highly effective at executing tasks such as software discovery, patch management, and performance monitoring. However, device management systems cannot account for the addition and removal of IT assets or answer the inevitable question, "Where did that laptop go?" They manage an organization's devices at a single point in time and are not workflow driven.

IT service management tools (e.g., ticketing systems) can be integrated with IT general controls to ensure accurate and precise asset management through standard performance management activities.[23]

5.M.B	***Procurement***	***NIST FRAMEWKORK REF:*** ID.AM

Once the ITAM system is implemented and configured, it is important to integrate normal supply chain processes with the ITAM processes. The goal is to leverage supply chain processes to proactively register each technology asset, endpoint, server, or networking equipment into the ITAM system as it is acquired.

To achieve this, IT organizations must work with supply chain departments to streamline technology acquisition channels. When technology acquisitions are specifically categorized, a trigger can be established to capture the details of each technology purchase. At a minimum, this involves generating a ticket in the IT ticketing system that prompts a designated IT professional to manually capture details

23. "CIS Control 1: Inventory and Control of Hardware Assets," Center for Information Security Controls, accessed September 24, 2018, https://www.cisecurity.org/controls/inventory-and-control-of-hardware-assets/.

for the new asset when it is acquired. New asset details can be captured physically, at a shipping dock, or virtually for virtual technology purchases.

In more advanced organizations, the procurement process may be automated to capture salient details for new assets. This reduces the manual labor required and the exposure to human error in collecting the data.

As an asset is acquired, it is critical to tag it with an asset tag. These tags can be physical or logical. The tagging process ensures that the asset has a unique ID that can be used to identify it in the ITAM system. Using existing data (e.g., hostname, IP address, MAC address) as the unique ID is not recommended, because these fields may change, potentially creating duplicate records.

5.M.C	***Secure Storage for Inactive Devices***	***NIST FRAMEWKORK REF:*** PR.AC-2

Assets that are not in circulation should be returned to the appropriate IT department for secure storage. Storage areas (e.g., lockers, cages, rooms) should be secured with physical access controls. Access should be limited to those who require it. Physical access controls may include badge readers, video camera surveillance, and door alarms.

If an asset is identified for redeployment, it should be securely imaged to deploy a "fresh" computer system for the new user. This ensures that old sensitive data are removed and that the asset has a clean bill of health.

When an asset is sent to storage for redeployment or processing, the ITAM system should be updated to reflect a change of ownership and new physical location (i.e., storage) for the asset. If the asset is redeployed or decommissioned, the ITAM system should be updated again to reflect its new status.

5.M.D	***Decommissioning Assets***	***NIST FRAMEWKORK REF:*** PR.IP-6, PR.DS-3

It is critical to properly dispose of retired assets, because these assets may contain sensitive information. When executing destruction and certification procedures, update the ITAM to indicate that the device has been decommissioned. This establishes a permanent record in your asset management source of truth, the ITAM. The following procedures should be completed when decommissioning an IT asset:

- *Central collection:* IT assets should be collected and stored in centralized, physically locked areas prior to decommissioning. Your workforce must be trained to turn in any asset that they no longer use.
- *Central destruction/wipe:* Assets that are collected for decommissioning must undergo a secure process to destroy or electronically wipe the storage media. This ensures that devices are properly sanitized before leaving the organization's possession for destruction/ Permanent removal of storage media may be completed by your IT organization or an external service provider. It is a good practice to obtain and archive a certificate of destruction for audit purposes.

Record keeping: Once the IT asset has been cleared for removal from the organization, the ITAM record of the asset information should be registered for destruction or decommissioning. Certificates of destruction can be stored in the ITAM record for easy access. It is highly advisable not to delete the asset record/ Instead, update the asset's status in the ITAM system to reflect that it has been

decommissioned and is no longer owned by the organization. You may need to refer to the asset record in the future.

Sub-Practices for Large Organizations

5.L.A	***Automated Discovery and Maintenance***	***NIST FRAMEWKORK REF:*** PR.MA-1, PR.MA-2, PR.DS-3

Once your ITAM system is in place and your procurement processes are registered, the challenge is to maintain these records. The following fictitious example describes a common IT asset in a large organization with the following characteristics:

- Number of endpoints: 10,000
- Number of servers: 1,000
- Number of data elements managed per asset: 11
- Total number of data elements required to maintain accurate details: 121,000

It is very difficult to manually maintain 121,000 data elements. After an asset is acquired, it is often deployed throughout its lifecycle in unforeseen ways. For example, a new laptop may be issued to a user. That user may leave the organization, turning in the laptop to a supervisor. The supervisor may assign the laptop to the new employee who fills the open position. Unless IT is informed and the ITAM is updated, the asset record for the laptop, now assigned to a different user, will be wrong.

Another classic example relates to an upgrade or hardware change to an existing asset. This asset might change operating system or patch levels. Maintaining that information manually in the ITAM is nearly impossible.

Automated discovery systems can maintain these records and account for both scenarios described above. In the case where an asset changes hands to a new user, discovery tools can register login occurrences for the “assigned user” and for the “actual logged in user.” If a threshold is triggered indicating that the assigned user no longer logs in and a different user continually logs in, a change-in-ownership process can be triggered. This process may be automated, requiring no intervention, or manually completed by generating a ticket to validate the change of ownership. In the case of OS and patching levels, automated discovery systems can provide snapshot views of current patching levels for assets. When these snapshots are compared by cybersecurity vulnerability management systems, vulnerabilities due to obsolete software versions will be identified across the fleet.

5.L.B	***Integration with Network Access Control***	***NIST FRAMEWKORK REF:*** PR.AC-4, PR.AC-5, PR.AC-6

The practices outlined so far assume normal acquisitions processes. There are times, however, when IT assets are integrated in the organization by means other than standard supply chain channels. Examples include personal devices (BYOD) and assets that are donated or provided free-of-charge as part of a third-party contract.

Without oversight, it is difficult to detect and track these assets. Outliers can be controlled by integrating your NAC and ITAM systems. Further details can be found in **Cybersecurity Practice #6: Network Management**.

Threats Mitigated

1. Ransomware attacks
2. Loss or theft of equipment or data
3. Insider, accidental or intentional data loss
4. Attacks against connected medical devices that may affect patient safety

Suggested Metrics

- Percentage of devices added to ITAM system through procurement channels, trended over time. The goal is to establish a baseline and achieve a higher percentage over time.
- Number of devices added to the ITAM because of NAC, trended over time. The goal is to analyze spikes that occur after initial deployment, which may indicate a problem capturing or maintaining asset records.
- Number of devices properly removed from asset management system using proper decommissioning channels, trended over time. The goal is to ensure devices are properly decommissioned. Lack of execution of these processes over a period may indicate a compliance issue.

Cybersecurity Practice #6: Network Management

Organizations leverage IT networks as a core infrastructure to conduct business operations. Without networks, there would be no interoperability. Networks must be deployed securely to limit exposure to and the potential impacts of cyberattacks.

Cybersecurity Practice 6: Network Management		
Data that may be affected	PHI	
Medium Sub-Practices	6.M.A	Network Profiles and Firewalls
	6.M.B	Network Segmentation
	6.M.C	Intrusion Prevention Systems
	6.M.D	Web Proxy Protection
	6.M.E	Physical Security of Network Devices
Large Sub-Practices	6.L.A	Additional Network Segmentation
	6.L.B	Command and Control Monitoring of Perimeter
	6.L.C	Anomalous Network Monitoring and Analytics
	6.L.D	Network Based Sandboxing/Malware Execution
	6.L.E	Network Access Control
Key Mitigated Risks	• Ransomware Attacks • Loss of Theft of Equipment or Data • Insider, Accidental or Intentional Data Loss • Attacks Against Connected Medical Devices that May Affect Patient Safety	

Sub-Practices for Medium-Sized Organizations

6.M.A	***Network Profiles and Firewalls***	***NIST FRAMEWKORK REF:*** PR.AC-5, PR.AC-6

An effective network management strategy includes the deployment of firewalls to enable proper access inside and outside of the organization. Firewall technology is far more advanced than standard router-based access lists and is a critical component of modern network management. Organizations should deploy firewall capabilities in the following areas: on wide area network (WAN) pipes to the internet and perimeter, across data centers, in building distribution switches, in front of partner WAN/VPN connections, and over wireless networks.

There should be clear boundaries that determine how traffic is permitted to move throughout the organization, including a default-deny ruleset whenever possible. At the perimeter, inbound and outbound rules must be configured with a default-deny ruleset to limit accidental network exposures. This often-complicated process can be achieved by establishing security zones through network segmentation.

Consider limiting the outbound connections permitted by assets in your organization. This can be a challenge to implement across the board. However, for zones of high sensitivity, egress limiting can prevent malicious callbacks or data exfiltration. The SOC should monitor egress logs.

Firewall rules may change when technology is added or removed. A robust change management process should include reviewing every firewall to identify necessary changes. These change requests

should comply with standard IT operations change management processes and be approved by cybersecurity departments before any firewall is modified.

As part of standard rule management for firewalls, it is important to periodically review firewalls to ensure they are properly structured as required by cybersecurity teams. Consider a monthly or quarterly review of the highest-risk rulesets.

6.M.B	***Network Segmentation***	***NIST FRAMEWKORK REF:*** PR.AC-5

Partitioning networks into security zones is a fundamental method of limiting cyberattacks. These zones can be based on sensitivity of assets within the network (e.g., clinical workstations, general user access, guest networks, medical device networks, building management systems, IoT networks) or standard perimeter segmentations (e.g., DMZ, middleware, application servers, database servers, vendor systems). Examples of standard network zones follow:

- *Perimeter defenses:* Most organizations host services that are accessed through the internet. A robust defense strategy should be deployed to monitor these "front doors."[24]

  Best practices for perimeter defenses include the following:

  - Implement highly restrictive rules on inbound and outbound ports and protocols. Use default-deny rules in firewalls and enable access only when clearly understood.
  - Restrict DMZ from middleware, application, and database servers. DMZ controls are critical, because these servers are exposed to the internet and have a large threat footprint.
  - Restrict the ability for DMZ servers to log in directly to servers on the inside network, specifically using remote desktop protocol, server message block, secure shell (SSH), or other remote access ports (tcp/3389, tcp/445, tcp/139, tcp/22).
  - Ensure that local administrator passwords are unique to each DMZ server and do not use these passwords for any other server in the organization.
  - Ensure that DMZ servers cannot connect directly to the internet. Instead, these servers should access the internet through outbound proxy services. Outbound proxy rules should limit the sites, URLs, IPs, and ports that a DMZ server can access to only whitelisted sites required for updates or application functionality. Be cautious of whitelisting hosting organizations like Amazon Web Services: malicious actors may use them to download malware to a compromised server.
  - Consider this type of restriction configuration for partner WAN links or site-to-site VPN connections. Do not permit access to systems/applications that are not required by the user.

24. *CIS Control 12: Boundary Defense*. (2018). Retrieved from Center for Information Security Controls: https://www.cisecurity.org/controls/boundary-defense/

- *Data center networks:* Servers in the data center should be segmented into appropriate zones. Several different layers of segmentation may occur within data center networks, including
    - database servers;
    - application servers; and
    - middleware.
- *Critical IoT asset*s: It is important to restrict access to assets that have a potentially high impact on the business or patients if compromised. Management and patching of security vulnerabilities in IoT devices is often limited. Examples include medical devices, security cameras, badge readers, temperature sensors, and building management systems. These assets generally exist outside of the data centers. Without proper segmentation, they may infiltrate general access networks. To achieve segmentation in the physical buildings, leverage multiprotocol label switching to build out virtual networks and place these network access restrictions behind core firewalls.
- *Vendor access:* Vendor access should be limited based on need. It should be temporary, and only access to required information should be granted. Some assets are managed exclusively or accessed by third-party vendors. These vendors may need continual access to the organization's network. It is important to segment this vendor access from other networks and limit the vendor's ability to access other parts of your corporate network. Whether these networks exist inside or outside of the data center, the principles are the same. In 2015, Target was the victim of a cyberattack leveraging these exact channels.[25] Common examples include building management systems, security systems, physical access controls, and persistent tunnels required to enable cloud functionality.
- *General access networks:* The majority of your workforce will operate on general access networks. These are "edge" networks that provide connectivity back to the services offered in data centers, the internet, or other assets. General access networks require a sense of openness when communicating with services that are hosted by the organization. However, restrictions should be implemented that prohibit the assets in one general access network from communicating with the assets in another general access network. This critical control that can help stop the outbreak and spread of malware and ransomware attacks.
- *Guest networks:* It is common for organizations to provide guest access to the internet, especially in provider organizations visited by patients and their friends and families. Access to the internet is a core value of provider organizations. However, it must be restricted and controlled appropriately. These restrictions should exist on wireless networks, where it is most common, as well as wired networks often located in public spaces or conference rooms. Explicitly prohibit access to the internal network; guest users should access the organization

25. *Anatomy of the Target data breach: Missed opportunities and lessons learned*. (2015, Feb 2). Retrieved from ZDNet: http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

using the same front door through which they access the rest of the internet. Lastly, as much as possible, limit the ability of your workforce to access guest networks.

6.M.C	Intrusion Prevention Systems	NIST FRAMEWKORK REF: DE.CM-1

An intrusion prevention system (IPS) is important for your network perimeter, data center, and partner connections. An IPS is capable of reading network traffic to detect and potentially prevent known attacks.

Today, these signature-based systems are not as prevalent as they once were, owing to limited effectiveness. However, they still serve as vital input to an organization's SOC providing context to the types of attacks that occur. Though they might not identify every single attack, they provide information enabling your IR team to conduct forensic activities.

6.M.D	Web Proxy Protection	NIST FRAMEWKORK REF: PR.AC-3, PR.AC-5

Web proxy systems provide important protections against modern phishing and malware attacks. These systems are implemented at the perimeter of the network or in the cloud to provide protections for your mobile workforce. Because most phishing and malware attacks are web-based, web proxy systems provide users with friendly error pages explaining that the user has been restricted from accessing a known malicious website. Such pages also provide informative feedback for users. When configured properly, web proxy systems leverage the following methods to limit client-side attacks:

- *Reputation blocking:* Many blackhole lists are available publicly or through ISACs and ISAOs; proxies can use such lists to prevent users from accessing malicious websites. The lists are usually integrated into proxy systems through automated feeds.
- *Organizational block lists:* As part of an organization's IR, malicious websites and other sites can be identified based on actual attacks against the organization. Web proxy systems are critical shut-off points to limit access to websites quickly.
- *Category blocking:* Most modern, commercial web proxy technologies will pre-categorize websites on behalf of the organization. Considering the millions of websites that exist, this is a highly useful service. Consider blocking categories that contain malicious, suspicious, or illegal websites.

6.M.E	Physical Security of Network Devices	NIST FRAMEWKORK REF: PR.AC-2

Network devices are deployed throughout an organization's facilities. Inside the general user space, physical data closets that contain network devices must be secured. Additionally, it is useful to limit network ports on switches. Consider the following controls:

- Data and network closets should always be locked. Consider using badge readers instead of traditional key locks to monitor access.
- Disable network ports that are not in use. Ensure that procedures are in place to maintain ports in shutdown mode until an activation request is submitted and approved.

- Establish guest networks in conference rooms that are configured to access only these networks.

Sub-Practices for Large Organizations

This section includes methods to detect and potentially prevent cyberattacks against an organization's network. These methods should be engineered into network management practices. Once network-level detection and prevention methods are established, cybersecurity departments can follow **Cybersecurity Practice #8: Security Operations Center and Incident Response** to monitor and respond to attacks on the network.

6.L.A	***Additional Network Segmentation***	***NIST FRAMEWKORK REF:*** PR.AC-5, PR.AC-6, PR.PT-4

As your network expands, other strategies can be deployed to maintain secure segmentation. Consider the following:

- *Required VPN access for data center:* Consider implementing a VPN, or bastion hosts, that must be enabled before access is granted to privileged servers in the data center. These VPN or bastion hosts should be equipped with MFA. Only authorized IT administrators should be granted access. Logs should be routed to the SOC for monitoring.

6.L.B	***Command and Control Monitoring of Perimeter***	***NIST FRAMEWKORK REF:*** DE.CM-1, DE.CM-7

Hackers commonly use layered command and control (C2) traffic to maintain access to compromised computers. C2 traffic consists of beacons, typically outbound from the computer, that check back in to a central server. Identifying such traffic can help detect where an attacker has maintained persistence. There are many methods to look for C2 traffic, including the following:

- *Direct to compromised server via Internet Protocol (IP) or Internet Control Message Protocol (ICMP):* In this method, traffic runs over the network using outbound ports or protocols that are generally open (e.g., HTTP, HTTPS, or ICMP protocols). C2 traffic can be in encrypted or cleartext forms, depending on the attacker's level of sophistication. The attacker must have compromised a series of servers or other assets This method tends to be less effective for hackers than others, because it is easy to shut down offending systems once the compromise has been detected. When a shutdown occurs, the attacker loses persistence control.
- *DNS queries:* In this method, the attacker establishes control using a DNS query embedded in malware that is downloaded to a computer. As long as the DNS record is maintained, the servers that maintain C2 communications can switch out and flex as they are discovered. This method is also fairly easy to detect and resolve. When the DNS name has been identified, the organization can implement a DNS sinkhole. The sinkhole can be an entry on the local cache in the organization's DNS resolvers to remove a nonexistent IP address, such as 127.0.0.1. Once the fully qualified domain name is identified, these DNS registrations can be taken down through abuse reporting to DNS hosting services.
- *Fast flux DNS queries:* In this method, the hacker leverages DNS to maintain persistence, knowing that the DNS registrations will likely be taken down at some point. When this occurs, malware downloaded to the local client and C2 services runs an algorithm that checks the first

several bytes of well-known sites (e.g., cnn.com, nbc.com) to create and register fake DNS names on the organization's DNS resolvers. These domains tend to live for 24 hours or less. Using the same algorithm, the clients switch to the next domain until command is reestablished. Fast flux methods are fairly successful. Defending against fast flux DNS queries requires analytics that relate to local DNS lookups and can discover "gibberish" domain names. "Oiewr921ai/evil/com" is an example of a gibberish domain name.

6.L.C	***Anomalous Network Monitoring and Analytics***	***NIST FRAMEWKORK REF:*** DE.CM-1, DE.CM-7

A variation on C2 monitoring is to analyze network traffic, rather than focus on a particular vector or attack style. This requires specialized tools that can profile inbound and outbound network traffic. Some versions of these tools provide "deep inspection," which allows the full contents of a packet to be analyzed, categorized, and built into massive databases of network-based metadata.

Once metadata on the network traffic profile are gathered, analytics can be conducted to look for outliers, anomalous traffic, and other highly sophisticated methods of discovery. Network monitoring tools are not preventative in nature. Rather, they are intended to widely increase the SOC's visibility, facilitating detection, confirmation, or validation of suspicious actions. These tools are especially useful in replaying events that occurred as part of an attack to support network forensic activities.

6.L.D	***Network Based Sandboxing / Malware Execution***	***NIST FRAMEWKORK REF:*** (DE.CM-5 / DE.CM-7)

By monitoring common protocols that allow downloading of binaries and files, organizations can check a download prior to permitting it to run on the organization's devices. Downloaded binaries, executables, or even data files (e.g., docx, xlsx) are run in a virtual environment that looks for malicious activities when the file executes.

Common methods include

- watching what registry keys are queries, amended, added, or deleted;
- monitoring for outbound network connections;
- launching processes in memory; and
- conducting anomalous system calls.

Tools that facilitate automated sandboxing look for suspicious outputs or actions rather than attempting to base actions on a particular signature of a particular configuration.

To be effective, these technologies monitor network flows. This can occur passively or actively. Passive systems monitor network traffic at the stream level, not residing in line with the communication flows. Active systems insert themselves inline to the communication flows and conduct checks on the fly, denying access to downloaded files until they are cleared.

Sandboxing systems provide protection against malicious files. However, they do not provide protection against active attacks inside your network.

6.L.E	Network Access Control	NIST FRAMEWKORK REF: PR.AC-5, PR.AC-6, PR.AC-4

NAC systems are engineered to automatically profile new IT assets that connect to network resources, such as wireless networks, wired networks, or VPN. They help ensure that the controls discussed in **Cybersecurity Practice #2: Endpoint Protection** are in place on each asset. NAC systems execute these controls in real time when the asset connects to the network.

NAC systems are highly effective at discovering personal devices leveraged on the network (BYOD). They can be configured to permit authorized BYOD devices to access the network or prohibit them entirely.

When basic NAC controls are implemented and you can monitor the security of endpoints that connect to your network, there are other interesting, advanced techniques that can be leveraged to provide checks and balances for general IT controls.

One example is to integrate your NAC solution with your ITAM repository. As discussed in **Cybersecurity Practice #5: IT Asset Management***,* ITAM repositories should be populated using your organization's standard procurement processes. That said, not all processes run perfectly, and there are other ways that assets are integrated into an organization's environment, often due to human error or sidebar procurement channels that are not leveraged consistently.

Configuring your NAC solution to check against your ITAM enables assets to be profiled spontaneously, providing self-directed work streams to users. Such a configuration can be achieved as follows:

- Set up application programming interfaces between the NAC solution and the ITAM solution that enable read and write options.
- Query the ITAM database when an asset connects to the network. If the asset does not exist, present the user with a splash page.
- Determine whether the asset is organizationally owned (purchased with organizational funds) or personally owned (purchased by the user).
- Register the selection, conduct the NAC security scan, and publish the results in the ITAM.
- Execute IT general controls that reconcile assets that are out of compliance with standard asset management procedures. Such controls can include
    - ensuring that appropriate monitoring controls are in place;
    - registering the asset with the right identifiers (asset IDs); and
    - updating asset ownership based on actual human interaction.

These mechanisms are effective at providing visibility to the devices being used on the network, increasing the IT! M system's accuracy and consistency/

Threats Mitigated

1. Ransomware attacks
2. Loss or theft of equipment or data
3. Insider, accidental or intentional loss of sensitive data

4. Attacks against connected medical devices that may affect patient safety

Suggested Metrics

- Number of assets on the network that have not been categorized, trended over time. The goal is to establish a process to register and understand all assets on the network. After the baseline is complete, minimize the number of uncategorized assets.
- Number of organizationally owned assets discovered using NAC that were not previously categorized through asset management procedures, trended by month. The goal is to monitor this lagging metric that measures effectiveness of the supply chain and IT operations processes. Increases in the number of organizationally owned assets that were not previously categorized indicates that standard processes are not being executed properly. Implement continuous improvement processes for IT operations.
- Percentage of assets that comply with security policies, trended by week. The goal is to establish a baseline, then set stepwise goals to improve compliance over time. Ultimately, compliance percentage should range from 95 to 99 percent.
- Number of malicious files captured and secured with advanced networking tools (sandboxing), trended by week. The goal is to capture all malicious files. An extended trend of no detected malicious files may indicate that sandboxing solutions are not working.
- Number of malicious C2 connections discovered and removed, trended by week. The goal is a weekly report showing that all detected C2 connections are mitigated successfully.
- Number of approved servers/hosts in the DMZ compared to hosts in the DMZ, trended by week. The goal is zero servers/hosts in the DMZ that are not understood. IT operations practices should be reviewed if servers are added that were not previously authorized.

Cybersecurity Practice #7: Vulnerability Management

Cybersecurity Practice 7: Vulnerability Management		
Data that may be affected	PHI	
Medium Sub-Practices	7.M.A 7.M.B 7.M.C 7.M.D	Host/Server Based Scanning Web Application Scanning System Placement and Data Classification Patch Management, Configuration Management & Change Management
Large Sub-Practices	7.L.A 7.L.B	Penetration Testing Remediation Planning
Key Mitigated Risks	• Ransomware Attacks • Insider, Accidental or Intentional Data Loss • Attacks Against Connected Medical Devices that May Affect Patient Safety	

Organizations use vulnerability management to proactively discover vulnerabilities. These processes enable the organization to classify, evaluate, prioritize, remediate, and mitigate the technical vulnerability footprint from the perspective of an attacker. The ability to mitigate vulnerabilities before a hacker discovers them gives the organization a competitive edge and time to address these vulnerabilities in a prioritized fashion.[26]

There are multiple types of vulnerability scanning. The most well-known methods are scans against servers (or hosts) and against web applications. These two scan types focus on different considerations.

Sub-Practices for Medium-Sized Organizations

7.M.A	*Host/Server-Based Scanning*	*NIST FRAMEWKORK REF:* DE.CM-8

In this model, vulnerability scanners are leveraged to identify weaknesses in OS or third-party applications that reside on a server. There are two scan options: unauthenticated and authenticated.

In the unauthenticated model, the scanner has no extra sets of server privileges and queries the server based on ports that are active and present for network connectivity. Depending on the level of sophistication of the software scanner, each server is queried and checked for vulnerabilities. Scan results provide the perspective of an attacker who lacks server access. Vulnerabilities that rate high in this space should be mitigated first, as they are the most likely points at which a hacker could enter the server.

Authenticated scans are conducted by letting the vulnerability scanner log in to the server and query all running software with all running versions. The resulting vulnerability lists are usually compared against a database (maintained by the scanner's vendor), and vulnerabilities are enumerated based on the

26. "CIS Control 3: Continous Vulnerability Management," Center for Information Security Controls, accessed September 24, 2018, https://www.cisecurity.org/controls/continuous-vulnerability-management/.

known software version's disclosed issues. While this type of scanning provides a much higher degree of accuracy in enumerating vulnerabilities, it does not necessarily provide context that describes how the vulnerabilities might be exploited. An advantage of this type of scan is that it will identify client-side vulnerabilities that exist on the server and that may otherwise be difficult to discover, such as vulnerable versions of Java.

Most scanning systems can categorize vulnerabilities against the MITRE Common Vulnerability Scoring System (CVSS). The CVSS system helps organizations prioritize identified vulnerabilities, which enables development of a prioritized response. Version 3 of the system considers the following three factors: base score, temporal score, and environmental score. These factors, along with their sub-factors, are used to calculate vulnerabilities on a scale ranging from 1 to 10. For more information, refer to the CVSS Specification Document, available online.[27]

7.M.B	***Web Application Scanning***	***NIST FRAMEWKORK REF:*** DE.CM-8

In this model, specialized vulnerability scanners interrogate a running web application to check for vulnerabilities in the application design. Most web applications run dynamic code, run atop a web server, interact with middleware, and connect to databases. If the web application is not coded securely, this architecture may enable unanticipated access to data or systems.

Common web application attack types include Structured Query Language injection, cross-site scripting, and security misconfigurations. In these cases, attackers can

- bypass web application security controls and pull data directly from the database;
- steal an already authenticated cookie on a vulnerable website to get access; or
- exploit misconfigurations that can permit properly formatted commands or scripts to execute privileged content on the webserver itself.

More information can be found on the Open Web ! pplication Security Project's Top 10 website.[28]

In all cases, vulnerabilities to web applications with sensitive information represent a high risk to the organization. It is important to understand these vulnerabilities to conduct appropriate and prioritized remediation.

7.M.C	***System Placement and Data Classification***	***NIST FRAMEWKORK REF:*** ID.RA-5

Organizations should apply **Cybersecurity Practice #4: Data Protection and Loss Prevention** and **Cybersecurity Practice #5: IT Asset Management** to understand IT assets and asset classifications. These cybersecurity practices answer the question, "How bad would it be if this asset were breached?"

---

27. "Common Vulnerability Scoring System v3.0: Specification Document," FIRST, accessed September 24, 2018, https://www.first.org/cvss/specification-document.

28. *OWASP Top 10 - 2017: Ten Most Critical Web Application Security Risks*, OWASP, 2017, https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.

It is important to understand the exposure of each system in your environment. Organizations should apply **Cybersecurity Practice #6: Network Management** to determine the likelihood that each this system can be compromised.

The level of risk related to vulnerabilities in your systems is directly related to the exposure of these systems and the types of data they contain.

7.M.D	***Patch Management, Configuration Management, & Change Management***	***NIST FRAMEWKORK REF:*** PR.IP-1, PR.IP-3, PR.IP-12

All organizations should have a routine to patch security flaws in their servers, applications (including web applications), and third-party software. Although the patching process may vary, large organizations should use centralized systems to interrogate servers and determine which software updates should be implemented.

At least monthly, organizations should implement patches that are produced by the vendor community. IT operations should collect these patches, conduct appropriate regression tests to ensure that patches do not negatively impact the business, and schedule patch implementation during routine change windows. This process should be executed and measured using standard IT operations activities.

Not all vulnerabilities are created equal. Some are easier to exploit than others. The National Vulnerability Database (NVD) has produced the CVSS, a standard measurement across all industries that normalizes and ranks the severity of a vulnerability.[29]

The more a vulnerability is exposed, the higher priority an organization will generally assign to mitigate it. Exposure may be a more critical variable than the potential impact to an asset, considering that hackers attempt to gain a foothold on organizational assets before conducting additional internal attacks. Another factor to consider is the level of active exploitability in the wild. A less-critical vulnerability may have an active threat against it. In such a case, an organization might want to consider proactively executing IR processes, organizing the response team, and quickly patching systems. The WannaCry exploit of 2017 was a classic example of organizations identifying an active threat and quickly implementing patches that were previously neglected[30].

If your systems are running end-of-life OS or software, associated vulnerabilities should be identified and steps taken to bring these systems back to a supported state. This may include decommissioning systems that run on unsupported OS, which may require additional investments. Once systems are unsupported, it is usually impossible to apply security patches, potentially increasing the organization's risk posture.

Table 8 provides general guidelines for planning remediation efforts based on criticalities.

29. "CVSS," NIST National Vulnerability Database, accessed September 24, 2018, https://nvd.nist.gov/vuln-metrics/cvss.

30. "Report. The IT Response to WannaCry," accessed September30, 2018, https://www.techrepublic.com/article/report-the-it-response-to-wannacry/.

Table 8. Recommended Timeframes for Mitigating IT Vulnerabilities

Vulnerability Criticality	Days to Mitigate in DMZ	Days to Mitigate in Data Center
Critical	< 14 days	< 30 days
High	< 30 days	< 90 days
Medium	< 90 day	< 180 days
Low	< 180 days	At your discretion

The vulnerability scanning process is a quality check on the effectiveness of an organization's patch management practice, otherwise referred to as a *lagging metric*. Organizations with a robust patch management practice are better positioned to mitigate residual vulnerabilities.

In addition to conducting routine patch management activities, organizations should ensure that proper security configuration management activities are in place. Common vulnerabilities can be introduced in systems with insecure configurations. Examples of insecure configurations include permitting a file transfer protocol (FTP) server to allow anonymous login, making that login credential accessible to the internet, or failing to change default account passwords on applications. Organizations that follow **Cybersecurity Practice #2: Endpoint Protection Systems** and expand those practices to their servers will be positioned to minimize these issues.

Lastly, consideration needs to be given to changes made to systems, servers, and networks, along with the vulnerabilities that may be exposed as a result. A testing plan should be part of the change management process. It should include a vulnerability scan of new network connectivity (such as a firewall change) or a new system function or service. This scan should be conducted during the test phase of the change process, before the change is implemented into the production environment. Such a process enables the identification and mitigation of security exposures.

Sub-Practices for Large Organizations

7.L.A	***Penetration Testing***	***NIST FRAMEWKORK REF:*** ID.RA-1, PR.IP-12, DE.CM-8, RS.AN-5

In addition to vulnerability scanning, it is also important to consider conducting penetration tests. These types of tests are sometimes called *red teaming*; the goal is to actively exploit your own environment before malicious actors do.

Penetration tests involve more than simply conducting vulnerability scans and attempting to exploit the findings. A proper penetration test should mimic the same attack methodologies that are deployed by

the adversaries. Per SANS Critical Control #20, penetration testing involves mimicking the actions of computer attackers to identify vulnerabilities in a target organization, and exploiting them to determine what kind of access an attacker can gain. Penetration tests typically provide a deeper analysis of security flaws than a vulnerability assessment.[31]

Penetration tests should blend client-based, internet-based, web application–based, and wireless-based attacks. When selecting a testing method, consider the types of attacks that might occur most frequently against your organization. With these scenarios, you can test the resiliency of your cybersecurity program.

Penetration tests can be run internally by qualified individuals, or they can be run by external partners. No matter who will conduct the test, proper authority to perform the test must be documented, clearly defining the scope of the assets that may be tested, the methods that may be deployed, and the timing for conducting the tests. Assets and methods not permitted should be clearly articulated. This documentation is especially important if internal staff will conduct the test, and documentation may be necessary to comply with legal and HR obligations.

Multiple variations of penetration tests that can be conducted. Outlined in Table 9 are a few options for consideration. Review each of the factors in the table below and select what works best for your organization.

Table 9. Factors for Consideration in Penetration Test Planning

Factor	Options	Description
Type	1. *White box:* Tester is permitted to know all aspects of the target 2. *Grey box:* Tester is permitted to know some aspects of the target 3. *Black box:* Tester is not permitted to know any details of the target	Depending on the type of test you want to conduct, it might be useful for the tester to already know some details of the target or organization. Such knowledge might reduce the effort of common reconnaissance activities, such as finding e-mail addresses for phishing targets or discovering all vulnerabilities on externally facing servers.

31. "CIS Control 20. Penetration Tests and Red Team Exercises," Center for Internet Security, accessed September 24, 2018, https://www.cisecurity.org/controls/penetration-tests-and-red-team-exercises/.

Factor	Options	Description
Resources	1. *External expert:* A subject matter expert (SME) who specializes in the specific methodologies you wish to deploy 2. *Internal expert:* A SME on an internal team who has context to the environment	Either type of resource can be useful. The benefit of using internal staff is that they understand the technical nuances of your environment. However, in some cases, targeted tests requiring specialized skillsets might be desired. External experts are useful in these cases, or when internal resources are committed to other activities.
Methods	1. *Social engineering:* Attacks geared towards "tricking the human" 2. *Web application:* Attacks centered on attacking web application infrastructure 3. *Host based:* Attacks centered on attacking host infrastructure, inclusive of servers, or endpoints 4. *Client based:* Attacks centered on attacking the client, such as laptops or desktops (usually bypassing perimeter protections) 5. *Network based:* Attacks against the network infrastructure itself, such as physical connections or wireless attacks 6. *Privileged escalation:* Once a foothold has been made, conducting secondary attacks to further escalate privileges for more lateral movement	Many methods exist; those listed here are common. These methods can be combined, based on the type of attack you are looking to carry out. For example, if you want to see whether it is possible for an external attacker to gain access to your EMR, you might use social engineering, client-based, and privileged-escalation attacks. The goal of each of these attacks is to discover a user with sensitive EMR access, compromise the user's credentials, and get remote access to the environment to be able to log in to the EMR with those credentials.

Factor	Options	Description
Targets	1. *Data:* Discover and exfiltrate sensitive data to test data security controls 2. *IT assets:* Compromise IT assets, such as servers or endpoints, to test system security controls 3. *People:* Compromise individuals to test educational controls 4. *Medical technologies:* Determine how vulnerable the organization is to attacks against medical devices 5. *Infrastructure:* Determine how vulnerable the organization is to digital extortion attacks, such as ransomware outbreaks	Each test conducted should have different targets and goals in mind. In some cases, you might want to test how susceptible your user population is to phishing attacks- in that case, you will set "People" as the target. In other cases, you might want to understand how vulnerable your organization is to a ransomware attacks; in that case, you might select "IT !ss ets" and "Infrastructure" as your targets/

7.L.B	***Remediation Planning***	***NIST FRAMEWKORK REF:*** PR.IP-12

It is important to classify and prioritize vulnerabilities that remain after completion of standard patch management practices. Typically, these remaining vulnerabilities are issues that cannot be mitigated with a patch. They may require system configuration changes, code updates, or perhaps even a full-blown version upgrade. The process of resolving these vulnerabilities tends to be more time-consuming and complex.

Like risk management activities, remediation efforts should be prioritized to resolve identified vulnerabilities. The most common practice is to first patch identified vulnerabilities and then rescan the system to validate that those vulnerabilities are closed. Most vulnerability scanning systems can track the opening, closure, and reopening of vulnerabilities over time. It is highly encouraged to track these metrics.

Mitigation of some vulnerabilities requires far more effort than a simple patch. In these cases, it is best to develop structured remediation plans that include the following elements:

- *Remediation owner:* The single individual accountable for ensuring that the vulnerabilities are addressed. It is important to assign remediation plans to a single owner, otherwise they are likely to stall due to lack of leadership.
- *Plan:* A full description of the remediation plan to be completed. The remediation plan owner and the information security office should develop this plan. Once the plan is approved, execution tasks can be started.

- *Stakeholders:* The individuals responsible for completing tasks in the remediation plan, or organizing other individuals who will complete tasks. Stakeholders may include individuals who need to be informed of remediation activities as well as those who complete the work.
- *Dates:* Major milestone dates and remediation plan due dates must be captured on the remediation plan. The remediation plan owner must commit to these dates.
- *Status:* Periodically, the plan should be updated to remain current. Updating generally occurs between once per week and once per month. The remediation plan owner may be accountable for providing status updates.

After a remediation plan is completed, the organization's information security office should implement a monitoring process. This monitoring process may include all remediation plans in progress and current activities. The security office may provide support to activities that are behind schedule. Consider engaging in such a monitoring process once per week to maintain momentum.

Threats Mitigated

1. Ransomware attacks
2. Insider, accidental or intentional data loss
3. Attacks against connected medical devices that may affect patient safety

Suggested Metrics

- Stacked aggregate of vulnerabilities in DMZ trended by month, with vulnerabilities categorized using CVSS categories (Critical, High, Medium, Low, None) and plotted as a simple stacked bar. The goal is to mitigate the most severe vulnerabilities first, through patching and configuration management. Of the remaining vulnerabilities, the most critical should be mitigated within 30 days. The total number of vulnerabilities should be reduced over time.
- Stacked aggregate of vulnerabilities in data center trended by month, with vulnerabilities categorized using CVSS scores and plotted as a simple stacked bar. The goal is to mitigate the most severe vulnerabilities first, through patching and configuration management. The total number of vulnerabilities should be reduced over time.
- Number of unmitigated new vulnerabilities introduced into the environment trended by week. The goal is to keep the number of new vulnerabilities as low as possible, defined by your organization's level of risk tolerance.

Cybersecurity Practice #8: Security Operations Center and Incident Response

Cybersecurity Practice 8: Security Operations Center and Incident Response	
Data that may be affected	PHI
Medium Sub-Practices	8.M.A Security Operations Center 8.M.B Incident Response 8.M.C Information Sharing and ISACs/ISAOs
Large Sub-Practices	8.L.A Advanced Security Operations Center 8.L.B Advanced Information Sharing 8.L.C Incident Response Orchestration 8.L.D Baseline Network Traffic 8.L.E User Behavior Analytics 8.L.F Deception Technologies
Key Mitigated Risks	• Phishing Attacks • Ransomware Attacks • Loss or Theft of Equipment • Insider, Accidental or Intentional Data Loss • Attacks Against Connected Medical Devices that May Affect Patient Safety

Most cybersecurity programs begin by implementing controls designed to prevent cyberattacks against an organization's IT infrastructure and data. This is a good place to start and there is a lot of value in basic cyber hygiene, implementing the cybersecurity practices that are discussed in this volume. However, in the modern age of cyber threats, not all attacks can be prevented with these basic controls. It is equally important to invest in and develop capabilities to detect successful attacks and respond quickly to mitigate the effects of these attacks.

A good example is the threat of phishing attacks. Even if organizations followed every practice discussed in **Cybersecurity Practice #1: E-mail Protection**, they would still be susceptible to phishing attacks. It is therefore important to detect, in near real time, phishing attacks that successfully infiltrate your environment and to neutralize their effects before widespread theft of credentials or malware installation occurs. This is a classic example of what it means to shore up your detection capabilities (detecting the phishing attack that gets past your basic controls) and response capabilities (neutralizing the effects before serious damage to the organization occurs).

Maintaining detection and response capabilities requires establishing an IR program and an SOC to manage the IR, along with security engineering that enhances an organization's ability to detect and respond to cyberattacks.

Sub-Practices for Medium-Sized Organizations

8.M.A	***Security Operations Center***	***NIST FRAMEWKORK REF:*** RS.RP

An SOC is an organizational structure that leverages cybersecurity frameworks, people, tools, and processes to provide dedicated cybersecurity operations. SOCs are the areas within an organization that dedicate 100 percent of their time to cybersecurity prevention, detection, or response capabilities, providing the execution arm of cybersecurity IR.

An SOC is generally segmented into four main functions, depending on the organization's level of maturity. These functions are as follows:

- *Engineering:* The process of building new cybersecurity capabilities into the existing toolsets in an environment. Examples include building new alerts within a security incident and event management (SIEM) system, establishing new log sources for log management systems, establishing new analytics patterns for detection, or simply implementing new cybersecurity systems to add capabilities into the environment.
- *Operations:* The process of managing and maintaining the cybersecurity tools within the SOC. This is sometimes referred to as *keeping the lights on*. Keeping the lights on generally means monitoring critical cybersecurity systems to ensure that they operate at agreed-upon performance levels.

Threat intelligence: A specific function that focuses entirely on how to discover cybersecurity threats that may be relevant to the organization, along with the means and methods these threats may use to infiltrate the organization. This function focuses on the threat actors themselves, the tools they leverage, and the digital signatures they leave in the process of conducting their activities. Once these digital footprints, sometimes called indicators of compromise (IOCs) are established, engineering teams can use integrate IOC patterns into cybersecurity systems and establish IR plays to execute when the IOCs are activated.

Incident response: the process of conducting a structured and consistent response to any IR plays that have been created. The goal of this function is to

  - validate an IR process that has been triggered;
  - contain any successful cybersecurity attacks to the organization;
  - eliminate the threat from the environment;
  - recover systems or data that might have been affected by the attack; and
  - ensure that any attack vectors that were exploited are well understood and fed back to the security engineering teams for future prevention or enhanced detection capabilities, further minimizing the impacts of those vectors.

It is critical to create a continuous feedback loop between your IR and engineering teams so the organization continues to learn and grow based on the actual success of threats and threat actors.

As SOCs are developed, a core concept is to ensure that IR teams and handlers apply consistent methods to execute response practices. SOCs and IR teams should establish playbooks, also known as *runbooks*, that describe existing detection mechanisms and the procedures to be followed if the mechanisms are triggered. For each detection, the triggered process may be referred to as a *play*, like plays that football teams maintain in their playbooks.

Examples of plays that might be found in an IR playbook are provided in Table 10. The table provides high-level play details, including what the play seeks to accomplish and the types of source data that must be collected to successfully detect it. The list below will not

discuss specific technical log event data required. Information on how to configure this information can be found in multiple publications.[32,33]

Table 10. Example Incident Response Plays for IR Playbooks

Play Category	Play	Description	Source Data
Reconnaissance	Vulnerability scanning sweep of DMZ	Large numbers of vulnerabilities are scanned across the DMZ spectrum. Could involve scanning a single server over multiple ports or scanning multiple servers on a single port.	• Server list in DMZ • Intrusion detection system (IDS) or intrusion prevention system (IPS) logs configured to detect vulnerability scanning • Firewall logs • Netflow data
Reconnaissance	Vulnerability scan from known malicious IPs	Vulnerability scans of the DMZ or other servers/endpoints exposed to the internet over channels that are shared and known to be malicious (IOC).	• IOC list from threat-sharing sources (e.g., ISACs) • IDS/IPS logs • Firewall logs • Netflow data
Reconnaissance	Successful access from known malicious IPs	Successful authentications from known malicious IP addresses. Authentications through standard remote access channels, such as VPNs, virtual terminals, jump boxes, or other mechanisms.	• Authentication logs • Firewall logs • IOC list from threat-sharing sources (e.g., ISACs)

32. David Swift, *Successful SIEM and Log Management Strategies for Audit and Compliance,* The SANS Institute, 2010, https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528.

33. Peter Czanik and BalaBit, "The 6 Categories of Critical Log Information," S!NS Technology Security Laboratory, last modified 2013, accessed February 4, 2018, https://www.sans.edu/cyber-research/security-laboratory/article/sixtoplogcategories.

Play Category	Play	Description	Source Data
Reconnaissance	Internal attacks from third-party VPNs	Detection of attacks coming through partnering third-party VPN connections, such as organizations that provide building automation	• Firewall logs (from segmented networks) • IDS/IPS logs • Authentication log
Exploitation	Phishing attacks successfully delivered to users	Detection of phishing attacks by IT systems, or users reporting phishing attacks. Contain the issue by blocking URLs provided, proactively resetting passwords for users that clicked, and conducting AV scans against endpoints where malicious attachments were opened.	• E-mail protection systems • Firewall logs • Web proxy logs • Endpoint AV management logs
Exploitation	Successful ransomware attack	Detection of ransomware attacks that occur inside the organization. These may be small outbreaks or larger issues. Consider 1) Setting up detection alerts for indicators of known ransomware (AV, threat feeds, etc.) 2) Setting up detection alerts for symptoms of ransomware attacks (such as large IOPs on file systems, encryption of large amounts of files, user experience issues) 3) Determining severity; lower severity issues can be dealt with operationally; high severity issues should instantiate the CIRT 4) Containing and responding accordingly 5) Recovering through backups *(do not simply clean a system with an AV scanner, but rather rebuild and reimage)*	• File system logs • Endpoint AV management logs • Firewall logs • Web proxy logs • Threat feeds • E-mail security logs

Play Category	Play	Description	Source Data
Persistence	Creation of local user accounts on static systems	Detection of a local user account being created on an asset, such as a Windows *nix server, where local user account creations normally do not occur. This may indicate malicious activity.	• Logs from local servers
Persistence	After exploit persistence hold	Detection of malicious users attempting to maintain permanent access. Look for launch or changing of scheduled tasks, script downloads, and new process creation.	• Critical server lists • Known process baselines • Logs from server task or scheduled job management • URL filtering logs by server
Privilege Escalation	Privileged account brute force success	Large number of invalid login attempts followed by a successful login to a known privileged account.	• Privileged account list • Authentication logs (e.g., active directory, servers)
Privilege Escalation	Default account password guessing	Large number of invalid login attempts followed by a successful login to a known default user account.	• Default account list • Authentication logs (e.g., active directory, servers)
Privilege Escalation	Interactive login to service accounts	Detection of a service account being used as an interactive login (a user logging in to a terminal session). Service accounts should only be used for applications or services.	• Service account list • Authentication logs (active directory, servers)
Data Exfiltration	Data transfer	Detection of data transfers occurring outside of the organization from servers that normally do not conduct such activities. Must normalize/baseline server network behavior and detect anomalous activities off baseline.	• Netflow data, or firewall traffic profile data • List of permitted remote storage sites (e.g., box)

Play Category	Play	Description	Source Data
Data Exfiltration	Lost/stolen device	User reports that a device was lost or stolen from their possession. Conduct standard actions to immediately reduce the impact, including, at minimum 1. Issuing a device wipe and remote lock 2. Checking for last encryption status in control systems 3. Executing CIRT if device is unencrypted	• Users • Mobile device management systems • Endpoint configuration systems

In each of these cases, the source data provided will include events or log information that is critical to detect the play being constructed. Specialized security systems can ingest these logs and apply pattern matching, rule matching, and analytics capabilities to specific events in the logs to call out potential incidents of interest. These specialized systems are referred to as SIEM systems.

8.M.B	***Incident Response***	***NIST FRAMEWKORK REF:*** PR.IP-9, RS.AN-1, RS.MI-1, RS.MI-2, RC

One of the most basic and most important functions in a cybersecurity organization is the IR process. This process provides the organization with standardized procedures to respond to cyberattacks. The attack may be as simple as an attempted phishing attack against users or a highly sophisticated extortion attack that shuts down digital operations. In both cases, from minimal to significant impact, the organized manner of an IR is critical to managing these threats.

The following procedure is a summary of NIST's *Computer Security Incident Handling Guide*.[34] Generally, a structured IR process is segmented into the following steps:

- *Preparation:* Before you respond to a cybersecurity incident, it is important to have policies, processes, and procedures in place, including the following components:
- *IR policy:* a policy that defines the categorization and severity of incidents, the stakeholders involved in IR, the roles and responsibilities of each person, the entry criteria when a security incident occurs, and the person who oversees IR plays. Stakeholders may range from the standard blocking and tackling personnel in IT operations to legal, marketing, and public affairs

34. Paul Cichonski et al., *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (NIST Special Publication 800-61r2, August 2012, Gaithersburg, MD), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

personnel for high-impact incidents. A template IR policy is provided in Appendix G *in the Main document*.

- *fCybersecurity incident response team (CIRT):* a pre-formed and "on the ready" group that knows how to navigate issues when critical- or high-severity security incidents arise. This team develops and manages your organizational response. Most commonly, CIRTs are formed in the HPH sector when potential data breaches occur and the organization must manage the potential breach in compliance with HITECH. It is important to identify the incident commander, the most senior official who will oversee managing cybersecurity incidents. The incident commander is usually the CISO or equivalent. Note that the incident commander should not dive into the technical weeds of the incident, but should keep the various teams organized and focus on their objectives. Table 11 describes the teams may be involved in resolving a critical security incident and potential breach.

Table 11. Roles and Responsibilities for an Organizational CIRT

Team	Description
Executive/Senior Leadership	!n organiza tion's C-suite or most senior executives. They provide overall direction and approvals required to resolve significant cybersecurity breaches. These individuals should be kept informed throughout the lifecycle of a significant cybersecurity incident.
Cybersecurity Teams	Teams comprising people with cybersecurity expertise who understand attacks, vulnerabilities, and the methods by which threat vectors are exploited. They provide technical depth and detail to technical teams and execute procedures in the playbook.
Technical Teams	Teams comprising SMEs for the technologies that have been compromised and who are engaged in developing and implementing the response. These SMEs may be system owners, system administrators, or other individuals with specialized IT expertise. They take instruction from the cybersecurity teams as part of the playbook execution.
Legal Teams	Teams comprising attorneys in your general counsel (internal or external) that help manage the incident under privilege as well as consult on regulatory expectations.
Public Affairs/Marketing and Communications	People who manage external communications to deliver a consistent voice and message in the event of a high-visibility cybersecurity incident. This team is important to managing the reputation of the organization.

Team	Description
HIPAA Compliance Team	Teams responsible for understanding the full extent of a cybersecurity incident that involves PHI. This includes conducting a breach analysis in compliance with HITECH and providing consultation on any patient-facing communications that should occur.

- *Playbook, or runbook:* a document that contains standard operating procedures to respond to different types of cyberattacks. Procedures to respond to a phishing attack are different from those required to respond to a system intrusion or a ransomware attack. Each of these three types of attack is a distinct play in an organization's cybersecurity playbook. For each play, it is important to describe the steps that will be followed to mitigate the attack so that your response is not "made up on the fly." Though each attack has its own unique characteristics and nuances, your procedures should follow the steps provided in your playbook for that type of attack. A template playbook is provided in *Appendix G in the Main document*.
    - *Tools and technologies:* After you establish your policies, CIRTS, and playbook, the next level of improvement is to configure your tools and technologies to streamline the execution of your plays. Streamlining connects your IR processes to your security engineering processes to create a continual feedback loop, which is essential to becoming a resilient organization.
- *Identification:* The first response to any cyberattack is to understand the scope and extent of the attack. The identification phase of an attack response involves categorizing and classifying components of the attack based on your policies and procedures. Critical and sophisticated attacks warrant a well-organized and effective response.

  For example, a general phishing attack that targets a small user set and that is easily identified as malicious may be assigned a lower level of concern than a targeted phishing attack against a select user base leveraging the nomenclature of your organization. These highly specialized attacks are known to be very successful and can easily compromise a user's credentials or introduce remote-access malware into your environment.

  The identification exercise in a phishing process may be as simple as the following example:
    - Receive notification from your user base or through your own detection systems of a phishing attack or campaign.
    - Profile and understand the extent and scope of the phishing attack. Determine its level of sophistication and intent.
    - Conduct a basic investigation to determine whether links were clicked or malware was delivered.
- *Containment:* After the extent and scope of the attack is understood, the next step is to contain the attack before it penetrates further into your organization. This phase is critical and must not be overlooked; less mature organizations may start fixing the vulnerability that was exploited before they stop the attack. Your playbook should include containment procedures for each play. In some cases, containment may require shutting down information systems to prevent them from being compromised if they are vulnerable to the attack.

  A containment exercise for a phishing attack may be as simple as the following:

- Shun/prevent any remote access C2 traffic that might be established as part of the attack.
- Change credentials proactively for users who clicked to open a credential-theft phishing campaign.

- *Eradication:* This phase of your response focuses your IR effort on eliminating all traces of the attack, including the attack foothold. This step includes
  - identification of all e-mails that were delivered to your user base;
  - removal of these e-mails from mailboxes of the same user base; and
  - reimaging of endpoints where malicious binaries or malware were downloaded to ensure no foothold exists.

- *Recovery:* After the threat is neutralized and all malicious activity is removed from the organization's systems, you must determine whether to reactivate the compromised technology. In most cases, the answer to this question will be "of course," since these technologies fulfill a larger purpose in your organization. In cases where legacy technologies were compromised, however, it might not be worth the effort and investment to bring them back online.

  In either case, the process to restore technical capability in the organization is as important as the process to remove the threats and malicious activities in your systems. As you restore functionality, shut down the vectors that made the attack successful. This may be done by patching an exploited vulnerability or rebuilding an entire system to leverage hardening processes such as those identified in **Cybersecurity Practice #2: Endpoint Protection Systems**.

- *Lessons Learned/After-Action Report:* Arguably, the most important stage of your IR process is a full debrief with your IR teams after the attack is mitigated and systems are returned to full functionality. This debrief should profile the successful attack vectors and identify short-term adjustments to introduce enhanced prevention, detection, or response capabilities, as well as long-term strategic elements that require more detailed planning.

  For example, if your organization falls prey to a sophisticated phishing attack that results in the theft of multiple credentials, followed by the installation of remote-access tools, a multifaceted set of mechanisms may be considered for short-term and long-term improvement. Examples may include the following:
  - Refine a play within the playbook that did not execute as efficiently as possible. Timeliness is one of the most critical aspects of any response; taking too long to ramp up your IR playbook increases your exposure to a successful attack.
  - Refine and expand logging capabilities to detect threats more quickly. Implementing these capabilities into your SIEMs. Delve into the specific patterns of the attack as much as possible for lessons learned.
  - Share attack details and information with participating ISACs and ISAOs. This helps other organizations to prevent validated and vetted threats. It provides greater credence to the intelligence and increases resiliency of the sector.
  - Leverage advanced analytics-based phishing protection tools such as "click protection" or "attachment sandboxing/" These usually require investment and budget allocation by the organization.

- Refocus and prioritize resources to build out greater capabilities to identify and respond to phishing attacks. From a strategic perspective, it is important to refocus your resources in response to a threat that is ramping up against your organization.

A feedback loop from your IR processes back into engineering and operations is a key to becoming a resilient organization. This type of feedback loop enhances an organization's cybersecurity capabilities over time and organically, while increasing flexibility and agility in IR response processes.

To read an example case of a mock attack, consider "! Pra ctical Example of Incident Response to a Network Based !t tack" from the S! NS Reading Room.[35]

Further details associated with IR playbooks can be found in the SANS Reading Room article, "Incident Handler's Handbook."[36]

8.M.C	***Information Sharing and ISACs/ISAOs***	***NIST FRAMEWKORK REF:*** ID.RA-2

Security engineering and operations activities tend to focus on preventing cyberattacks and building out systems that enable streamlined execution of IR functions. That said, not all attacks are equal. They range from simple "script kiddies" that attempt to gain entry to any target to advanced persistent threats backed by substantial resources and a strong desire to gain entry to your specific organization. The means to differentiate these types of attacks falls under the discipline of threat intelligence.

Sophisticated threat intelligence is realized through involvement with and participation in ISACs and ISAOs. ISACs and ISAOs tend to focus on a specific vertical (such as the Health Information Sharing and Analysis Center within the health care sector) or community (such as the Population Health ISAO[37]). In all cases, the primary function of these associations is to establish and maintain channels for sharing cyber intelligence. The means to share this intelligence vary in sophistication; most mature ISACs leverage common standards and formats, such as Structure Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII), as well as flash reports that profile current attacks. ISAC or ISAO participation offers substantial value to an organization. It connects your cybersecurity professionals with the greater cybersecurity community.

As with all disciplines, there are multiple levels of maturity within the threat intelligence discipline. The most basic sharing of threat intelligence involves consuming lists of "vetted bad IP addresses" or "feeds" from commodity sources. These sources have been well curated to identify where the loudest and most obvious attack space resides. Organizations can use multiple means to consume these feeds, but the most usual process is to subscribe to a daily download of IOCs.

---

35. Gordon Fraser, *A Practical Example of Incident Response to a Network Based Attack*, The SANS Institute, 2017, https://www.sans.org/reading-room/whitepapers/incident/practical-incident-response-network-based-attack-37920.

36. Patrick Kral, *The Incident Handlers Handbook*, The SANS Institute, 2011, https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

37. "Population Health Information Sharing & !nalysis Organization, " International IS!O Network, accessed March 10, 2018, http://www.isaonetwork.org/population-health/.

Sub-Practices for Large Organizations

8.L.A	***Advanced Security Operations Centers***	***NIST FRAMEWKORK REF:*** N/A

In addition to the basic SOC practices already discussed, an organization's move to more advanced security management should include expanding its SOC to a 24x7x365 model. In this model, the SOC is staffed and monitored 24 hours per day, 7 days per week, 365 days per year.

There are multiple methods to achieve this model, all of which have benefits and constraints. Some of these methods are described below:

- *Fully outsourced:* In the fully outsourced model, all SOC and threat actions are outsourced to a third-party provider who has the required infrastructure, staff, and capabilities. Such providers normally install sensors on your networks and use them to collect necessary log information that enriches detection and response activities. SOC analysts actively look for threats and provide your internal IR personnel with specific actions to take when threats are identified.

  This model has the advantage of scale and capability. It is difficult to hire and retain qualified security analysts to provide this dedicated function. Additionally, organizations benefit from the shared intelligence discovered by the service provider's other clients. The main disadvantage is that these analysts often do not fully complete response actions, requiring engagement from your internal teams. Additionally, investments made by your organization in cybersecurity tools might not be fully leveraged, because the service providers are likely to use their own tools.

- *Fully insourced:* In the fully insourced model, all SOC and threat actions are handled with internal staff and infrastructure. This model requires the buildout of a dedicated physical space with the IT infrastructure and tools necessary to support your IR personnel. It requires a combination of skills from security engineers, incident handlers, and threat hunters.

  This model has the advantage of situational awareness and an in-depth understanding of the organization's business requirements and nuances. Internal staff are accustomed to the specific needs of the organization. Additionally, internal staff understand the context of an organization's various systems in far more depth than an outside service provider could. The main disadvantages of this model relate to cost, workforce retention, and threat intelligence. Building out an internal SOC can costly if the organization lacks existing facilities to support it. Moving to a 24x7 operation requires hiring new employees and supervisors to ensure effective management and coverage during holidays and time off. Lastly, in this model, the organization does not necessarily get current information about threat actions occurring in other organizations.

- *Hybrid:* In the hybrid model, the SOC and incident handling functionalities attempt to take advantage of the strengths of the fully outsourced and the fully insourced models while minimizing the disadvantages. In this model, organizations contract with a service provider who provides 24x7x365 monitoring and response by remotely accessing the organization's existing security technologies (e.g., SIEMs, IPS, firewalls). The service provider provides facilities and staff for monitoring and response actions, and the organization provides the tools and escalation processes.

This model tends to offer flexibility and scaling of existing investments made in cybersecurity technologies, processes, and people. However, it requires specific and scripted procedural playbooks to be effective. The organization is required to drive these procedural playbooks and ensure that the service provider complies with them. Lastly, in this model, organizations lose some of the situational awareness normally provided by internal handlers. Precise roles and responsibilities must be established to achieve the desired outcome.

8.L.B	***Advanced Information Sharing***	***NIST FRAMEWKORK REF:*** ID.RA-2

Leveraging threat intelligence can be challenging. The organization must establish a threat model, ingest data according to the model, and automate data collection and response. This requires dedicated human and technology resources to be successful.

MITRE has developed a model to manage threats. "Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)" is a curated knowledge base and model for cyber adversary behavior. It addresses the phases of an adversary's lifecycle and the platforms that are targeted. ATT&CK is useful for understanding security risks from known adversary behavior, planning security improvements, and verifying that defenses work as expected.[38] It is recommended that organizations consider using this model in addition to STIX and TAXII automation methods to build out a robust threat intelligence program.

Beyond ISACs and ISAOs, there are individual intelligence gathering organizations or departments within organizations that have a vested interest in getting "deep intelligence" directly from the attacker community. This capability requires substantial investment and specialized talent (think intelligence officers), so this level of maturity is not achievable in most large organizations. However, with proper investigation, the fruits of intelligence organizations' labor can assist the HPH sector immensely.

8.L.C	***Incident Response Orchestration***	***NIST FRAMEWKORK REF:*** PR.IP-9

Because many specialized tools exist to provide organizational cybersecurity, it can become complicated to leverage all these tools at once. Examples include SIEMs, user behavior analytics, deception technologies, e-mail protection platforms, and endpoint detection and response technologies. Though tools like SIEMs are designed to ingest information from multiple sources and provide context, this capability is dependent on the extensibility of log data, as well as the workflow and process capabilities of the SIEM technology. SIEMs are good at developing alerts and notifying security resources about emergent issues, but they are generally not as robust in the process of executing IR playbooks.

This is where IR orchestration tools come in handy. Once playbooks have been created and approved, IR orchestration tools ensure that playbook execution is consistent. Without IR orchestration, cybersecurity personnel must manage IR consistency. IR orchestration tools enable cybersecurity

38. "Adversarial Tactics, Techniques & Common Knowledge, MITRE Partnership Network, accessed March 7, 2018, https://attack.mitre.org/wiki/Main_Page.

personnel to focus on the incident, rather than on the consistent execution and documentation of a response play.

In addition to monitoring workflow, IR orchestration tools can pull data from system security stacks and present it to the incident responder in a centralized dashboard. Examples of data that may be pulled into this dashboard include: SIEM, log data, Dynamic Host Configuration Protocol logs, asset inventories, antimalware consoles, vulnerability management data, threat intelligence information, identity management systems, and endpoint security technologies. Each of these data types provides a unique perspective on the threat that your organization is experiencing.

8.L.D	***Baseline Network Traffic***	***NIST FRAMEWKORK REF:*** ID.AM-3 / DE.AE-1

It is useful to baseline your network traffic and implement capabilities to alert upon anomalous changes to the baseline. This can be accomplished by leveraging netflow data and systems that can ingest netflow data. Each system that operates in the ecosystem will have a standard digital footprint for its network communications and will generally operate within those parameters. By conducting a baseline operation on each of the major and core systems, you can compare what is expected to what is occurring. This can be done manually, or you can invest in technologies that can automate the process.

8.L.E	***User Behavior Analytics***	***NIST FRAMEWKORK REF:*** PR.PT-1 / DE.AE-1

User Behavior Analytics (UBA) is a technique that may be considered as the "SIEM for Users." In most modern threats, the threat actors attempt to leverage access that already exists in the user space. Although attackers can generate new accounts for access attempts, they understand most organizations monitor systems for new accounts, especially those with privileged access. The exploitation of existing accounts, however, might go unnoticed.

UBA systems provide analytics context from a user perspective. Like conducting a baseline activity over network access, UBAs baseline user activity and actions throughout the organization's digital ecosystem. The tool ingests the most relevant user activity logs from these systems as well as existing authentication and authorization systems. Deviations are discovered after the user has been profiled, enabling IR actions to be executed according to the proper playbooks.

One note of importance: UBA protects against external as well as internal threat actors.

8.L.F	***Deception Technologies***	***NIST FRAMEWKORK REF:*** N/A

Deception technologies expand on the honeypot and honeynet techniques of old, scaling them for larger enterprises. These techniques place "fake systems" or "fake breadcrumbs" throughout the digital ecosystem and wait for them to be "tripped." They work on the principle that communications should not occur in a system that serves no purpose in the organization. If such communication occurs, it should be brought to the attention of the IR teams for further investigation.

Deception technologies discover attackers who have placed a foothold in your organization's network and are attempting to pivot to find targets of interest. These targets may be simple (e.g., file storage systems, e-mail systems) or they may be complicated (e.g., EMR or imaging systems). In all cases, the

goal of the attacker is to leverage access already obtained to pilfer data, conduct an extortion attack (i.e., ransomware), or other maleficence. The organization's approach is to generate hundreds or thousands of these fake systems, so that it is difficult for the hacker to differentiate them from real assets. In the process the organization's information security office will be triggered to respond accordingly.

Your IR teams can profile threat actors by watching their behavior on fake systems. For example, technologies exist to create a complete fake file system that interacts and responds like a real file storage system, even generating files that appear to be legitimate. By watching the threat actor enumerate the file system, your IR teams can develop certainty of the malicious intent and identify the threat actor's foothold in the organization's network.

Threats Mitigated

1. Phishing attacks
2. Ransomware attacks
3. Loss or theft of equipment
4. Insider, accidental or intentional data loss
5. Attacks against connected medical devices that may affect patient safety

Suggested Metrics

- Time to detect and respond in aggregate, trended by week. The goal is that an IR response should kick off within *x* hours after detection of an incident, and the incident should be mitigated within *y* hours after response. Lag time between occurrence and detection of a security incident should be fewer than *z* days.
- Number of true positive incidents executed by incident category on a weekly basis. Though there is no specific goal for this metric, it is important to monitor trends in incidents that occur in your organization. This will inform the larger security strategy over time based on actual threats in your organization.
- Number of backup failures by week. The goal is to minimize the number of backup jobs that fail and to provide continual assurance that backup jobs are executing as intended.
- Number of notable (or critical- and high-rated) security incidents per week, providing a profiled enumeration of each incident. Each response to a notable security incident should be executed consistently and thoroughly. Each incident should have an after-action report. The goal is to demonstrate that after-action reports and incident reports are written for each notable security incident. This will help with the development and implementation of continual improvement processes.

Cybersecurity Practice #9: Medical Device Security

Cybersecurity Practice 9: Medical Device Security		
Data that may be affected	PHI	
Medium Sub-Practices	9.M.A	Medical Device Management
	9.M.B	Endpoint Protections
	9.M.C	Identity and Access Management
	9.M.D	Asset Management
	9.M.E	Network Management
Large Sub-Practices	9.L.A	Vulnerability Management
	9.L.B	Security Operations and Incident Response
	9.L.C	Procurement and Security Evaluations
	9.L.D	Contacting the FDA
Key Mitigated Risks	• Attacks Against Connected Medical Devices that May Affect Patient Safety	

Health care systems use many diagnostic and therapeutic methods for patient treatment. These range from technological systems that capture, render, and provide detailed images of scans to devices that connect directly to the patient for diagnostic or therapeutic purposes. Such devices may have straightforward implementations, such as bedside monitors that monitor vital signs during an inpatient stay, or they may be more complicated, such as infusion pumps that deliver specialized therapies and require continual drug library updates. These complex and interconnected devices affect patient safety, well-being, and privacy, and they represent potential attack vectors in health delivery organizations' (HDOs') digital systems. As such, these devices should be robustly designed and properly secured.

This section focuses on the methods that HDOs can employ to protect connected medical devices. Specifically, it addresses the actions that HDOs are permitted to take, how to align with the Medical Device and Health IT Joint Security Plan, and how to best work with device manufacturers and the U.S. FDA.

Any device that connects directly to a patient for diagnosis or therapy should undergo extensive quality control to that it is safe for use. Rigorous stipulations, managed by the FDA, are in place for the development and release of such systems. The organizations that produce these devices, referred to as *device manufacturers*, should comply with regulations. Organizations that purchase devices and use them for the treatment of patients are the *clinical providers*. In the context of this relationship, they are the HDOs.

Given the highly regulated nature of medical devices and the specialized skills required to modify them, it is ill-advised for HDOs to make configuration changes without the support of the device manufacturer. Doing so may put the HDO at risk of voiding warranties, result in legal liabilities, and, at worst, harm the patient. Therefore, traditional security methods used to secure assets cannot necessarily be deployed in the case of medical devices. For example, one cannot simply apply a patch to a vulnerable component of the OS that runs a medical device.

In 2018, the Healthcare Sector Coordinating Council's Joint Cybersecurity Working Group released a guidance document for device manufacturers on developing and releasing secure medical devices.[39]

39. *Medical Device and Health IT Joint Security Plan*, 2018.

This Joint Security Plan (JSP) was the result of a public–private partnership between health care providers, device manufacturers, and the FDA. The JSP focuses on ensuring that vendors deliver secure products to HDOs and have concrete plans to maintain the security of these products. This section takes this context into account when addressing what HDOs should do upon receiving medical devices from manufacturers.

For a practical example of full lifecycle management, risk analysis, management, leading practices, and detailed configuration specifications to secure wireless pumps (one type of medical device), see the NIST/NCCOE report, *Securing Wireless Infusion Pumps In Healthcare Delivery Organizations 2017.*[40] Another common framework to leverage is the ISO 80001:2010 standard.[41]

Sub-Practices for Medium-Sized Organizations

9.M.A	***Medical Device Management***	***NIST FRAMEWKORK REF:*** PR.MA-2

Medical devices are a specialized type of IoT device, specific to providing clinical diagnosis or treatment within HDOs. Nevertheless, cybersecurity for medical devices follows many of the cybersecurity practices already discussed in this document:

- **Cybersecurity Practice #2: Endpoint Protections**
- **Cybersecurity Practice #3: Identity and Access Management**
- **Cybersecurity Practice #5: Asset Management**
- **Cybersecurity Practice #6: Network Management**
- **Cybersecurity Practice #7: Vulnerability Management**
- **Cybersecurity Practice #8: Security Operations and Incident Response**

Rather than recreating these cybersecurity practices, HDOs are encouraged to extend the relevant cybersecurity practice from each section, implementing it appropriately for medical device management. The following sections expand on how the broad practices listed above apply in the specialized case of medical devices.

Typically, medical devices connect to larger information systems or applications. For example, a CT scanner may connect to a picture archiving and communication system, which, in turn, is connected to specialized image-reading workstations. In such environments, the safeguards listed below are

40. Gavin O'Brien et al/,*Securing Wireless Infusion Pumps In Healthcare Delivery Organizations* (NIST Special Publication 1800-8, May 2017, Gaithersburg, MD), https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8-draft.pdf.

41. "IEC 80001-1:2010: Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities", https://www.iso.org/standard/44863.html.

important, not only for the medical device itself (in this case the CT scanner), but also for the larger information systems and connected endpoints. Consider all these safeguards, as applicable.

9.M.B	***Endpoint Protections***	***NIST FRAMEWKORK REF:*** PR.MA-2, DE.CM-4, PR.AC-5, PR.DS-1, PR.AC-1, PR.IP-1

Where feasible, medical devices should have the following controls enabled:

- *AV software:* Usually, the medical device manufacturer should directly support AV software, or it should be cleared for operation by the manufacturer. Ensure that a compliant AV technology is enabled. If AV cannot be implemented, compensating controls should enforce an AV scan whenever the device is serviced prior to reconnecting to the device network.

Local firewalls: Medical devices should be configured to communicate only with required systems. Unused services and ports should be disabled if they are supported by the manufacturer.

- *Encryption:* If supported by the manufacturer, medical devices should have local encryption enabled in the case the device is stolen.
- *Application whitelist:* Configure medical devices, or implement software, to only allow known processes and executables to run on the devices. This control alone can significantly reduce the exploitability of devices.
- *Default password changes:* If supported by the manufacturer, default passwords, especially those enabling privileged access, should be changed to long, complex passwords used only for the medical device. Do not tie unique device credentials to any general systems management credential, because you do not want general credential compromises to affect the medical device.

Routine patching: As part of preventative maintenance cycles, medical devices should be patched with supported cybersecurity patches released by the device manufacturers. Given the special sensitivity of the configuration and management of these devices, patching should not take place on these devices unless cleared by the manufacturer. This control, along with whitelisting, can significantly reduce the exploitability of the device.

9.M.C	***Identity and Access Management***	***NIST FRAMEWKORK REF:*** PR.AC, PR.AC-7, PR.AC-4

As much as feasible, medical devices should have the following controls enabled:

- *Authentication:* If supported by the manufacturer, the device should bind its authentication capabilities with systems enterprise authentication domains. This automates termination of access to the device upon termination of employment for the user.
- *Vendor support passwords:* Passwords should be complex and not shared among the vendor team. A unique logon credential should be established for each vendor employee. Ensure the manufacturer does not use the same account and password to manage medical devices in your organization and others.
- *Remote access:* If remote access is required to manage medical devices, MFA capabilities should be deployed, with HDO acceptance of the system access mode to be used. Depending on the

deployment scenario, the device manufacturer may be required to support remote access capabilities. Otherwise, such capabilities should be deployed on a separate component of your existing MFA system to limit exposure if the MFA system is compromised.

9.M.D	***Asset Management***	***NIST FRAMEWKORK REF:*** ID.AM, ID.AM-1, PR.IP-6

As much as feasible, medical devices should have the following controls enabled:

- *Inventory, hardware:* All medical devices should be added to an inventory that is capable of reflecting the core components of the devices themselves. You may use your general ITAM inventory, as described in **Cybersecurity Practice #5: IT Asset Management**. Alternatively, you may have to employ specialized tools designed specifically for tracking the lifecycle of medical devices. Such systems can be useful for maintaining preventative maintenance schedules.
- *Inventory, software:* Implement a software component inventory for your medical devices. Manufacturers should be able to deliver to the HDO a full listing of software components (including operating systems and software application components developed by vendors, as well as components licensed from third parties), with at least major version information. Such lists are sometimes referred to as *bills of materials*. Information about software components should be maintained in a scalable database managed by the HDO, and updated as part of the standard device management practices.
- *Wiping:* When a medical device is slated for decommissioning, it is critical to ensure that all data on the device are wiped. Typically, these devices are returned to the vendor and potentially resold or delivered to other organizations for destruction. You do not want your organization's data to be accessed by these other parties.

9.M.E	***Network Management***	***NIST FRAMEWKORK REF:*** PR.AC-5

As much as feasible, medical devices should have the following controls enabled:

- *Segmentation:* Given the critical nature of medical devices and the organization's general inability to configure them to reduce vulnerabilities, it is critical to segment these devices separately from general access or data center networks. The ability to restrict access to the device is essential to its safe operation.

  Dedicated, highly restricted networks should be set up. The only traffic allowed on these networks should be profiled based on required operation of the devices connected to that network. Access to device management systems should be heavily restricted to limit its exposure. Lastly, it is important to ensure that these networks are segmented such that any vulnerability scanning systems are *not* permitted access in a clinical setting. Given the delicate nature of medical devices, execution of a rogue vulnerability scan could disrupt the devices.

  As part of the segmentation strategy, review data flows and interfaces between the medical devices and their connected systems. Be sure not to limit the essential functionality of the medical device, including its ability to be patched remotely, if required.

Device manufacturers may require installation of their own physical networks in the organization. In these cases, access to the manufacturer's physical network should be limited with the same restrictions as if the HDO were implementing its own segmentation strategy.

Sub-Practices for Large Organizations

9.L.A	***Vulnerability Management***	***NIST FRAMEWKORK REF:*** ID.RA-1, PR.IP-12, ID.RA-5, RS.CO-5, DE.CM-8

As much as feasible, medical devices should have the following controls enabled:

- *Vulnerability and risk categorization:* In 2016, the FDA issued the *Postmarket Management of Cybersecurity in Medical Devices* guidance.[42] This guidance document presents components for the proper management of medical devices after they have been deployed in an HDO. Focusing on the risk to patient safety, this guidance stipulates that manufacturers should implement vulnerability and risk-management practices to categorize risks according to the device's effectiveness and the potential to cause harm to the patient.

  HDOs should work with device manufacturers to arrive at a common understanding of the framework for the risk categorizations. Upon disclosure of a high risk, HDOs should take escalated action to secure the device.

- *Vulnerability disclosure programs:* Each device manufacturer should have a program that informs HDOs of vulnerabilities that exist in their devices. These programs should have a communication channel to report information and inform parties. HDOs should work with the manufacturers so that all parties understand the respective points of contact between the manufacturer and the HDO.

  In addition to direct communication channels, other channels exist for the disclosure of medical device vulnerabilities. These include the Department of Homeland Security National Cybersecurity and Communication Integration Center, the Health Sector Cybersecurity Coordination Center, and the Industrial Control Systems – Computer Emergency Response Team; manufacturers can include these as part of their vulnerability releases, as can ISACs or ISAOs with which the manufacturers participate.

  The HDO should have a program in place to accept inbound vulnerability disclosures, evaluate the HDO's exposure to these vulnerabilities, and identify, alongside the manufacturers, response actions to remediate or mitigate each vulnerability according to its level of risk.

  With a well-established vulnerability disclosure program, medical device manufacturers and HDOs will have bidirectional communication for managing medical device vulnerabilities. Communication is key to maintaining patient safety. Table

42. *Postmarket Management of Cybersecurity in Medical Devices*, Food and Drug Administration, December 12, 2016, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/uc m482022.pdf.

12 provides a general rule for the response timeframes (including interim compensating controls) for medical device vulnerabilities; this general rule is in line with expectations in the *Postmarket Management of Cybersecurity for Medical Devices* guidance.

Table 12. Timeframes for Resolving Medical Device Vulnerabilities

Vulnerability Criticality	Days
Uncontrolled Risk	
Vendor communicates to HDO; HDO determines interim mitigation step	30 days
Vendor produces a risk remediation solution; HDO implements solution	60 days
Controlled Risk	As defined by routine patching and preventative maintenance

- *Software bill of materials (SBOM) and vulnerability lookups:* Using SBOMs registered in the organization's IT!M , the HDO can compare data from the NVD against data in the organization's software libraries. This comparison provides the HDO with information on current potential vulnerability postures in the medical device space.

  A simple search of the NVD can be conducted by using the web interface located at https:// nvd.nist.gov/vuln/search. This search tool allows HDOs to look up vulnerabilities in products that they currently have. It does not require SBOM material to be preregistered.

- *Vulnerability scanning:* The final action that an HDO can take to understand its vulnerability posture is to conduct vulnerability scans against the medical devices.

  WARNING: UNLESS APPROVED BY THE DEVICE VENDORS, THIS ACTION SHOULD BE TAKEN WITH EXTREME CAUTION DUE TO THE POTENTIAL IMPACTS ON MEDICAL DEVICES WITHIN THE PRODUCTION ENVIRONMENT. HDOS SHOULD NOT ATTEMPT TO CONDUCT VULNERABILITY SCANS UNLESS ABSOLUTELY CERTAIN THAT THE MEDICAL DEVICE IS NOT IN PRODUCTION, IS NOT CURRENTLY IMPLEMENTED IN A CLINICAL SETTING, AND IS NOT CONNECTED TO PATIENT.

  There are two opportune times to conduct vulnerability scans against medical devices:

  - When the device is first procured and tested before deployment in the production environment
  - When a device is taken offline for preventative maintenance and routine patching

  In both scenarios, it is important for the device to be in a highly controlled setting and not connected to a patient. A vulnerability scan can be configured to profile the device and determine whether potential vulnerabilities exist, or to confirm that vulnerabilities have been mitigated as part of a remediation or patching plan.

To conduct such an exercise, it is best for the cybersecurity team to work with the clinical engineering teams and establish a profiled scan template in the vulnerability management software. This template should allow the scan to be executed only against a specific nonproduction network and only by specific individuals. To provide further assurance that the vulnerability scan cannot cause harm to the medical device while it is connected, the scanners' IP addresses scanners should be blocked as part of the segmentation strategy noted above.

When these preparations are complete, the clinical engineering teams can be granted access to the scanning software in a restricted manner that allows the scan to be run only against the network used for preventative maintenance. Vulnerabilities discovered can be shared with the information security office to determine the relative risks. Upon classification of these risks, the teams should contact the device manufacturer and work together to develop and implement a remediation plan.

9.L.B	***Security Operations and Incident Response***	***NIST FRAMEWKORK REF:*** PR.IP-9, DE.CM-8, DE.CM-1, DE.CM-7

Expanding on the SOC and IR processes found in **Cybersecurity Practice #8: Security Operation Center and Incident Response***,* HDOs can provide better monitoring, detection, and response activities around their medical device ecosystems. Using the segmentation strategy outlined above, HDOs should monitor for malicious activity into and within the segment. To provide visibility into the daily operations of the medical device systems, the following sources should be configured to send logs to the HDO's log management systems, SIEMs, or both:

- Firewalls providing segmentation to the medical device network segment
- Information systems that control the operation of the medical devices
- Netflow data from the medical device network segment
- Intrusion prevention systems in front of the medical device network segment
- Logs from any deception technology deployed in the medical device network segment

Using these logs as a source, plays can be enumerated and added into IR playbooks, as described in Table 13.

Table *13*. Incident Response Plays for Attacks Against Medical Devices

Play Category	Play	Description	Source Data
Reconnaissance	Vulnerability scanning sweep of medical device segment	Scan large numbers of vulnerabilities across the medical device network. May involve scanning a single server over multiple ports, or scanning multiple servers over a single port.	• Medical device management system • IDS/IPS logs in front of the medical device network, configured to detect vulnerability scanning • Firewall logs in front of the medical device network • Netflow data from within the medical device network
Lateral Movement	Detection of unknown source clients accessing medical device remote access ports	Detect attacks coming from sources outside of known management sources attempting to gain access to remote access ports (e.g., FTP, SSH).	• Firewall logs in front of the medical device network • Network data from within medical device network
Lateral Movement	Triggered decoy within medical device network	Respond to triggers of decoys being communicated from within or across the medical device network segment. These communications should not occur; they indicate malicious or broken processes.	• Deception technology logs from within the medical device network • Firewall logs in front of the medical device network • Network data from within the medical device network

If any HDO experiences a security incident and requires the assistance of the manufacturer, the HDO should leverage their contact information, which should have been established as part of the vulnerability disclosure program, outlined within section L.B above.

9.L.C	***Procurement and Security Evaluations***	***NIST FRAMEWKORK REF:*** ID.SC

HDOs should establish a set of cybersecurity requirements during the acquisition of new medical devices. These requirements should be embedded in your contracting processes and shared with your supply chain and procurement offices. Ideally, cybersecurity requirements are included requests for information or requests for proposals. These requirements should include high-value items such as supported and patchable OS, AV or whitelisting, no hardcoded or default passwords, and minimal use of administrative privileges.

All technology acquisitions and integrations, including medical devices, require security evaluation as part of the HDO's supply chain process. Implementing cybersecurity evaluation as part of the supply chain process provides an opportunity for the organization to understand, evaluate, and mitigate cyber risks prior to technology deployment. When a security evaluation is undertaken it should include all the other devices required for the device to perform its clinical functions. Examples include the need to both evaluate both the infusion pump and the server it connects to update the formulary, or to evaluate an MRI device that and all the specialized workstations to control it.

- *Security evaluation:* The first part of the medical device acquisition process should be a security evaluation of the device. This evaluation should uncover any risks or flaws in the current design of the medical device and establish transparent communications between stakeholders representing the supply chain, clinical engineering, and manufacturing. The HDO should insist on receiving a Manufacturer Disclosure Statement for Medical Device Security (MDS2). The MDS2 is a standardized form used by most manufacturers and developed by the Health Information Management and Systems Society and the American College of Clinical Engineering. It provides a list of comprehensive cybersecurity questions for medical devices, with responses from the manufacturer of the device in question. Questions in the MDS2 include the following:
    - "Can this device display, transmit, or maintain private data (including electronic Protected Health Information)?"
    - "Can the medical device create an audit trail?"
    - "Can users be assigned different privileged levels within an application based on 'roles' (e.g., guests, regular users, power users, administrators)?"
    - "Can the device owner/operator reconfigure product security capabilities?"

  A copy of the latest MDS2 can be found on the Association of Electrical Equipment and Medical Imaging Manufacturers website.[43] Answers to these questions assist the HDO in completing a meaningful evaluation of the medical device.

- *Contract negotiation:* After the security evaluation is complete, the cybersecurity department should review and provide input into the contract with the manufacturer. This should occur in tandem with the supply chain and legal negotiations and should highlight key security requirements from the HDO. These requirements should reference the FDA's *Postmarket Management of Cybersecurity for Medical Devices* guidance and industry standards describing components that are critical for the safe operation of the devices.

  Armed with the results of the cybersecurity evaluation, scenarios to resolve any unmitigated risks should be included in the contracting process to limit the HDO's liability, especially with constraints around the HDO's ability to alter the medical devices.

- *SBOM:* The HDO should request an SBOM as part of the procurement process. The SBOM is a list of software components that the medical device comprises; it can be thought of as a list of software libraries that make up the device, like the ingredients of a recipe. Understanding the

43. *The Association of Electrical Equipment and Medical Imaging Manufacturers* (MDS2 form HN 1-203, October 7, 2013), http://www.nema.org/Standards/ComplimentaryDocuments/MDS2%20form%20HN%201-2013-1.xlsx.

software libraries that make up the device enables the HDO to understand the impact of vulnerabilities announced by the NVD.

- *End of life / end of support:* Over time, the effectiveness of medical devices will diminish, especially as hardware and software ages and is eventually decommissioned. As part of the evaluation of these devices, manufacturers should disclose to the HDO their life expectancy, which forms part of the HDO's cybersecurity management plan. The plan should include an expectation for when the end of life (EOL) and end of support (EOS) of the devices will occur. If there are no EOLs or EOSs established, then the manufacturers should agree to notify the HDO at least 3 years in advance of EOL or EOS. HDOs are responsible for making risk-based decisions about devices nearing EOL or EOS. In most cases, when a device becomes unsupported, or *legacy*, the device should be replaced as part of established asset refresh cycles. In some cases, it is not possible to replace legacy devices due to financial or other resource constraints. The HDO should then implement compensating controls, with the understanding that the devices will no longer be supported by the manufacturer, and their decommissioning should be strategically planned.

9.L.D	***Contacting the FDA***	***NIST FRAMEWKORK REF:*** RS.AN-5

If an HDO is stuck managing a high-risk cybersecurity vulnerability and cannot get support from the medical device manufacturer to mitigate this risk, the HDO's final recourse is to contact the FDA directly to express concern about the vulnerability. Contacts to the FDA should be limited to critical or high-risk scenarios, especially those with the potential to cause harm to patients.

The Center for Devices and Radiological Health emergency contact information is provided below:

- E-mail: CyberMed@fda.hhs.gov
- Phone: 301-796-7436

Threats Mitigated

1. Attacks against connected medical devices

Suggested Metrics

- Number of medical devices not currently segmented on wireless or wired networks, trended over time. The goal is to limit medical devices on the general access network, data center network, or other locations that do not meet the requirements of specific network segmentation strategies.
- Number of unmitigated high-risk vulnerabilities on connected medical devices, trended over time. The goal is to reduce the number of unmitigated risks to as near zero as possible. Each high-risk vulnerability should have a remediation action plan, as defined in **Cybersecurity Practice #7: Vulnerability Management**.
- Number of medical devices procured that did not receive security evaluation, trended over time. The goal is to reduce the number of procurement actions without security evaluation to as near zero as possible. Share this metric with your supply chain and clinical engineering departments to ensure that the procure process is executing as intended.

- Number of medical devices that do not conform to basic endpoint protection cybersecurity practices, trended over time. The goal is to reduce the number of medical devices that do not meet basic hygiene management practices or to implement practices for these devices. It is not always possible to reduce this number to zero. Mitigating factors should be employed to keep it as low as possible.
- Number of devices that have unknown risks due to lack of manufacturer-disclosed information, trended over time. The goal is to ensure that device manufacturers have vulnerability disclosure programs and that your organization is privy to them.

Cybersecurity Practice #10: Cybersecurity Policies

Cybersecurity Practice 10: Cybersecurity Policies	
Data that may be affected	N/A
Medium Sub-Practices	10.M.A Policies
Large Sub-Practices	N/A
Key Mitigated Risks	• E-mail Phishing Attacks • Ransomware Attacks • Loss or Theft of Equipment or Data with Sensitive Information • Insider, Accidental or Intentional Data Loss • Attacks Against Connected Medical Devices and Patient Safety

Cybersecurity policies must be established for the workforce to understand how they are expected to behave within regard to cybersecurity. These policies should be written for the various user audiences that exist in the organization. There are differences between the general workforce user, IT user, and high-profile or high-risk users (e.g., finance, HR, or health information management).

To set proper expectations, organizational policies should support new cybersecurity hygiene controls. Without such policies, it may be unclear to the workforce what level of adherence is required and what activities put the organization at risk for the threat types discussed in this document.

Several policy templates have been provided in Appendix G *of the Main Document.*

Sub-Practices for Medium-Sized Organizations

10.M.A	***Policies***	***NIST FRAMEWKORK REF:*** ID.GV-1

There is only one general safeguard for this section: a list of policies that organizations can consider, presented in Table 14.

Table 14. Example Cybersecurity Policies for Consideration

Policy Name	Description	User Base
Roles and Responsibilities	Define all cybersecurity roles and responsibilities throughout the organization. This includes who will establish policy and who will implement and conduct security practices.	All users

Policy Name	Description	User Base
Education and Awareness	Define the mechanisms that will be used to train the workforce on cybersecurity practices, threats, and mitigations. Ensure that education includes common cyberattacks (such as phishing), lost/stolen devices, and methods for reporting suspicious behavior on their computers.	All users Cybersecurity department
Acceptable Use / E-mail Use	Describe actions that users are permitted and not permitted to take. Explicitly define how e-mail is to be used.	All users
Data Classification	Define how data are to be classified, with usage parameters around those classifications.	All users
Personal Devices	Define the organization's position on the use of personal devices (i.e., BYOD). If these are permitted, establish expectations for how the devices will be managed.	All users
Laptop, Portable Devices, and Remote Use	Define policies for the security of mobile devices and how they are to be used in a remote setting.	All users IT department
Incident Reporting and Checklist	Define user requirements to report suspicious activities within the organization. Define the responsibilities of the cybersecurity department for managing incidents.	All User Cybersecurity department
Disaster Recovery Plan	Define the standard practices for recovering IT assets in the case of a disaster, including backup plans.	IT department
IT Controls Policies	Describe the requirements for IT security controls in a series of policies or a single long policy. Examples include access control, identity management, configuration management, vulnerability management, and data center management.	IT department
IT Acquisition Policy	Define the actions that must be taken to ensure proper identification and protection of all IT assets purchased by the organization.	Supply chain / procurement users IT department

Threats Mitigated

1. E-mail phishing attacks
2. Ransomware attacks
3. Loss or theft of equipment or data
4. Insider, accidental or intentional data loss
5. Attacks against connected medical devices that may affect patient safety

Suggested Metrics

- Number of policies reviewed over a specified timeframe. The goal is to establish a standard practice to review policies and to monitor compliance with this standard.
- Number of workforce members who review and sign off after reading policies over a specified timeframe. The goal is to establish a standard practice for workforce members to review applicable policies and attest to the review, and for the organization to monitor compliance with this standard.

Appendix A: Acronyms and Abbreviations

Table 15. Acronyms and Abbreviations

Acronym/Abbreviation	Definition
ABAC	Attribute Based Access Control
AHIP	!meric a's Health Insurance Plans
ASL	Assistant Secretary for Legislation
ASPR	Assistant Secretary for Preparedness and Response
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
AV	Antivirus
BYOD	Bring Your Own Device
C2	Command and Control
CEO	Chief Executive Officer
CHIO	Chief Health Information Officer
CIO	Chief Information Officer
CIRT	Cybersecurity Incident Response Team
CISO	Chief Information Security Officer
CISSP	Certified Information Security Systems Professional
CMS	Centers for Medicare and Medicaid
CNSSI	Committee on National Security Systems Instruction
COO	Chief Operations Officer
CSA	Cybersecurity Act
CT	Computed Tomography
CVSS	Common Vulnerability Scoring System
DCC	Distributed Checksum Clearinghouse
DEP	Device Enrollment Program
DKIM	Domain Key Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication Reporting and Conformance
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSRBL	Domain Name System Real-time Blackhole List
DoD	Department of Defense
DOS	Denial of Service

Acronym/Abbreviation	Definition
DRP	Disaster Recovery Plan
DSM	Direct Secure Messaging
EDR	Endpoint Detection and Response
EHR	Electronic Health Record
EMR	Electronic Medical Record
ERP	Enterprise Resource Planning
FDA	Food and Drug Administration
FERPA	Family Educational Rights and Privacy Act
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GINA	Genetic Information Nondiscrimination Act
HCIC	Health Care Industry Cybersecurity
HDO	Health Delivery Organization
HIDS	Host Based Intrusion Detection Systems
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Host Based Prevention Systems
HIT	Health Information Technology
HITECH	Health Information Technology Economic and Clinical Health Act
HMO	Health Maintenance Organization
HPH	Health Care and Public Health
HR	Human Resources
HRSA	Health Resources and Services Administration
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance
IAM	Identity and Access Management
IBM	International Business Machines
ICMP	Internet Control Message Protocol
ICU	Intensive Care Unit
IDS	Intrusion Detection System
INFOSEC	Information Security
IOC	Indicator of Compromise
IoT	Internet of Things
IP	Intellectual Property or Internet Protocol
IPS	Intrusion Prevention Systems
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization

Acronym/Abbreviation	Definition
IT	Information Technology
ITAM	Information Technology Asset Management
LAN	Local Area Network
LANMAN	Local Area Network Manager
LLC	Limited Liability Corporation
MAC	Media Access Control
MACRA	Medicare access and the Children's Health Insurance Program Reauthorization Act
MDM	Mobile Device Management
MDS2	Manufacturer Disclosure Statement for Medical Device Security
MFA	Multi-Factor Authentication
MITRE	The MITRE Corporation
MRI	Magnetic Resonance Imaging
NAC	Network Access Control
NCI	National Cancer Institute
NIST	National Institute of Standards and Technology
NNCOE	NIST National Cybersecurity Center of Excellence
NVD	National Vulnerability Database
OCIO	Office of the Chief Information Officer
OCR	Office for Civil Rights
ONC	Office of the National Coordinator (for Healthcare Technology)
OS	Operating System
PCI-DSS	Payment Card Industry Data Security Standard
PCS	Patient Care Service
PHI	Personal Health Information
PII	Personal Identifiable Information
RBAC	Rule Based Access Control
ROM	Read Only Memory
SAMHSA	Substance Abuse and Mental Health Services Administration
SBOM	Software Bill of Materials
SIEM	Security Incident and Event Management
SME	Subject Matter Expert
S/MIME	Secure Multi-Purpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SOC/IR	Security Operations Center / Incident Response
SPF	Sender Policy Framework

Acronym/Abbreviation	Definition
SSH	Secure Shell
SSN	Social Security Number
SSO	Single log
STIX	Structure Threat Information eXpression
SVP	Senior Vice President
TAXII	Trusted Automated eXchange of Indicator Information
TLS	Transport Layer Security
TXT	Text
UBA	User Behavior Analytics
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
VAR	Value Added Reseller
VP	Vice President
VPN	Virtual Private Network
WAN	Wide Area Network

Appendix B: References

"Adversarial Tactics, Techniques & Common Knowledge/" MITRE Partnership Network. Accessed March 7, 2018. https://attack.mitre.org/wiki/Main_Page.

"Attribute Based Access Control/" NIST Computer Security Resource Center. last updated Feburary 13, 2013. https://csrc.nist.gov/Projects/Attribute-Based-Access-Control.

Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (NIST Special Publication 800-61r2, August 2012, Gaithersburg, MD). https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

"CIS Benchmarks/" Center for Information Security. Accessed September 24, 2018. https://www.cisecurity.org/cis-benchmarks/.

"CIS Control 1: Inventory and Control of Hardware Assets/" Center for Information Security Controls. Accessed September 24, 2018. https://www.cisecurity.org/controls/inventory-and-control-of-hardware-assets/.

"CIS Control 2: Inventory of Authorized and Unauthorized Software/" Center for Internet Security Controls. Accessed Sember 24, 2018. https://www.cisecurity.org/controls/inventory-of-authorized-and-unauthorized-software/.

"CIS Control 20: Penetration Tests amd Red Team Exercises". Center for Internet Security. Accessed September 24, 2018. https://www.cisecurity.org/controls/penetration-tests-and-red-team-exercises/.

"CIS Control 3: Continous Vulnerability Management/" Center for Information Security Controls. Accessed September 24, 2018. https://www.cisecurity.org/controls/continuous-vulnerability-management/.

"CIS Control 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers." Center for Information Security Controls. Accessed September 24, 2018. https://www.cisecurity.org/controls/secure-configuration-for-hardware-and-software-on-mobile-devices-laptops-workstations-and-servers/.

"Common Vulnerability Scoring System v3.0: Specification Document/" FIRST/ !ccessed September 24, 2018. https://www.first.org/cvss/specification-document.

"Controlling Root Access/" Redhat Customer Portal. Accessed September 24, 2018. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-controlling_root_access.

Cross, KC, and Denise Vangel/ "Configure Your Spam Filter Policies/" Microsoft TechnNet. Last modified December 13, 2017. https://technet.microsoft.com/en-us/library/jj200684(v=exchg.150).aspx.

Cross, KC, Denise Vangel, and Meera Krishna/ "Use DMARC to Validate E-Mail in Office 365/" Microsoft TechNet. Last modified October 8, 2017. https://technet.microsoft.com/en-us/library/mt734386(v=exchg.150).aspx.

"CVSS." NIST National Vulnerability Database. Accessed September 24, 2018. https://nvd.nist.gov/vuln-metrics/cvss.

Czanik, Peter and BalaBit. "The 6 Categories of Critical Log Information/" SINS Technology Security Laboratory. Last modified 2013. Accessed February 4, 2018. https://www.sans.edu/cyber-research/security-laboratory/article/sixtoplogcategories.

DEP Guide. Apple.com. Last modified October 2015. https://www.apple.com/education/docs/DEP_Guide.pdf.

Ferrazzi, Keith/ "7 Ways to Improve Employee Development Programs/" Harvard Business Revew. Last modified July 31, 2015. https://hbr.org/2015/07/7-ways-to-improve-employee-development-programs.

Fraser, Gordon. *A Practical Example of Incident Response to a Network Based Attack*. The SANS Institute. 2017. https://www.sans.org/reading-room/whitepapers/incident/practical-incident-response-network-based-attack-37920.

Grassi, Paul A., James L. Fenton, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, Justin P. Richer, Naomi B. Lefkovitz, Jamie M. Danker, Yee-Yin Choong, Kristen K. Greene, and Mary F. Theofanos. *Digital Identity Guidelines: Authentication and Lifecycle Management* (NIST Special Publication 800-63B, June 2017, Gaithersburg, MD). https://pages.nist.gov/800-63-3/sp800-63b.html#appA.

Grassi, Paul A., Michael E. Garcia, and James L. Fenton. *Digital Identity Guidelines* (NIST Special Publication 800-63, June 2017, Gaithersburg, MD). https://pages.nist.gov/800-63-3/sp800-63-3.html.

Mathers, Bill, John Flores, yishengjin1413, Sudeep Kumar, Patti Short, Liza Poggemeyer, and Catherine Watson/ "Implementing Least-Privilege Administrative Models." Microsoft Windows IT Pro Center. Last modified May 31, 2017. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models.

McCallister, Erika, Tim Grance, and Karen Scarfone. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. (NIST Special Publication 800-122, April, 2010, Gaithersburg, MD). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

Medical Device and Health IT Joint Security Plan. 2018.

Murphy, Ian/ "How susceptible are you to enterprise phishing?" Enterprise Times. Last modified December 1, 2017. https://www.enterprisetimes.co.uk/2017/12/01/susceptible-enterprise-phishing/.

O'Brien, Gavin, Sallie Edwards, Kevin Littlefield, Neil McNab, Sue Wang, and Kangmin Zheng. *Securing Wireless Infusion Pumps In Healthcare Delivery Organizations* (NIST Special Publication 1800-8, May 2017, Gaithersburg, MD). https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8-draft.pdf.

OWASP Top 10 - 2017: Ten Most Critical Web Application Security Risks. OWASP, 2017. https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.

"Population Health Information Sharing & !nalysis Organization/ " International IS! O Network/ Accessed March 10, 2018. http://www.isaonetwork.org/population-health/.

Postmarket Management of Cybersecurity in Medical Devices. Food and Drug Administration. December 12, 2016. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/ guidancedocum ents/ucm482022.pdf.

Raju, Murthy. "Using RBL and DCC for Spam Protection/" Linux/com/ Last modified June 14, 2007/ https://www.linux.com/news/using-rbl-and-dcc-spam-protection.

"Security Technical Implementation Guides (STIGs)." Information Assurance Support Environment (IASE). Accessed September 24, 2018. https://iase.disa.mil/stigs/Pages/index.aspx.

Sedgewick, Adam, Murugiah Souppaya, and Karen Scarfone. *Guide to Application Whitelisting*. (NIST Special Publication 800-167, October 2015, Gaithsburg, MD). http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

Shackleford, Dave/ "Keys to the Kingdom: Monitoring Privileged User Actions for Security and Compliance/" Last modified May 2, 2010/ https://www.sans.org/reading-room/whitepapers/analyst/keys-kingdom-monitoring-privileged-user-actions-security-compliance-34890.

Sherry, David, Erik Decker, Andrea Beesing, Matthew Dalton, Jacob Farmer, Shirley Payne, Miguel Soldi, Stephen Vieira, and Donald Volz/ "Toolkit for Developing and Identity and Access Management (IAM) Program." EDUCAUSE. Last modified May 7, 2013. https://library.educause.edu/resources/2013/5/toolkit-for-developing-an-identity-and-access-management-iam-program.

Stone, Michael, Chinedum Irrechukwu, Harry Perper, and Devin Wynne. *IT Asset Management*. (NIST Special Publication 1800-5b, October 2015, Rockville, MD). https://nccoe.nist.gov/sites/default/files/library/sp1800/fs-itam-nist-sp1800-5b-draft.pdf.

Swift, David. *Successful SIEM and Log Management Strategies for Audit and Compliance.* The SANS Institute. 2010. https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528.

The Association of Electrical Equipment and Medical Imaging Manufacturers (MDS2 form HN 1-203, October 7, 2013). http://www.nema.org/Standards/ComplimentaryDocuments/MDS2%20form%20HN%201-2013-1.xlsx.

Zaw, Tim/ "2017 Verizon Data Breach Investigations Report (DBIR) from the Perspective of Exterior Security Perimeter/" Verizon Digital Media Service/ Last modified July 26, 2017. https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/.