This is a working document of all the HICP updates that have been implemented in the 2023 Edition.

Overview

Since 2019, the 405(d) Task Group has been hard at work updating the HICP Publication's Technical Volumes to ensure the ten practices are relevant and actionable for today's cybersecurity threats. In this document you will find a high-level overview of the **major** updates and changes made in each of the technical volumes.

Key Updates

- Email Phishing is now Social Engineering.
- Cybersecurity Practice #10 is now Cybersecurity Oversight and Governances.
- New sub-practices added:
    - Cyber insurance (Cybersecurity Practice #10)
    - Cybersecurity Risk Assessment and Management (Cybersecurity Practice #10)
    - Attack Simulations (Cybersecurity Practice #7)

While completing your review, please pay close attention to these key changes. Also note that the list in this document does not include every change, therefore, a thorough review of the entire document is recommended.

Key Updates to Technical Volume 1, Small Organizations

Cybersecurity Practice #1: E-mail Protection Systems

Sub-practice A: E-mail System Configuration

- Updated editorial content for how to identify e-mail offerings that are more likely to offer some level of security safeguards and protection.
- Encouraged the use of multi-factor authentication and refence a resource to support its implementation.

Sub-practice B: Education

- Recommended process steps for designating and reporting suspicious email messages to appropriate resource. Provided additional resources.

Cybersecurity Practice #2: Endpoint Protection Systems

Sub-practice A: Basic Endpoint Protection Controls

- Revised Table 4 to add new sections for managing administration accounts, the auditing of software applications, and managing end-of-life operating systems.
- Added practical advice on how to turn on vendor-supplied endpoint protection in hardware and software applications. Provided references to products from the Federal Trade Commission (FTC) developed for small business regarding securing remote access and the use of VPNs to encrypt endpoint internet sessions.
- Additional advice on communicating with IT resources or third-party vendors about managing endpoints.

Cybersecurity Practice #4: Data Protection and Loss Prevention

Introduction:

- Modified the definition of a security breach to align with terms commonly found in federal and state law.

Sub-practice B: Procedures

- Extensive revisions to account for the individually identifiable health information created, stored or transmitted by a small healthcare organization across all types of internet facing technology.
- Provide references to OCR guidance on the sending of unencrypted emails to patients that contain protected health information to patient.
- Refer reader to Technical Volume #2 for more advanced technologies to safeguard information systems from unauthorized access.

Cybersecurity Practice #6: Network Management

Sub-practice C: Intrusion Protection

- Added recommendation to seek third-party vendor to implement and manage state-of-the-art intrusion prevention systems.

Cybersecurity Practice #8: Incident Response

Sub-practice A: Incident Response

- Significant revision to align with the resources, capability and needs of the small healthcare organization in the development of an incident response plan.
- Add references to NIST guide for small business incident recovery and a Federal Trade Commission guide developed for small business.
- A new Table 7 produced to describe the roles and responsibilities of an incident response team.

Cybersecurity Practice #10: Cybersecurity Oversight and Governance

NOTE: Section scope and introduction completely revised to focus on alignment with the resources, capability and needs of the small healthcare organization.

Sub-practice A: Policies

- Revised to align taxonomy and scope for applicability to a small healthcare organization.

Sub-practice B: Cybersecurity Risk Assessment and Management

- Significant revision to scope and discussion to encompass thorough exploration of the role of the risk assessment in managing the security of information technology.

Sub-practice C: Security Awareness and Training

- Complete revision with newly added content.

Sub-practice D: Cyber Insurance

- New sub-practice added. Content same as the revised sub-practice in Technical Volume #2.

Key Updates to Technical Volume 2, Medium and Large Organizations

Introduction:

- Added two new examples of laws, such as the California Consumer Privacy Act (CCPA) and Stark Laws to the list of legal and regulatory environments for medium and large health care organizations.

Cybersecurity Practice #1: E-mail Protection Systems

Sub-Practices for Medium Organizations

- Added additional explanation for the importance of Multi-Factor Authentication.
- Added high value assets and spear phishing consideration to Ongoing and Targeted Training bullet under the Workforce Education section.
- Also added recommendation to appoint a Change Leader and an explanation of that role to the Workforce Education section.

Sub-practices for Large Organizations

- Provided additional explanation under Average Time To Detect bullet in the Analytics-Driven Education section.

Cybersecurity Practice #2: Endpoint Protection Systems

Sub-Practices for Medium Organizations:

- New and revised Implementation Specifications added to full disk encryption, hardened baseline images, patching, End-of-Life (EOL) Management rows.

Sub-Practices for Large Organizations:

- Added a suggested metric concerning active endpoints with EOL issues within the Micro-Segmentation/Virtualization Strategies sub-practice.
- Added content to explain how to implement and authorize the process for whitelisting.

Cybersecurity Practice #4: Data Protection and Loss Prevention

Sub-Practices for Medium Organizations:

- Added further clarification on determining data classifications.
- Added a bullet for Disk-to-disk-to-cloud strategies within the Backup Strategies sub-practice.

Sub-Practices for Large Organizations:

- Added more content for mapping data flows in addition to the inherent value of this practice.

Cybersecurity Practice #5: Asset Management

Sub-Practices for Medium Organizations:

- Added a process of steps and removed previous summary under Procurement sub-practice.

Cybersecurity Practice #7: Vulnerability Management

Sub-Practices for Medium Organizations

- Added Change Management sub-practice.

Sub-Practices for Large Organizations:

- Added frameworks that could assist an organization with attack simulations.

Cybersecurity Practice #8: Incident Response

Sub-practices for Large Organizations

- Added paragraph on usage of access logs within applications like Electronic Health Records (EHRs) and Electronic Medical Records (EMRs) in the User Behavior Analytics sub-practice.

Cybersecurity Practice #9: Medical Device Security

Sub-Practices for Medium Organizations

- Added unique IoT considerations and other unique challenges specific to medical devices.
- Added Goals of Risk Mitigation for Medical devices.
- Added guidance for applying other practices already covered in HICP toward medical devices.

- Moved Asset Management to the first sub-practice of Cybersecurity Practice #9 and added graphics to illustrate the need for Asset Discovery and Security tools.
- Added Zero-Trust model to discussion of Endpoint Protections.
- Added steps for implementing and maintaining Identity and Access Management, including further explanation of Remote Access.
- Added a section on micro-segmentation under Network Management.

Sub-practices for Large Organizations

- Added risk-based approach to Vulnerabilities Management with an example Common vulnerabilities and Exposures (CVE) list.
- Added guidance to address contract negotiations within Vulnerabilities Management.
- Added information regarding the Department of Commerce's National Telecommunications and Information Administration (NTIA) software bill of materials (SBOM) initiative.
- Added section for Security Orchestration and Automated Response (SOAR).
- Added content to explain a request for SBOM and Enterprise Architecture Diagram as part of a complete Vendor Assessment Package.

Cybersecurity Practice #10: Cybersecurity Oversight and Governance

Sub-Practices for Medium Organizations

- Added Social Media to "Examples of Cybersecurity Policies for Consideration" table in the Policies sub-practice.