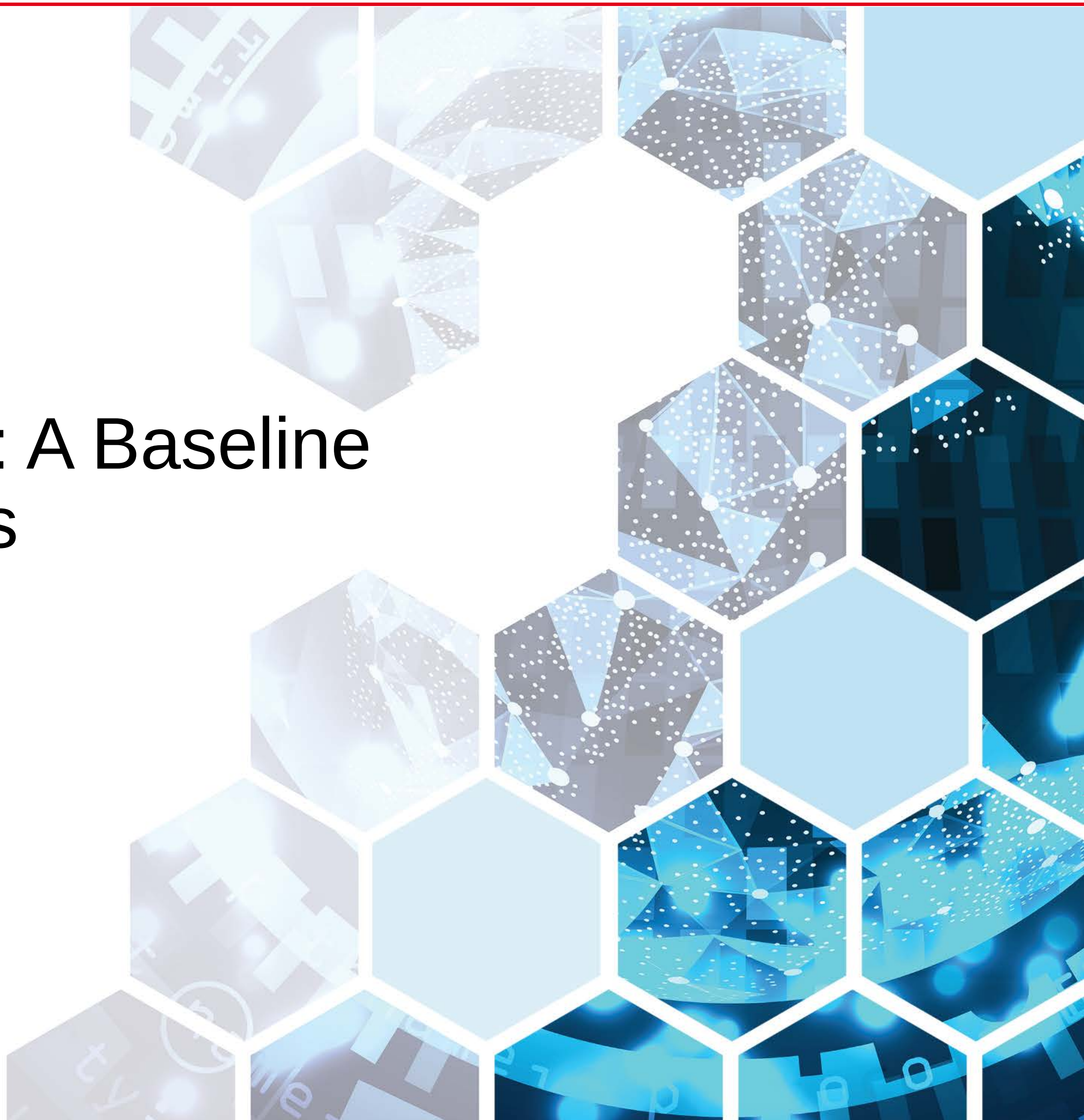
Carnegie Mellon University
Software Engineering Institute



Cyber Hygiene: A Baseline Set of Practices

Matt Trevors

Charles M. Wallen

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM17-0937

Cyber Hygiene – A Baseline Set of Practices

Cybersecurity hygiene is a set of practices for managing the most common and pervasive cybersecurity risks faced by organizations today.

1. Identify and prioritize key organizational services, products and their supporting assets.
2. Identify, prioritize, and respond to risks to the organization's key services and products.
3. Establish an incident response plan.
4. Conduct cybersecurity education and awareness activities.
5. Establish network security and monitoring.
6. Control access based on least privilege and maintain the user access accounts.
7. Manage technology changes and use standardized secure configurations.
8. Implement controls to protect and recover data.
9. Prevent and monitor malware exposures.
10. Manage cyber risks associated with suppliers and external dependencies.
11. Perform cyber threat and vulnerability monitoring and remediation.

Sources:
- *10 Steps to Cybersecurity*, UK Government Communications Headquarters (GCHQ)
- *20 Critical Security Controls*, Center for Internet Security (CIS) aka SANS 20
- *Cybersecurity Framework*, National Institute of Standards and Technology (NIST)
- *Resilience Management Model*, Carnegie Mellon University, Software Engineering Institute CERT Division
- *Review of Cyber Hygiene Practices*, European Union Agency for Network & Information Security (ENISA)
- *Strategies to Mitigate Cyber Security Incidents*, Australian Signals Directorate (ASD)

Cyber Hygiene: A Baseline Set of Practices

CERT-RMM Practices Associated with Cyber Hygiene

CERT Resilience Management Model (CERT-RMM)

CERT-RMM and its resilience management methodologies help organizations consider resilience to be a foundational property of all policies, plans, processes, and procedures. CERT-RMM has more than 200 resilience management practices spread across 26 process areas, ranging from Asset Definition and Management, to External Dependencies Management, to Vulnerability Analysis and Resolution. Though all the CERT-RMM practices are important for an organization's viability and sustainability, they are a lot for an organization to absorb. That's why we've introduced the 11 cyber hygiene areas, which comprise 41 CERT-RMM practices that are paramount to every organization's success. The following slides detail each of the 11 cyber hygiene areas.

The CERT-RMM practice documentation includes practice goals, concepts, implementation guidance, work products, and suggestions on how to build and manage operational resilience. You can download the complete list of CERT-RMM practices from the SEI website. The practices are organized by Practice Area (e.g., Enterprise Focus - EF) with Specific Goals (SG) and Specific Practices (SP) that provide more detailed information and guidance. The information can be readily found in the CERT-RMM documentation by referring to the naming convention of *Practice Area: Specific Goal: Specific Practice*, for example, EF:SG1:SP1.

1. Identify and prioritize key organizational services, products, and their supporting assets.

1. Enterprise Focus – EF:SG1.SP3 – Establish Organizational Services
2. Asset Definition and Management – ADM:SG1.SP1 – Inventory Assets

Summary

What are the organization’s most important activities and assets—the “crown jewels?”

The first principle of risk management is to focus on the critical few: find out what is most important to the organization, figure out where it lives, and build the cybersecurity risk management strategy around it.

2. Identify, prioritize, and respond to risks to the organization’s key services and products.

1. Risk Management – RISK:SG2.SP2 – Establish Risk Measurement Criteria
2. Risk Management – RISK:SG3.SP2 – Identify Service-Level Risks
3. Risk Management – RISK:SG4.SP1 – Evaluate Risks
4. Risk Management – RISK:SG4.SP3 – Develop Risk Disposition Strategy
5. External Dependency Management – EXD:SG2.SP1 – Identify and Assess Risks Due to External Dependencies

Summary

What are the key cyber-risks faced by the organization, potential impacts if those risks are realized, and how should they be addressed?

The organization must identify and assess the risks to its operations, assets, and individuals (including mission, functions, and reputation). The response to the identified risks typically includes mitigation or acceptance and monitoring to reduce the probability of occurrence and/or minimize impact.

3. Establish an incident response plan.

1. Incident Management and Control – IMC:SG1.SP1 – Plan for Incident Management

Summary

Is there a plan in place for responding to significant cyber and physical disruptions?

Document and exercise response procedures and plans that include escalation, personnel roles and responsibilities, and external partner coordination for handling disruptions.

4. Conduct cybersecurity education and awareness activities.

1. Organizational Training and Awareness – OTA:SG1.SP1 – Establish Awareness Needs
2. Organizational Training and Awareness – OTA:SG2.SP1 – Perform Awareness Activities
3. Organizational Training and Awareness – OTA:SG3.SP1 – Establish Training Needs
4. Organizational Training and Awareness – OTA:SG4.SP1 – Deliver Training

Summary

Do employees, senior leaders, and partners have adequate cybersecurity skills and awareness?

Personnel and partners are provided ongoing cybersecurity awareness education and are adequately trained to perform their information-security-related duties and responsibilities.

5. Establish network security and monitoring.

1. Vulnerability Analysis and Resolution – VAR:SG2.SP2 – Discover Vulnerabilities
2. Vulnerability Analysis and Resolution – VAR:SG2.SP3 – Analyze Vulnerabilities
3. Technology Management – TM:SG4.SP2 – Perform Configuration Management
4. Technology Management – TM:SG4.SP4 – Perform Release Management
5. Monitoring – MON:SG1.SP3 – Establish Monitoring Requirements
6. Monitoring – MON:SG2.SP2 – Establish Collection Standards and Guidelines
7. Monitoring – MON:SG2.SP3 – Collect and Record Information

Summary

Does the communications network have adequate protection and monitoring?

Utilize leading practice network design principles when configuring perimeter and internal network segments, and ensure all network devices are configured consistently and appropriately. Filter all traffic at the network perimeter to limit traffic to what is required to support the organization, and monitor traffic for unusual or malicious incoming and outgoing activity that could indicate an exposure, attack, or attempted attack. Conduct regular testing of the network for potential vulnerabilities and exposures.

6. Control access based on least privilege and maintain the user access accounts.

1. Access Management – AM:SG1.SP1 – Enable Access
2. Access Management – AM:SG1.SP3 – Periodically Review and Maintain Access Privileges
3. Knowledge Information Management – KIM:SG1.SP2 – Categorize Information Assets
4. Knowledge Information Management – KIM:SG4.SP2 – Control Access to Information Assets

Summary

Are controls in place to limit information access to only those need it?

Limit access based on the classification level (e.g., confidential, secret, public) of information in documents or data stored on servers. Locate sensitive information in secure areas and on systems that limit access to only individuals who need it. Ensure user access information is current and accurate.

7. Manage technology changes and use standardized secure configurations.

1. Technology Management – TM:SG4.SP2 – Perform Configuration Management
2. Technology Management – TM:SG4.SP3 – Perform Change Control and Management
3. Technology Management – TM:SG4.SP4 – Perform Release Management

Summary

Are change control and configuration management procedures utilized consistently?

Ensure configuration and change control processes are in place and managed. Establish standard secure configurations for hardware, operating systems, and software applications. These configurations should be regularly validated and refreshed to update them in light of recent threats, vulnerabilities, and attack vectors.

8. Implement controls to protect and recover data.

1. Service Continuity – SC:SG3.SP2 – Develop and Document Service Continuity Plans
2. Service Continuity – SC:SG5.SP1 – Develop Testing Program and Standards
3. Service Continuity – SC:SG5.SP3 – Exercise Plans
4. Service Continuity – SC:SG6.SP2 – Measure the Effectiveness of the Plans in Operation
5. Knowledge Information Management – KIM:SG4.SP2 – Control Access to Information Assets
6. Knowledge Information Management – KIM:SG5.SP1 – Control Modification of Information Assets
7. Knowledge Information Management – KIM:SG6.SP1 – Perform Information Duplication and Retention
8. Technology Management – TM:SG5.SP1 – Perform Planning to Sustain Technology Assets
9. Technology Management – TM:SG5.SP2 – Manage Technology Asset Maintenance

8. Implement controls to protect and recover data. (con’t)

Summary

Have adequate cybersecurity controls and recovery solutions been implemented and tested?

Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information. Ensure that each system is automatically backed up at least weekly, more often for systems storing sensitive information. Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls. Regularly test/audit the efficacy of controls, backups, and continuity procedures to ensure they are functioning as intended.

9. Prevent and monitor malware exposures.

1. Incident Management and Control – IMC:SG2.SP3 – Collect, Document, and Preserve Event Evidence
2. Incident Management and Control – IMC:SG2.SP4 – Analyze and Triage Events
3. Technology Management – TM:SG2.SP2 – Establish and Implement Controls
4. Monitoring – MON:SG1.SP3 – Establish Monitoring Requirements
5. Monitoring – MON:SG2.SP2 – Establish Collection Standards and Guidelines

Summary

Does the organization have processes established to prevent malware and manage those risks?

Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and intrusion protection functionality. All malware detection events should be sent to enterprise and event log servers for analysis.

10. Manage cyber risks associated with suppliers and external dependencies.

1. External Dependencies Management – EDM:SG1.SP1 – Identify External Dependencies
2. External Dependencies Management – EDM:SG1.SP2 – Prioritize External Dependencies
3. External Dependencies Management – EDM:SG3.SP2 – Establish Resilience Specifications for External Dependencies
4. External Dependencies Management – EDM:SG4.SP1 – Monitor External Entity Performance

Summary

Are cyber risks associated with suppliers, and are third-party dependencies identified and managed?

Supplier and third-party dependencies are identified, prioritized and managed. The organization establishes processes to manage threats, vulnerabilities, and incidents that may result from supplier and third-party dependencies throughout the lifecycle of those relationships. Where possible and appropriate, collaborative cybersecurity risk management processes (e.g., information sharing and controls testing) should be utilized.

11. Perform cyber threat and vulnerability monitoring and remediation.

1. Vulnerability Analysis and Resolution – VAR:SG2.SP1 – Identify Sources of Vulnerability Information
2. Vulnerability Analysis and Resolution – VAR:SG2.SP2 – Discover Vulnerabilities
3. Vulnerability Analysis and Resolution – VAR:SG2.SP3 – Analyze Vulnerabilities
4. Vulnerability Analysis and Resolution – VAR:SG3.SP1 – Manage Exposure to Vulnerabilities

Summary

Collect threat and vulnerability information from information sharing forums and sources. Establish a process to risk-rate threats and vulnerabilities based on their probability, exploitability, and potential impact. Mitigate the highest risk threats and vulnerabilities using leading practice controls. Establish expected controls implementation and patching timelines based on the risk rating level.