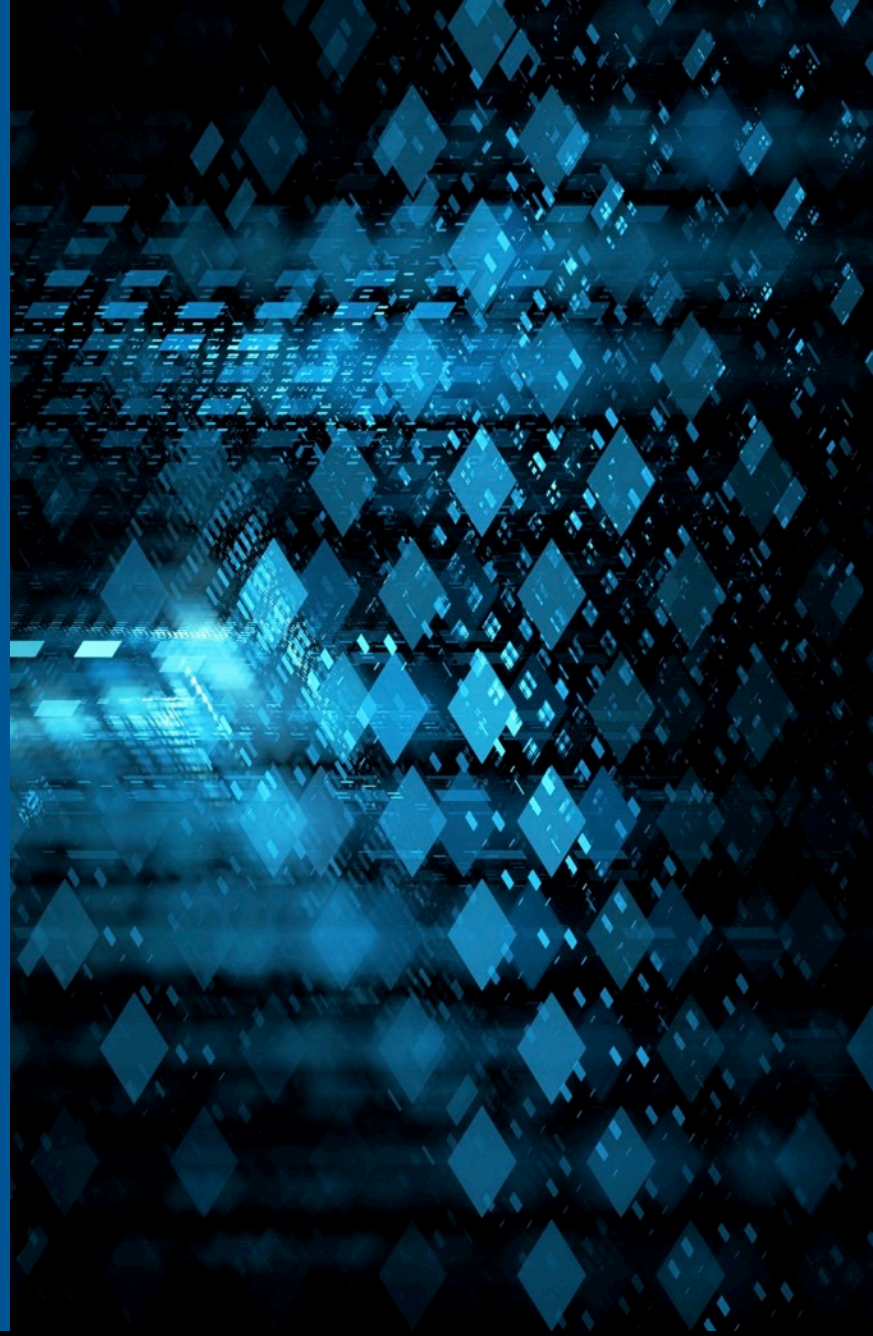
Offense Informs Defense: Building Resilience into Healthcare

Matt Trevors

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Distribution Statements

Copyright 2017 Carnegie Mellon University. All Rights Reserved.

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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM17-0604

Agenda

- Who Am I
- What is Resilience
- Tactics vs Strategy
- The HIPAA Rules
- The Center for Internet Security
- Addressing the Security Rule with the CSC
- RMM/CRR/Cyber Hygiene

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Who Am I

- 20 Years in Information Technology/Security
- 10 Years in healthcare sector
  - IT Management (claims/insurance)
  - Medical Device Manufacturing
- Technical Notes regarding healthcare
  - Addressing the Security Rule with CIS CSC
  - Measuring your healthcare cyber program with the CRR
  - Securing your medical device manufacturing SDLC
- Developed Master's Courses for Developing Secure Systems and Policy Implementation
- Education – MSCIS (Health Informatics/Security), BCS, CISSP, CCSP, CEH

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Cyber Resilience

- What makes a resilient system?
  - System remains viable and sustainable under stress
- How do we address resilience?
  - Protection and Sustainment Requirements
  - Often expressed as:
    - Confidentiality
    - Integrity
    - Availability
- How do you know if you're resilient?

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Tactics vs. Strategy

- WannaCry Example
- Tactical Response:
  - Review bulletin
    - Patch boxes
- Strategic Response:
  - Review bulletin in accordance with IR plan/incident criteria
    - Does it meet criteria for an incident?
    - Discuss response options
    - Execute applicable SOP (patch boxes)

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

HIPAA Security Rule

- One of four rules
  - Privacy Rule
  - Security Rule
  - Breach Notification
  - Enforcement
- Security Rule Safeguards
  - Administrative (164.308)
  - Physical (164.310)
  - Technical (164.312)
- According to DHHS OCR Breach Portal
  - 2014 – 2016 over 127,000,000
  - 2017 - Already about 2,500,000
- Is this ***enough?***

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Center for Internet Security

- 2000 - Founded
- 2015 – Integrated with Council for Cybersecurity
- Home of
  - MS-ISAC
  - Benchmarks
  - CIS-CAT (Lite/Pro)
  - Critical Security Controls

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Critical Security Controls

- Formerly Known As:
  - SANS Top 20
  - Council for Cybersecurity CSC
- Updated from time-to-time
- 5 Tenets
  - Offense Informs Defense
  - Prioritization
  - Metrics
  - Continuous Diagnostics and Mitigation
  - Automation
- Very Dense
  - 1 CSC == *n* NIST SP 800-53 controls

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Critical Security Controls

- Top 5 “Cyber Hygiene”
  - Inventory of Authorized/Unauthorized Devices
  - Inventory of Authorized/Unauthorized Software
  - Secure configurations for hardware/software
  - Continuous Vulnerability Assessment and Remediation
  - Controlled use of administrative privileges
  - Can reduce cyber risk by 85%
- Addresses ~90% of HIPAA Security Rule (308,310,312)
  - Crosswalk CIS CSC to NIST CSF (CIS)
  - Crosswalk NIST CSF to HIPAA SR (DHHS)

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

1. Inventory of Authorized/Unauthorized Devices

- *Automated* asset inventory software
- DHCP Logging
- Equipment acquisition *automatically* updates inventory
- Inventory should include:
  - Address
  - Name
  - Purpose
  - Business Owner
  - Location
- 802.1x – Network Authentication
- Client Certificates - *

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

2. Inventory of Authorized/Unauthorized Software

- Create a list of approved software
- Whitelist applications
- Deploy software inventory tools
- “Sandbox” risky applications - *

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

3. Secure Configurations for Hardware/Software

- Establish standard secure OS configurations
- Strict configuration management
- Secure storage of OS images
- Use secure channels for remote management
- File Integrity Checkers
- *Automated* configuration monitoring
- *Automated* configuration management

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

4. Continuous Vulnerability Assessment and Remediation

- *Automated* vulnerability scanning
- Correlate information
- Perform authenticated scans
- Subscribe to threat intelligence feeds
- *Automated* patch management
- *Monitor* scan logs
- Compare back-to-back scans
- *Prioritize* (risk-rate) vulnerabilities

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

5. Controlled Use of Administrative Privileges

- Use only when required
- *Automated* inventory of admin accounts
- Eradicate default credentials
- Generate alert when changes to admin group
- Generate alert for failed admin login
- Multi-factor authentication or long passwords
- Admins have two sets of credentials
- Dedicated machine for administrative tasks - *

© 2017 Carnegie Mellon University

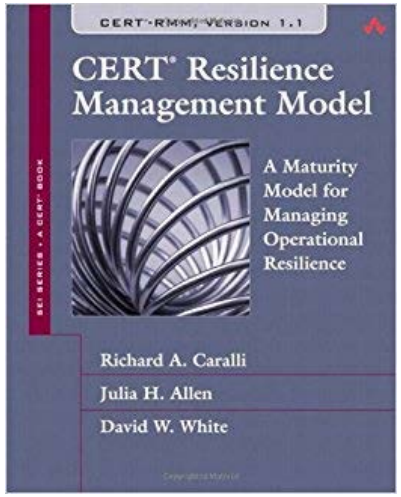
This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Cyber Resilience

- What makes a resilient system?
  - System remains viable and sustainable under stress
- How do we address resilience?
  - Protection and Sustainment Requirements
  - Often expressed as:
    - Confidentiality
    - Integrity
    - Availability
- How do you know if you're resilient?

© 2017 Carnegie Mellon University
This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

CERT-RMM - Resilience Management Model



- Process Improvement approach to Operational Resilience
- More than a decade of research
- 26 Process Areas across the Enterprise
- Efficiency!!!
- Three Advantages
  - Convergence Advantage
  - The Process Advantage
  - The Maturity Advantage

© 2017 Carnegie Mellon University
This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

CRR - Cyber Resilience Review

- Derived from CERT-RMM
- 1-Day Facilitated Assessment or Self-Assessment
- Evaluates Maturity of Operational Resilience
  - 5 Levels
    - Performed
    - Planned
    - Managed
    - Measured
    - Defined

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

CRR - Cyber Resilience Review

- Not an ***audit!!!***
- Protected Critical Infrastructure Information
- Protected from:
  - FOIA requests
  - SLTT Disclosure Laws
  - Regulatory Action
  - Civil Litigation
- 10 Domains
  - Asset Management
  - Controls Management
  - Vulnerability Management
  - Incident Management
  - Risk Management
  - Config and Change Management
  - Service Continuity Management
  - External Dependency Management
  - Training and Awareness
  - Situational Awareness

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

CRR - Cyber Resilience Review

1. Asset Management

Save

The purpose of Asset Management is to identify, document, and manage assets during their life cycle to ensure sustained productivity support critical services.

Goal 1 - Services are identified and prioritized.

	Yes	Incomplete	No
1. Are services identified? [SC:SG2.SP1]	○	○	○
2. Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	○	○	○
3. Is the organization's mission, vision, values and purpose, including the organization's place in critical infrastructure, identified and communicated? [EF:SG1.SP1]	○	○	○
4. Are the organization's mission objectives and activities prioritized? [EF:SG1.SP3]	○	○	○

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

CRR - Cyber Resilience Review

Goal 1 - Services are identified and prioritized.

	Yes	Incomplete	No
1. Are services identified? [SC:SG2.SP1]	○	○	○

Question Intent: *To determine if* ***services are identified.***

- *A* ***service is a set of activities*** *that the organization carries out in the* ***performance of a duty*** *or in the* ***production of a product.***
- ***Services*** *can be* ***externally or internally focused. Examples can include:***
- *a customer-facing website such as an online payment system*
- *human resources transactions*
- *A fundamental operational resilience objective is to* ***focus on activities to protect and sustain the identified services and assets*** *that most directly affect the organization's ability to achieve its mission.*

Criteria for "Yes" Response:

- *The organization has* ***identified all services.***

Criteria for "Incomplete" Response:

- ***The organization has identified some services.***

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

CRR - Report

CRR Performance Summary

Domain Summary	MIL-1 Performed Domain practices are being performed.	MIL-2 Planned: Domain practices are supported by planning, policy, stakeholders, and standards.	MIL-3 Managed: Domain practices are supported by governance and adequate resources.	MIL-4 Measured: Domain practices are supported by measurement, monitoring, and executive oversight.	MIL-5 Defined: Domain practices are supported by enterprise standardization and analysis of lessons learned.
Asset Management	G1 G2 G3 G4 G5 G6 G7	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3	Q1 Q2
Controls Management	G1 G2 G3 G4	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3	Q1 Q2
Configuration and Change Management	G1 G2 G3	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3	Q1 Q2
Vulnerability Management	G1 G2 G3 G4	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3	Q1 Q2
Incident Management	G1 G2 G3 G4 G5	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3	Q1 Q2
Service Continuity Management	G1 G2 G3 G4	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3	Q1 Q2
Risk Management	G1 G2 G3 G4 G5	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3	Q1 Q2
External Dependencies Management	G1 G2 G3 G4 G5	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3	Q1 Q2
Training and Awareness	G1 G2	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3	Q1 Q2
Situational Awareness	G1 G2 G3	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3	Q1 Q2

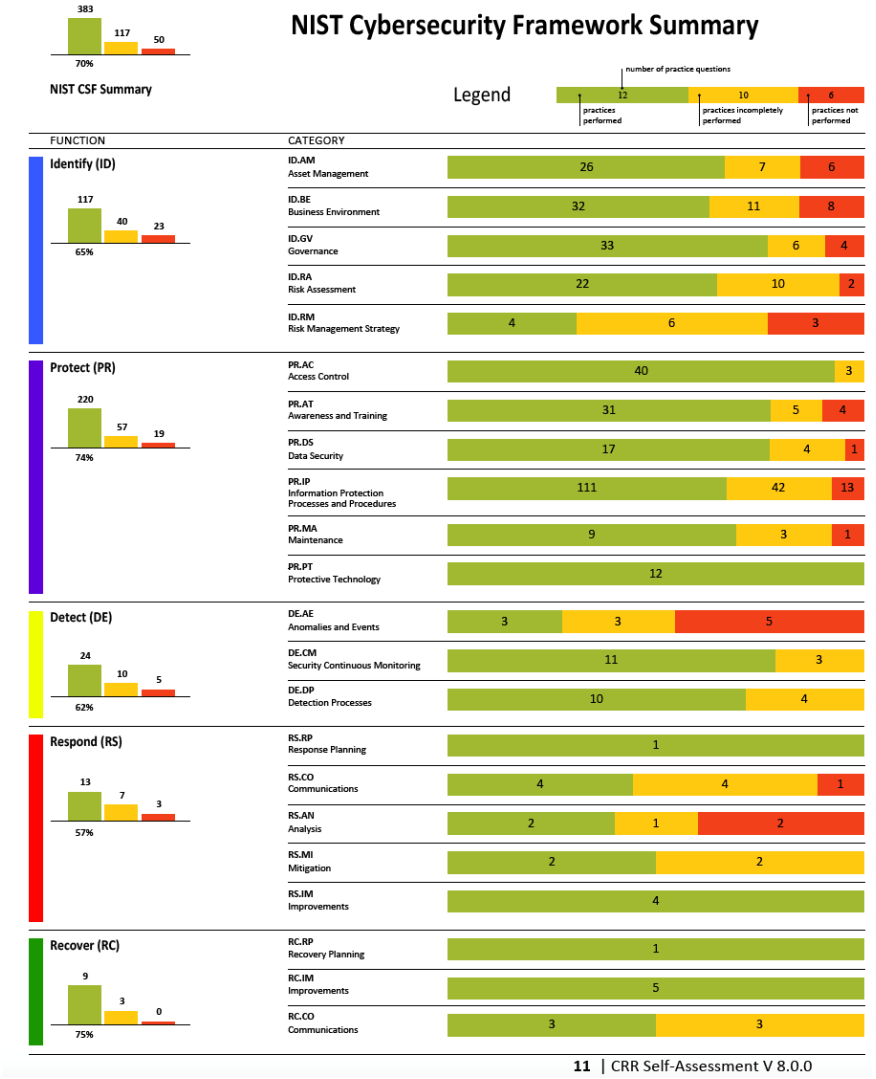
Legend = Performed = Incompletely Performed = Not Performed
Q1 = Question Number G1 = Goal Number

10 | CRR Self-Assessment V 8.0.0

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

CRR - Report



© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

CRR - Report

Goal 3-The relationship between assets and the services they support is established.		
1.	Are the associations between assets and the critical service they support documented? [ADM:SG2.SP1]	
	People	Yes
	Information	Incomplete
	Technology	Yes
	Facilities	Yes
2.	Are confidentiality, integrity, and availability requirements established for each service-related asset? [RRD:SG2.SP1]	
	People	Yes
	Information	Yes
	Technology	Yes
	Facilities	Yes
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[ADM:SG2.SP1]** Assign assets in the asset database to one or more services. The relationship between assets and the services they support must be understood in order to effectively develop, implement, and manage resilience strategies that support the accomplishment of the service's mission. **Additional References** Special Publication 800-18 Revision 1 "Guide for Developing Security Plans for Federal Information Systems", Page 21 NIST CSF References: ID.BE-4	
Q2	**CERT-RMM Reference** **[RRD:SG2.SP1]** Document confidentiality, integrity, and availability requirements for each service-related asset. The needs of the organization are satisfied by consistent and efficient performance of services. These services depend on the contributions and support of assets to meet their missions. Thus, the resilience of these assets is paramount to mission assurance. **Additional References** FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems, Page 2 NIST CSF References: ID.BE-5, ID.GV-3	

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

CRR – What Next?

- Most organizations are “immature”
  - Maturity Indicator Level of less than 1 across most domains
- “Where do we start?”
  - Let your risk analysis process guide you
- “Immature” Risk Analysis Process
  - Catalyst for Cyber Hygiene Practices

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Cyber Hygiene Practices

- Hygiene 1 – Identify and Prioritize Key Organizational Services, Products, and Their Supporting Assets
  - Establish Organizational Services (EF:SG1.SP3)
    - Business Services
    - Check your mission statement
  - Inventory Assets (ADM:SG1.SP1)
    - People
    - Technology
    - Information
    - Facilities

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Cyber Hygiene Practices

- Hygiene 2 – Identify, Prioritize, and Respond to Risks to the Organization's Key Services and Products
  - Establish Risk Measurement Criteria (RISK:SG2.SP2)
    - Patient Safety
    - Regulatory
    - Customer Satisfaction
    - Brand Damage
    - Etc.
  - Identify Service-Level Risks (RISK:SG3.SP2)
  - Evaluate Risks (RISK SG4.SP1)
  - Develop Risk Disposition Strategy (RISK:SG4.SP3)
  - Identify and Assess Risks Due to External Dependencies (EXD:SG2.SP1)
    - Their vulnerabilities are ***YOUR*** vulnerabilities

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Cyber Hygiene Practices

- Hygiene 3 – Establish an Incident Response Plan
  - Plan for Incident Management (IMC:SG1.SP1)
  - NIST 800-61
    - Prepare
    - Detection & Analysis
    - Containment, Eradication, & Recovery
    - Post Incident Activity

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Cyber Hygiene Practices

- Hygiene 4 – Conduct Cybersecurity Education and Awareness Activities
  - Establish Awareness Needs (OTA:SG1.SP1)
  - Perform Awareness Activities (OTA:SG2.SP1)
  - Establish Training Needs (OTA:SG3.SP1)
  - Deliver Training (OTA:SG4.SP1)

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

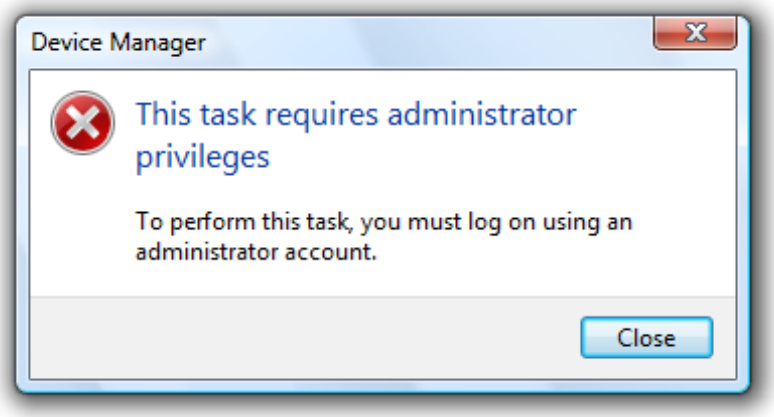
Cyber Hygiene Practices

- Hygiene 5 – Establish Network Security and Monitoring
  - Discover Vulnerabilities (VAR:SG2.SP2)
  - Analyze Vulnerabilities (VAR:SG2.SP3)
  - Perform Configuration Management (TM:SG4.SP2)
  - Perform Release Management (TM:SG4.SP4)
  - Establish Monitoring Requirements (MON:SG1.SP3)
  - Establish Collection Standards and Guidelines (MON:SG2.SP2)
  - Collect and Record Information (MON:SG2.SP3)

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Cyber Hygiene Practices



- Hygiene 6 – Control Access Based on Least Privilege and Maintain the User Access Accounts
  - Enable Access (AM:SG1.SP1)
  - Periodically Review and Maintain Access Privileges (AM:SG1.SP3)
  - Categorize Information Assets (KIM:SG1.SP2)
  - Control Access to Information Assets (KIM:SG4.SP2)

Security Principles

- Minimise Attack Surface Area
- Establish Secure Defaults
- Principle of Least Privilege
- Principle of Defence in Depth
- Fail Securely
- Separation of Duties
- Avoid Security by Obscurity
- Keep Security Simple
- Fix Security Issues Correctly

© 2017 Carnegie Mellon University
This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Cyber Hygiene Practices

- Hygiene 7 – Manage Technology Changes and Use Standardized Secure Configurations
  - Perform Configuration Management (TM:SG4.SP2)
  - Perform Change Control and Management (TM:SG4.SP3)
  - Perform Release Management (TM:SG4.SP4)

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Cyber Hygiene Practices

- Hygiene 8 – Implement Controls to Protect and Recover Data
  - Develop and Document Service Continuity Plans (SC:SG3.SP2)
  - Develop Testing Program and Standards (SC:SG5.SP1)
  - Exercise Plans (SC:SG5.SP3)
  - Measure the Effectiveness of the Plans in Operation (SC:SG6.SP2)
  - Control Access to Information Assets (KIM:SG4.SP2)
  - Control Modification of Information Assets (KIM:SG5.SP1)
  - Perform Information Duplication and Retention (KIM:SG6.SP1)
  - Perform Planning to Sustain Technology Assets (TM:SG5.SP1)
  - Manage Technology Asset Maintenance (TM:SG5.SP2)

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Cyber Hygiene Practices

- Hygiene 9 – Prevent and Monitor Malware Exposures
  - Collect, Document, and Preserve Event Evidence (IMC:SG2.SP3)
  - Analyze and Triage Events (IMC:SG2.SP4)
  - Establish and Implement Controls (TM:SG2.SP2)
  - Establish Monitoring Requirements (MON:SG1.SP3)
  - Establish Collection Standards and Guidelines (MON:SG2.SP2)

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Cyber Hygiene Practices

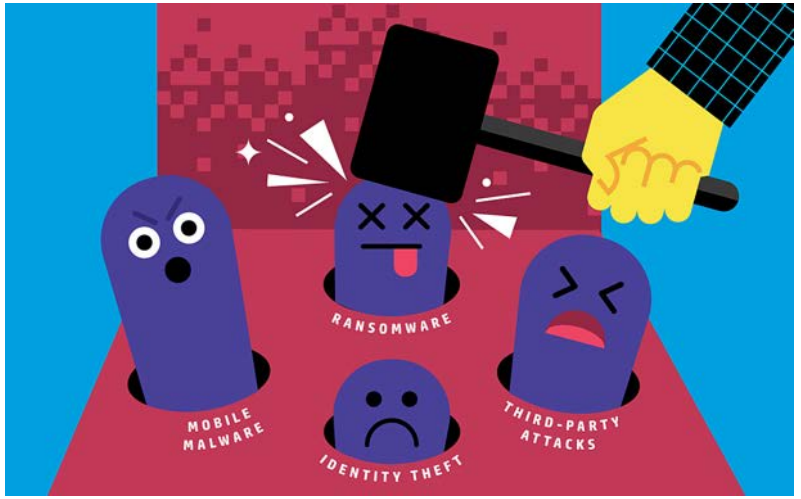
Hygiene 10 – Manage Cyber Risks Associated with Suppliers and External Dependencies

- Identify External Dependencies (EXD:SG1.SP1)
- Prioritize External Dependencies (EXD:SG1.SP2)
- Establish Resilience Specifications for External Dependencies (EXD:SG3.SP2)
- Monitor External Entity Performance (EXD:SG4.SP1)

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Cyber Hygiene Practices



- Hygiene 11 – Perform Cyber Threat and Vulnerability Monitoring and Remediation
  - Identify Sources of Vulnerability Information (VAR:SG2.SP1)
  - Discover Vulnerabilities (VAR:SG2.SP2)
  - Analyze Vulnerabilities (VAR:SG2.SP3)
  - Manage Exposure to Vulnerabilities (VAR:SG3.SP1)

© 2017 Carnegie Mellon University
This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

US-CERT CRR – How To Schedule?

- Visit the Critical Infrastructure Cyber Community Voluntary Program @ https://www.us-cert.gov/ccubedvp/assessments
- Review available information
- Contact CSE@hq.dhs.gov

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

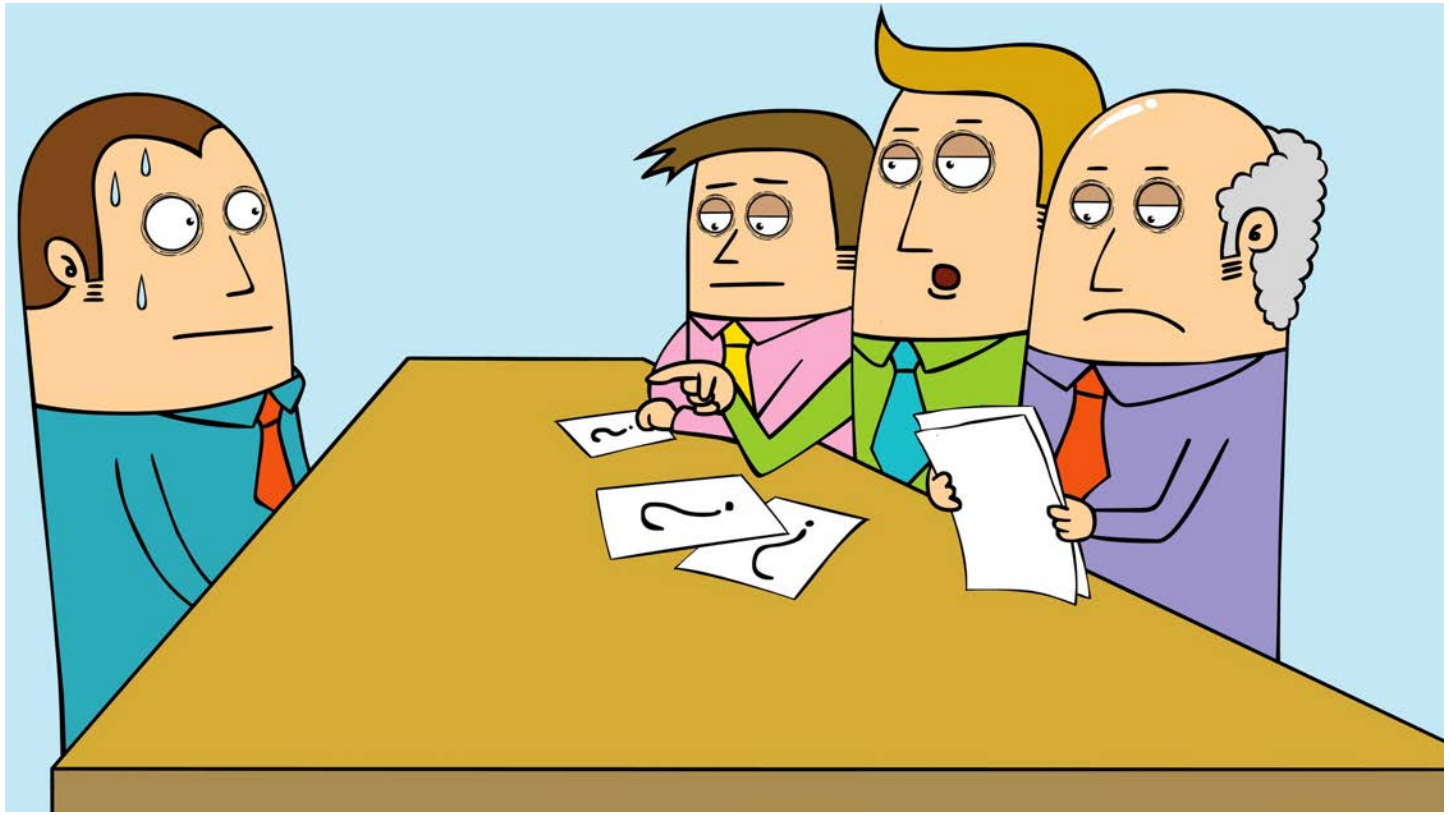
Summary

- The HIPAA Security Rule
- The Center for Internet Security
- Addressing the Security Rule with the CSC
- Measuring Your Security Program
- Cyber Hygiene Practices

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.

Thank You – Questions?



© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Please see Copyright notice for non-US Government use and distribution.