Cyber Hygiene: Why the Fundamentals Matter

Matthew Butkovic
Matt Trevors
Randall Trzeciak

CERT Division of the Software Engineering Institute
Cyber Risk and Resilience Directorate
VIDEO/Podcasts/vlogs This video and all related information and materials ("materials") are owned by Carnegie Mellon University. These materials are provided on an "as-is" "as available" basis without any warranties and solely for your personal viewing and use. You agree that Carnegie Mellon is not liable with respect to any materials received by you as a result of viewing the video, or using referenced web sites, and/or for any consequence or the use by you of such materials. By viewing, downloading and/or using this video and related materials, you agree that you have read and agree to our terms of use (http://www.sei.cmu.edu/legal/index.cfm).

DM19-1054
Contact Information

Matthew Butkovic
Director – Cyber Risk & Resilience Directorate
CERT Faculty – Heinz College MS Information Security, Policy & Management
mjb101@cert.org

Matthew Trevors
Technical Manager – Cyber Risk & Resilience Directorate; Cybersecurity Assurance Team
mtrevors@cert.org

Randall Trzeciak
Director – National Insider Threat Center
Program Director – Heinz College MS Information Security, Policy & Management
rft@cert.org

www.sei.cmu.edu
www.heinz.cmu.edu
“Definition of Cyber Hygiene

Cyber hygiene is a reference to the practices and steps that users of computers and other devices take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted. Much like physical hygiene, cyber hygiene is regularly conducted to ward off natural deterioration and common threats.”

Hygiene as a Minimum Baseline
Hygiene Requires Institutionalization

The study, by researchers at the University of NSW and the Clinical Excellence Commission, found that before the campaign, the hand hygiene compliance rate was only 30 per cent for doctors. It improved to 58 per cent by November, 2006, at the peak of the campaign, but dropped again to 39 per cent in July last year.

Operational Resilience Defined

**Resilience**: The physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit

[wordnet.princeton.edu]

**Operational resilience**: The emergent property of an organization that can continue to carry out its mission after disruption that does not exceed its operational limit [CERT-RMM]
CERT Resilience Management Model

Framework for managing and improving operational resilience

“...an extensive super-set of the things an organization could do to be more resilient.”

- CERT-RMM adopter

http://www.cert.org/resilience/
Core Principle and Focus of CERT-RMM

Premise at the core of CERT-RMM

The ability of the organization to sustain operations in the face of operational risk is highly influenced by the quality of the process used to ensure assets remain protected and sustained.

Focus of CERT-RMM

Transforming some (emergent) quality of the organization, called operational resilience, focuses on the processes or activities that support operational resilience management system.
<table>
<thead>
<tr>
<th>Engineering</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADM Asset Definition and Management</td>
<td>AM Access Management</td>
</tr>
<tr>
<td>CTRL Controls Management</td>
<td>EC Environmental Control</td>
</tr>
<tr>
<td>RRD Resilience Requirements Development</td>
<td>EXD External Dependencies Management</td>
</tr>
<tr>
<td>RRM Resilience Requirements Management</td>
<td>ID Identity Management</td>
</tr>
<tr>
<td>RTSE Resilient Technical Solution Engineering</td>
<td>IMC Incident Management and Control</td>
</tr>
<tr>
<td>SC Service Continuity</td>
<td>KIM Knowledge and Information Management</td>
</tr>
<tr>
<td></td>
<td>PM People Management</td>
</tr>
<tr>
<td></td>
<td>TM Technology Management</td>
</tr>
<tr>
<td></td>
<td>VAR Vulnerability Analysis and Resolution</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Management</td>
<td></td>
</tr>
<tr>
<td>COMM Communications</td>
<td></td>
</tr>
<tr>
<td>COMP Compliance</td>
<td></td>
</tr>
<tr>
<td>EF Enterprise Focus</td>
<td></td>
</tr>
<tr>
<td>FRM Financial Resource Management</td>
<td></td>
</tr>
<tr>
<td>HRM Human Resource Management</td>
<td></td>
</tr>
<tr>
<td>OTA Organizational Training and Awareness</td>
<td>OPD Organizational Process Definition</td>
</tr>
<tr>
<td>RISK Risk Management</td>
<td>OFP Organizational Process Focus</td>
</tr>
<tr>
<td>Process Management</td>
<td></td>
</tr>
<tr>
<td>MA Measurement and Analysis</td>
<td></td>
</tr>
<tr>
<td>MON Monitoring</td>
<td></td>
</tr>
<tr>
<td>OPD Organizational Process Definition</td>
<td></td>
</tr>
<tr>
<td>OPF Organizational Process Focus</td>
<td></td>
</tr>
</tbody>
</table>
Cyber Hygiene and RMM

• Minimum expected baseline of expected capabilities
• Contained within the Goals and Practices of RMM v1.2
• Aligned with other standards of practice (e.g., CIS Top 20, and NIST CSF)
• A total of 11 Goals and 43 Practices
• Ecosystem of related processes
• Measures the maturity (institutionalization) of the practices
Cyber Hygiene – A Baseline Set of Practices

Cybersecurity hygiene are practices that are used to manage 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.
10. Manage cyber risks associated with suppliers and external dependencies.
11. Perform cyber threat and vulnerability monitoring and remediation.

Sources:
- Center for Internet Security (CIS) aka SANS 20 – 20 Critical Security Controls
- Cybersecurity Framework – National Institute of Standards and Technology (NIST)
- Resilience Management Model – Carnegie Mellon University, Software Engineering Institute (SEI)
- UK Government Communications Headquarters (GCHQ) – 10 Steps to Cybersecurity
- European Union Agency for Network and Information Security (ENISA) – Whitepaper and Strategy
- Infosec Institute (Australia) – The Importance of Cyber Hygiene in Cyberspace
Cyber Hygiene Goal-1

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
Hygiene 2 – Identify, Prioritize, and Respond to Risks to the Organization’s Key Services and Products

- Establish Risk Measurement Criteria (RISK: SG2.SP2)
  - Physical 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
Cyber Hygiene Goal-3

- 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
Cyber Hygiene Goal-4

- 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)
Cyber Hygiene Goal-5

- 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)
Cyber Hygiene Goal-6

- Cyber Hygiene Goal-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)
Cyber Hygiene Goal-7

- 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)
Cyber Hygiene Goal-8

- 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)
Cyber Hygiene Goal-9

- **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)
Cyber Hygiene Goal-10

- 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)
Cyber Hygiene Goal-11

- 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)
Questions
Conquered Cyber Hygiene, What Next?

Review the SEI plan for improvement guide

Assess your policies, plans, processes, and procedures through a lightweight tool such as the Cyber Resilience Assessment

Determine your greatest needs and map out a plan to improve

- Consider using a maturity model for guidance
  - Progressing your capabilities (crawl -> walk -> jog -> run -> sprint)
  - Institutionalize your processes (write down what you do, do what you wrote down. Define policies, assign resources, etc.)
Resources

Software Engineering Institute Website:
https://www.sei.cmu.edu/

CERT Resilience Management Model
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084

Cyber Risk and Resilience Blog:
https://insights.sei.cmu.edu/

SEI Training
https://www.sei.cmu.edu/education-outreach/courses/index.cfm