MSS Lunch & Learn Series

YALE-MSS-2: System Inventory
YALE-MSS-3: Disaster Recovery (DR)
YALE-MSS-10: Network Exposure
YALE-MSS-12: Intrusion Detection

Aaron Wilkey
Tim Wright
James Tucciarone III
Jessica Flower

May 17, 2024
What are the MSS?

• The Minimum Security Standards (MSS) are baseline requirements for securing Yale IT Systems based on risk.

• The MSS apply to any Yale IT System that uses Yale data and/or operates in support of Yale’s mission.
Why do you we have the MSS?

"I keep our secure files in a coffee can buried behind the office. You can’t hack into that with a computer!"
What MSS will we review today?

- YALE-MSS-2: System Inventory
- YALE-MSS-3: Disaster Recovery (DR)
- YALE-MSS-10: Network Exposure
- YALE-MSS-12: Intrusion Detection
Yale-MSS-2: System Inventory

• Yale MSS 2.1: Establish the scope of the IT system
  • Describe/inventory all components of the system including hardware, software, and facilities.
  • Consider which systems/services are dependent on your system. (This may affect availability requirements)

• Yale MSS 2.2: Use a private IP address if direct Internet access is **not** required
  • Using a private IP address reduces the system’s attack surface
• REQUIRED FOR HIPAA

• Yale MSS 3.1: Create a disaster recovery (DR) plan
  • Make a step-by-step procedure to restore the IT system

• Yale MSS 3.2: Test the DR plan
  • Testing confirms your plan is complete and effective
Yale-MSS-10: Network Exposure

• Yale MSS 10.1: Enable ports, protocols, and services on an as needed basis
  • Enabling more than is needed adds additional risk

• Yale MSS 10.2: Configure host firewalls to deny all unsolicited inbound traffic by default
  • **Required for PCI**

• Yale MSS 10.3: Utilize host firewalls to control and log all inbound and outbound traffic
  • **Required for Moderate- or High-risk Internet Accessible servers or endpoints**
Yale-MSS-12: Intrusion Detection

- Yale MSS 12.1: Capture inbound and outbound network flow data
  - Required for Internet Accessible devices: Low-, Moderate-, and High-risk servers and network printers, and High-risk endpoints
  - Network flow data should contain a timestamp, IP addresses of source and destination, network protocol and port, duration of the flow, and number of bytes sent/received.
• Yale MSS 12.2: Utilize a network firewall to allow the least amount of access possible
  • Required for Low-, Moderate-, or High-risk Internet Accessible servers
• Yale MSS 12.3: Implement an intrusion detection and prevention system
  • Required for Moderate- or High-risk Internet Accessible servers
What is a SPA

• A SPA is used to:
  • Think through questions about how to meet and maintain the MSS for your IT system
  • Contribute to a registry of IT systems which is used for security testing
  • Identify and understand risk related to your IT system

• A SPA is not:
  • A detailed review of the security of an IT system
  • A statement of approval from the Information Security Office (ISO) about an IT system
Questions and Answers
Appendix
SPA at a Glance

**WHAT IS A SPA**

A SPA is used to:
- Think through questions about how to meet and maintain the MSS for your IT system
- Contribute to a registry of IT systems which is used for security testing
- Identify and understand risk related to your IT system

A SPA is not:
- A detailed review of the security of an IT system
- A statement of approval from the Information Security Office (ISO) about an IT system

**IMPORTANT LINKS**

- Risk Classification: [https://cybersecurity.yale.edu/risk-classification](https://cybersecurity.yale.edu/risk-classification)
- MSS Calculator: [https://cybersecurity.yale.edu/mss/calculator](https://cybersecurity.yale.edu/mss/calculator)
- Submitting a SPA: [https://cybersecurity.yale.edu/spa](https://cybersecurity.yale.edu/spa)
- Submitting an Exception Request: [https://cybersecurity.yale.edu/exception-request](https://cybersecurity.yale.edu/exception-request)