Defense Industrial Base (DIB) Sector Coordinating Council (SCC) Supply Chain Cyber Training

Cyber/Cybersecurity Maturity Model Certification (CMMC) v2.0

CyberAssist

Agenda

- Module 1: Cybersecurity: Why it is Important?
- Module 2: Cybersecurity Maturity Model Certification
- Module 3: Assessment Process - Interim
- Module 4: Incident Reporting
- Module 5: Cybersecurity Best Practices
- Module 6: Risk Management
- Resource Guide: Glossary, Acronym Guide and Resources for Additional Information
- CMMC Domains
- Survey

Cybersecurity Best Practices

Module 5

Disclaimer and Overview

Note: CMMC is still going through the rule-making process and certain aspects and requirements may change. Refer to the *Resources Guide* provided in this training for the most updated information.

- The intent of this training is to build awareness for Defense Industrial Base (DIB) suppliers of the likely requirements of the Cybersecurity Maturity Model Certification (CMMC) and their obligation to meet FAR 52.204-21 (basic cyber hygiene) and DFARS 252.204-7012 (specialized data handling and protection requirements).
- This training is self-paced and intended for a range of roles and responsibilities including, but not limited to, executives, project managers and technical staff from organizations seeking certification (OSC) and need to comply with CMMC. Currently, CMMC does not apply to any contractor.
- Note: Completion of this training DOES NOT certify your organization. This training is intended for the purposes of providing awareness of the subjects outlined above.
- The DIB Sector Coordinating Council (SCC) Supply Chain Task Force does not take responsibility for suppliers' certification by the CMMC 3rd Party Assessment Organization (C3PAO).
- This training focuses on U.S. regulations and industry best practices:
  - U.S. Department of Defense (DoD) Chief Information Officer (CIO) Cybersecurity Maturity Model Certification (CMMC) Information
  - National Institute of Standards & Technologies (NIST) publications
  - National Archives & Records Administration (NARA) definitions
  - DIB SCC Supply Chain Task Force – CyberAssist website

Module Topics and Objectives

Helpful Hint:
Refer to the Resource Guide for a Glossary and Acronym Guide

Topics covered in this module:

- The Importance of Cybersecurity Awareness
- Top 10 High Value Controls
- Threat Scenario Shop Floor Example
- Threat Scenario Example: Phishing
- Cyber Attacks: Types of Threat Actors
- Cyber Attack Methods and Mitigation

The objectives of this module are:

- Provide understanding of cybersecurity awareness;
- Identifies the top 10 high value controls;
- Provides a real-life scenario to help with understanding the threat; and
- Provide understanding of cyber attacks – threat actors, methods and mitigations.

A legend has been provided to assist with determining the content that you will need to know for each of the CMMC levels and what is additional content that will assist your organization with your cybersecurity posture. The corresponding symbol will be located at the top left corner of the slide.

Content Legend


= CMMC L1 Content


= CMMC L2 Content


= CMMC L3 Content


= Non-CMMC Content/Extra

CyberAssist

The Importance of Cybersecurity Awareness

Cybersecurity awareness is the process of learning and building knowledge about keeping IT resources secure by maintaining the confidentiality, integrity, and availability of those IT resources. Building the awareness and knowledge on how to protect those IT resources that store and process information from:

- **Threats:** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Source: NIST SP 800-30 Rev 1
- **Vulnerabilities:** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Source: NIST SP 800-30 Rev 1

Top 10 High Value Controls

The DIB SCC Task Force Working Group has prioritized a set of *Top 10 High Value Controls* that are separate from the CMMC domains but help facilitate many of the practices within CMMC.

Click on each of the controls to obtain additional information on the implementation and assessment of these controls.

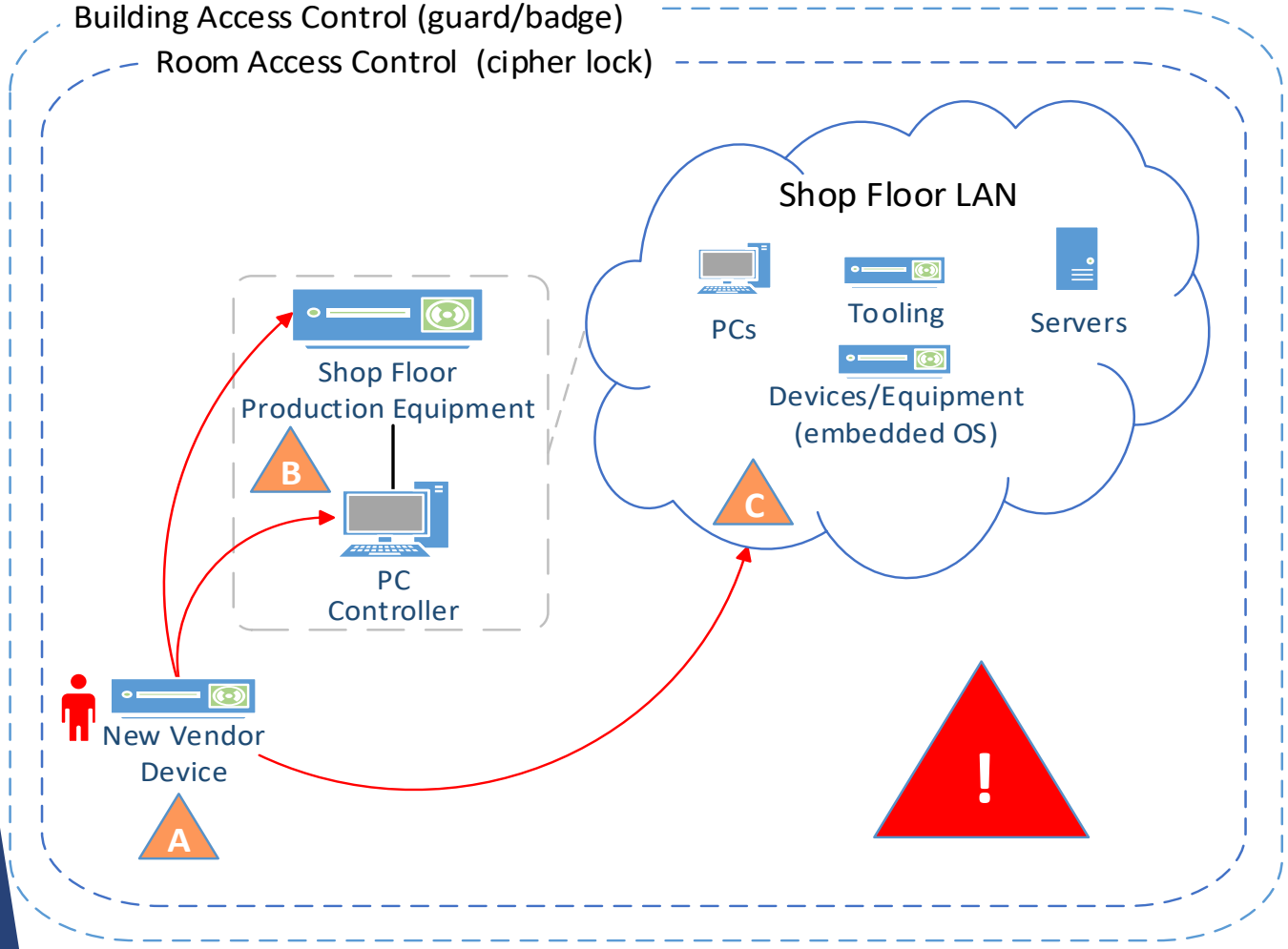
Next, we will present a threat scenario to help your understanding.

1. Administrative Rights and Privileges
2. Antivirus/Malware
3. Default Passwords
4. DNS Mitigations
5. Email Filtering
6. Employee Training and Awareness
7. Multi-Factor Authentication
8. Patching
9. Perimeter Hardening
10. Web Content Filtering

Source: https://ndisac.org/dibscc/implementation-and-assessment/top-10-high-value-controls/

Threat Scenario Example: Shop Floor

Note: This example is based on a real-world example TSMC outage/attack



A A company allows one of their vendors to introduce test, diagnostic, or new equipment directly into the production environment. The device contains software that spawns malicious processes (e.g., malware, ransomware).

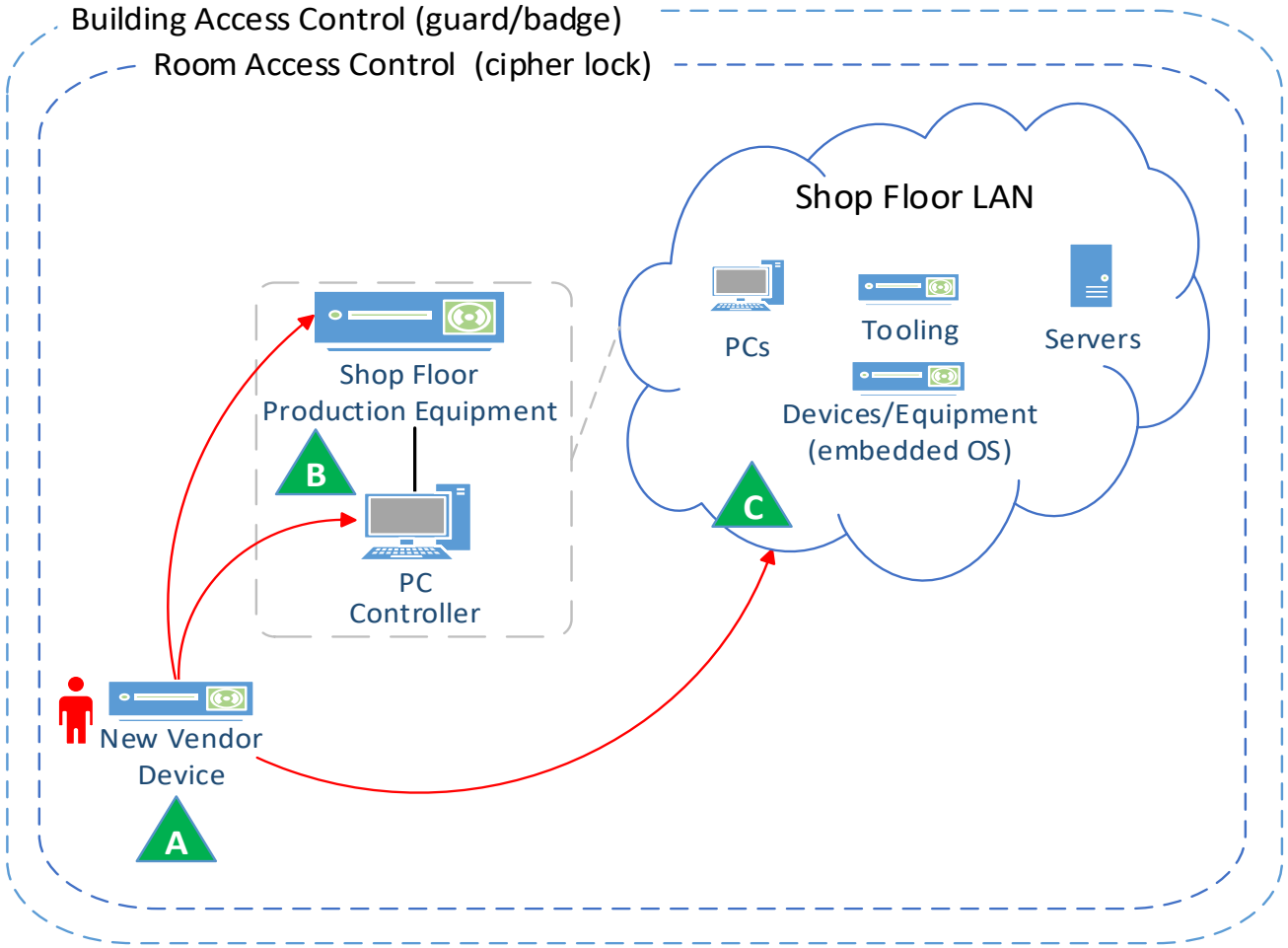
B Once the device is connected to a shop floor production device or PC, it scans the machine to determine if a vulnerable OS and patch level are present. If so, these devices are compromised and are used for further attack propagation.

C Compromised production device or PC is used to scan the entire local network (connected devices) to determine if additional vulnerable machines can be compromised. If so, they are compromised.

! Compromised devices are encrypted with adversary keys and are unusable. Equipment can no longer be operated, **production stops**!

CyberAssist

Threat Scenario Example: Shop Floor with Implemented CMMC Practices



A

Access Control

AC.L1-3.1.1 Limit information system access to authorized users, **processes acting on behalf of authorized users, or devices** (including other information systems).

A B C

System and Information Integrity

SI.L1-3.14.1 Identify, report, and correct system flaws in a timely manner (patch).

SI.L1-3.14.2 Provide protection from malicious code at designated locations within organizational information systems.

SI.L1-3.14.4 Update malicious code protection mechanisms when new releases are available.

SI.L1-3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

CyberAssist

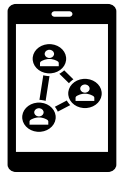
Threat Scenario Example: Phishing

Most cyber attacks will involve an element of social engineering in which the adversary attempts to use psychological manipulation to gain your trust and manipulate you into disclosing information or performing an action that could compromise security.

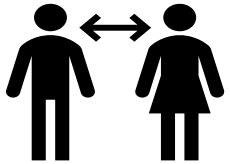
How can the threat actors initiate contact?

Email

Phone



Social Media & Text Messages



Face-to-face

What should you look out for?

- Requests to provide information or click on embedded links or attachments which could lead to legitimate-looking fraudulent websites that attempt to deceive you into entering information

Maintain a healthy level of skepticism and scrutinize all unexpected messages, even if they appear to come from someone you know.

Threat Actors Types

ROGUE ACTORS

- Anyone who developed hacking skills (student started hacking school computers and move on)
- Tools are becoming widely available

HACKTIVISTS

- Can be similar in expertise to rogue actors, or can bring more expertise… but **Organized around a cause**

INSIDER

- Authorized to access data… Partner with Intelligence organization to ID threats
- Could be a current or former employee, contractor, or business partner
- Exceeded or misused that access, either intentionally or unintentionally

ADVANCED PERSISTENT THREATS (APT)

BROADBASED & CRIMINAL

- **Organized criminals** seek to steal personal information, such as birthdates, social security numbers, and bank routing information, for financial gain
- **APT actors** aim to compromise information systems to conduct espionage, steal valuable intellectual property, destroy resources (such as data and infrastructure), and create back doors to maintain an ongoing connection to compromised systems

Cyber Attack Methods and Mitigation

Regardless of the exploit method an adversary uses, following some simple security practices will help you defend your company, your customers and yourself against their attacks.

- Secure and protect all IT assets and printed information.
- Do not open unexpected email, click on unexpected links or attachments, or reply to spam.
- Be mindful of what you share on social media and use privacy settings to restrict who can see it.
- Verify an individual's identity, authorization, and need to know before providing personal or company information.
- Be aware of your surroundings. Control line-of-site access and the volume of your voice/audio so that unauthorized people cannot view or hear information.
- Promptly report actual and suspected information protection and cybersecurity incidents.

Module Summary

- Using good cybersecurity practices not only helps protect your company from cyber attacks, but also your defense contractor customers
- Cybersecurity threats can come from inside or outside your company
- Being aware of threats and how to mitigate them keeps your business running
- Cybersecurity is about making sure that untampered data is available and accessible only to the people who require the data
- For questions on the content, please send them to DIB SCC Cyber Training.

Next: Module 6 – Risk Management