Basic Cyber Hygiene
(CMMC Level 1)
Learning Objectives

- The primary cyber threat to small businesses
- Role of National Institute of Standards and Technology - NIST
- Role of Cybersecurity Maturity Model Certification - CMMC
- Steps to reach CMMC Level 1 Maturity
The North Star CMM

CMMC

- Utilizes the collection of existing frameworks and standards
- Core programming built from Cybersecurity Maturity Model (CMMC) while also mapping to other frameworks
- Consists of 6 domains
  - Access Control
  - ID & Authentication
  - Media Protection
  - Systems & Information Integrity
  - System & Communication
  - Physical Protection

www.AmericasSBDC.org
www.AmericasSBDC-Resilience.org/Cyber/
The content and instruction in this presentation is meant as a guideline for you to define your cybersecurity practices.

It cannot prevent a breach on its own, nor will specific information about your company, your legal liability or your computing assets be addressed.

It is recommended you consult a Cybersecurity or IT specialist to address specific questions regarding your unique cybersecurity strategy.

It may also be advisable to seek legal assistance regarding questions of legal liability.
You Are A Target

- Have little to no cybersecurity protocols in place
- Have access to larger companies’ and government systems
- Have desirable data:
  - PII – Personal Identity Information
  - FCI – Federal Contract Information
  - PCI DSS – Credit Card Transaction Data
  - CUI – Controlled Unclassified Information
  - HIPPA – Medical Records and Related Data
NIST Cybersecurity Framework

Identify
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect
- Awareness Control
- Awareness & Training
- Data Security
- Info Protection & Procedures
- Maintenance
- Protective Technology

Detect
- Anomalies & Events
- Security Continuous Monitoring
- Detection Process

Respond
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover
- Recover Planning
- Improvements
- Communications
CMMC Level 1

Level 1 Maturity is accomplished by Performance – NOT documented processes – You must be capable of demonstrating intentional, consistent and auditable security actions.

You MUST go beyond a policy manual.

Most processes are doable in-house at minimal cost.

It may still be advisable to use a professional cybersecurity resource.
Access Control
CMMC AC.1.001 – Log In Credentials

Control:

“Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).”

- Determine who uses your systems and assign strong, individual passwords to each user – use dual authentication. Keep passwords secure (not written down) Ensure all employees are logging out or physically locking access while away

- Allow access without passwords, use common passwords, leave unattended computers logged in
CMMC AC.1.002 – Assign Permissions

Control:

“Limit information system access to the types of transactions and functions that authorized users are permitted to execute.”

Each user is assigned access based on permissions unique to their job function. Should apply to file use (sharing, copying, printing) as well as access.

All employees have the same access. Employees have “admin” level access at their desktop.
CMMC AC.1.003 – Exclusive Networks

Control:

“Verify and control/limit connections to and use of external information systems.”

Do not mix equipment or networks. Keep business and personal network equipment, computers and wi-fi connections separate.

Use a common, shared public network to access files. Allow personal devices to access business networks with federal contract information.
CMMC AC.1.004 – No Data Sharing

Control:

“Control information posted or processed on publicly accessible information systems.”

Cloud services and storage should have sharing turned off. Limited access with strong passwords should be in place.

Allow users to upload/download files through your website or directly to your cloud storage service with sharing enabled and/or a weak passwords.
Identification & Authentication
CMMC IA.1.076 – No Group Log Ins

Control:

“Identify information system users, processes acting on behalf of users, or devices.”

Assign individual accounts so access is maintained and can be monitored and traced at all times.

Share login credentials within a group to allow easier, faster access and provide freedom to access higher permissions.

www.AmericasSBDC.org/Cybersecurity
CMMC IA.1.077 – No Default Passwords

Control:

“Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.”

- All devices (desktop, mobile, IoT) require login credentials. PINs for phones and time-out settings should exist to prevent exposure using unattended devices.

- Keeping factory settings and passwords on networking and IoT devices.
CMMC MP.1.118 – Secure Trash

Control:

“Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.”

Discarded equipment should have hard drives and memory wiped, removed and destroyed (crushed, shredded, forensic overwrite) Also shred, destroy hard copies and removable data storage before discarding.

Donate or sell a computing device, copier or box of CDs. Allow someone to use removable data after it has had data deleted or throw away documents without shredding them.
Business Process – Paper(less) Flow

- Only print what is necessary and do not leave papers with confidential information lying around.
- If still filing paper in filing cabinets, make sure they are protected with a lock and key.
- Be aware of all personnel that has access to print confidential information and track where it is at all times.
- Arching is important, and digitally arching hard copies.
Physical Protection
CMMC PE.1.131 – Physical Security

Control:

“Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.”

- Physically secure equipment, files and network equipment especially when unattended. Determine what areas of your location(s) should be kept off limits to outsiders.

- Leave equipment rooms unlocked. Walk away from devices in public places.

www.AmericasSBDC.org/Cybersecurity
CMMC PE.1.132 – Track Visitors

Control:

“Escort visitors and monitor visitor activity.”

- Use sign-in procedures and make someone responsible for the movements of visitors and non-employees. Use badging and personal recognition to verify personnel movements.

- Permit non-employees to work unattended. Do not account for all persons who access sensitive areas of the building. Allow someone to work without a badge.

www.AmericasSBDC.org/Cybersecurity
CMMC PE.1.133 – Archive Access History

Control:

“Maintain audit logs of physical access.”

Maintain access logs for long-term auditing. Digitally record personnel movements if possible using cameras and/or key card access.

Discover unlocked access or missing equipment without any record of entry or exit.
CMMC PE.1.134 – Keys/Badges/Codes

Control:
“Control and manage physical access devices.”

Limit distribution of keys/codes/badges. Perform periodic inventory audits and collect all access devices upon exit interview.

Freely distribute the alarm codes to multiple employees. Leave locks unchanged after an employee termination.
System & Communication
CMMC SC.1.175 – Stay Behind Firewall

Control:

“Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.”

- Internal systems are kept “inside” the router/firewall and within a private network protected from outside/inbound internet traffic.

- Using wi-fi for external devices (or guests) and ethernet for internal devices thinking this keeps the two separate.
CMMC SC.1.176 – Diversify Web Access

Control:

“Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.”

Separate systems with internet access. Website server, internal server, security systems. Keep web connections unlinked.

Provide an open port to the internet from within your network for security cameras or VOIP phone access.

www.AmericasSBDC.org/Cybersecurity
Hardware Solutions

WiFi Routers:
- TP-Link
- Netgear
- Asus
- Linksys

VPNs:
- ExpressVPN
- Surfshark
- CyberGhost VPN

Physical Firewalls:
- Sophos
- Ubituiqi
- Watchguard

Two Factor Apps:
- LastPass
- Google Authenticator
- Microsoft Authenticator
System & Information Integrity
CMMC SI.1.210 – Stay Updated

Control:

“Identify, report, and correct information and information system flaws in a timely manner.”

- Allow auto updates and patches to all software and devices including peripherals. Remove any unused drivers, software and apps.
- Use unsupported software or refuse to allow legitimate updates when prompted.
CMMC SI.1.211 – Maintain Antivirus

Control:

“Provide protection from malicious code at appropriate locations within organizational information systems.”

Every device has industry standard antivirus loaded with auto update enabled. Include email filters and router traffic filters.

Allow users to disable antivirus or bypass updates. Don’t scan mobile storage devices connected to your systems.
CMMC SI.1.212 – Subscriptions

Control:
“Update malicious code protection mechanisms when new releases are available.”

- Regularly audit software subscriptions and periodically test each device to ensure it is able to connect and install updates. Maintain inventory of software licenses and their expiration dates.

- Forget to update the “road laptop” with the latest virus protection since it is not connected to the network regularly. Use public wi-fi instead of the company VPN and miss enterprise updates.
CMMC SI.1.213 – Full, Regular Scans

Control:

“Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.”

- Enable real-time malware scans and set a schedule for full-system scans at least weekly.
- Disable or skip full-system scans on mobile or desktop devices because it interferes with productivity.
Additional Recommendations
Employee Behavior – Training

Topics:
• New Threats
• Response Protocol
• Recent Breaches/Attempts
• Integration into all business operations

Methods:
• Lecture
• Email/Newsletter
• Test Phishing
• Employee Handbook
What Types of Backups Do You Do?

There are different types of backups and the level of sensitivity of the data and the importance of it, will dictate what type of backup up should run.

For Windows 8 or higher there is a file level backup called File History. For all businesses running macOS there is Time Machine.
Putting The Pieces Back Together

- Who are you going to call first?
- How do you ensure your actions will help your company prevent harm to its reputation?
- Have a response team within the company ready to go

Legal Responsibilities

In the event of breach your first call should likely be to legal support, an attorney with knowledge of breach response and remediation.

Managing Your Brand

- Keep the public informed
- Be timely, open, honest and accurate
Insurance as a Defense

First-Party Liability Coverage
Covers general cost incurred
- Legal fees
- Cost of notifying affected customers
- Forensics investigation costs
- Business interruption costs
- Public relations expenses
- Expenses to recover or restore lost data

Third-Party Liability Coverage
Covers defense costs if the affected parties seek legal action
- Payments to affected parties
- Cyber extortion costs
- Regulatory fines and penalties
- Settlements, damages & judgments
- Bookkeeping costs
- Cost to responding to regulatory inquires

America’s SBDC Partnership
America SBDC has partnered with insurance providers to offer a comprehensive cyber insurance policy for all SBDC clients.
Check out:
https://www.360coveragepros.com/sbdc

www.AmericasSBDC.org/Cybersecurity
General To Do’s...

- **Physical Control**
- **Stay Updated**
- **Remove unused applications and software**
- **Enable Password Protection**
- **Turn off Bluetooth & WiFi**
- **Use Encryption**
- **Understand what apps are using**
- **Watch auto-installs**
- **Configure your browser correctly**
General Do Not’s…

- Do NOT use public USB ports
- Do NOT use public WiFi
- Do NOT scan random QR codes
- Do NOT download apps from unknown sources
- Do NOT set laptop to auto-connect to networks
Additional Resources

Reach out to your local SBDC for further assistance.

Want More Material?

www.AmericasSBDC.org/Cybersecurity