Basic Cybersecurity Awareness
Protecting Critical Confidential Information

All businesses have critical confidential information

• Your own personal info
• Employees
• Clients
• Partners

Why It’s Important

• Protect business value
• Creating a competitive advantage
• Reputation protection
• Regulatory requirements

Culture Change

Process implementation, mostly no/low-cost adjustments for basic awareness (CMMC Level 1)
The North Star CMM

- Utilizes the collection of existing frameworks and standards
- Core programing 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/Cybersecurity
Primary Considerations

- **Identify**: What information to protect
- **Protect**: Systems and data
- **Detect**: Problems
- **Respond & Recover**: Have a plan ready

www.AmericasSBDC.org/Cybersecurity
Critical Confidential Information

What is Critical Information?
Who, What, When, Where, & How

Types of Data Classification
Restricted, Private, & Public

Critical Information Example
PII – Personal Identity Information
PCI DSS – Credit Card Transaction Data
PCI DSS – Credit Card Transaction Data

CUI – Controlled Unclassified Information
HIPPA – Medical Records and Related Data

www.AmericasSBDC.org/Cybersecurity
Critical Confidential Information

Limit the data you collect and only keep it as long as you need it

FCI – Federal Contract Information
HIPPA – Medical Records and Related Data

PCI DSS – Credit Card Transaction Data
Vulnerability

Malicious code is programming that purposefully creates an unauthorized function or process to negatively impact data confidentiality, integrity, or the availability of an information system.

Viruses
Programs designed to damage, steal information, change data, send email, show messages, or any combination of these

Spyware
Programs designed to gather a user’s information unknowingly and is usually installed without the user's knowledge.

Trojan Horse
Type of malware made to look like legitimate/real software and used by cyber criminals to get access to your systems.
Common Threats

- Employees
- Social Engineering
- Email Spoofing
- Phishing
- Ransomware
- Brute Force

www.AmericasSBDC.org/Cybersecurity
Access Control
Access Control

- Establish system access requirements
- Control internal system access
- Control remote system access
- Limit data access to authorized users and processes
CONTROL ACCESS TO COMPUTER RESOURCES

Control who can use company computers and who can log on to the company network (internal/external).

Limit the services and devices, like printers, that can be accessed by company computers.

Set up your systems so unauthorized users and devices cannot get on the company network.

Make sure to limit users/employees to only the systems, roles, or applications they are permitted to use and that are needed for their jobs.

www.AmericasSBDC.org/Cybersecurity
Control and Manage Connections

Control and manage connections between your company network and outside networks (public internet or neighboring wi-fi)

Control and limit access from personal devices (laptops, tablets, and phones)

Be aware of applications that can be run by external systems (print, voicemail)

Limit how and when your network is connected to outside systems

www.AmericasSBDC.org/Cybersecurity
Safeguard Sensitive Information

It is important to know which users/employees are allowed to publish information on publicly accessible systems, like a business website.

Limit and control information posted on the company’s web properties that can be accessed by the public.
Identification & Authentication
Identification & Authentication

- Identify all users on all systems
- Create ability to track users' access across network and devices
- Proper authentication is done when granting a user access to a system
- Use multi-factor authentication wherever possible.
Authenticate

Authentication helps you to know who is using or viewing your system

Make sure to assign individual, unique identifiers, like usernames, to all employees/users who access Company systems

Confirm the identities of users, processes, or devices before allowing them access to the Company’s information system-usually done through passwords
Media Protection
Media Protection

- Protect access to all media, both digital and non-digital
- Media includes internal/external hard drives, flash drives, disks, film, paper – anything containing PII
- All media is properly sanitized or disposed of
- Media should be tracked from user to user
Physical Protection
Physical Protection

- Protect physical access to all critical information systems
- Controls range from simple door locks to complex redundant infrastructures with guarded access.
- Facilities needing protection include, buildings, rooms, datacenters, offices, and file cabinets
CONTROL WHO HAS FACILITY ACCESS

- Do not allow visitors, even those people you know well, to walk around your facility without an escort.

- Make sure that all non-employees wear special visitor badges and/or are always escorted by an employee while on your property.

- Make sure you have a record of who is accessing both your facility (office, plant, factory, etc.) and your equipment.

- Have employees and visitors sign in and sign out as they enter and leave your physical space, and by keeping a record of who is coming and going from the facility.

www.AmericasSBDC.org/Cybersecurity
Physical Access Devices

Controlling physical access devices like locks, badging, key cards, etc. is just as important as monitoring and limiting who can physically access certain equipment.

Locks, badges, and key cards are only strong protection if you know who has them and what access they allow.
System & Communication
System & Communication

- Involves Physical and virtual controls protecting stored data and data in transit.
- Physically separate data from exposure to external networks.
- Data in transit can be encrypted and transmitted over virtual private networks.
- Creating boundaries with firewalls and restricted, monitored network access points.

www.AmericasSBDC.org/Cybersecurity
System & Communications Protection

Web Proxy

When an employee uses a company computer to go to a website, a web proxy makes the request on the user’s behalf, looks at the web request, and decides if it should let the employee go to the website.

Firewall

A firewall controls access from the inside and outside, protecting valuable information and resources stored on the company’s network. A firewall stops unwanted traffic on the internet from passing through an outside “fence” to the company’s networks and information systems.
Separate Publicly Accessible Systems

Separate publicly accessible systems from internal systems that need to be protected. Don't place internal systems on the same network as publicly accessible systems.

Demilitarized Zones (DMZ) - A DMZ is part of a network put in a “neutral zone” between an organization’s internal network (the protected side) and a larger network, like the internet.

Boundary Control Devices separate networks (i.e., routers, gateways, firewalls). This can also be done on a separated cloud network.

Physical separation might involve a separate network infrastructure, dedicated network equipment with separate LAN segments and a firewall between the internal network and the external network.
System & Information Integrity
Systems & Information Integrity

- Continuous monitoring for unusual activity, malware, and active attacks.
- Antivirus software, network monitoring services and regularly updating software and hardware
- Includes detecting and removing data abnormalities and responding in an appropriate and timely manner
- Reporting and correcting shortfalls within the security infrastructure

www.AmericasSBDC.org/Cybersecurity
Periodic scans check previously saved files against updated malware information.

Real-time scans will look at the system whenever new files are downloaded, opened, and saved.

Use anti-malware software to scan and identify viruses in your computer systems. Have a plan for how often scans are conducted.
Update

Protect a business by staying up to date on new security releases that stop malicious code and monitor the system regularly.

Malicious code is always changing, so it is important to always have up-to-date protections, such as anti-malware tools.
Update/Patch Management

All software and firmware have potential flaws. Many vendors work to reduce those flaws by releasing vulnerability information and updates to their software and firmware.

1. Purchase support from vendors to ensure timely access to updates.

2. Have a process to review relevant vendor newsletters with updates about common problems or weaknesses.

3. After reviewing the information, execute a process called patch management that allows for systems to be updated without adversely affecting the organization.

www.AmericasSBDC.org/Cybersecurity
Closing & Review
Other Important Information

Hiring Outside Help
- Forensic Investigators
- Attorney's

Social Media & Online Content

Things That Get Overlooked
- Hardware - POS, Copiers, Printers, IoT
- Low-Tech - Paper, Trash Cans, In-baskets
- Mobile Tech - Thumb Drives, Cell Phones
- Testing - Backups, Users

Cyber Liability Insurance
(First Party vs. Third Party)

www.AmericasSBDC.org/Cybersecurity
Make Mitigation a Top Priority - Employees

Cybersecurity Policies (employees, vendors, customers, onboarding, ongoing)
  - Password Usage (Pass Phrase, login attempt limits), Internet Usage, Incident Response

Control Access (Authentication, Role Assignments, Monitoring)

Monitoring Remote Access (Inbound/Outbound)

Tracking Digital Assets (Portable Media, Systems, Access Devices)

Learning & Training

Managing Personal Devices

www.AmericasSBDC.org/Cybersecurity
Thank You!