Understanding the Security Landscape and Cybersecurity

Maggie Glover

CEO, Excellence in Measurement Technology, LLC

High Maturity Lead Appraiser, ISO 27001 Lead Auditor, Certified Cloud Security

247 Deming St, South Windsor, CT

Excellence in Measurement Technology

Your Speaker

Margaret Tanner Glover: Former Captain, USAF

Undergrad: University of Connecticut: Pre-Med

Graduate: Webster U: Management Information Systems

High Maturity CMMI Lead Appraiser

CMMI Foundations Instructor/DEV and SVC

CMMI High Maturity Instructor

Scaled Agile Framework Program Manager

Certified Scrum Master, Product Owner

Certified Cloud Security Knowledge

ISO 27001, 9001 Lead Auditor

CMMC Provisional Assessor #46

CMMC Provisional Instructor

Understanding Requirements: the Need for Cyber Security

The Digital Threat

207 days is the average time it took, in 2020, for organizations to discover that they were breached. What's most troubling about this 207 days, in 2018, that number was about 170 days.

What is Cybersecurity?

The Cybersecurity & Infrastructure Security Agency (CISA) provides this definition: “Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information” (Department of Homeland Security, 2019)

So, what is cybersecurity actually?

"The state of being protected against criminal or unauthorized use of electronic data or measures taken to achieve this particular state."

Why is there a need for Cyber Security?

The DoD estimates over $700 billion dollars in loss related to cyber security / poor cyber hygiene

Key Terms

Data: Information that's stored in or used by a device

Networks: Groups or systems of interconnected devices

Devices: Physical hardware that process and store data

Data: What type of data needs protecting?

When you visit a website on the internet, you're using your device that can store and process data.....

To access another device called a web server.....which can also store and process data.

You are accessing this data on that webserver using a bunch of connected networks that allow data to move from place to place.

...This includes your own network at home and at work.

Networks: When data moves, it generally moves from one network to another. How does your data move from one place to another all the way and how to understand basic monitoring and analysis techniques.

Wireless, the IOT.

VPNs: Internet service providers, hacker and other can collect a treasure trove of use data. VPNs can offer more privacy.. Sometimes.

To use a VPN, you download an app, fire it up. The app creates a private channel over the open web, it encrypts your data, it masks your IP address.

VPNs can block you from malware, viruses, and worms.

Malware is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy.

The Best VPN I have found so far.

Bitdefender Home Solutions

Home / Solutions / Bitdefender Digital Identity Protection /

Bitdefender Digital Identity Protection

Have you been exposed? →

Keep your identity safe against the rising tide of data breaches

Bitdefender Digital Identity Protection scans the web for unauthorized leaks of your personal data, monitoring if your accounts are exposed and making it easy to take action well before disaster strikes.
Take control of your online privacy, starting now.

Choose Your Plan

56% Discount

30-Day Money-Back Guarantee

What type of data needs protecting?

Personal Data- examples

Your data that is shared with your bank, your school, your place of work, your family.

- Personal Identity
- Purchase history
- Location history
- Search history
- Facial recognition

Amazon, Google, Facebook (Meta), Apple, Instagram, Banking data, Store membership, Health data, TikTok

Devices: physical devices or hardware that process data, i.e. phones, laptops, tablets (known as endpoints). These can be an open door if you don't have internet security.

Endpoint security is **the practice of securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns**. Endpoint security systems protect these endpoints on a network or in the cloud from cybersecurity threats.

Protecting the data in an Organization

Confidentiality, Integrity, Availability, this must be the goal of any organization.

The CIA Triad

The founding principles of cybersecurity are:

Confidentiality: Data is only available to authorized parties.

- Example: Encryption/Authentication

Integrity: The certainty that the data is not tampered with or degraded.

- Example: Hashing

Availability: The information is available to authorized users when it is needed.

- Example: Redundancy

Why is there a need for Cyber Security?

Almost every organization processes Personally Identifiable Information (PII).

- The quantity and types of PII processed is increasing, as is the number of situations where an organization needs to cooperate with other organizations regarding the processing of PII.
- Protection of **privacy** in the context of the processing of PII is a societal need, as well as the topic of dedicated legislation and/or regulation all over the world.

Why is there a need for Cyber Security?

Almost every organization processes Personally Identifiable Information (PII).

- The quantity and types of PII processed is increasing, as is the number of situations where an organization needs to cooperate with other organizations regarding the processing of PII.
- Protection of **privacy** in the context of the processing of PII is a societal need, as well as the topic of dedicated legislation and/or regulation all over the world.
- A word about PASSWORDS

Scammers are on the rise

- Grandma calls
- Car insurance is running out
- This is your bank. We want to send you money but need your bank account and authorization.
- Phishing
- You have won a prize, click on this to win
- This amazon order is almost complete
- Online dating scams
- Public Wi-Fi.

Why is there a need for Cyber Security?

Today's organizations are facing more distributed teams at a time of increased security threats and reduced IT and security staffing.

This year, Gartner predicts that over half of US workers will be remote. At the same time, 61% percent of organizations experienced a jump of 25% or more in cyber threats or alerts since the start of COVID-19.

Security teams need an easier way to enforce security everywhere.

What about my business, do I need to worry?

Federal Contract Information (FCI) – information provided by or generated for the Government under contract not intended for public release.

Controlled Unclassified Information (CUI) – information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government wide policies.

What About My Business?

Do you use Controlled Unclassified Data?

https://www.archives.gov/cui/registry/category-list

Examples:

- Taxes
- Proprietary Business Information
- Procurement and Acquisition
- Nuclear
- Patent
- Defense
- Export Control
- Immigration
- Law Enforcement
- Legal

What are the Risks?

Risk and Opportunity Management

Risk: a potential uncertain event that may be harmful or may negatively impact be achieving objectives.

Risk and Opportunity Management

- Intent: **Identify, record, analyze** and **manage** potential risks or opportunities
- Value: **Mitigate** adverse impacts or **capitalize** on positive impacts to increase the likelihood of meeting objectives.

Safeguarding is key

A System Security Plan

Identifies all the functions and features of a system.

Identifies all the hardware and software installed on a system.

Defines the security measures that limit the access to unauthorized users.

It defines the training given to sys admins and other users on the secure use of a system.

It includes the details for auditing and maintaining the system and how to responds to security incidents that occur on the system.

Comprehensive summary of all security practices and policies that keep data secure.

Cybersecurity Maturity Certification (CMMC)

How We Prepare You for a CMMC Audit

Our compliance solution gets you prepared in 2 steps:

1. Assessment, SSP, & PO&AM

We perform a detailed assessment of your current network and compare it with the cyber security controls required in NIST 800-171. We prepare a System Security Plan (SSP) & Plan-of-Action & Milestones (PO&AM) providing documented evidence to the DoD or your Prime that you're on your way towards compliance.

2. Remediation

In this step, the items called out in the Plan-of-Action & Milestone (PO&AM) are addressed. Depending on the current state of your IT systems, this can be as simple as implementing multi-factor authentication and security awareness training or as complex as refreshing an entire aging infrastructure.

What are your business capabilities? Cybersecurity Maturity Model Certification

Table 1. CMMC Capabilities

Domain	Capability
Access Control (AC)	• Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes
Asset Management (AM)	• Identify and document assets
Audit and Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs
Awareness and Training (AT)	• Conduct security awareness activities • Conduct training
Configuration Management (CM)	• Establish configuration baselines • Perform configuration and change management
Identification and Authentication (IA)	• Grant access to authenticated entities
Incident Response (IR)	• Plan incident response • Detect and report events • Develop and implement a response to a declared incident • Perform post incident reviews • Test incident response
Maintenance (MA)	• Manage maintenance
Media Protection (MP)	• Identify and mark media • Protect and control media • Sanitize media • Protect media during transport
Personnel Security (PS)	• Screen personnel • Protect CUI during personnel actions
Physical Protection (PE)	• Limit physical access
Recovery (RE)	• Manage back-ups
Risk Management (RM)	• Identify and evaluate risk • Manage risk
Security Assessment (CA)	• Develop and manage a system security plan • Define and manage controls • Perform code reviews
Situational Awareness (SA)	• Implement threat monitoring
Systems and Communications Protection (SC)	• Define security requirements for systems and communications • Control communications at system boundaries
System and Information Integrity (SI)	• Identify and manage information system flaws • Identify malicious content • Perform network and system monitoring • Implement advanced email protections

What Can Your Organization Do?

Contact EMT for help with your security questions and concerns.

We can educate and inform you.

Excellence in Measurement Technology.com

Asset Management

Know what assets you have and where the data is!

Capabilities:

1. Identify and document assets
2. Manage Asset Inventory

servicenow ManageEngine asset panda solarwinds

Audit & Accountability

Define where data is and can be stored. Retain system, event, & access logs to assist in the ability audit this access.

Capabilities:

1. Define audit requirements
2. Perform auditing
3. Identify and protect audit information
4. Review and manage audit logs

splunk> EventTracker by Netsurion RAPID7 ALIEN VAULT

Awareness & Training

Ensure employees have the appropriate skills & knowledge.

Capabilities:

1. Conduct security awareness activities
2. Conduct training

CYBRARY CompTIA SANS INSTITUTE

Configuration Management

Standardize and manage system configurations.

Capabilities:

1. Establish configuration baselines
2. Perform configuration and change management

DoD CYBER EXCHANGE PUBLIC

CIS Hardened Images

puppet labs

PalletOps

Identification & Authentication

Ensure those who access the system are who they say they are and are properly authenticated.

Capabilities:

1. Grant access to authenticated entities

RSA yubico LastPass eset SECUREAUTH

Incident Response

Create an ability to respond and recover from an incident.

Capabilities:

1. Plan incident response
2. Detect and report events
3. Develop and implement a response to a declared incident
4. Perform post incident reviews
5. Test incident response

RSA NETWITNESS ORCHESTRATOR BUILT ON THREATCONNECT™ Exostar PolicyPro Forcepoint

Maintenance

Ensure systems are kept up to date (hardware, firmware, patches, etc.)

Capabilities:

1. Manage maintenance

Microsoft System Center Configuration Manager

WSUS

solarwinds

ManageEngine Patch Manager Plus

Media Protection

Define how media is stored, transported, and handled.

Capabilities:

1. Identify and mark media
2. Protect and control media
3. Sanitize media
4. Protect media during transport

Personnel Security

Establish a process that allows for thorough screening of each person accessing the system/data. This includes employees, subs, contractors, etc.

Capabilities:

1. Screen personnel
2. Protect CUI during personnel actions

Physical Protection

Ensure systems are protected from physical theft.

Capabilities:

1. Limit physical access

KeyWatcher®

Guidepost

KASTLE SYSTEMS

Recovery

Back-up data and ensure those back-ups remain available.

Capabilities:

1. Manage back-ups

R1Soft powered by continuum

solarwinds

Amazon Glacier

Risk Management

Assess risk of the system and effectiveness of the controls.

Capabilities:

1. Identify and evaluate risk
2. Manage risk
3. Manage supply chain risk

Security Assessment

Test, review, and update security controls (as needed).

Capabilities:

1. Develop and manage a system security plan
2. Define and manage controls
3. Perform code reviews

NIST Exostar PolicyPro Crucible FORTIFY

Situational Awareness

Maintain awareness of the threats to the environment.

Capabilities:

1. Implement threat monitoring

FireEye solarwinds SecurIT360 The physics of securing IT

Systems & Communications Protection

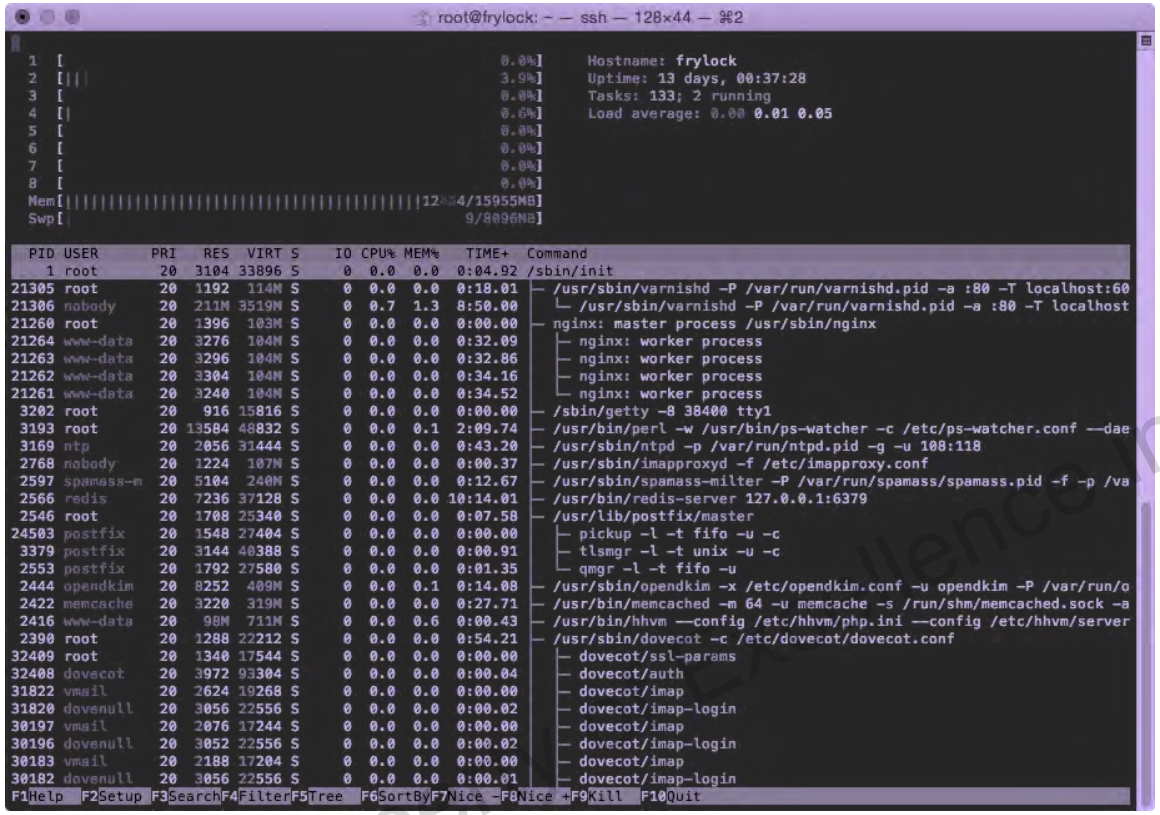
Protect data from unauthorized exposure.

Capabilities:

1. Define security requirements for systems and communications
2. Control communications at system boundaries

FORTINET CISCO Barracuda

System & Information Integrity



Ensure systems are trustworthy and have not been intentionally or accidently altered.

Capabilities:

1. Identify and manage information system flaws
2. Identify malicious content
3. Perform network and system monitoring
4. Implement advanced email protections

In Summary:

- Companies can leverage existing policies and procedures to get a jump start on compliance
- Leveraging existing frameworks, like CMMC, can assist a company understand the multi-tiered maturity levels
- Do not wait to get started. You must be certified before being allowed to bid on contracts
- Stand by for more clarity from the DoD and the CMMC Accreditation Board in the near future