Cybersecurity Gaps in Manufacturing

Who am I?

- Ryan Harvey, CMMC Registered Practitioner
- Cybersecurity Consultant at Winsor Consulting
- rharvey@winsorgroup.com
- www.winsorconsulting.com

Where did we get this information from?

- Winsor Consulting partnered with IMEC as part of their “Move Ahead Faster” program
- The data is compiled from 35+ Illinois manufacturers between the months of March and August 2021.
- The control indicator (ex. AC.1.003) will be based on the most recent revision of CMMC which includes practices from NIST 800-171, NIST 800-53, ISO 27001, etc.

What is CMMC?

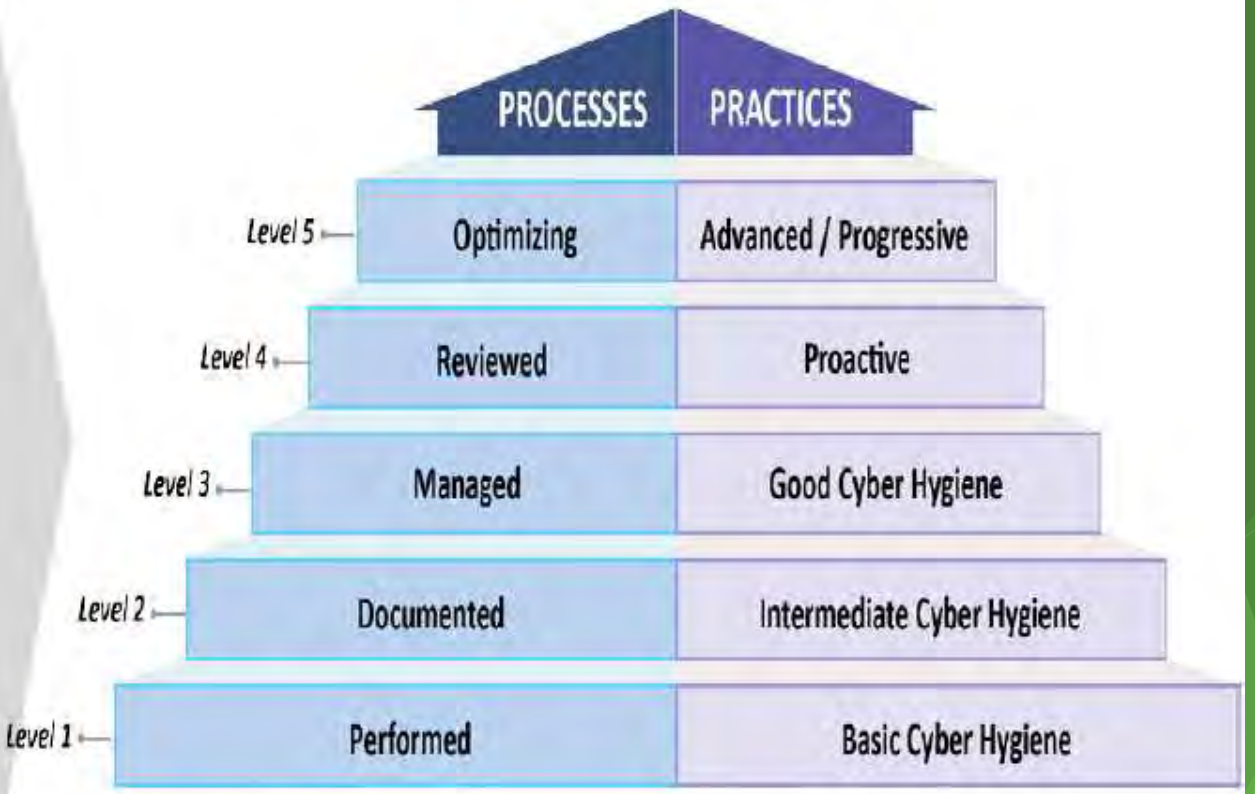
- CMMC stands for “Cybersecurity Maturity Model Certification”
- Version 1.02 was released on 3/20/20
- Includes 5 levels that range from "Basic Cybersecurity Hygiene" to "Advanced"
- The required minimum level to be listed on the RFP and used as a "go/no go decision"
- EVERY company performing work for the DoD or supply chain will be required to comply, even companies that do not handle CUI will require Level 1

Other Cybersecurity Frameworks and Standards

- NIST CSF (Cybersecurity Framework)
- CIS (Center for Internet Security)
- NIST 800-171
- NIST 800-53
- ISO 27002

The Entire Maturity Model and Domains

Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)
Configuration Management (CM)	Physical Protection (PE)	System and Information Integrity (SI)
Identification and Authentication (IA)	Recovery (RE)	



Control 1 - AC.1.003

What does it say?

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

What does it mean?

Control/manage connections between your company network and outside networks. Organizational resources should be used for organizational tasks.

How do I apply it?

Implement and policy/procedure to control/manage network connections, as well as limiting personal devices from accessing company networks and information.

Control 2 - IA.1.076

What does it say?

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

What does it mean?

Make sure to assign individual, unique identifiers (e.g., user names) to all users and processes that access company systems.

How do I apply it?

Do not use shared accounts. Know who/what is logging in. Always use unique identifiers.

Control 3 - PE.1.131

What does it say?

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

What does it mean?

Designate public and private areas within the organization, where devices are only accessible to authorized personnel.

How do I apply it?

For those parts of your company to which you want only specific employees to have physical access, monitor or limit who can enter those spaces with badges, key cards, etc.

Control 4 - AT.2.056

What does it say?

"Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems."

What does it mean?

You need to train management, administrators, and end users alike to understand the security risks they face daily. Policies and procedures should be put in place and employees trained properly.

How do I apply it?

Create a security awareness and training program. The training should consist of preparing them for risks as a computer user, train users of policies and procedures, and make sure end users are aware of the reason behind said policies and procedures.

Control 5 - AU.2.044

What does it say?

“Review audit logs.”

What does it mean?

Have a place where logs are stored and can be reviewed regularly

How do I apply it?

Ensure that you review your audit logs.
Logs should be checked regularly.

Control 6 - MP.2.121

What does it say?

“Control the use of removable media on system components.”

What does it mean?

Any type of media storage that you can remove from your computer needs to be controlled: CDs, DVDs, USB drives.

How do I apply it?

Limit the use of removable media to the smallest number needed. Scan all removable media for viruses. Track removable media that you own and make sure you reuse and dispose of it properly.

Control 7 - RE.2.137

What does it say?

“Regularly perform and test data backups.”

What does it mean?

Regularly back up your data so you can recover it if there’s a hardware or software failure. Test the backups.

How do I apply it?

Schedule backups to run automatically or manually and then test it on a regular basis. Our recommendation is to constantly “test” the backups to confirm they are working, but once a year do a live test of your disaster recovery plan.

Control 8 - IA.3.083

What does it say?

“Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.”

What does it mean?

Passwords alone aren’t enough. Another factor is needed.

How do I apply it?

Implement an MFA solution for accounts that have elevated access and for outside network access. Although some users might complain, you can’t put MFA on too many things!

Control 9 - IR.2.092

What does it say?

"Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities."

What does it mean?

Have an incident response plan.

How do I apply it?

Develop an incident response plan. Make sure all employees have access and are trained in this plan (during the security awareness training or in a separate tabletop exercise)

Control 10 - RM.3.146

What does it say?

"Develop and implement risk mitigation plans."

What does it mean?

You'll need a strategy for mitigating risk.

How do I apply it?

Identify risks and have a response to each one. Develop a business impact analysis to assess all risks associated with your business and how you want to handle them. Note: Some companies can decide to accept some risks.

That’s all…for now.


ANY
QUESTIONS?
HOW?
WHEN?
WHAT?
WHERE?
When?
What?
Why?

How can we help?

Ryan Harvey
CMMC Registered Practitioner
Cybersecurity Consultant at Winsor Consulting
rharvey@winsorgroup.com
www.winsorconsulting.com

This can be a daunting task. Don’t go it alone.

Emily Lee will provide a copy of the slides from this presentation.