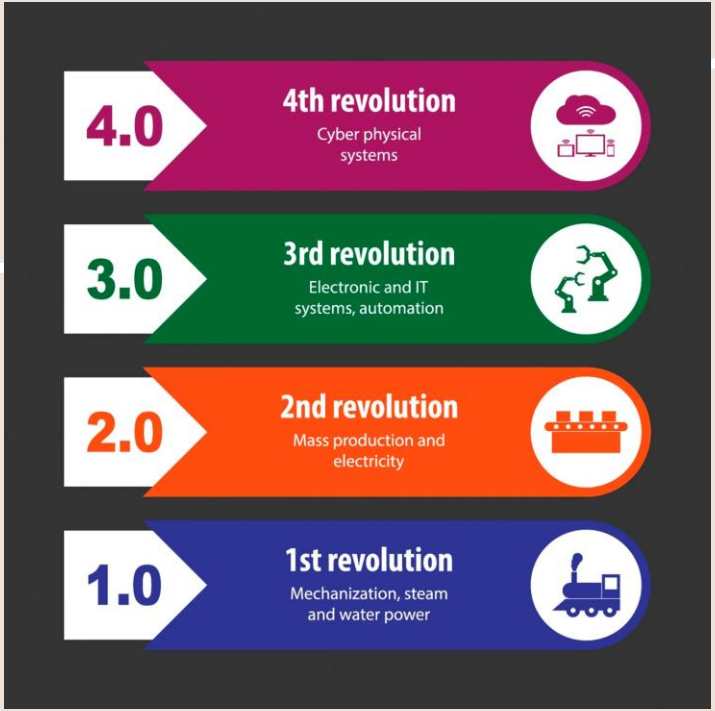
UCI SMART Industrial Assessment Center

Incorporating Cybersecurity Into Operations at Small and Medium Manufacturing Facilities

Akhil Pulianda

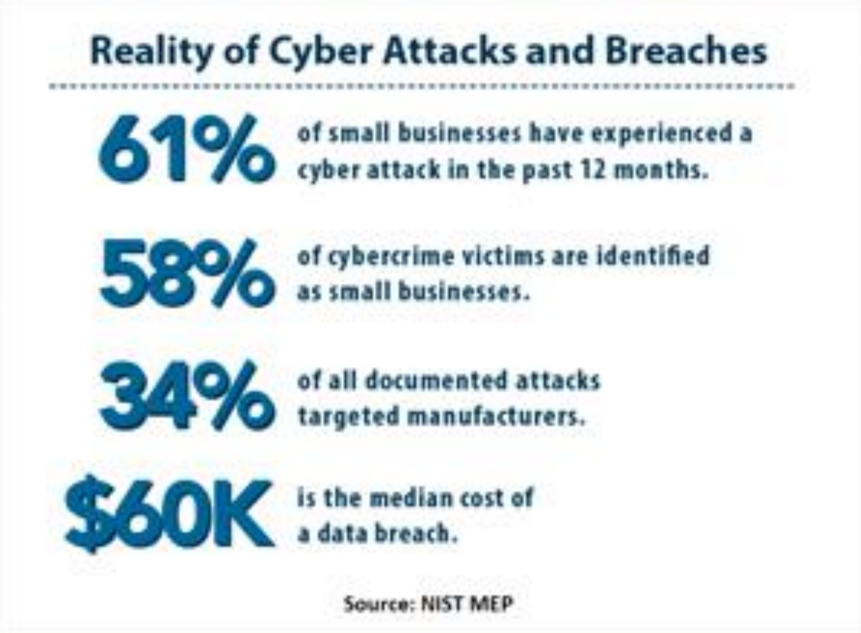
Introduction

- The Fourth Industrial Revolution (Industry 4.0)
- Connected manufacturing
- Why is cybersecurity so important?


4.0
4th revolution
Cyber physical systems
3.0
3rd revolution
Electronic and IT systems, automation
2.0
2nd revolution
Mass production and electricity
1.0
1st revolution
Mechanization, steam and water power

Reality of Cyber Attacks

- 50% increase in attacks from 2020
- 2nd most targeted industry
- SMMs can be at a greater risk



Reality of Cyber Attacks and Breaches

61% of small businesses have experienced a cyber attack in the past 12 months.

58% of cybercrime victims are identified as small businesses.

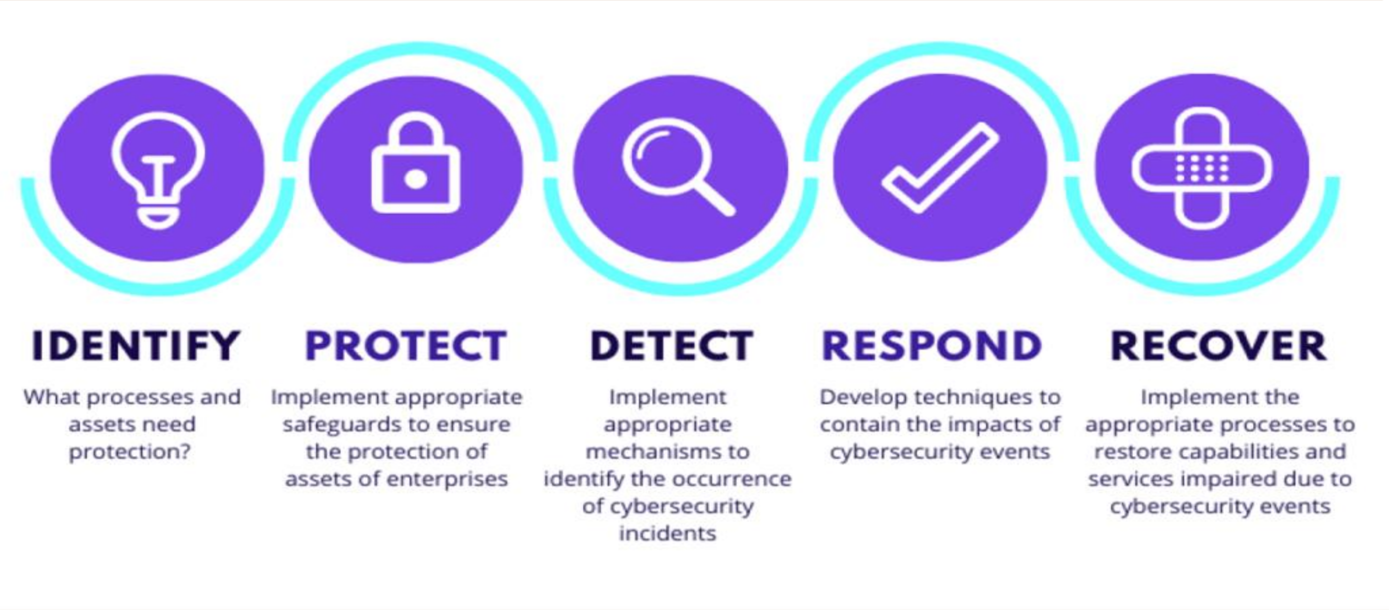
34% of all documented attacks targeted manufacturers.

$60K is the median cost of a data breach.

Source: NIST MEP

Implementation – NIST

- 5 Step Cybersecurity Framework



IDENTIFY

What processes and assets need protection?

PROTECT

Implement appropriate safeguards to ensure the protection of assets of enterprises

DETECT

Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents

RESPOND

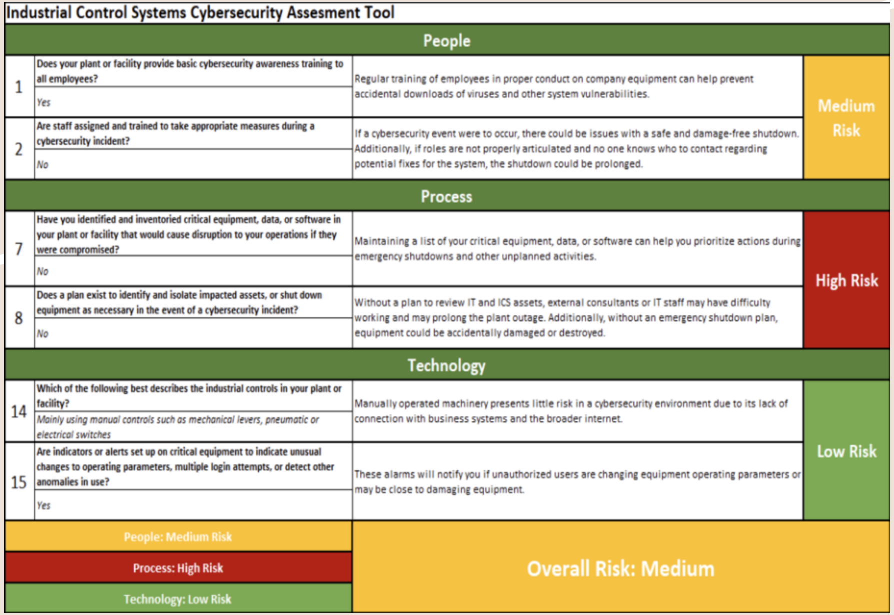
Develop techniques to contain the impacts of cybersecurity events

RECOVER

Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events

Implementation – IAC

- Cybersecurity Assessment Tool
  - Overview
  - Checklist
  - Action items
  - Key
- User Guide
- Additional Technical Resources



Industrial Control Systems Cybersecurity Assesment Tool			
	People		
1	**Does your plant or facility provide basic cybersecurity awareness training to all employees?** *Yes*	Regular training of employees in proper conduct on company equipment can help prevent accidental downloads of viruses and other system vulnerabilities.	Medium Risk
2	**Are staff assigned and trained to take appropriate measures during a cybersecurity incident?** *No*	If a cybersecurity event were to occur, there could be issues with a safe and damage-free shutdown. Additionally, if roles are not properly articulated and no one knows who to contact regarding potential fixes for the system, the shutdown could be prolonged.	
	Process		
7	**Have you identified and inventoried critical equipment, data, or software in your plant or facility that would cause disruption to your operations if they were compromised?** *No*	Maintaining a list of your critical equipment, data, or software can help you prioritize actions during emergency shutdowns and other unplanned activities.	High Risk
8	**Does a plan exist to identify and isolate impacted assets, or shut down equipment as necessary in the event of a cybersecurity incident?** *No*	Without a plan to review IT and ICS assets, external consultants or IT staff may have difficulty working and may prolong the plant outage. Additionally, without an emergency shutdown plan, equipment could be accidentally damaged or destroyed.	
	Technology		
14	**Which of the following best describes the industrial controls in your plant or facility?** *Mainly using manual controls such as mechanical levers, pneumatic or electrical switches*	Manually operated machinery presents little risk in a cybersecurity environment due to its lack of connection with business systems and the broader internet.	Low Risk
15	**Are indicators or alerts set up on critical equipment to indicate unusual changes to operating parameters, multiple login attempts, or detect other anomalies in use?** *Yes*	These alarms will notify you if unauthorized users are changing equipment operating parameters or may be close to damaging equipment.	
	People: Medium Risk	Overall Risk: Medium	
	Process: High Risk		
	Technology: Low Risk		