Manufacturing: Security Challenges

Introduction to the Manufacturing Industry

The manufacturing industry refers to the industry sector that processes new products. Manufacturing involves the mass production of items that involve technology, robotics, scientific processing, such as biological and chemical goods, through the means of machines and robots.

Well known manufacturing companies include Apple, which mass produces products such as iPhones, iPads, and Apple watches; Boeing, an airplane producer, and 3M that has produced multiple safety products.

Manufacturing, in a nutshell, is divided into two types:

- Process-based
  - Continuous manufacturing – phase based
  - Batch manufacturing – has distinct steps
- Discrete-based
  - It conducts a series of operations to create the end product

This industry has always been exposed to its surrounding environment but lacks sufficient layers of protection. Many manufacturers are restricted by security compliance, yet they still do not have a cybersecurity plan or process. For example, Executive Order 13636 was initiated to improve the critical infrastructure of the cybersecurity framework. The framework core is meant to identify, protect, detect, respond, and recover.

IEC 62443

The International Electro-Technical Committee (IEC) 62443 is entitled, "Security for Industrial Automation and Control Systems." It defines the compliance standards for manufacturing companies through the improvement of safety, availability, integrity, and confidentiality. IEC 62443 constructs a vector of seven foundational requirements and each requirement is given a value from 0 to 4. The higher the value the better the security.

The seven foundational requirements are:

- Identification and Authentication (IAC)
- Use Control (UC)
- System Integrity (SI)
- Data Confidentiality (DC)
- Restricted Data (RDF)

- Timely Response (TRE)
- Resource Availability (RA)

And the vector is formed as:

[IAC, UC, SI, DC, RDF, TRE, RA] which means that a basic level of security (low level) is [1, 1, 1, 1, 1, 1, 1].

Manufacturing Security Standards and Compliance

The National Institute of Standards and Technology promotes and maintains measurement standards.

Cybersecurity Framework Manufacturing Profile (from the NIST)

NIST's initiative is to promote a Cybersecurity Framework Manufacturing Profile. This provides companies with a Cybersecurity Framework and implementation details for the manufacturing environment. In turn, this reduces the cybersecurity risk for the company.

Executive Order 13636 was directed to have the cybersecurity framework become:

- Prioritized
- Flexible
- Repeatable
- Performance-based
- And cost-effective.

All of these are intended to manage the cybersecurity risk.

The purpose of the initiative is to create a target profile that focuses on cybersecurity outcomes so that manufacturers can compare their current profile against the target. The comparison identifies gaps so that manufacturers can perform "gap mitigation". Below is the NIST Cybersecurity Framework profile.

Manufacturing Security Issues

In 2016, the manufacturing industry was the second most attacked industry. Most likely because it's an expansive industry that includes automobiles, textiles and electronics.

The Industrial Control Systems (ICS) manage and monitor different aspects of production and have unique vulnerabilities. However, these ICS's are isolated systems meaning that there is no interface with the company's network to protect it, and these

systems are regulated against compliance standards. The result is a lack of security features, such as authentication and encryption. Employees either do not have passwords or passwords are not encrypted. Passwords might be shared and can be easily stolen from another employee.

Data Breaches in the Manufacturing Industry – History

In 2017, data breaches hit a record high – especially in the manufacturing industry. In the manufacturing industry alone there have been 620 separate data breaches, which is 40% of all data breaches in 2017 (1,579). This is because of the highly connected technology (e.g., robotics), which leads to high vulnerability. Below are a few examples of data breaches within manufacturing.

1. **LC Industries**
   In June 2015, hackers breached 3700 customer records to gather personal information.
2. **FACC**, an aircraft supplier
   In 2016, hackers posing as the FACC CEO were able to steal $54 million through email.
3. **HANESBRANDS**, an undergarment manufacturer
   In either June 2015 or July 2015, 900,000 customer records were hacked through a "guest account" on the website login page and they obtained data including phone numbers.
4. **FOXCONN**, an Apple manufacturer
   Hackers released sensitive data (including the usernames and passwords) from very large corporations.
5. **BOEING**, an airplane manufacturer
   36,000 Boeing employee records were emailed to contact(s) outside of the workplace
6. **DUPONT**, scientific research
   An ex-employee downloaded 40,000 sensitive files and delivered them to his new employer
7. **Royal Dutch Shell**, an oil and gas company
   They had sensitive data stolen from 176,000 employees.
8. **Apple**, a leading tech manufacturer
   “Keyraider” was able to obtain sensitive information for 225,000 iPhone users.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM

Function	Category	ID
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Links as references:

NIST (National Institute of Standards Technology) (9/8/17):
https://www.nist.gov/publications/cybersecurity-framework-manufacturing-profile

TrendMicro: (10/31/17)
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/taking-steps-towards-secure-manufacturing

IEC 62443:
https://ez.analog.com/b/engineerzone-spotlight/posts/iec-62443-series-of-cyber-security-standards-an-overview

Manufacturing Cyber Stats:
https://www.marshmma.com/blog/why-manufacturing-companies-are-now-more-susceptible-to-data-breaches

Manufacturing Industry Data Breach:
https://digitalguardian.com/blog/biggest-manufacturing-data-breaches-of-the-21-century