BATCH 1 - GROUP 5

Adesaanu Mujeeb

Gbadebo kehinde

Omobolaji Akeem

Samson Salimo

Salawudeen Zainab

POTENTIAL SECURITY RISK IN THE MANUFACTURING COMPANY

Manufacturing companies currently exist in a period of rapid change deemed the Fourth Industrial Revolution. Driven by technological innovation, this era represents unparalleled productivity and potential that includes not only multi-million dollar international industry leaders but also small and medium-sized businesses. This is because many implicated technologies do not require a significant financial investment.

While this offers many opportunities for manufacturers, their partners, and consumers to benefit from new technologies, it also comes with significant cybersecurity risks. Manufacturing is already a prime target for cybercriminals.

For the most part, cyber threats are broad and can affect the entire industry. Some technologies are prone to certain potential vulnerabilities, but it's more useful to consider that new technologies enhancing the manufacturing sector may also increase attack surfaces, providing more endpoints via which hackers can access systems.

Below are view severe cyber risks associated with manufacturing companies:

Assets	Threath	Likelihood	Impact	Risk	Justification
Employees' Record	Unauthorized Record	2	2	4	it is low because there is adquate security in the protection of employees' records
machine and Equipment	Machine and equipment Sabotage	2	2	4	it is low because There is implementation of security meesures, access control list and activity monitoring
Supply chain	Supply Chain Attack	2	2	4	it is low because There is implementation of security meesures like supply risk assessment and activity monitoring. Also emplyees are being trained in security awareness and best supply practices
Telecommunication	Telecommunication Risk	3	5	15	it is medium because Emplyees work from Home, thereby causing employees use personal devices for work purpose thereby making it more successptible to phising attacks and other types of cyber attack
Intellectual Property	Intellectual Property theft	5	7	35	This is very high because This is carried out by the employees and or insider who have access to the company network /system. once they accessed the network, they can steal data like valuable trade production secrets and an other sensitive information or plant malware to give them continued access to the company network
Data Spillage	Accidental Release of Sensitive information	2	2	4	this is low because data loss prevention and activity monitoring to avoid data leakage

Industrial control system (ICS	Ransomware	7	9	72	this is extremely high because these systems run outdated software with known vulnerabilities and lack modern and advanced cybersecurity defenses.

Legend:

1-3 => low

3-5 => medium

5-7 => high

7-9 => very high

>9 => extreme high

RISK MANAGEMENT STRATEGIES TO IN MANUFACTURING COMPANY

1. **UNAUTHORIZED RECORD:**

this is a common type of attack is the internal breach, in which an attacker gains access to a company network by exploiting vulnerabilities within the organization and have gain access to the employees record. in this case **RISK MITIGATION STRATEGY** would be employed As Companies must take measures to prevent data loss such as employees's bio-data loss prevention and activity monitoring. They must also provide staff training on security awareness and best practice

2 . **MACHINE AND EQUIPMENT SABOTAGE:**

Is a type of internal breach when an attacker physically damages equipment in order to disrupt operations. While this type of attack is less common than other cyber threats, it can be extremely damaging to a manufacturing company.

In order to protect against internal breaches **RISK MITIGATION STRATEGY** would be employed As this involved implementation of security measures to reduce the liklihood and impact

on the company. This measures may include: Access contro, activity monitoring, provision of training for employees on security measures awareness and best practices.

3. SUPPLY CHAIN ATTACKS

Supply chain attacks are a type of cyberattack in which an attacker targets a company's suppliers or other business partners. This can be done by compromising the systems of these third-party companies or by sending phishing emails to employees of these organizations. Once the attacker has gained access to the supplier's network, they can then launch attacks on the manufacturing company. This can include stealing data, planting malware, or disrupting operations.

to tackle this **RISK AVOIDANCE** would be employed which means Companies must take precautions to prevent attacks on their supply chains, such as supplier risk management and activity monitoring. Employees must also be trained in security awareness and best practices.

4. TELECOMMUTING RISKS

for example, The COVID-19 pandemic has forced many companies to allow their employees to work from home. While this arrangement has its benefits, it also creates new risks for companies.

For example, telecommuters may use personal devices for work purposes. This can create new vulnerabilities if these devices are not properly secured. Telecommuters may also be more susceptible to phishing attacks and other types of cyberattacks.

To protect against these risks, **CONTINUOUS MONITORING** would be employed continuously monitor and reassess risk and the need to stay updated with emerging threats and vulnerabilities. Also companies need to implement security measures such as device management and activity monitoring. They also need to provide training to employees on security awareness and best practices.

5. IP THEFT

Intellectual property theft is a serious problem for manufacturing companies. This is because these businesses often have valuable trade secrets and other types of sensitive information. In

many cases, IP theft is carried out by employees or other insiders who have access to the company network. In other cases, attackers may gain access to the network through social engineering or other means.

Once they have accessed the network, attackers can steal data or plant malware that gives them continued access to the company's systems. **RISK MITIGATION STRATEGY** would be employed As Companies must take measures to prevent IP theft, such as data loss prevention and activity monitoring. They must also provide staff training on security awareness and best practices.

6. DATA SPILLAGE

Data spillage is a type of data breach in which sensitive information is accidentally released. This can occur when an employee sends an email to the wrong person or posts confidential information on a public website. Data spillage can also occur when data storage devices are lost or stolen.

RISK AVOIDANCE would be employed as panies must implement security measures such as data loss prevention and activity monitoring to avoid data leakage. They must also provide staff with information on security awareness and best practices.

7. INDUSTRIAL CONTROL SYSTEM (ICS)

ICS are prime targets for ransomware due to their critical role in manufacturing operations. An attack can halt production, leading to significant financial losses, delayed orders, and potentially unsafe conditions. The manufacturing sector is increasingly targeted by ransomware actors, as these systems often run outdated software with known vulnerabilities and lack modern and advanced cybersecurity defenses. Ransomware can render the ICS inoperable until a ransom is paid, crippling the company's ability to function

CONTINOUS MONITORING would be employed as this involves continous monitoring and assesses risk and being updated with emerging threaths and vulnerabilities with the advanced cyber security defences.

CONCLUSION

Why Does Manufacturing Need Cyber Security?

As manufacturing increasingly moves towards Industry 4.0 and the Internet of Things, the need for **cyber security** is also on the rise. With interconnected systems and machines, there is a greater risk of cyber-attacks that can lead to production stoppages, data breaches, and financial losses. In fact, the manufacturing sector is now one of the most targeted industries for cybercriminals.

While **manufacturing companies** have traditionally been focused on physical security, they must now also invest in cyber security to protect their operations.

There are a number of reasons why manufacturing needs cyber security. These include the following:

- **To safeguard production**: Manufacturing companies rely on computer-controlled machinery and industrial control systems to operate. If these systems are breached, it can lead to Production Stoppage. This not only disrupts the manufacturing process but can also result in costly repairs.
- **To protect data and intellectual property**: Manufacturing companies often have a large amount of confidential data, such as customer information and product designs. If this data falls into the wrong hands, it could be used to competitive advantage or for other malicious purposes.
- **To avoid financial losses**: A cyber-attack can have a significant financial impact on a manufacturing company. Not only will there be the direct cost of repairs and lost production, but there may also be indirect costs such as loss of customer confidence and legal liabilities.
- **To safeguard against physical damage**: In some cases, a cyber-attack can lead to physical damage to machinery or other critical systems.