Using NIST ,ISO standards discuss potential cybersecurity risks faced in the manufacturing industry (data loss and systems downtime).

Here are the potential risks faced in data loss and systems downtime using the six core functions of cybersecurity:

1. \_Identify\_:

- identify sensitive data and systems

- Inadequate asset management

- Insufficient risk assessments

2. \_Protect\_:

- Inadequate access controls and authentication

- Insufficient data encryption

- Unpatched software vulnerabilities

- Poor network segmentation

3. \_Detect\_:

- Detect data breaches and system intrusions

- Inadequate monitoring and logging

- Insufficient incident response planning

4. \_Respond\_:

- Quick response to data breaches and system intrusions

- adequate incident response planning

- sufficient communication and coordination

5. \_Recover\_:

- adequate backups and disaster recovery plans

- sufficient data restoration capabilities

- system resilience and redundancy

6. \_Govern\_:

- adequate cybersecurity policies and procedures

- sufficient training and awareness

- Proper compliance with regulations and standards

Potential risks faced in data loss and systems downtime include:

- Data breaches and theft

- System intrusions and hacking

- Ransomware and malware attacks

- Hardware and software failures

- Human error and insider threats

- Natural disasters and physical damage

- Supply chain disruptions

By understanding these risks, organizations can take proactive measures to mitigate them and ensure the security and resilience of their data and systems.