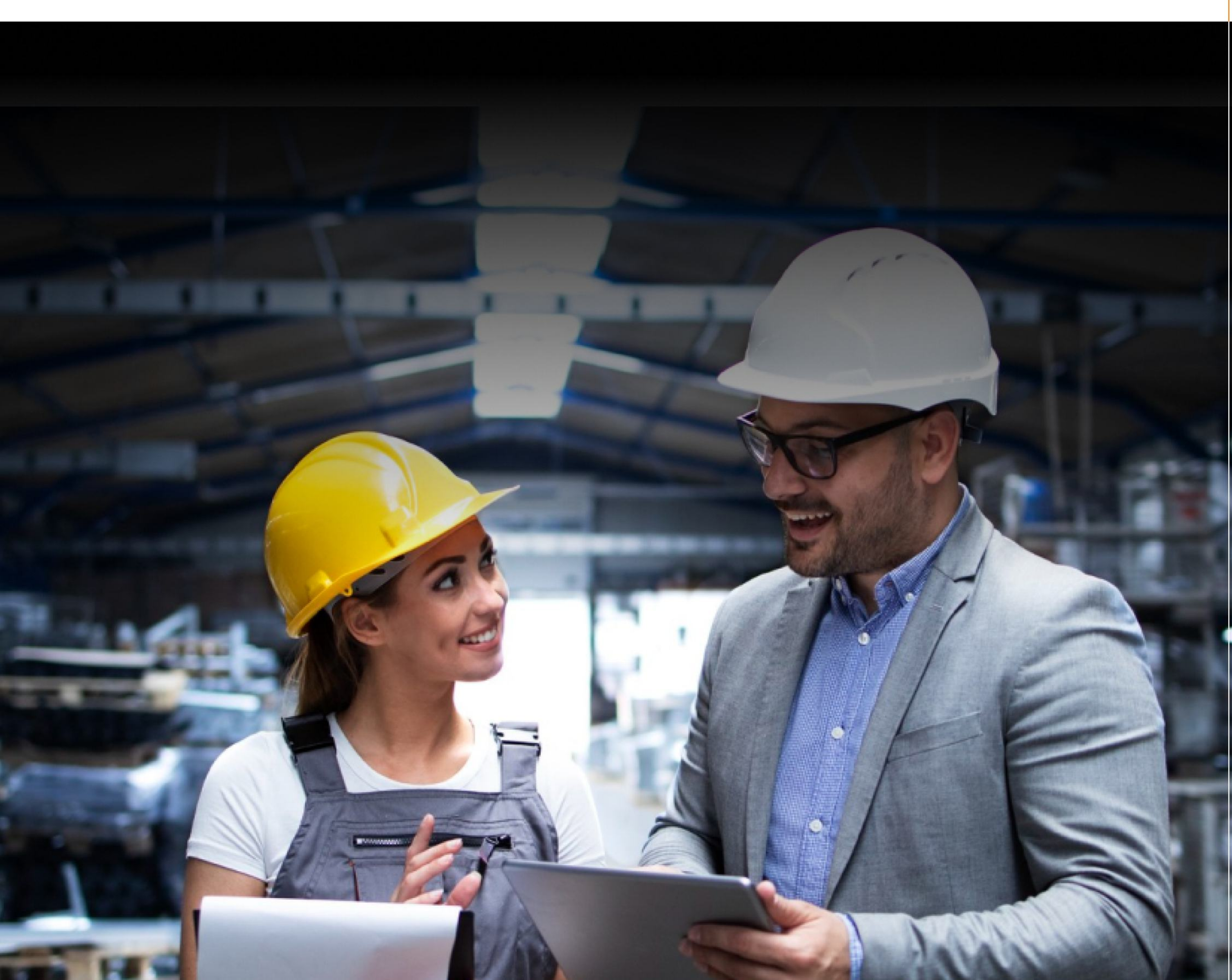
Trout

Cybersecurity Checklist for Small & Mid-Size Manufacturing: Safeguarding Infrastructure and Reducing Risk



Trout

Introduction

Purpose

This checklist is designed to assist C-suite leaders and IT teams in manufacturing facilities to implement essential security controls that safeguard their infrastructure and data. By following these recommendations, organizations can significantly reduce their risk of cyberattacks and data breaches.

Tiered Classification System

To cater to the varying levels of maturity within manufacturing organizations, we've categorized the recommendations into three tiers:

- Level 1 - Fundamentals: These are the basic security controls that every manufacturing organization should implement.
- Level 2 - Mature: These controls are more advanced and are recommended for organizations that have a solid security foundation.
- Level 3 - Advanced: These are highly specialized controls that are often required for organizations dealing with critical infrastructure or highly sensitive data.

01 Governance and Compliance

- [ ] **Create IT Security Policies:**

Fundamentals

Set up and keep updated IT security policies that explain how the organization manages and protects sensitive information and systems.

- [ ] **Compliance with Industry Standards**

Mature

Ensure that the security practices align with relevant industry standards (NIST 800-171) to foster a culture of compliance and accountability.

- [ ] **Regular Risk Assessments and Audits**

Conduct monthly risk assessments to identify potential vulnerabilities and threats.

Implement audits to evaluate adherence to security policies and procedures.

Fundamentals - yearly audit

Mature - quarterly audit

Advanced - monthly audit

Ref - https://www.cisecurity.org/controls/policy-templates

Ref - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

02 Asset Management

- [ ] **Build an Inventory of IT Assets:**

  Fundamentals

  Maintain an up-to-date inventory of all IT assets, including hardware, mobile assets and software, to ensure visibility and control over resources. Add information like mac address, Static IP or “DHCP”, location, owner.

- [ ] **Implement a process to regularly update the inventory**

  Fundamentals

  Set a reminder to check the inventory and update it with any important info. The more often you do it, the fewer changes you'll have to make each time, so we suggest doing a review every month to start.

- [ ] **Follow an onboarding / offboarding checklist**

  Fundamentals

  This checklist should contain a list of all the steps you need to enforce when an employee, contractor, intern, etc... joins your company. A similar list can also be used when someone is leaving your team.

- [ ] **Comprehensive Inventory of OT Assets**

  Mature

  Maintain an up-to-date inventory of all operational technology (OT) assets, including production machines, cameras, sensors... with hardware and software details. This should follow the same structure as your IT inventory and list if possible information like mac address, Static IP or “DHCP”, location, expert.

- [ ] **Asset Classification Based on Sensitivity**

  Advanced

  Sort assets by how sensitive and critical they are to our operations so we can focus our security measures and response strategies more effectively. This sorting can be used to create a purdue analysis of your assets.

  Ref - https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture

03 Access Control

- [ ] **User Account Management**

  Fundamentals

  Establish procedures for the creation, modification, and deletion of user accounts to ensure that access is managed effectively and promptly.

- [ ] **Use Multi-Factor Authentication (MFA)**

  Fundamentals

  Require MFA for all user accounts, particularly for accessing sensitive systems, to enhance security and reduce the risk of credential theft.

- [ ] **Use a password manager to ensure you only use strong passwords**

  Mature

  Using a complex and unique password for every system is great advice, but it can be very difficult to remember all of them. Password managers are a great way to manage these, since they will remember everything for you with a master password.

- [ ] **Implement Role-Based Access Control (RBAC)**

  Mature

  Implement RBAC to ensure users have access only to the information and systems necessary for their roles, minimizing the risk of unauthorized access.

Ref - https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture

04 Network Security

- [ ] **Implementation of Firewalls**

Fundamentals

Deploy firewalls to monitor and control incoming and outgoing network traffic based on predetermined security rules, effectively acting as a barrier between trusted and untrusted networks.

- [ ] **Network Segmentation**

Mature

Implement network segmentation to separate environments, reducing the attack surface and preventing lateral movement in case of a breach. Define segments based on specific use case, and legitimate reason to communicate.

- [ ] **Guest WIFI Access**

Mature

Avoid sharing Wi-Fi networks with guests or neighbors, as it can provide them with access to your network and potentially compromise resources protected by source IP. Instead, create a separate and dedicated guest Wi-Fi network. Set a calendar reminder to change the password every month, as this password will be shared.

- [ ] **Implement Role-Based Access Control (RBAC)**

Advanced

Enforce authentication for connection between your assets, based on the strategy of “zero-trust”. Record communication between assets in your network, using your switch, firewall or router tooling. Store logs in a log sink (filesystem or SIEM).

Ref - https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-41r1.pdf

05 Media Protection

- [ ] **Regular Backups and Restoration Testing**

  Fundamentals

  Set up a regular backup schedule and test our restoration procedures to make sure we can recover data if it gets lost or compromised.

- [ ] **Encryption of Sensitive Data in your filesystem**

  Fundamentals

  Employ encryption for sensitive data in your filesystem (on-premise, cloud or SAAS) to protect against unauthorized access and ensure data confidentiality.

- [ ] **Data Classification policy**

  Mature

  Establish a framework for categorizing data based on sensitivity and importance. A tiered classification - Confidential, Sensitive, None - is usually a good starting point. This should help employees label data according to its classification level.

- [ ] **Encryption of Sensitive Data in physical storage**

  Mature

  Make sure USB keys and flash drives with sensitive data are encrypted. If you can, keep them stored in closed compartments.

- [ ] **Disaster Recovery Planning**

  Advanced

  Develop and maintain a comprehensive disaster recovery plan outlining the steps to restore operations after a significant security incident or disaster.

- [ ] **Data Storage in separated physical sites**

  Advanced

  Ensure data is stored across separate physical locations.

Ref - https://www.atlassian.com/incident-management/template-generator

06 Endpoint Security

- [ ] **Deployment of Endpoint Monitoring**

  Fundamentals

  Ensure that all endpoints have up-to-date antivirus and anti-malware software installed to detect and mitigate threats.

- [ ] **Encrypt all employee laptops & phones**

  Fundamentals

  By encrypting all laptops, you protect both your company's assets, and your employee's private files.

- [ ] **Regular Updates and Patch Management**

  Fundamentals

  Maintain a schedule for regularly updating and patching systems to protect against known vulnerabilities.

- [ ] **Control the use of USB keys**

  Mature

  Implement a solution to log security information from endpoints into a centralized sink, with the ability to query this information - filesystem, log sink or SIEM.

- [ ] **Logging**

  Mature

  Implement a solution to log security information from endpoints into a centralized sink, with the ability to query this information - filesystem, log sink or SIEM.

- [ ] **Policies for Mobile and Remote Device Usage**

  Mature

  Implement policies governing the use of mobile and remote devices, including security configurations and acceptable usage guidelines. Define what data can be access on these devices.

  Ref - https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-41r1.pdf

  Ref - https://learn.microsoft.com/en-us/windows-hardware/drivers/usbcon/usb-event-tracing-for-windows

07 Industrial Security (OT Security)

- [ ] **Secure Remote Access**

  Fundamentals

  Use VPN capabilities to enforce encryption and authentication when remote access to an industrial asset is required. Log connections and commands done through remote access.

- [ ] **Accustom your team to locking their machines while away**

  Mature

  Each user should have their account to access the different machines. Maximum session length on computers should be 30 minutes.

- [ ] **Harden your devices**

  Mature

  That’s one key part of a straightforward cybersecurity strategy. When setting up a system on your shop floor, aim to limit the available options as much as possible. For instance, tape over USB ports if they’re not needed, remove internet browsers if they are not required or other unnecessary applications.

- [ ] **Logging**

  Advanced

  Implement a solution to log security information from OT assets into a centralized sink, with the ability to query this information - filesystem, log sink or SIEM.

Ref - https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltc96a4c2cb0dcef43/636db4142e16be076e6e003f/Remote_Access_Policy.pdf

08 Security Monitoring and Incident Response

- [ ] **Development of an Incident Response Plan**

  Fundamentals

  Create and refer to an incident response plan detailing what to do in case of a cyber incident. Save your past incident response into a filesystem you can refer to.

- [ ] **Centralize and archive your logs and make them meaningful**

  Mature

  Logs are necessary to trace what happened after an incident, find where the attacker came from, and possibly even who they are. Many solutions exist to gather your logs. You need to take care that the system time configured on each of your machines is in sync so that you can easily cross-correlate logs.

- [ ] **External Incident Reporting Procedures**

  Advanced

  Implement a procedure for reporting security incidents to external stakeholders - customers, suppliers. This will help build trust from external stakeholders in your organization.

09 Security Awareness and Training

- [ ] **Cybersecurity Training for Employees**

  Fundamentals - once a year

  Mature / Advanced - quarterly and office hours

  Provide cybersecurity training for all employees to educate them about potential threats and safe practices.

- [ ] **Take special care of your non tech employees**

  Mature

  Non tech employees are less used to technical tricks and can be deceived more easily than others, opening the door to ransomware or confidentiality issues. They should be trained and empowered to be distrustful and to preserve the company's assets.

- [ ] **Phishing and Social Engineering Awareness Training**

  Mature

  Hold training sessions that help everyone spot and handle phishing attempts and social engineering tricks. 80% of cyber attacks start with phishing emails, and it's better to address this early.

Trout