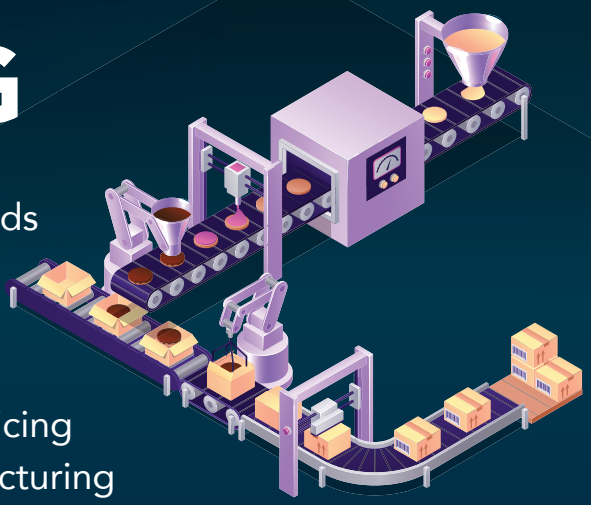
FUSION Computing
416-566-2845
www.FusionComputing.ca

MANUFACTURING



Manufacturing is an endpoint-rich industry. Some industrial operations can have hundreds if not thousands of endpoints, and each must be secured, maintained, updated and given a secure connection to apps and other network resources. Any organization in the manufacturing sector, including the supply chains servicing the sector, is at a high risk of cyber-attacks. As manufacturing organizations grow, they must innovate and take advantage of automation, AI and hyper connected network comms, leaving a large attack surface that cyber criminals can target.

Some Key Areas To Review:

PHISHING

Phishing attacks within the manufacturing industry are very common.

Suspect emails with malicious links/fraudulent attachements.

Web-based malware downloads that contain viruses or other malicious content.

Because the manufacturing industry primarily focuses on production and distribution, security can become laxed.

If a manufacturer has government contracts, they are a prime target for Industrial Espionage.

RANSOMWARE

Cybercriminals can deploy ransomware on an organization's infrastructure and hold sensitive and vital data for ransom.

Attackers rely on the ripple effect when manufacturing organizations have their production flow disrupted.

47% of the attacks within the manufacturing industry were due to vulnerabilities that companies didn't patch.

SUPPLY CHAIN ATTACKS

Threat actors access an organization's network via a third-party vendor or supplier.

In recent years, supply chain attacks within the manufacturing industry have become more prominent.

It can take the form of hardware, software and firmware-based supply chain attack.

INDUSTRIAL IOT ATTACKS

Industrial IoT (Internet of Things) devices like printers and smart TVs are at a high risk of attack.

Each device should have a strong, unique ID and up-to-date software. Unnecessary services and ports must be disabled.

Devices utilizing manufacturing processes, such as Remote Production Control and Industrial Asset Management, are at risk.

Network activity must be monitored to determine unauthorized use.

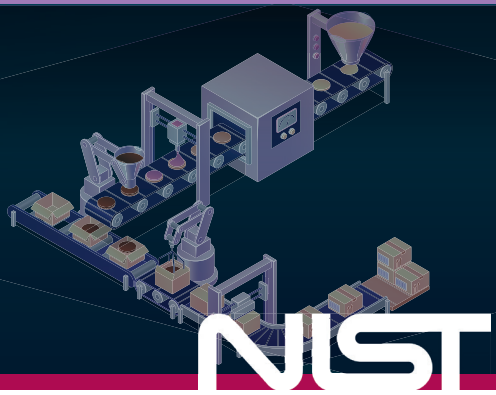
CYBER ATTACKS IN MANUFACTURING HIGHLIGHT

In 2017, Mondelez, a multinational food and beverage company, succumbed to an attack that leveraged the encrypting malware NotPetya. The attack permanently damaged 1,700 servers and 24,000 laptops. It also impacted production facilities around the globe. The attack included the theft of thousands of user credentials and impacted the company's ability to complete customer orders.

FUSION Computing

MANUFACTURING

Key NIST/CyberSecure Canada control points:



MOBILE COMPUTING

Ensure your laptop and personal digital assistant (PDA) are encrypted and password-protected.

If a computer or PDA uses wireless connections, ensure all wireless communications are encrypted.

Ensure encrypted backups are in place.

When using USB flash drives, use only devices that have built-in encryption and require passwords.

Implementation of mobile device management to deploy org-wide configuration and compliance policies.

ENDPOINT DETECTION & RESPONSE

Install Endpoint Detection & Response (EDR) tools or Extended Detection & Response tools.

Continuously monitor end-user devices to detect and respond to cyber threats like ransomware and malware.

Pair comprehensive visibility across all endpoints and apply behavioural analytics to detect traces of suspicious behaviour.

EMAIL SECURITY

Use appropriate signatures and standard disclaimers on email messages, faxes and other documents.

Train employees on analyzing and detecting spam/phishing emails.

Be cautious of communicating sensitive information via email - Set up policies to apply rules when sending emails.

GENERAL

Perform weekly scans to ensure endpoints are up to date and unauthorized software is not installed.

Make regular secure backups.

Ensure policies are in place preventing access to restricted websites and software.

Implement Multi-Factor Authentication (MFA).

According to IBM, Manufacturing was the sector most attacked in Canada in 2021, with the total number of attacks projected to grow in the coming years.

FUSION COMPUTING targeted remediation:

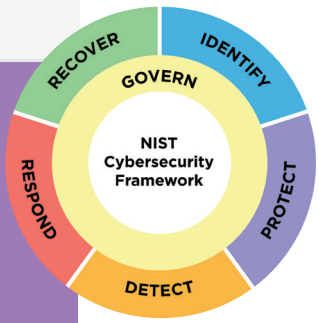
RISK ASSESSMENTS

Risk must be gauged based on factors such as probability of occurrence, impact on the organization, and risk prioritization.

Risk assessments should be conducted or reviewed regularly and at least once per year.

SECURITY CONTROLS

- Anti-virus and MDR
- Secure encrypted backups
- Data Loss Prevention
- Encryption at rest and in transit
- Firewall
- Incident Response Plan
- Mobile Device Management
- Policies and procedures
- Security Awareness Training
- Vulnerability Management
- Multi-Factor Authentication



CIS Controls