

The Guide to Business IT Security in the Plastics Extrusion Industry

Introduction

The plastics extrusion industry is increasingly adopting digital technologies to streamline production, manage supply chains, and ensure quality control. However, this digital evolution also introduces new cybersecurity risks. From ransomware attacks that halt production to intellectual property theft, the consequences of poor IT security can be devastating.

This guide is designed to help plastics extrusion businesses understand their unique cybersecurity challenges and implement effective strategies to protect their operations, data, and reputation.

1: Why Plastics Extrusion Businesses Are Vulnerable

- **Industrial Control Systems (ICS):** Many extrusion lines rely on programmable logic controllers (PLCs) and SCADA systems that are often not designed with security in mind.
 - **Legacy Equipment:** Older machinery may lack modern security features or patching capabilities.
 - **Supply Chain Dependencies:** Integration with suppliers and logistics partners increases exposure to third-party risks.
 - **Intellectual Property:** Proprietary formulations, tooling designs, and process data are valuable targets for cyber espionage.
-

2: Common Cyber Threats in Plastics Manufacturing

- **Ransomware:** Can lock down production systems, causing costly downtime.
 - **Phishing & Social Engineering:** Targeting staff with fake invoices or supplier communications.
 - **Data Breaches:** Theft of customer data, production specs, or financial records.
 - **Insider Threats:** Disgruntled employees or accidental data leaks.
-

3: Core IT Security Measures

a. Risk Assessment

- Identify critical assets such as extrusion control systems, ERP platforms, and design files.
- Evaluate vulnerabilities in both IT and OT (Operational Technology) environments.

b. 2. Access Control

- Implement role-based access to systems and data.
- Use multi-factor authentication (MFA) for remote access and administrative accounts.

c. 3. Network Segmentation

- Separate production networks from office IT systems.
- Use firewalls and VLANs to limit the spread of potential attacks.

d. 4. Endpoint Protection

- Secure all devices, including operator terminals and mobile devices.
- Use antivirus, EDR (Endpoint Detection and Response), and patch management tools.

4: Compliance & Industry Standards

- **ISO/IEC 27001:** A globally recognized standard for information security management.
- **NIST Cybersecurity Framework:** A practical model for assessing and improving security posture.
- **GDPR:** If handling personal data, ensure compliance with data protection regulations.

5: Employee Awareness & Training

- Conduct regular cybersecurity training tailored to both office and factory staff.
 - Simulate phishing attacks to test awareness.
 - Encourage a culture of vigilance and reporting.
-

6: Incident Response & Business Continuity

- Develop a documented incident response plan.
 - Include procedures for isolating infected systems and restoring operations.
 - Maintain secure, off-site backups of critical data and configurations.
 - Test disaster recovery plans regularly.
-

7: Partnering with a Managed IT Provider

A trusted IT partner with manufacturing experience can provide:

- 24/7 monitoring and threat detection
- Secure remote access solutions for engineers and technicians
- Compliance support for audits and certifications
- Scalable infrastructure for production growth

Nubis 365 Ltd is such a provider

8: Future-Proofing Your Cybersecurity

- **IoT & Smart Factory Security:** Secure connected sensors and devices with firmware updates and access controls.
 - **AI & Automation:** Use AI-driven tools for anomaly detection and rapid response.
 - **Zero Trust Architecture:** Assume no device or user is trusted by default.
 - **Continuous Improvement:** Regularly review and update your security strategy based on emerging threats.
-

Conclusion

In the plastics extrusion industry, cybersecurity is essential for maintaining uptime, protecting intellectual property, and ensuring customer trust. By adopting a proactive, layered approach to IT security, manufacturers can safeguard their operations and position themselves for long-term success.

Disclaimer – Cyber Security Guides by Nubis 365 Ltd

The information provided in these Cyber Security Guides is intended for general informational purposes only. While Nubis 365 Ltd has made every effort to ensure the accuracy and relevance of the content, the guides do not constitute legal, regulatory, or professional advice.



Cybersecurity requirements vary by industry, organisation size, and operational complexity. Therefore, the recommendations outlined in these guides should be considered as a starting point. We strongly advise consulting with a qualified IT security professional or engaging with our team for tailored advice specific to your business needs.

Nubis 365 Ltd accepts no liability for any loss or damage arising from reliance on the information contained in this guide. All product and service recommendations are made on a case-by-case basis and are subject to change based on evolving threats, technologies, and vendor capabilities.

By using this guide, you acknowledge and agree that Nubis 365 Ltd is not responsible for any decisions made or actions taken based on the content provided.