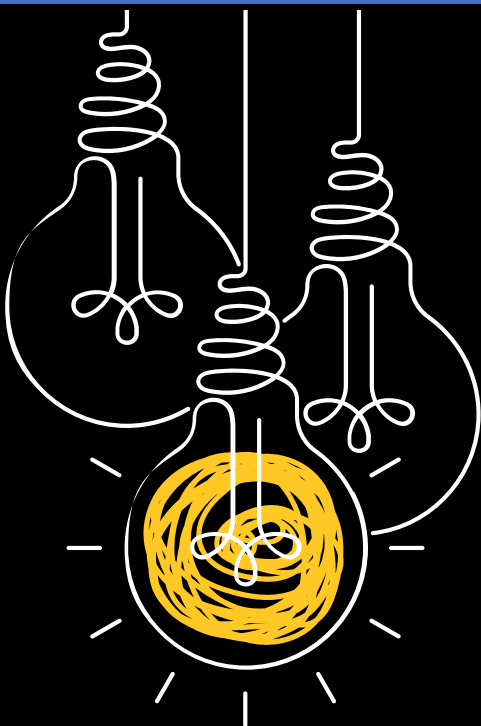


Quick Facts/Stats

60% of manufacturers experienced a cyberattack in the past year — with phishing and malware leading the list. ¹

43% of industrial cyber incidents now involve compromised IoT or connected devices. ³



AI-generated phishing emails are up over 200% year-over-year, thanks to generative text tools. ²

Average downtime after an ICS cyberattack: 6–12 days — with significant production and financial impact. ⁴

Key Emerging Threats

01

AI-Powered Phishing & Deepfakes

Attacks now mimic internal emails, vendor messages, or even executive voices.

Watch for urgency, unfamiliar tone, or unexpected requests.



02

Adaptive Malware

Malware learns from defenses and reconfigures itself to evade detection.

Keep antivirus, endpoint detection, and firmware current.

03

IoT & Connected Device Risks

Smart sensors and controllers can expose entry points if left unpatched.

Change default passwords, isolate production networks.



04

Supply Chain Targeting

Attackers exploit smaller vendors or service providers to reach your environment.

Vet vendors' cybersecurity practices and limit data access.

Actionable Steps for Employees

01

Spot & Stop Phishing

- Double-check sender addresses and URLs before clicking.
- Verify unexpected payment or approval requests by calling the person directly.

02

Protect Devices

- Install updates promptly—even if downtime is needed.
- Use strong, unique passwords for every account or device.

03

Stay Alert

- Report any suspicious email, pop-up, or device behavior immediately.
- If you're unsure—don't click, connect, or approve.

04

Secure the Line

- Don't plug in unknown USB drives or connect personal devices to the network.
- Lock your workstation when stepping away.

Defensive Technology Highlights

AI-powered monitoring detects unusual data flows or system behavior.

Predictive analytics identify weak points before attackers do.

Threat intelligence feeds continuously update to recognize new attack patterns.

¹IBM X-Force. (2024). IBM X-Force Threat Intelligence Index 2024: Manufacturing still leads cyber-attack target list. IBM. SecurityHQ+2newsletter.radensa.ru+2
²SlashNext. (2024). Prepare for 2025: 2024 Phishing Intelligence Report. SlashNext. slashnext.com+3slashnext.com+3PR Newswire+3
³Pt Security / Global Research. (2025). "Cyber-threats to industrial IoT in the manufacturing sector." Pt Security. ptsecurity.com
⁴(If you include the stat from DeepStrike) DeepStrike. (2025). "IoT hacking statistics 2025: Threats, risks & regulations." DeepStrike. deepstrike.io

