Cybersecurity in Manufacturing:

Cyberthreats to the factory expand and intensify

How do you defend your network and data?

90%

increased audit efficiency expected by 2025, with **a projected 30% of manufacturers using blockchain and IoT** to provide reliable provenance.
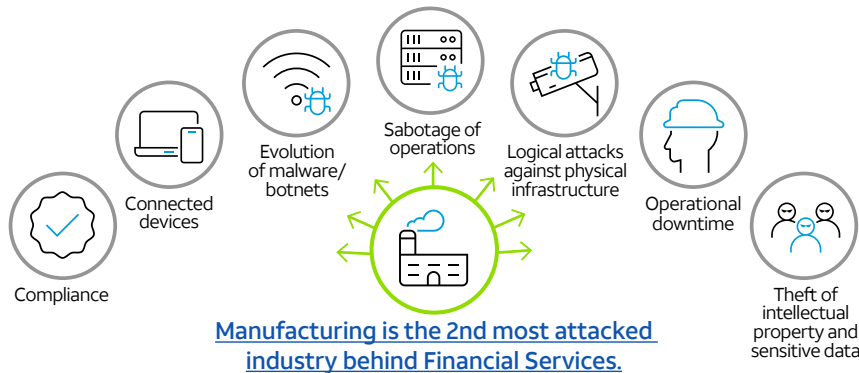Manufacturing Insights, IDC.

40%

of original equipment manufacturers by 2024 **will use IoT field data to diagnose issues and cut downtime by 25%.**
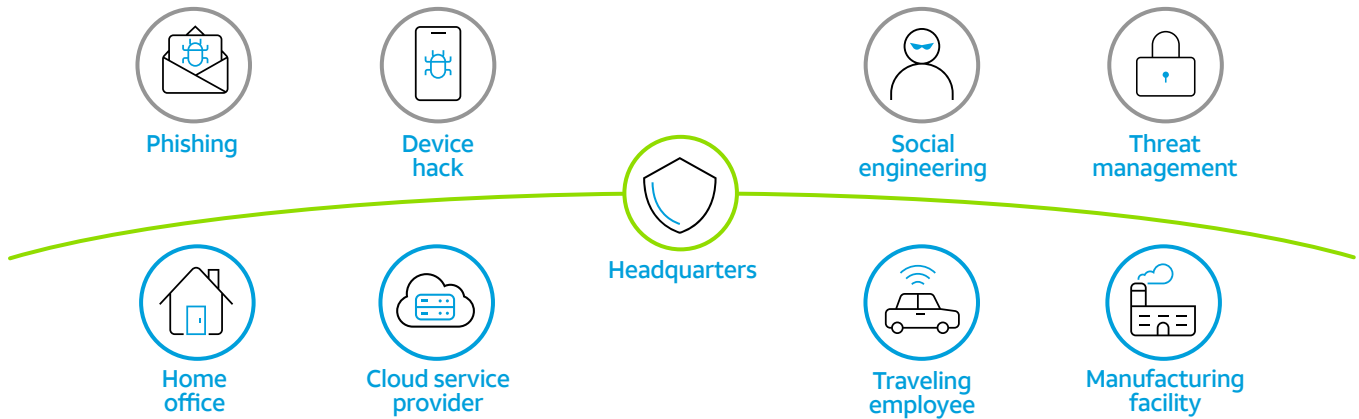Manufacturing Insights, IDC.

70%

of manufacturers will use **cloud-based innovation platforms and marketplaces for cross-industry and customer co-development by 2022.**
Manufacturing Insights, IDC.

The very nature of manufacturing creates cybersecurity challenges that other industries do not.

Compliance

Connected devices

Evolution of malware/ botnets

Sabotage of operations

Logical attacks against physical infrastructure

Operational downtime

Theft of intellectual property and sensitive data

Manufacturing is the 2nd most attacked industry behind Financial Services.

"Hackers continue to target industrial control systems (ICS) and legacy security measures primarily because they utilize outdated processes and technology that expose vulnerabilities. As manufacturing supply chains become increasingly automated and rely heavily on remote access, leaders must focus on cyber hygiene."

Hill, Roger. "Manufacturing's Newest (and Biggest) Challenge." Manufacturing.Net.

Protect your operations and intellectual property.

Phishing

Device hack

Social engineering

Threat management

Headquarters

Home office

Cloud service provider

Traveling employee

Manufacturing facility

Current security challenges	AT&T Cybersecurity solutions
Demonstrate manufacturing-specific due diligence and effective risk management	• Risk assessment • Industry standards assessment • Strategy and roadmap services • Security maturity benchmarking
Protect sensitive information	• Managed Vulnerability Program (MVP) • Penetration testing services • Third-party risk managment • Firewalls • Application shielding
Protect intellectual property, plant assets, and production integrity with converged-access security products, technologies, and services	• Threat manager • Incident response table top exercises • Incident response retainer • DDoS defense
Invest in employee education	• Security awareness and training • Social engineering assessment
Protect industrial operations	• SOC transformation • Secure Email Gateway • Cloud Web Security Services • Cloud Security Assessments • IoT cybersecurity consulting
Compliance with industry standards and framework	• ISO 270001 assessments • NIST framework assessment and implementation • CMMC (Cybersecurity Maturity Model Certification)

Safeguard your organization with a multi-layer approach powered by threat intelligence and advanced data analytics to help protect against security breaches.

To learn more about AT&T Cybersecurity Consulting, visit www.att.com/security-consulting.