COMTRADE
FAST FORWARD

Cybersecurity in Logistics

From compliance to continuity: embedding security across IT and OT systems.

Executive Summary

Cybersecurity can't be an afterthought or postponed.

Regulatory compliance is an important driver — alongside business continuity, customer requirements, and operational resilience — for cybersecurity investments.

Threats are evolving, with increased sophistication and frequency. Success requires a proactive approach to risk management, continuous monitoring, and a culture of security awareness.

At Comtrade Fast Forward, we embed security and resilience into our logistics solutions through secure-by-design development, OT risk assessments, supplier assurance, and tested incident response plans — helping our clients operate more securely and recover faster from incidents.

Why Cybersecurity Matters in Logistics

Logistics companies are increasingly reliant on digital technologies to run their operations, making them more vulnerable to cyber threats.

Being part of critical infrastructure means that any disruption can have far-reaching consequences, affecting not just the company but also its partners and customers.

Logistics environments often combine IT (WMS, TMS, ERP) and OT/ICS (conveyors, PLCs, sensors, SCADA).
OT systems have unique requirements (availability and safety > confidentiality), slower patch cycles, and require dedicated standards such as IEC/ISA 62443 for risk management.

Rising Regulatory Pressure

Governments worldwide are implementing stricter cybersecurity regulations. In Europe, for example:

- **NIS2 Directive (2022/2555) —** imposes mandatory security and incident reporting obligations on essential and important entities, including many logistics and transport operators.

- **GDPR (2016/679)** — protects personal data, with fines up to €20M or 4% of global annual turnover.
- **EU Cybersecurity Act (2019/881)** — establishes a cybersecurity certification framework and strengthens ENISA's role.
- **ISO/IEC 27001** — internationally recognized auditable standard for information security management.
- **NIST Cybersecurity Framework (CSF)** — widely used framework for structuring cybersecurity programs.

Compliance is not just a legal obligation but also a critical part of risk management and supplier assurance. Failure to comply can result in significant penalties, reputational damage, and loss of business.

Building a Security-First Culture

Cybersecurity must be embedded in the organizational culture, with leadership setting the tone for a security-first mindset. This includes:

- Regular employee training and awareness campaigns.
- Adoption of secure software development practices (see NIST SSDF / SP 800-218).
- Continuous monitoring and logging of IT and OT systems.
- Penetration testing and vulnerability assessments (based on NIST SP 800-115) to find weaknesses before attackers do.
- Careful testing approaches in OT systems, where safety and uptime are critical.
- Third-party and supply-chain security measures, including SBOM (Software Bill of Materials), supplier security assessments, and contractual requirements.

What Leaders Need to Consider

Focus Area	What to Know
Regulatory Compliance	Understand GDPR, NIS2, ISO 27001, and other applicable frameworks. Implement and regularly review compliance.
Secure Operations Mindset	Prioritize security in all operational decisions; treat it as part of business continuity, not IT overhead.
Safe Software Supply Chain	Enforce secure coding, SBOM usage, supplier vetting, and contractually require minimum security standards.
IT/OT Segmentation	Separate IT and OT networks; apply IEC/ISA 62443 principles; use firewalls and strict access controls.
Zero Trust & IAM	Apply least privilege, enforce MFA, and move towards a Zero Trust architecture.
Continuous Monitoring	Use SIEM/EDR solutions to detect threats in real time; monitor both IT and OT assets.
Incident Response	Maintain and regularly test an incident response and recovery plan (including ransomware scenarios).
Threat Intelligence	Leverage industry-specific threat intelligence (ENISA, ISACs) to stay ahead of new attack vectors.
Employee Training	Invest in regular training and phishing simulations; treat people as the first line of defense.

The Bottom Line

In-depth cybersecurity measures are no longer optional for logistics companies — they are a fundamental requirement for operational resilience and protection of sensitive data.

By adopting a proactive approach, organizations can:

- Mitigate risks.
- Strengthen compliance.
- Enhance reputation.
- Build trust with customers, partners, and regulators.

Comtrade Fast Forward Perspective

We at Comtrade Fast Forward understand the critical importance of cybersecurity in the logistics sector.

Our approach centers on:

- Embedding security into every stage of our software development lifecycle.
- Conducting regular risk assessments across IT and OT environments.
- Supporting compliance with frameworks such as ISO 27001, NIST CSF, GDPR, and NIS2.
- Implementing supply-chain assurance programs, including SBOM adoption and supplier vetting.

To our clients, we offer consulting on secure software development practices, risk assessments, and compliance strategies designed for the unique challenges of the logistics industry.

Swiss Precision.
Engineered for Logistics.

At Comtrade Fast Forward, we help logistics companies boost efficiency, cut costs, and stay competitive with AI solutions built for impact, not hype. We start with a deep understanding of your operations and goals, then design and deploy AI that delivers lasting value.

COMTRADE
FAST FORWARD

Grafenauweg 8, 6300 Zug,
Switzerland
fastforward@comtrade.com

comtradefastforward.com