Title: Report 1, Threat Modeling a Real System: FedEx Ground SCRA-0185

Name: Seid Cubro

Date: 1/22/2026

Course: CS 355, Network Security

Introduction:

The purpose of this report is to develop a practical, security-focused threat model for a real-world system. Threat modeling is an organized process used to identify important assets, trust boundaries, credible threat scenarios and prioritize mitigations based on risk. The objective is to think as a defender by focusing on realistic threats, likely attack paths and controls that provide the greatest reduction in risk (CS-355 Report Manual, 2025).

The environment selected for this report is the FedEx Ground warehouse facility in Pittston, PA (SCRA-0185). The environment was chosen due to my own familiarity with its operational processes, technology usage and employee workflows. As a large logistical warehouse, the facility depends heavily on interconnected systems such as handheld scanning devices, internal wired and wireless networks, centralized authentication services and cloud-hosted logistics platforms. Since FedEx is a global organization handling sensitive shipment, customer and employee data, this environment represents a realistic and relevant target for cybersecurity threats. Studying this system reinforces core network security concepts including asset identification, trust boundary analysis and risk-based mitigation prioritization (CS-355 Report Manual, 2025; NIST SP 800-30 Rev. 1).

System Scope:

The scope of this threat model is limited to the operational and networked systems within the FedEx Ground Pittston warehouse. The analysis focuses on systems that directly support package handling, tracking, and internal operations.

In scope:

- Employee endpoints and handheld scanners
- Internal wired and wireless networks
- Authentication and identity services
- Cloud-based logistics and tracking applications
- Internet connectivity to FedEx corporate systems

Out of scope:

- Proprietary FedEx application internals
- External FedEx data centers
- Third-party carrier systems not directly managed by FedEx

Some assumptions are made to structure the analysis. It is assumed that the facility uses professional-grade network security controls, centralized identity management and standard firewall protections. These assumptions are documented to ensure the threat model remains explainable and repeatable, as recommended by NIST SP 800-30 (NIST, 2012).

Asset Table:

Asset	Justification	CIA Properties	Location
Employee Credentials	Enable access to internal and cloud systems	C, I	Identity services
Handheld scanners	Enables package tracking	I, A	Warehouse dock
Logistics databases	Store shipment data	C, I, A	Cloud
Internal network	Supports operations	A, I	On-premises
Supervisor machines	Operational control	A, I	On-premises
Package tracking data	Contains customer information	C, I	Cloud
Authentication services	Enforces access control	A, I	Cloud

Trust Boundaries:

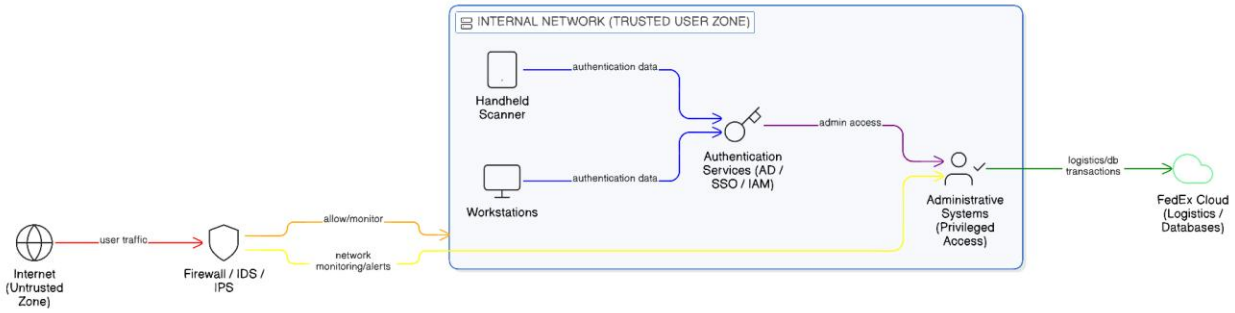
Trust boundaries represent a point where the levels of trust change and security must be enforced. Identifying trust boundaries helps reveal where attackers may attempt to cross from lower-trust zones into higher-trust systems (CS-355 Report Manual, 2025).

Key trust boundaries include:

- Internet to Internal Network: External traffic entering the facility must traverse firewalls and filtering controls.
- Employee Devices to Authentication Services: Users must authenticate before accessing internal or cloud resources.
- Internal Network to Cloud Services: Data exchanged with FedEx cloud systems crosses organizational and network boundaries.
- Standard User Access to Administrative Systems: Privileged access is restricted to authorized personnel.

Trust boundary analysis is consistent with the threat and asset-oriented approaches recommended by NIST SP 800-30. It highlights potential attack surfaces and movement paths (NIST SP 800-30 Rev.1).

Trust Boundary Diagram:



Threat Scenarios and Prioritization:

Threat scenarios were identified using a threat-oriented risk assessment approach, focusing on realistic threatening actions such as phishing, malware infection, unauthorized access and device loss. NIST SP 800-30 defines a threat event as an event with the potential to adversely impact organizational operations or assets, while NIST SP 800-61 defines a cybersecurity incident as an occurrence that jeopardizes the confidentiality, integrity or availability of systems or data (NIST SP 800-30 Rev. 1; NIST SP 800-61r3).

Threat Table:

Threat Scenario	Target Assets	Likelihood	Impact	Priority
Phishing compromising employee credentials	Credentials, cloud systems	High	High	High
Lost or stolen handheld scanner	Scanners, tracking data	Medium	Medium	Medium
Malware on supervisor workstation	Workstations, network	Medium	Medium	Medium
Rouge device on internal network	Network	Medium	Medium	Medium
Insider misuse of access	Databases	Low	High	Medium
Network denial-of-service	Internal network	Low	Medium	Low

Likelihood and impact were assessed qualitatively, consistent with SP 800-30 guidance, which emphasizes documenting assumptions and reasoning rather than relying solely on numeric values (NIST SP 800-30 Rev. 1).

Top 5 Mitigations and Trade-offs:

Mitigations were selected and prioritized based on their ability to reduce likelihood and impact, which aligns with the risk response options defined in the SP 800-30, mitigate, avoid, transfer, accept (NIST SP 800-30 Rev. 1).

1. Phishing awareness training – reduces likelihood
2. Multi-factor authentication (MFA) – reduces impact of credentials being compromised
3. Network segmentation and port security – limits lateral movement
4. Device inventory and remote wipe – reduces data exposure
5. Patch management program – reduces vulnerability exploitation

These controls also support incident prevention and response readiness, which is highlighted by NIST SP 800-61's emphasis on integrating incident response into the overall risk management system (NIST SP 800-61r3).

Conclusion:

This threat model identifies several vulnerabilities of the FedEx Ground facility in Pittston, PA. The largest threats are credential compromise and endpoint security. These vulnerabilities are highly prevalent and capable of causing substantial operational and data integrity impacts. By grounding likelihood and impact assessment in NIST risk assessment guidance and prioritizing mitigations accordingly, this report demonstrates a defensible, risk-based approach to network security decision-making (CS-355 Report Manual, 2025; NIST SP 800-30 Rev. 1).

References:

Carey, D. R. (2025). *CS-355 Network Security Report Manual*. Wilkes University.

National Institute of Standards and Technology. (2012). *NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments*.

National Institute of Standards and Technology. (2025). *NIST SP 800-61r3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management*.

NIST SP 800-30 Risk Assessment Overview Lecture Slides (Instructor-provided).