The Evolving Threat Landscape in Trucking

Ronnie Thomas

Vice President of Technology Solutions,

Werner Enterprises

WERNER®

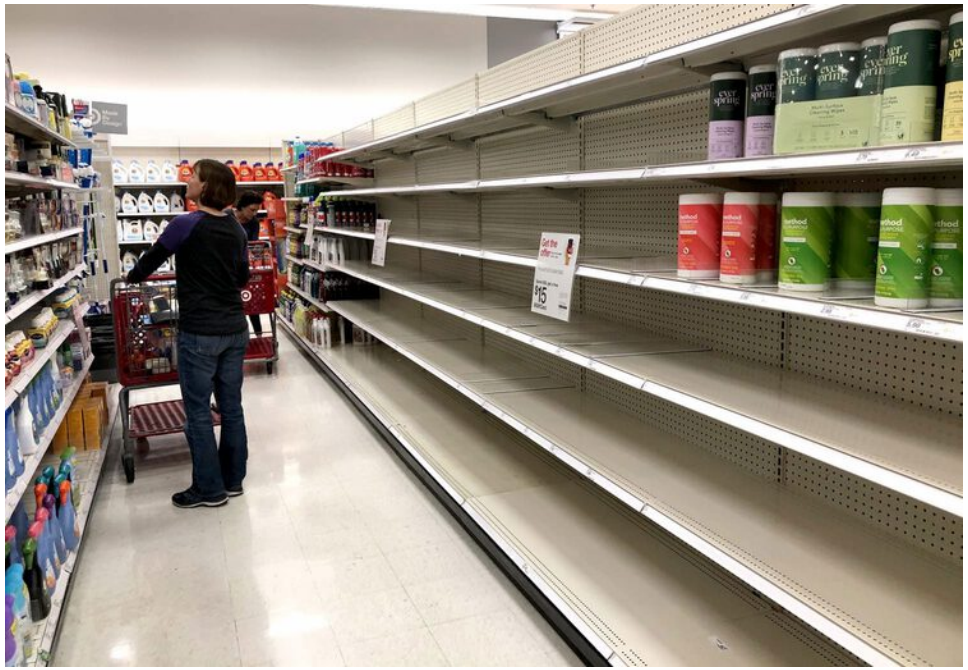
Securing the Road Ahead

Ronnie Thomas – VP Technology Solutions

SAFELY SERVING America EVERY DAY!

What's the WHY?

Cyberthreats surge against US logistics infrastructure



What's the WHY?

Cyber risk is no longer just an IT issue — it's a logistics and business continuity issue.

Transportation is now a prime target for cyber attackers (nation-state, criminal, insider).

The average cost of an individual ransomware attack has risen by 17% in the first half of 2025.

RISING CYBER THREATS

186% increase in ransomware attacks

70% OF ALL U.S. FREIGHT MOVES BY TRUCK

$10.4 TRILLION IN GOODS MOVED ANNUALY (U.S.)

The Evolving Threat Landscape

- Nation-state Advanced Persistent Threats and ransomware-as-a-service (RaaS) groups both actively target logistics.
- Russian GRU, Chinese APT41, and North Korea's Lazarus Group are known to:
  - Spy on freight movement (especially military/cross-border)
  - Hijack surveillance systems (as seen near Ukraine/Poland transport corridors)
  - Exploit third-party logistics platforms to leapfrog into OEM, shipper, or rail systems.
- AI is advancing the threat landscape

AI

- AI-Enabled Threats
- Offensive AI is now in use:
  - Deepfake phishing to impersonate dispatchers or executives.
  - AI-written malware that evades signature detection.
  - Automated reconnaissance bots scanning logistics APIs for flaws.
- AI boosts attacker speed — human defenders must use AI-enhanced defense to keep up.

AI

Operational Efficiency

- Launched AI TASKFORCE
- Conversational AI
- Document processing
- Intelligent Freight
- Intelligent response
- AI-enhanced detection
- AI-enhanced App development

Security

- AI-Powered Phishing Defense
- Data Protection & DLP
- Threat Detection & Response
- OT & IoT Security

Building Cyber Resilience

- Cyber risk is a board-level conversation.
- Cyber resilience starts at the top of an organization
- Assume breach → prioritize response and recovery.
- Emphasis on:
  - Asset visibility
  - Secure backups
  - OT segmentation
  - Incident Response simulations.
  - Awareness - Phishing, Vishing, etc.

Approach to Cybersecurity at Werner

- Cybersecurity as a business enabler, not a blocker.
- Cloud Native Cybersecurity toolset
- Defense-in-Depth strategy across:
  - Endpoints
  - Network
  - Data classification
  - Zero Trust model in action
  - Privileged Access Management / Privileged Endpoint Management
  - Onboarding/offboarding automation through SSO - prevent stale accounts & retaliation.

Incident Response – Assume Worst Case Scenario

- Preparation and Simulation – ‘Not if’ but ‘When’
- Regular IR Simulations – Tabletop Exercises
- Focus on Containment and Eradication
- Clear Communication – Internal and External
- Post-Incident Analysis – Learn from each Incident to get better

Why OEMs Matter in Fleet Cybersecurity

- **Trucks Are No Longer Just Mechanical Assets**
- Today's tractors are rolling networks with:
  - Dozens of ECUs
  - Built-in cellular modems, Wi-Fi, and Bluetooth,
  - Embedded infotainment systems,
  - OTA (over-the-air) firmware update pipelines.
- These components are often controlled, monitored, or updated remotely by OEMs or Tier-1 suppliers.

Start with Visibility

- Tools helps fill the visibility gap by:
  - Monitoring for unauthorized Bluetooth or WiFi signals even if introduced by OEM interfaces.
  - Flagging new cellular egress points not seen before (possible rogue firmware behavior).
  - Giving Werner a fleet-level detection layer outside the OEM's perimeter.
  - Dashboard alerts flow into IR process.

Conclusion – The Road Ahead

- The **THREATS** are Real
- AI is Changing the Game
- Proactive, Strategic Approach
- Visibility, Response, and the Partnership between Cybersecurity teams and Business Operations

THANK YOU

For more information, visit **werner.com**

Werner Enterprises Inc. | @One_Werner | @One_Werner | Werner Enterprises

WERNER®