Cybersecurity and its Relevance to CIT

US Department of Homeland Security has identified a growing digital threat to surface transportation in general.

Relatively unsophisticated attacks have successfully disrupted the system.

CIT is part of this ecosystem.

Cyber Threats

- Terrorism
- Crime
- Espionage
- Hacktivism
- Extortion

*** Mineta Transportation institute

Enterprise operating systems of CIT carriers are high value targets.

These systems control all facets of the companies' route logistics, inventory management, data surrounding pickups, deliveries, pavement amounts and are at significant risk of business interruption, hijack and ransom and state-sponsored cyber-attack.

- Delivery
- Customer
- Competitive
- Disclosure
- Product

Cyber Risks

*** Mineta Transportation institute

Safeguarding valuables increasingly must be more than physical security with guards, armored truck and vaults.

The industry must act proactively to protect cyber assets and technology infrastructure, as huge portions of deposits become digitized as they enter the federal banking system.

Past as Prelude to the Future - Target Evolution to Scale Over Time

1980's onward	Credit card users targeted
2000's onward	Online banking users targeted
2016 onward	Core banking systems targeted • SWIFT system and other international analogues

Attacks on these targets are increasingly sophisticated and have been spectacularly successful due to their scale.

Increased connectivity creates the need for greater collaboration.

Compliance / Security

Are we doing enough????

No one is doing enough

LowersRiskGroup®

Protecting People, Brands, and Profits

lowersriskgroup.com