


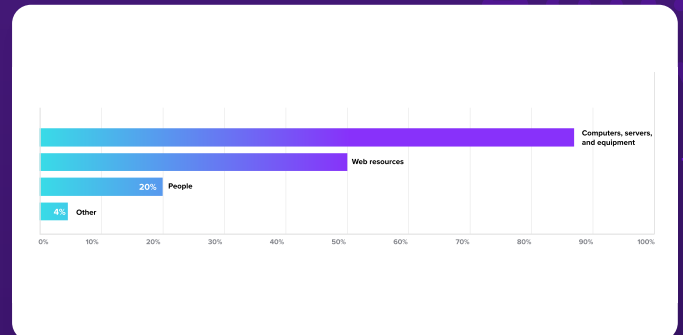


## INDUSTRY SPOTLIGHT SERIES

# Transportation and Logistics

### Top Trends

-  **Increased use of automation** to better connect logistics, scheduling, route and volume planning.
-  **Unique security challenges** include legacy equipment, long life cycles, and convergence with IT networks.
-  **Heavy adoption of IoT technology** to support GPS tracking of passenger flights, cargo, vessels, containers, vehicles and goods.



Targets of attacks on Transportation and Logistics Industry (percentage of successful attacks)

### Why is the Transport and Logistics Industry Suffering?



#### Complex, sprawling environments

with assets distributed and in motion. As a result, they are more easily susceptible to cyber exposure and attack.



#### Attacks on critical infrastructure

cause widespread disruption, making transportation and logistics prime targets.



#### Cybercriminals exploit economic importance

to demand high ransoms, knowing disruptions have major financial impacts.



#### Geopolitical motives

drive state-sponsored attacks on critical infrastructure, aiming to destabilize adversaries economically.



#### Legacy OT systems

in transportation and logistics are outdated and lack modern security, making them easy targets.

### Interested to learn how Armis delivers a holistic, proactive cybersecurity solution

to the transportation and logistics industry?



[READ THE SOLUTION BRIEF](#)



98%

2 in 5 transportation and logistics assets remain unmonitored and pose the biggest threat to organizations globally - Armis Labs



23 days

It takes a company 197 days to discover a breach, and up to 69 days to contain it - IBM



55%

At least 55 % of transport and logistics employees feel they are ill-equipped to identify or handle a significant cyberattack - Positive Technology



10x

36% YoY increase in the number of successful attacks on the global transportation industry - IMB

## INDUSTRY SPOTLIGHT SERIES

# Transportation and Logistics

Interconnection of IT/OT relies on orchestration of complex systems that may contain cyber vulnerabilities, which you cannot take down to patch at a moment's notice.

Organizations consistently grapple with patch rates at 62% for non-weaponized and 61% for weaponized. - Armis Labs



62% Non-weaponized



61% Weaponized

## Personas



### Industrial Engineer

You are responsible for the technology infrastructure and operational processes of assets on the ground that keep operations flowing.

#### Challenges:

- Lack of visibility into complex sprawling networks makes maintenance difficult
- Maintaining secure operations as attack surface grows
- Digital transformation and innovation yet being aware that these changes increase security risks
- Proactively working on risk resolution when you don't have the ability to prioritize vulnerabilities



### Security Analyst

Every event logged within the organization is monitored by you. In Transportation and Logistics where uptime is essential, making sure your proactive defences and response to vulnerabilities are in good order is critical to operations.

#### Challenges:

- Legacy hardware and software causing inefficiencies
- Lack of asset situational awareness makes prioritizing vulnerabilities impossible
- Cybersecurity threats are faster than defenses
- Choosing the right technology, and constant software updates after threats are dealt with
- Early detection of vulnerabilities

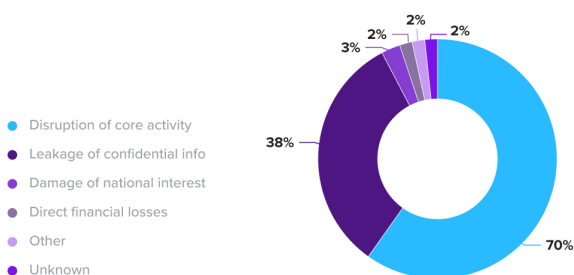


### Security Risk and Compliance Officer

You're strategic and focused on ensuring your organization has the right technology strategy and resources to deliver against mission critical goals and objectives.

#### Challenges:

- The pressure of personal culpability if your organization fails audits
- Transport has a heavy public touch point - if you get it wrong peoples lives are at risk
- Staying up-to-date with local and global security challenges, new technologies and compliance issues
- Delivering strategy and response reports to non-technical board and business leaders



Impact of successful breaches on the Transport and Logistics industry

"Ensuring robust cybersecurity in the transportation and logistics industry is not just a necessity, it's an imperative. As we increasingly rely on interconnected operational technologies (OT) to drive efficiency and innovation, the potential risks grow exponentially. It's our duty to safeguard these critical infrastructures against cyber threats, not only to protect our assets but also to maintain the trust and reliability that our industry hinges upon."

— Carlos Buenano, Chief Technology Officer, Armis