10 YEARS KALE LOGISTICS

Kale Logistics

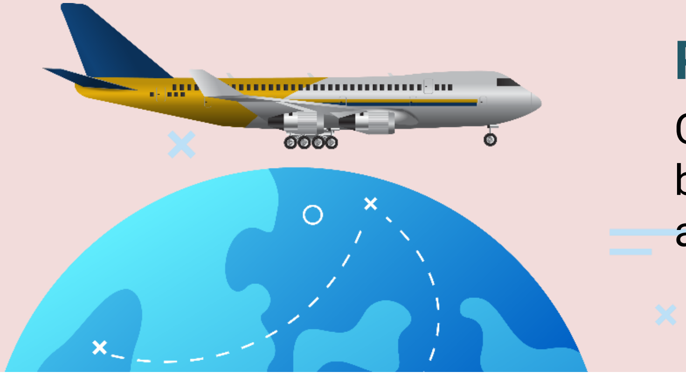
Technology that Transforms

Practical Measures for Air Cargo Security in MID and Beyond

Air Cargo security evolution

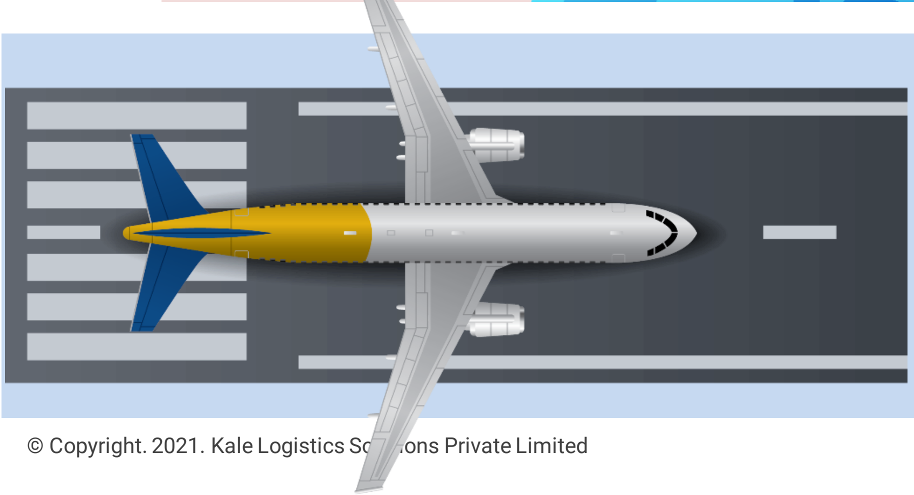
Now

- Cargo information (PLACI) shared before the aircraft takes off from the origin
- Harmonized and standardized procedures for advance cargo information



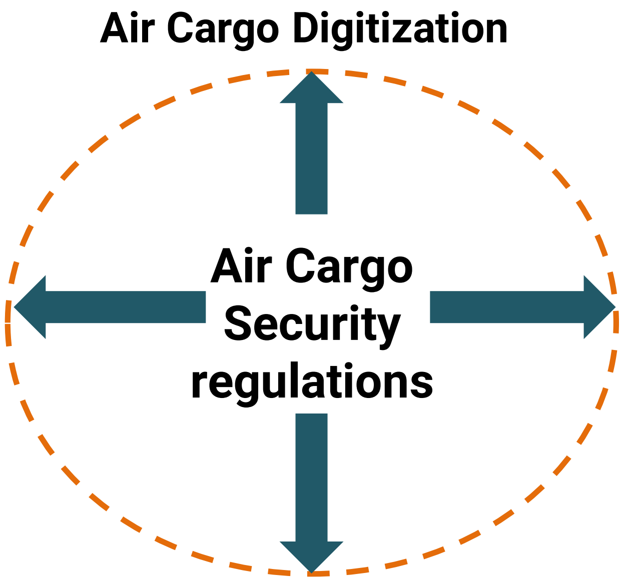
Post 9/11

Cargo information shared before the aircraft lands at destination



Last century

Cargo information shared after the aircraft lands at destination



Air Cargo Digitization

Air Cargo Security regulations

Other Key Air Cargo Security Initiatives shaping digitization

Authorised Economic Operator (AEO,) – Under the aegis of WCO (SAFE Framework), AEO promotes Customs-to-Business partnerships. Compliance with supply chain security standards.

e-CSD – This provides regulators with an electronic audit trail of how, when and by whom cargo has been secured along the supply chain. Warrants only secured cargo is shipped.

Advance Shipment Information (ASI) - This advance information ahead of the arrival of goods, aids processing and clearance of cargo. Mitigates security risks prior to loading or arrival.

Cyber security threats for Air Cargo

Most Air Cargo stakeholders are unaware of the breach until the hackers have been inside of their system for six to nine months

A shipment can often involve data or intellectual property transfer between up to 10 separate parties across the globe.

Communications and data nodes in Air Cargo, projected to generate 98 million terabytes of data by 2026

The loss of confidential information could give rise to data protection issues and breach of privacy laws, leaving airlines and airports with heavy fines, government audits and even criminal liability.

Findings of SITA Survey on Cybersecurity

Risk is acknowledged but still no emphasis on "C" level

Lack of resources, budgets and skills are key barriers to Cybersecurity

Less than 50% stakeholders have formal Information Security Strategy in place

Shift in mindset from compliance to proactive protection

Cybersecurity value chain

- Assess – Inventory & audit
- Detect and Report – Security Ops Center (SOC)
- Respond – Cyber resilience
- Learn and Improve

Cyber Vulnerabilities in Air Cargo

Every shipment requires multiple players

Sensitive data is added by every player in the air cargo supply chain

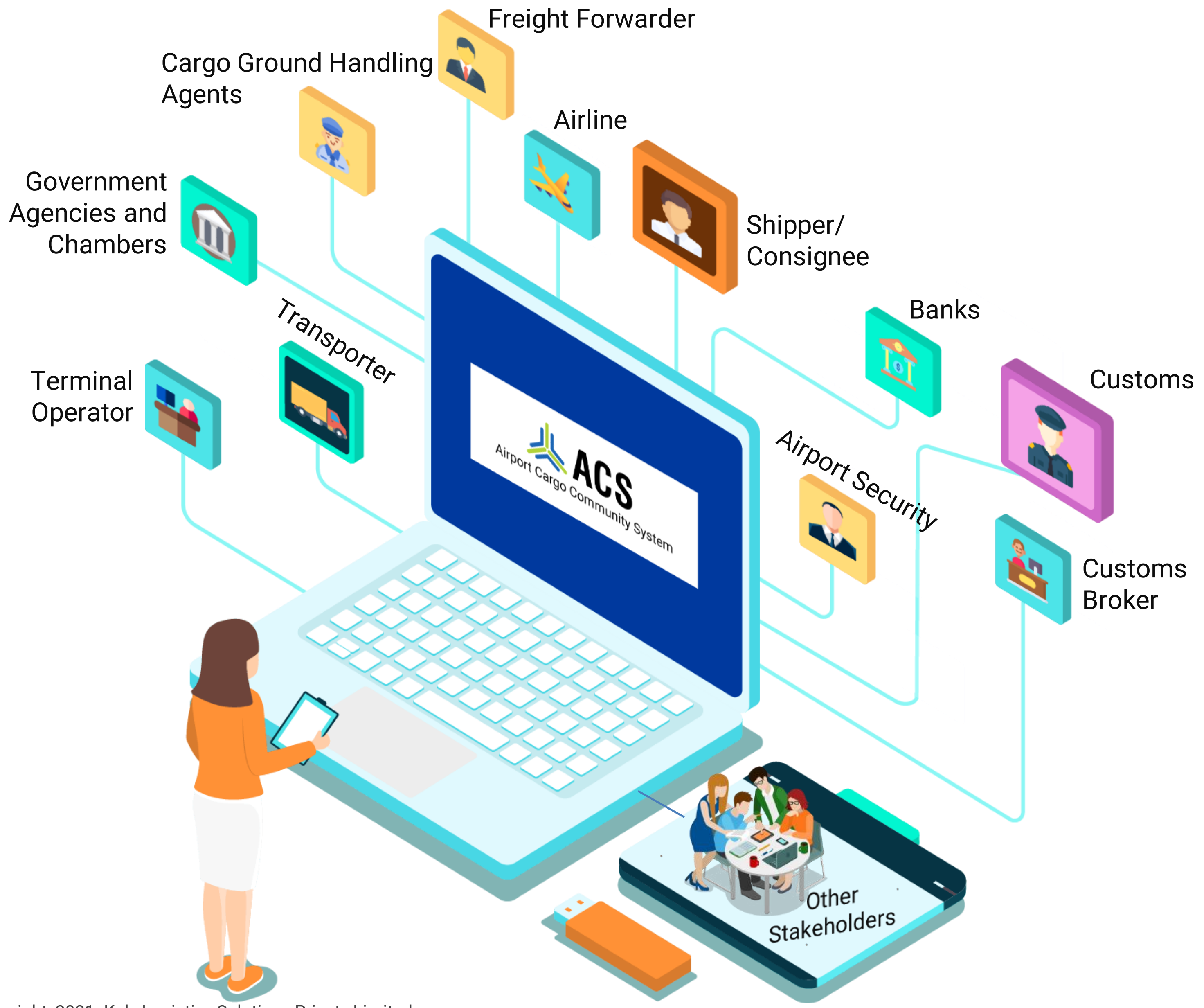
Larger players have strong internal Cyberattack prevention infrastructure in place. However, in a connected world they are dealing with numerous small players who can cause the chink in the armours

Air Cargo SME have very little capabilities as well as budgets to create impregnable cyber defense infrastructure

This has created need for **collaborative approach for Cyber Security**

Community platforms can facilitate cyber security needs of SMEs to a large extent

Community approach to security



Wherever possible connect to critical stakeholders' systems through single window controls like the community platforms to reduce the risks imposed by individual stakeholder systems

Potential of Blockchain in Air Cargo Information Security

1 Certifications

- e-Certificate of Origin
- e-Phyto Certificates
- Test certificates

2 Elimination of paper

- e-DO
- e-Customs
- Digital Corridors
- e-BL

3 Tracking

4 Finance

- Bill discounting
- Settlements

In summary

Each stakeholder shall have at least one resource trained on cybersecurity and there should be a program in place to educate the others in the organization

As a first step, every client desktop / laptop should be running with updated operating system patches, anti-virus software always in protected mode and most up-to-date. This will reduce end point vulnerability to larger extent because 90% of the time attacks are initiated from client desktop / laptops which are compromised.

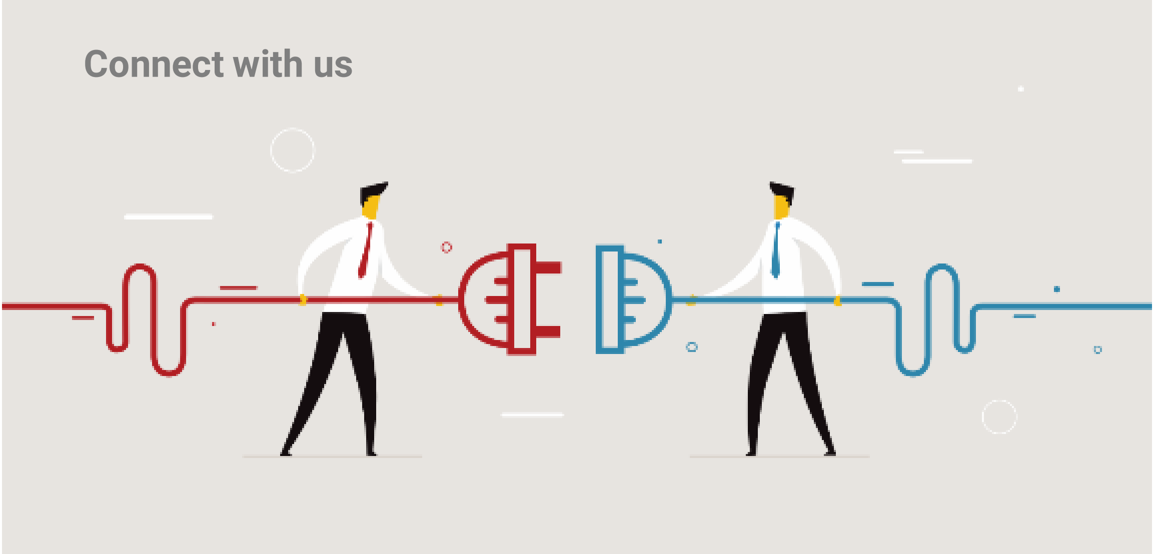
While service providers ensure their platforms are protected and tested for code vulnerabilities periodically and implementing Security Operations Center. Protecting community portals/industry platforms with well sophisticated tools, it is also very important to manage these at the software development (DevOps) stage itself. The framework is also termed as Dev-Sec-Ops, handle security postures at development itself moving potential vulnerable code to production and fixing it later.

There are various tools and practices organizations may follow to reduce the cyber attacks and protect their infrastructure to deliver Secured information to all stakeholders and offer desired / agreed service levels. These are now affordable in Software as a service model (SaaS)

As air cargo industry handles, processes personal information of customer (individual) it is utmost important to establish desired controls related to privacy and frequently arranging cyber security awareness training to their employees, third party providers, assess / review critical processes periodically, this will reduce the likelihood of cyber incidents. And should this occur the employees are well prepared to act and close.

Thank You

Connect with us



Kale Logistics Solutions Private Limited
9th Floor, Thane One Corporate Business Park,
Behind CineWonder Mall, Majiwada,
Thane (W), Maharashtra, INDIA - 400 610.

☎ +91 22 4113 4113 ☎ +91 22 4113 4123

✉ info@kalelogistics.com www.kalelogistics.com

India | UAE | Mauritius | Kenya | Netherlands | USA | Canada

This material was used during an oral presentation; it is not a complete record of the discussion. This work may not be used, sold, transferred, adapted, abridged, copied or reproduced in whole on or in part in any manner or form or in any media without the prior written consent. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners.