ADDRESSING RAIL CYBER THREATS IN ESCAP REGION

Basri Berahim
Associate Technical Director, AtkinsRéalis
Basri.Berahim@atkinsrealis.com

High Level Meeting on Deepening Digitalization of International Rail Transport in Asia Pacific
Xi'an, China

AtkinsRéalis

Introduction

Over **20 years of experience** across **railway systems engineering**, **telecommunications**, and **cybersecurity**, with a specialized focus on **rail and industrial control systems (ICS/OT)**.

Domains:

- Rail System Engineering & Assurance
- Physical & Cyber Security
- Telecommunications
- ICS/OT Cybersecurity
- System Integration & Testing
- Project and Risk Management

Industry Focus:

- Primarily **rail and transportation**, with additional experience in **oil & gas** and **aviation/air traffic systems**.

Geographic Scope:

- Worked across **Asia Pacific**, **Middle East, Australia.**

Key Strengths:

- Bridging technical and managerial roles
- Implementing cybersecurity in industrial and transport environments
- Leading multi-disciplinary teams in high-stakes infrastructure projects
- Deep familiarity with international cybersecurity standards (IEC 62443, TS 50701, EN 50126, ISO 27001, etc.)

AGENDA

01 ESCAP’s Urgent Challenges

02 ESCAP’s Cybersecurity Threats

03 Laws and Regulations

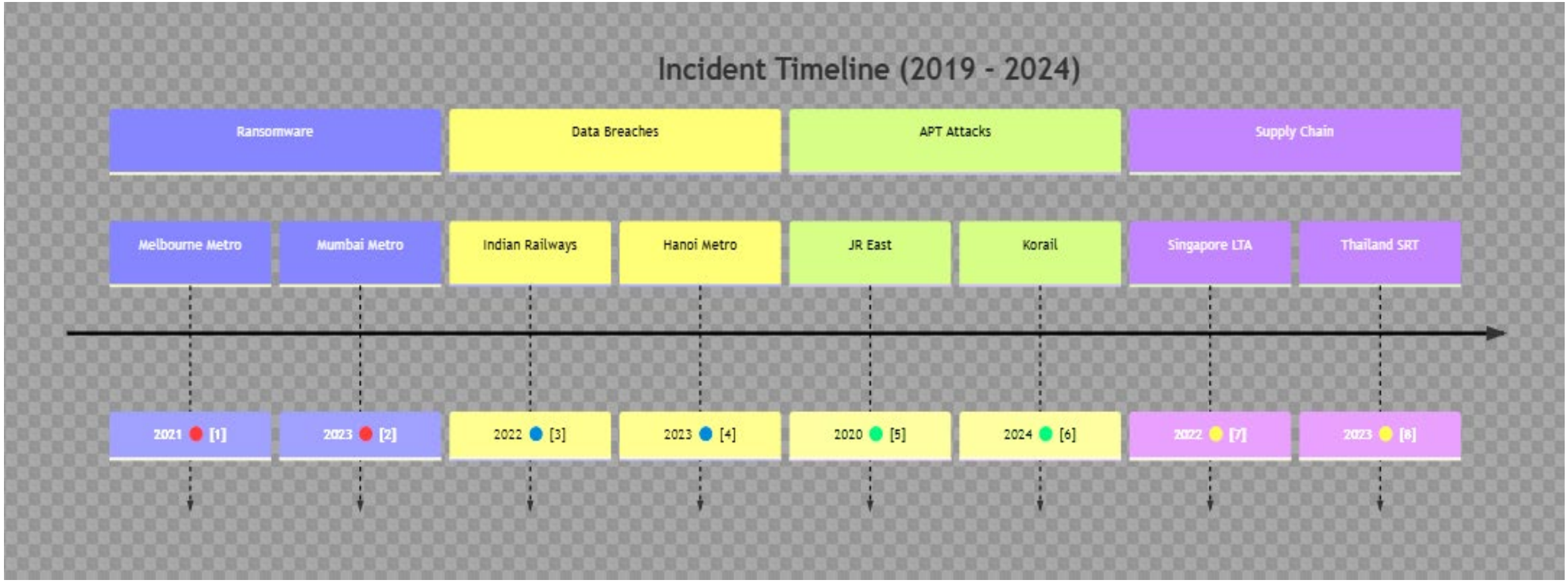
04 Lesson Learned

05 Keys Takeaway

06 Private Sector Engagement

07 Key Takeaway

ESCAP Regional Urgent Cyber Challenges



Private & confidential
AtkinsRéalis - Baseline / Référence

ESCAP Regional Urgent Cyber Challenges

1. Ransomware & Operational Disruptions

Australia (2021): Melbourne Metro Trains ransomware attack.

- Impact: Manual operations for days; >$1M AUD recovery costs.
- Source: ACSC Annual Cyber Threat Report 2020–21

India (2023): Mumbai Metro ticketing system ransomware attack.

- Impact: 48-hour outage; 500k+ passengers affected.

2. Data Breaches & Privacy Risks

India (2022): Northern Railways data leak (30M+ passenger records).

Vietnam (2023): Hanoi Metro payment data theft.

- Impact: Kiosks shut down for encryption upgrades.
- Source: VNISA Report

ESCAP Regional Urgent Cyber Challenges

3. Third-Party & Supply Chain Risks

- **Singapore (2022)**: LTA vendor breach (rail project data leaked).
  - **Source**: LTA Statement
- **Thailand (2023)**: SRT contractor ransomware attack.
  - **Impact**: Delayed maintenance schedules.
  - **Source**: Thai CERT Advisory

4. Emerging Threats (2024)

- **Indonesia (2024)**: Jakarta MRT insider threat incident.
  - **Impact**: Unauthorized access to signaling logs.
  - **Source**: BSSN (Indonesia's NSA) Bulletin

Most recent cyber incidents in the ESCAP region have focused on **IT systems** like **ticketing, passenger data, and vendor platforms**. However, as **IT and OT systems become more connected**, the risk of attackers moving into operational technology (OT) systems is growing.
Examples like the **Spanish power outage may cause by cyberattack** and the **Poland tram hack**—where a remote control was used to derail trains—show how real the **threat to OT systems** has become.

ESCAP countries must now expand their cybersecurity focus to protect OT Systems such as signaling, SCADA, and train control infrastructure.

ESCAP Cybersecurity Threats

Key ESCAP-Specific Threats Observed

1. Ransomware Targeting IT/OT Convergence
2. Phishing Attacks on Legacy Systems
3. Third-Party Vendor Risks
4. Data Leaks from Unsecured Databases

Top 3 ESCAP-Specific Threats:

1. Hybrid Attacks (e.g., phishing + OT breaches).
2. Supply Chain Compromises
3. Ransomware-as-a-Service (RaaS) targeting SMEs in rail ecosystems.





National Laws Protecting Rail & Transport Infrastructure

1. Comprehensive Rail Protections

- **China**:
  - *Cybersecurity Law (2017) + Critical Information Infrastructure (CII) Regulations (2021)*
  - Mandates **data localization** and **security reviews** for rail operators
  - Requires **MLPS 2.0** compliance for rail CII systems
- **Japan**:
  - *Basic Act on Cybersecurity (2021 Revision)*
  - Explicitly designates railways as **Critical Infrastructure**
- **South Korea**:
  - *National Cybersecurity Strategy 2024 + KS X ISO 27001*
  - Mandates **real-time OT monitoring** for metro/rail systems

2. Emerging Rail Frameworks

- **Australia**:
  - *Cyber Security Act 2024 + Security of Critical Infrastructure (SOCi) Act*
  - Requires **72-hour incident reporting** for rail operators
- **India**:
  - *Telecom Cyber Security Rules 2024* (under IT Act 2000)
  - NCIIPC classifies rail IT/OT as **Critical Information Infrastructure**
- **Singapore**:
  - *Cybersecurity (Amendment) Bill No. 15/2024*
  - Covers **overseas cloud-based rail assets** (e.g., SCADA systems)

3. Developing Frameworks

- **Malaysia**:
  - *Cyber Security Act 2024*
  - Protects **transportation system** under NCII but not rail specific.
- **Indonesia**:
  - *Presidential Regulation No. 47 of 2023*
  - Includes transport sector but **lacks rail-specific standards**
- **Vietnam**:
  - *Cybersecurity Law (2018)* + *Decree No. 53/2022/ND-CP*
  - Enforces **data localization** for passenger systems
- **Cambodia/Laos**:
  - Draft laws cover transport but **omit rail specifics**

From Fragmentation to Unified Standards

Key Gaps Identified

Definitional Gaps:

- *Example*: Malaysia's NCII vs. India's NCIIPC scope differences.

Vendor Rules:

- *Example*: Thailand's Cybersecurity Act lacks OEM cybersecurity clauses.

Legacy Systems:

- *Example*: Indonesia's Presidential Regulation doesn't address legacy rail OT.

Gap	Regional Solution	Model Law
Critical Infrastructure Definitions	Unified ESCAP rail CII list (signaling, ticketing, OT)	Japan's Basic Act
Vendor Compliance	Subregional OEM cybersecurity standards	Singapore's Amended Bill (2024)
Legacy System Upgrades	Phased modernization with risk assessments	EU's CENELEC TS 50701

ESCAP's Proposed Solutions

Private & confidential
AtkinsRéalis - Baseline / Référence

Regulations: Foundations for Regional Harmonization

SUBREGION	COUNTRY	KEY LAW/POLICY	RAIL-SPECIFIC PROVISIONS
Southeast Asia	Singapore	Cybersecurity (Amendment) Bill No. 15/2024	Covers overseas/virtual rail assets (e.g., cloud SCADA)
Southeast Asia	Malaysia	Cyber Security Act 2024	Mandates NCII protections for transportation systems
South Asia	India	Telecom Cyber Security Rules 2024	NCIIPC includes rail IT/OT systems
East Asia	Japan	Basic Act on Cybersecurity	Explicit railway inclusion in critical infrastructure
Oceania	Australia	Cyber Security Act 2024	Incident reporting for rail operators (72-hour window)

Learning from ESCAP's Rail Cybersecurity Experiences

1.India's RailCERT

- Centralized threat monitoring for railways.

2.Australia's SOCI Act Compliance

- Mandates cybersecurity audits for rail vendors.

3.Japan's AI-Driven Threat Detection

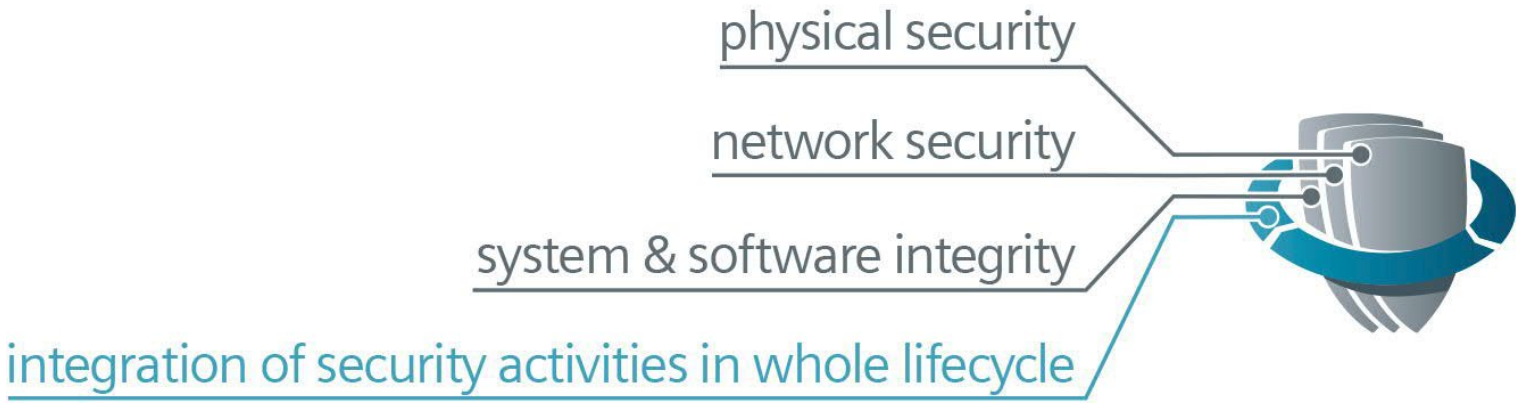
- Real-time anomaly detection in signaling systems.

Country	Incident	Response	Lesson for ESCAP
Japan	JR East signaling hack	Upgraded OT network segmentation	Isolate legacy signaling systems
India	Northern Railways breach	Launched RailCERT	Encrypt passenger/employee data
Australia	Metro Trains ransomware	SOCI Act compliance	Mandate vendor cybersecurity audits
South Korea	Korail APT breach	Nationwide phishing drills	Train staff on threat detection

Private & confidential
AtkinsRéalis - Baseline / Référence

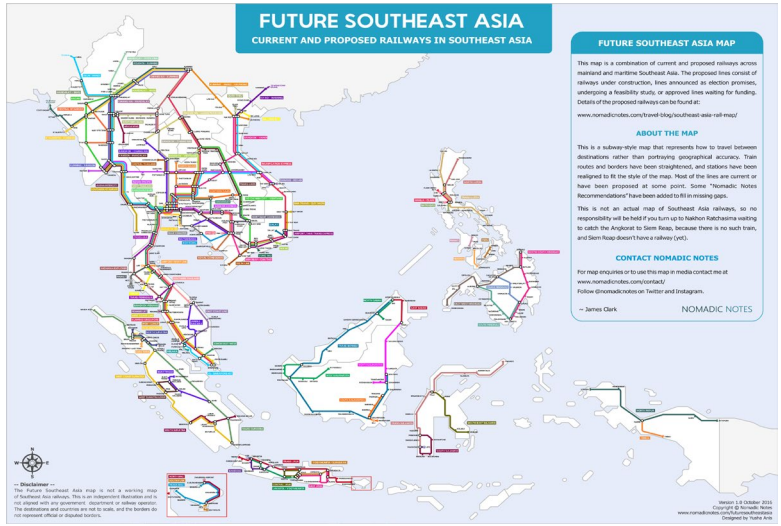
Lesson Learned Keys Takeaways

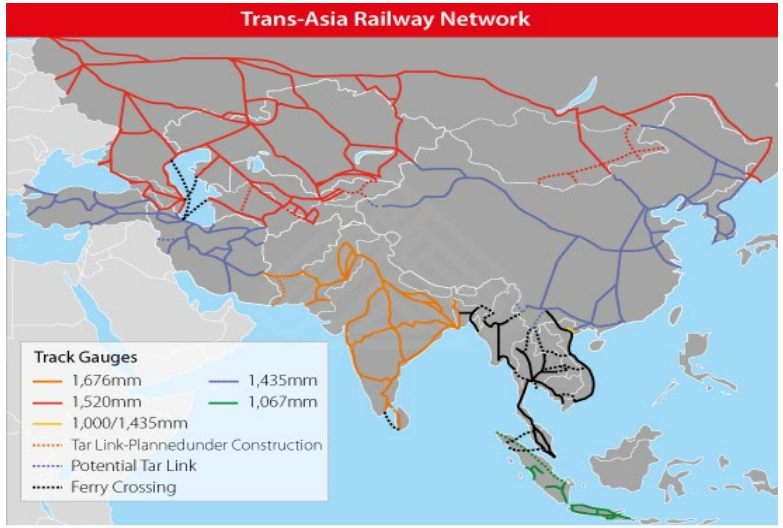
- Most ESCAP rail cyber incidents target IT systems (e.g., ticketing, databases).
- Ransomware, phishing, and data leaks remain major threats.
- OT systems (signaling, SCADA, train control) are increasingly at risk.
- Examples like the Spanish power outage and Poland tram hack show OT can be targeted.
- Urgent need for ESCAP members to expand focus from IT to OT cybersecurity.
- Regional cooperation and harmonized standards are essential for resilience.
- Cybersecurity-by-design must be embedded across the rail asset lifecycle.



ESCAP Rail Cybersecurity: Key Pillars

- **5-Pillar Overview**:
  - Policy harmonization.
  - Regional standards
  - Capacity building.
  - Regional Rail Cybersecurity Group (RRCG).
  - Private sector engagement.





Conclusion - From Dialogue to Action

- ESCAP rail systems face growing and complex cyber threats.
- Most attacks start in IT systems but can spread to OT systems like signaling and SCADA.
- Different national laws and standards **create gaps and risks in cross-border** rail projects.
- A **Regional Rail Cybersecurity Group (RRCG)** should be formed to lead coordination.
- ESCAP should develop a **common cybersecurity framework** for all member states.
- **Shared standards** will help with vendor requirements, incident response, and OT protection.
- **A united regional approach** will improve resilience and support safe digital rail operations.



"Cyber-resilient railways demand shared responsibility—across borders, sectors, and supply chains."

Basri Berahim
Associate Technical Director, AtkinsRéalis Asia
Basri.Berahim@atkinsrealis.com

AtkinsRéalis

Our Values

01 **Safety:** We put safety at the heart of everything we do, to safeguard people, assets and the environment.

02 **Integrity:** We do the right thing, no matter what, and are accountable for our actions.

03 **Collaboration:** We work together and embrace each other's unique contribution to deliver amazing results for all.

04 **Innovation:** We redefine engineering by thinking boldly, proudly and differently.

05 **Excellence:** We are proud to do our best, achieve high standards, creating environments where all can thrive.

Our values are the essence of our Company's identity. They represent how we act, speak and behave together, and with our clients and stakeholders.