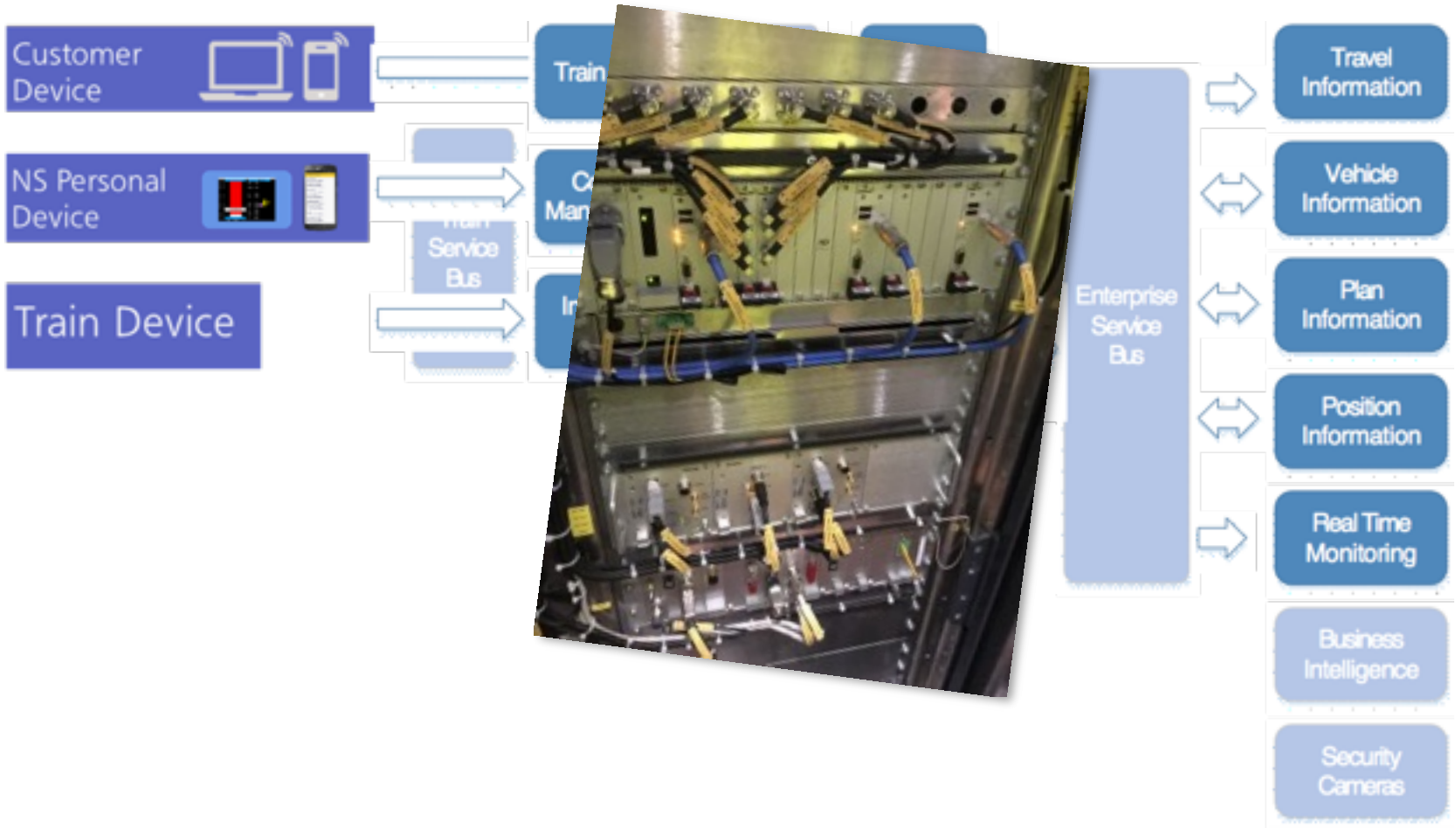
Implementing governance of train cyber security

Gertjan Tamis, Information Security Officer
NS/Dutch Railways
Vienna, November 29

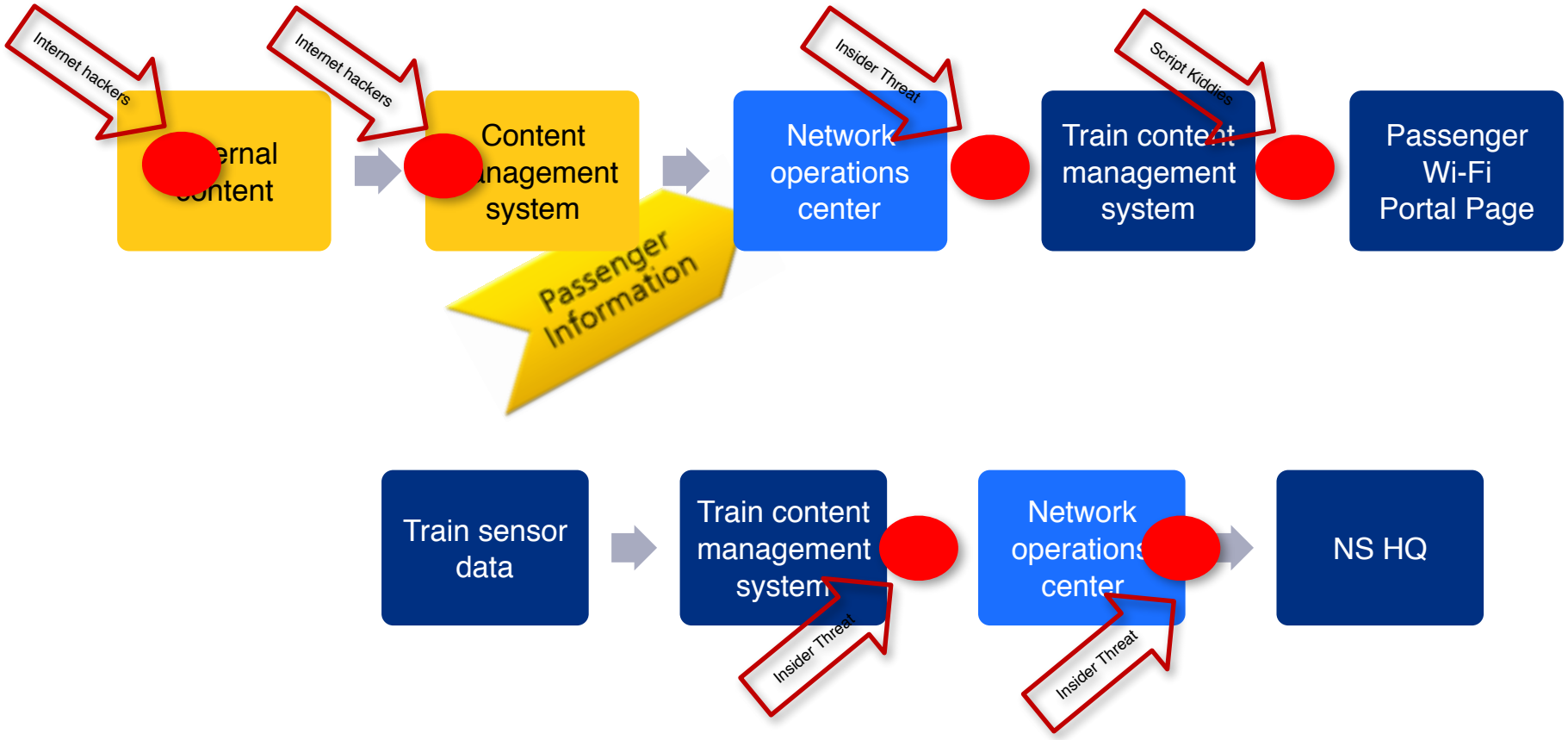
Agenda

- Setting the scene: train cyber security
- Performing cyber risk assessments for trains
- Implementing governance of internal risk reduction

Today trains are datacenters on rails

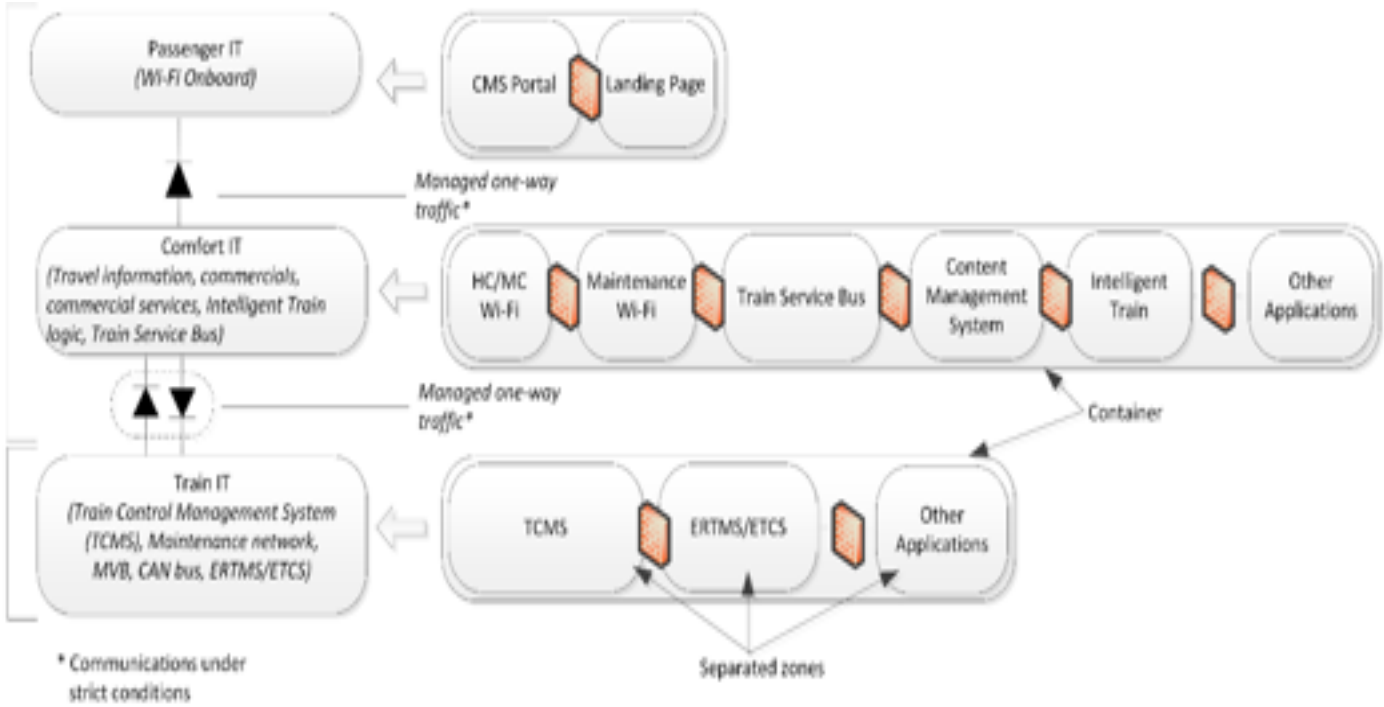


Which information flows through a train and where are the threats?

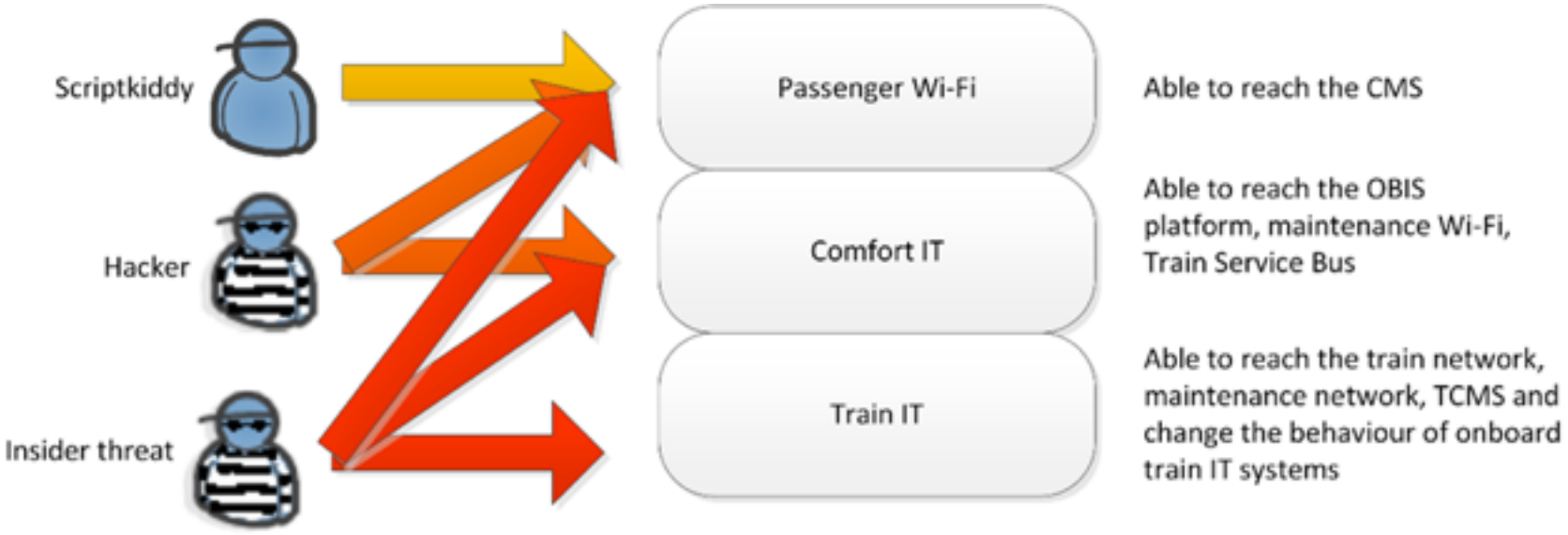


Some of the security measures in place

- Train IT security architecture
  - Separation of information flows
  - Managed connections
- Physical security measures
- Information chain security reviews
  - Passenger Wi-Fi
  - Comfort-IT
  - Way-side connections
- High level risk inventory in the IT Train domain

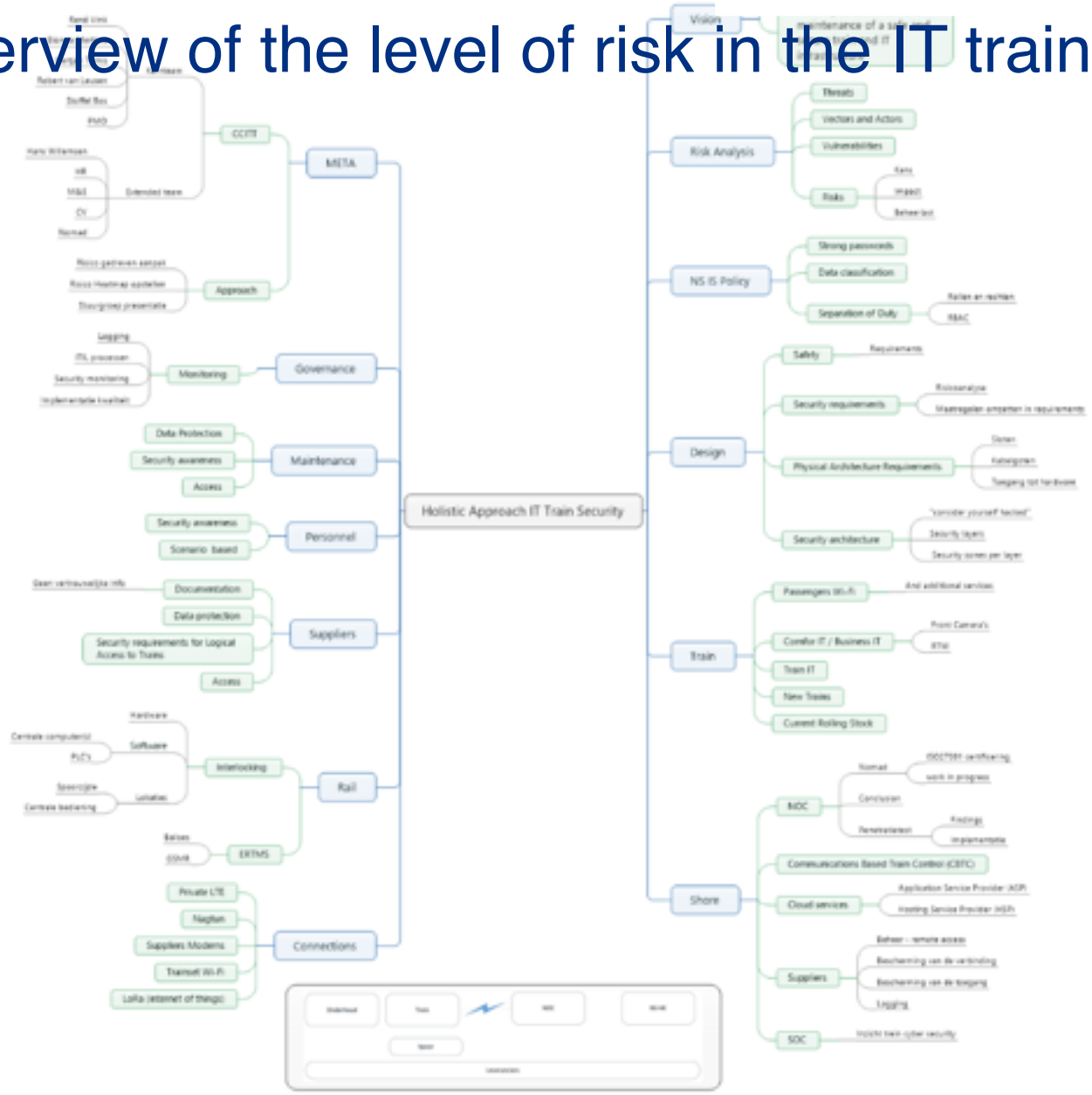


Determine IT risks for the train, and what are the actors



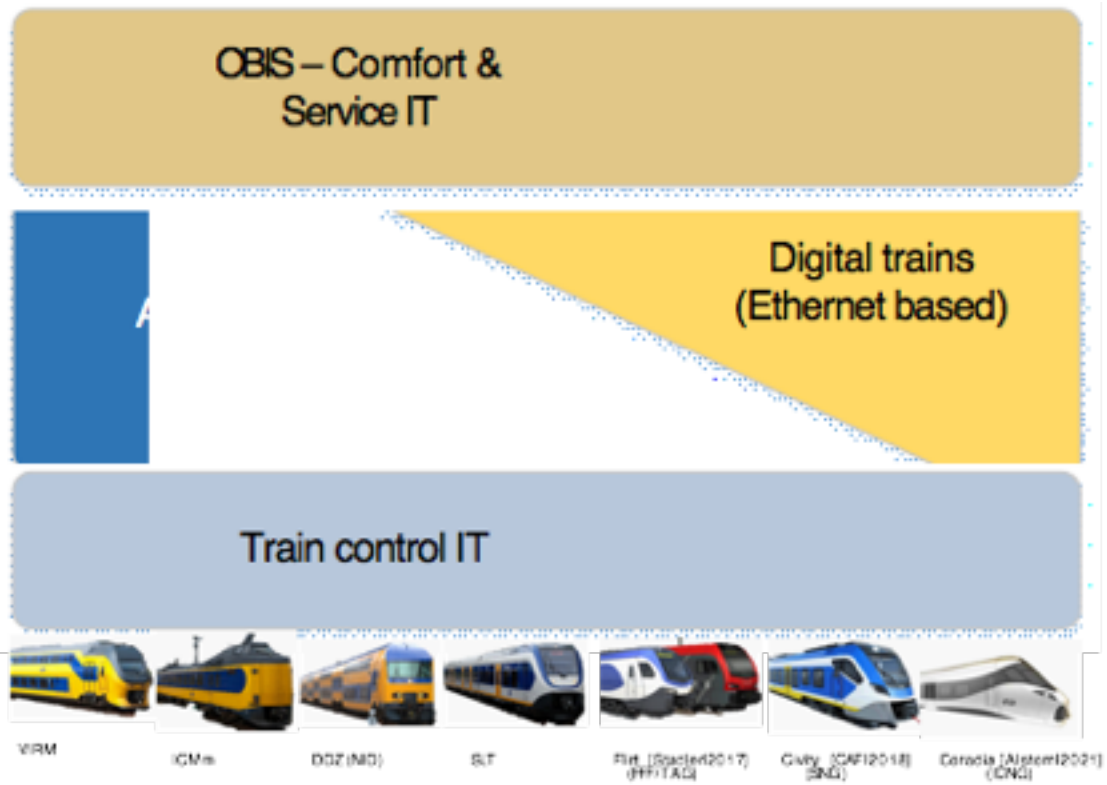
Legend
CMS: Content Management System
OBIS: Onboard Information Systems
TCMS: Train Control Management Systems

We need a complete overview of the level of risk in the IT train domain



Different train types mean different IT security risks

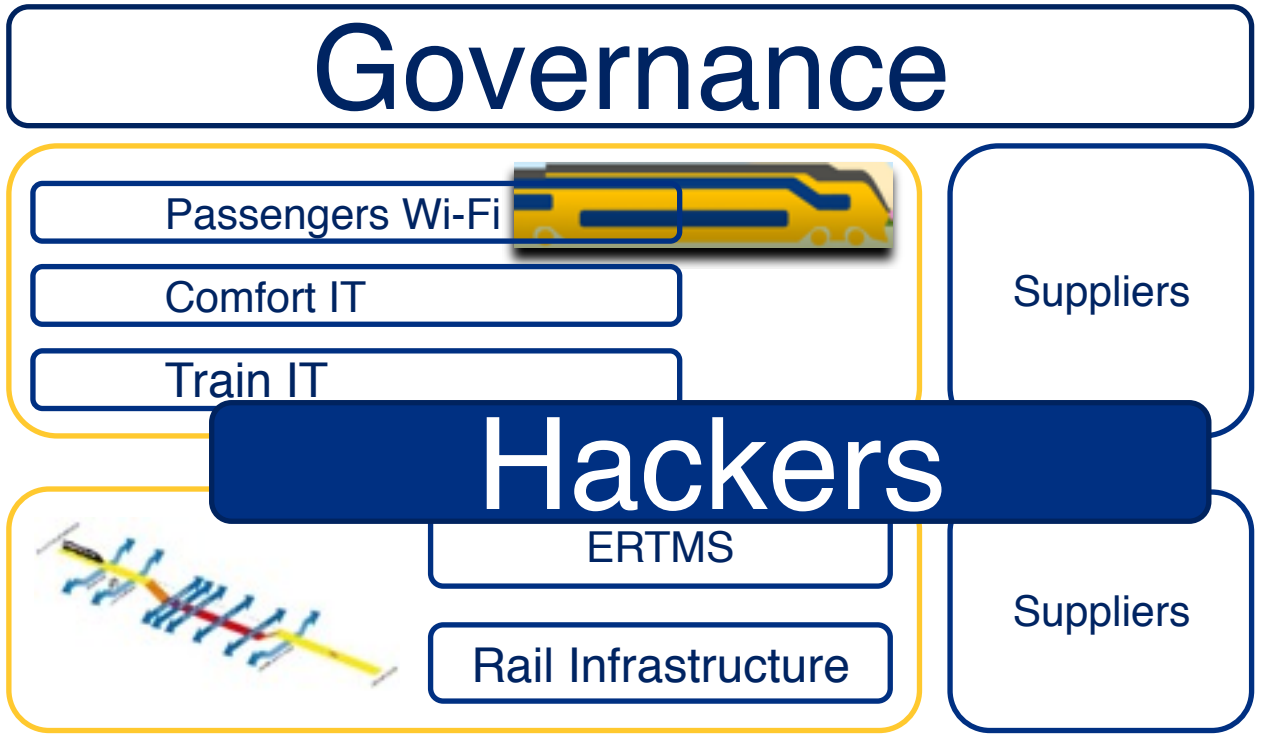
- Different hardware platforms
- Generic Comfort IT platform
  - On Train IT level the cyber risk may be different (CANbus, MVB, IP/ethernet based trains)
  - On Comfort IT we have the same level of cyber risk



Risk based approach to determine priorities

- ISF Information security baseline
- Risk inventory interviews
  - Maintenance/System/Reliability engineers
  - Maintenance managers
  - Train system architects
- Workshops
  - Risk consolidation
- Resulting in a Train Risk Bow-tie

NS has a need for integral security governance of trains



*note: Hackers ignore artificial separations of domains

Implementing governance to achieve appropriate risk reduction

- Implementation of risk governance
  - A follow-up of the IT train domain risk inventory
- Risk owners
  - Identify the possible risk owners
  - Do they understand their ownership and responsibilities?

Implementing governance to achieve appropriate risk reduction

- Processes
  - Software asset management
  - Change management
  - Threat and vulnerability management
- Projects
  - Further investigation of attack paths and security risks
  - Define acceptable risk
  - Investigate existing security measures
  - Implement necessary risk reduction

Ideas on how to implement governance of train cyber security

- Create a team with
  - Responsible stakeholder(s)
  - Operational managers
  - Subject matter expert(s)
- Direct improvements
  - Process implementation
- Monitoring and reporting
  - Define operational KPI's (or use existing KPI's)
  - Monitor progress
  - Act on lack of progress
- This sounds like your daily job

Take aways

- Make sure that you know where your risks are
  - In a mixed train environment you will have several risk levels
- Who are the risk owners?
  - Are they aware of their responsibilities?
- Are your IT processes in place?
  - Are you sure?
  - How about threat and vulnerability management?
- Use a project based approach
  - Monitor progress
  - Use internal knowledge

Gertjan Tamis

Information Security Officer

E gertjan.tamis@ns.nl

NS | IT BAS | CoE Information & Risk Management
Laan van Puntenburg 100
Postbus 2025, 3500 HA Utrecht