CER
The Voice of European Railways

The railway sector perspective on cyber security

CyberSecurity4Rail

Brussels, 4 October 2017

Dr Libor Lochman, CER Executive Director

CER – who we are

CER
The Voice of European Railways

More than
70
Members and partners

73%
of the European rail network length

80%
of the European rail freight business

95%
of rail passenger operations in Europe

CER's business priorities

CER
The Voice of European Railways

1. Legislation

- Contributing to the implementation of the 4th Railway Package's Technical Pillar

2. Digitalisation

- *Shaping digitalized railways to better serve rail customers: FSM, ERTMS, Connectivity, etc.*

3. Rail corridors

- Strengthening the development of the Core Network Corridors

4. Regulatory framework

- Improving rail's intermodal competitiveness, Road Package, Combined Transport, Noise

Railways' commitment to digitalisation

- Digitalisation = top priority
- Objective: highly efficient and attractive transport options
- Meet the specific demands of railways, their staff and customers
- Integration into the digital ecosystem
  - More joined-up work; building win-win partnerships
- Ensure safety, **security** & sustainability

From traditional physical to emerging cyber threats

CER
The Voice of European Railways

- From 'closed' IT network with high level of security to increasingly 'connected' systems → exposed to cyber-threats
- Intentional as well as accidental cyber security threats (sources: terrorists, criminals, hackers, competitors, malware developers, employees…)
- Cyber-attacks growing in scope and sophistication

What is at stake?

- Disruption of rail services
- Economic losses for railways and their customers
- Loss of commercial or sensitive information
- Reputational damage
- Potential risks to safety

Security a priority to railways

- Comprehensive security strategy
  - Holistic, proportionate and coordinated
  - Flexible and risk based
- Close cooperation between different players
  - RUs & IMs
  - National authorities
  - Suppliers
  - Service providers…

Railways' approach to cyber security

- (Cyber) security risk assessment
- A set of technical, procedural and managerial security measures
- Training and awareness-raising
- Information sharing & exchange of good practices with other stakeholders
- Regular review of introduced measures
- Implementation of NIS directive

Rail compliance with NIS Directive

- Understand cyber risk
- Protect railway assets
- Reduce the impact of cyber security incidents
- Ensure timely reporting of these events
- Share information on cyber activity with stakeholders

EURail-ISAC?

- Any initiative for an ISAC should not lead to duplication.
- Integrating ISAC in Rail Common Occurrence Reporting system is the opportunity to address security alert in a professional and robust way.
- In case of cyber threat, security contact person will first be involved but also safety manager should get the alert.
- ERA has key role to play

Cyber security at European level

- EU to continue addressing the issue of cyber security
- Enhanced cooperation & coordination among national authorities
- Better exchange of information & intelligence
- Development of guidance & practical tools at EU level
- Exchange of good practices

Further European action?

- Identify the main obstacles → create necessary policy framework
- Foster research & development
- Overcome imbalances between EU territories
- Financial instruments
  - ESI, EFSI, Horizon 2020 and others

For further information:

Dr Libor Lochman
Executive Director
Tel: +32 (0)2 213 08 71
E-mail: libor.lochman@cer.be

For regular updates on CER activities,
visit our website: **www.cer.be**
or follow **@CER_railways**

CER
The Voice of European Railways