"CyberSecurity4Rail"
Railway Industry Conference
Brussels 4th October 2017

hitrail
european railway IT & data communications

Conference Report

1. Welcome and overview: "Co-operation is essential in the quest to manage technology and people for security".

Helmut Grohman, Chair of Hit Rail, opened the conference and identified that digital security must be in the DNA of the Railway Sector. Herr Grohman shared many examples of recent security breaches that demonstrate widespread practices putting data, information and control systems at risk. Practices inside and outside organisations, as well as company arrangements for cyber security, indicate a broad range of risks arising from technology and people – their relationship is crucial. Herr Grohman emphasised that there are no easy technical solutions to management, but there are management solutions to technology and people. We need to manage technology and people in ways that ensure security, and we can only do that through cooperation in a European sector where everything is interconnected and therefore interdependent.

Herr Grohman clearly states criminals are often one step ahead of so-called security experts, and so time to react is becoming vital - we are in the middle of an intelligence race – and we need to win!

It was noted by **Karin Helmstaedt, the conference moderator,** that Mr Junker in his "state of the union address"[1] emphasised cyber security, and noted that "wannacry"[2] affected systems in 150 countries – no country and no organisation is free from the attention of cyber criminals, and collaborative improvement of cyber security is the only remedy.

[1] President Juncker "State of the Union" 2017 - https://ec.europa.eu/commission/state-union-2017_en
[2] "wannacry" ransomeware attack - https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

2. Cyber security – don't be a victim: "Information is power and control of information has unexpected consequences".

Corrado Giustozzi, senior Cybersecurity strategist from SELTA, reaffirmed that information is power for example: the largest taxi company owns no cars (Uber) yet its value is 15 times that of Hertz; the most popular media provider (Facebook) produces no content, yet holds data on millions of customers and the largest property rental company has no property (AirBnB). These and other examples confirm that value is often expressed in control of information and control of business processes. The example of Associated Press which was hacked to report President Obama being injured, showed how the US Stock Exchange value was negatively affected within minutes – control of information can impact finances in unexpected ways.

Examination of computer systems in the 1970's demonstrated that the main security risk was people, and the arrival of Internet has driven a massive rise in connected host systems, thereby providing opportunities to maliciously intrude on these hosts remotely via their network connection. With predicted Internet traffic of 5 Billion Terabytes per day by 2020, the opportunities for intrusion and information misuse are expanding enormously. This is greatly aided by the "Internet Of Things"[3], where smart devices in all aspects of life are connected to networks, providing further points of intrusion. Yet, the human factor is ever present since people can provide access routes either on purpose (insider threats) or by errors of judgement, emphasising need for resilient management.

The increasing references to Cyber Space, Cloud, etc. suggest a separate domain of activity, but in reality, cyber space is not topological – it is the real world and comprises all computer systems and networks – it is the 'here and now' – so cyber threats are threats to us, to our organisations, and to our information and control systems. Even systems that seem to do "nothing of interest" present risk, since they are interconnected with others and so present access routes – all interconnected systems are of interest to cyber criminals – and criminals have always exploited the weakest link.

Many real-world examples were presented to show the range of sophisticated methods used by cyber criminals, including access to Lockheed military secrets[4] simply by accessing RSA's Secure ID Tokens – the unexpected doorway is often the route for access.

[3] Security in Internet of Things, Bauer et.al. - https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things

[4] Lockheed security breach - https://www.theregister.co.uk/2011/06/06/lockheed_martin_securid_hack

3. The regulators' view on cyber security: "Multi-modal transport requires data exchange and interconnection".

Josef Doppelbauer of European Agency for Railways (ERA) welcomed the broad awareness of cyber security brought by the previous speakers, and brought the focus to railway-specific considerations. Herr Doppelbauer noted that railways themselves need to cooperatively identify the real risks to essential service operators in railway transport. We have a European Rail Area, yet we also have National rules, regulations and languages. The European rail policy aims to make rail more competitive, and has been very successful to date, especially around technical interoperability and safety. The remaining challenges of rail innovation, being largely focused on customer requirements around mobility and logistics, is even more dependent on digital technology. This is a disruptive innovation, bringing changes to very mature practices, and emphasising the security concerns. The multi-modal transport chain, including rail, requires data exchange between a wide range of actors and between a wide range of systems – their interconnection is the main risk to security.
While we are focused on data and the transport activities that depend on it, we must remember we are considering a range of critical life issues – security of passengers, security of freight, security of passenger- and freight-related data, and security of people and environments through which dangerous goods pass.

Current work is addressing a range of issues using different approaches. CENELEC standards on cyber security, along with the Shift2Rail response to rising demand for transport capacity, are also supported by the ERA Action Plan which takes account of emerging issues around cyber security. The ERA Action Plan development includes collaboration with other areas examining common interests (e.g. Maritime) and supports the formation of a European Rail ISAC[5].

[5] ISAC Definition - https://www.nationalisacs.org

4. Security in the SERA – policy considerations: "The need for common understanding, guidelines and best practices".

Carlos Mestre, Head of DG Move Unit "Security" presented the broad coverage of security issues addressed by DG Move, and confirmed the rapidly growing emphasis on cyber security, including focus on the Single European Rail Area (SERA). It was noted that traditionally, security relies on "inspection", and until now the idea of inspecting firewalls, etc., was a challenge, but it is increasingly the case that organisations emphasise deployment of good practice, and we can examine if and how good practice is deployed. The threat from cyber-crime and the recent impacts were considered in some detail, and it was noted that 80% of EU companies experience at least one cyber security incident, with many companies experiencing numerous attacks. The impacts and potential impacts on the transport sector are increasing, and cyber is recognised as the new frontier in fighting crime. European Commission advice and guidance on prevention of cyber-crime has been published and updated since 2013, and it is clear that we need to keep updating our knowledge of threats and solutions, not just annually but continuously - and so cooperation and exchange of knowledge is critical. While many organisations are capable in dealing with cyber security, the Commission emphasises the need to support all business, and to reduce fragmentation in the cyber security market – this will include a certification scheme for cyber security products.

The NIS directive includes emphasis on transport, and on collaboration between regulators, governments, business, and especially operators of "essential services" to exchange knowledge and cooperate in ensuring European resilience, especially of critical infrastructures. However, each Member State may interpret NIS requirements differently, and so in European transport we need to ensure a common understanding, supported by common guidelines and best practices. Cyber Security needs to become a core part of business operations and business continuity thinking. The lack of cyber security knowledge in staff dealing with routine IT practices is a challenge, and DG Move aims to deliver a toolbox to support training of staff in this regard.

It is up to all of us to implement measures to fight cyber-crime, and none of us can do it alone.

5. The Network and Information Security Directive (NIS Directive): "A host of European actions in cyber security"

Dr Florent Frederix of DG CNECT Trust and Security Unit presented the Network and Information Security Directive (NIS)[6] and the requirement for railway collaboration. Dr Frederix confirmed the importance of the messages from preceding speakers, and introduced several European actions on cyber security supported by a range of examples. Automatic train operation in the freight sector, digital signalling, and railway management on networked IT platforms were demonstrated as inter-connected examples where intrusions in one area can be used to access others. Networks, by definition, are pathways to selected targets.

The EU Cybersecurity Strategy[7]: An Open, Safe and Secure Cyberspace, launched by DG Home Affairs, drives the NIS Directive[8] and is aimed to increase national Cybersecurity Capability, EU Level cooperation, and improved Risk Management.

The CSIRT/CERT network, conceived by DG CNECT, includes a Cooperation Group (supported by EU, ENISA and Member States), as well as a network of National CSIRT/CERT organisations (Computer Security Incident Reporting Team – Computer Emergency Response Team). CSIRT/CERTs are driven by national competent authorities who provide a National Contact Point, and these in turn provide representation and active participation in the Cooperation Group. The EC will establish operational rules to support further development.

The NIS Directive emphasises "operators of essential services" and encourages Member States to interpret the Directive to meet needs for cooperation between such operators.

The Cybersecurity Contractual Public-Private Partnership will provide 450M Euros of grants as part of Horizon 2020 R&D budget to increase cybersecurity, including transport.

A Cybersecurity competence centre will also be established to address cybersecurity challenges.

[6] NIS Directive Summary and Links - https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[7] EU Cybersecurity Strategy - https://ec.europa.eu/home-affairs/what-is-new/news/news/2013/20130207_01_en

[8] NIS Directive source documents - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

6. The railway sector perspective on cyber security: "Integrated approach to security and safety without duplication".

Dr Libor Lochman, executive Director of the Community of European Railway and Infrastructure Companies (CER)[9] emphasised CER business priorities: Legislation; Digitalisation; Rail Corridors; Regulatory Framework. These are strongly inter-linked by concerns over Cybersecurity, especially since Railway Corridors cannot be realised without interconnection of information and control systems to meet the demand of railways, their staff, and their customers. Integration provides a win-win partnership, and needs a secure collaboration to ensure gains are not interrupted or challenged. Intentional as well as accidental cyber threats need to be better understood and remedied. A shared approach can ensure minimisation of disruption/loss of precious concerns: rail services; economic losses; commercial/sensitive information; reputation.

The coordinated security strategy should be proportionate, holistic, flexible, and based on cooperation between a range of actors (RU, IM, National Authority, Suppliers, Service Providers, Cybersecurity Expertise, etc.).

The railway approach must address a range of concerns: risk assessment; clear technical, procedural, managerial security measures; training and awareness; information sharing about good practice.

Rail compliance with the NIS Directive is necessary, and an EU-Rail ISAC should not lead to duplication. It should benefit from an integrated approach alongside current cooperative developments such as the "Common Safety Methods" which already includes the proposed Rail "Common Occurrence Reporting" System. Enhanced cooperation and coordination should emphasise a better exchange of information and best practices to benefit all actors in the development of an increasingly cyber-secure European Rail Area.

Dr Lochman recommended that further European action could usefully identify main obstacles, foster Research and Technology Development (RTD), overcome resistance, and help with finance of new shared actions.

[9] CER - http://www.cer.be

7. How airlines protect against cyber-attack: “Adversaries are not systems, but people who are smart and who pursue goals”.

Philippe-Emmanuel Maulion, Corporate Information Security Officer of SITA (Société Internationale de Télécommunications Aéronautiques) shared perspectives from the air transport sector, with numerous practical examples.

The threat landscape addressed by SITA includes airports, aircraft, air traffic management and all steps in between – the whole cycle of air transport covering both passenger and freight security. Motivated, sophisticated and targeted cyber-attacks are evident across the expanse of global air transport. Many attacks are not necessarily aimed at the air industry per se, but are part of global attacks aimed at specific countries or regions. Cyber security is therefore a key business issue, and cyber security related expenditure is forecast to grow 8.3% CAGR through 2020 in the air transport sector.

Cyber threat intelligence gathering reveals that adversaries are not systems, but people who are smart and who pursue goals. They are professionals and are well funded either by crime or by political aims.

Applying cyber threat intelligence tends to follow a military-style approach, is highly structured, and is based on years of experience. Intelligence reports support operational decision making and shared understanding between security actors.

Typical attacks show seven stages: reconnoitre; weaponize; deliver; exploit; control; execute; maintain. Defending each stage requires different intelligence / approaches to disrupt the flow of the attack. Proactive detection mitigation will address the early stages, while incident response processes deal with the later stages if they are achieved.

A range of actions to address each stage were presented. For example, self-reconnaissance can reveal your own weaknesses, and can allow you to identify what your adversaries can use/do against you – also fingerprints on your systems will show what is happening.
In general, cybersecurity intelligence must address:

- What campaigns are targeting my industry or similar companies to mine?
- Who are the adversaries I should be (most) concerned about?
- What is the nature of the attacker e.g. criminal, hacktivism, industrial espionage?
- What tactics, techniques and procedures (TTPs) are these attackers using?
- What are the TTPs most seen?
- What vulnerabilities are being exploited? Weaknesses most observed?
- How should I best adapt my defences to counter these attackers?
- How have other victims reacted?

These issues can be addressed in isolation, but with significant cost. Cooperation and sharing of information can reduce cost within a single industry, such as Rail, where issues to be addressed are greatly in common. Cooperation also speeds response and recovery.

The overarching goals should address:

- Identify weaknesses most observed.
- Identify vulnerabilities that are being exploited.
- Support informed decision making; clarify the risk landscape.
- Decrease the time to detect an attack.
- Prevent attacks.
- Augment incident response capability; facilitate investigation of attacks.
- Improve information security management practices.

All of these can be better addressed through cooperation within the European Rail Area.

Dr Maulion emphasised, in summing up: The cybersecurity threat is real, co-ordinated and happening now – across all industries, including rail; Cybersecurity intelligence can help individual organisations address and respond to threats; Industry-wide shared intelligence is most helpful to protect a specific industry.

8. Secure networks for collaborative services: “Networks are the risk – meshed networks provide a segmented and secure response”.

Mick Haynes, Technical Director of Hit Rail, addressed the theme of secure networks for collaborative services. Mr Haynes pointed out that without networks there would be few risks, and so we should be highly focused on reducing risks arising from networks – a network focus is mandatory. A range of different networks were reviewed (Internet, Internal business network and Virtual Private Networks), and it was shown that despite the many strategies deployed by business, the employees (human risk) using networks still manage to reduce resilience through common practices. These passive “insider threats” are greatly added to by connection to Internet, where cyber criminals exploit the fundamental insecurity of the Internet. Cyber criminals are tireless, and continually search for opportunities to enter any and all business systems where they may find ways to generate financial gains.

Mr Haynes then presented Hit Rail’s VPN (Virtual Private Network) as an example of how secure traffic can be ensured through segmentation of sensitive data away from other channels. The VPN is also used as part of a “meshed network” where strategies are deployed to ensure partition for highest security.

Access via a single Internet gateway ensures highest levels of monitoring for risk avoidance and has been completely successful. Only known private addresses are allowed to connect (no DNS hacking possible as there is no DNS). Virus detection is state of art, as is the Cyber Security Maturity Model. All incidents are recorded and analysed – changes of traffic /reduced activity / etc. are referred to a customer before being acted upon, and proactive recovery from incidents is assured. All assets are protected by latest measures, and no email is allowed (potentially risky traffic).

Hit Rail is failure free over the last 25 years, and its continuous review and improvement ensures keeping ahead of the risks.

It was shown how the various services in railway are protected, and how they show different levels of risk (e.g. signalling is high risk, and all services relying on Internet share the risk of easier intrusion).

Critical services are mainly:

- Control systems including signalling.
- SCADA networks.
- Sales services both passenger and freight- Infrastructure monitoring.
- Communication RU<->IM.
- International Communication for international services

It was noted that a range of attacks are well defended by the VPN strategy: physical access; hackers; browser hacks; ransomware; viruses; malware; denial of service (DDOS).
Even DDOS is protected against since reliance on typical Internet usage is avoided.
The business case for VPN was examined and shown to be such that just one incident would justify the costs over one year.

9. First panel discussion: Product liability, staff training & awareness, information sharing in both safety and security…".

The morning panel discussion raised a range of questions for debate.
The issue of regulation of technologies for security and risk was raised, and revealed a range of views on how to test and certify, and to maintain such an approach. The question of liability for products claiming to be cyber security products was suggested to be beyond current regulation, and required more attention. It was generally emphasised that liability for risk in software / hardware is an extremely complex area, and further underlines the need for railways to ensure usage of the most secure solutions so as to avoid risks.

Further discussion highlighted the need for railways to train and equip staff as specialists in cyber security. Debate underlined lack of maturity within railways in relation to this new area of challenges, and there is clear opportunity to share knowledge and experience around training to deliver the new capacities required.

The exchange of cyber security information was discussed in the context of common occurrence reporting, but speakers noted differences in objectives and the difference in focus. The special nature of Cyber Security may not easily be fitted into the current project which, in itself, faces difficulties in acceptance by Member States, some of which question the need for information exchange around physical safety (the original poject focus).

Other discussions focused the need to encompass all digital technologies that may provide cyber security risks, and the need to continually update that perspective, as well as each railway recognising and addressing system changes within a well-managed cyber security strategy.

10. Cyber security and resilience of transport infrastructure: "Current European initiatives in cyber security supporting Rail"

In the afternoon, the focus on implementing the NIS Directive was initiated by **Rossella Mattioli, Security and Resilience of Networks Officer, ENISA[10],** who presented further details of aspects of cyber security and resilience related to transport infrastructure. ENISA activities were presented, to set the context, and included numerous cyber security related publications, as well as actions such as Cyber Europe - an annual exercise around the IT, telecommunication and cybersecurity industries. The exercise includes technical incidents for the participants to analyse, covering forensic and malware analysis, mobile infection, open source intelligence, drones, etc.

Concerning the NIS Directive, ENISA provides information, advice and support for specific initiatives in areas such as Finance, Internet of Things (IoT), Smart Infrastructure, eHealth and Smart Hospitals, as well as Smart Cities (shown to be systems of systems).

ENISA is now also focused on transport, following events such as the San Francisco railway hacking, and presented cyber security for transport in a Smart Cities context – attack scenarios, threat analysis, good practice/security measures, and collaborations to enhance cyber security. Cooperation is emphasised since common threats are faced. Smart Cars are a new attack surface in the transport area - airports and SCADA were also addressed (reports available online[11]).

ENISA will soon bring more focus on Rail transport, and recommends in the meantime:

- Consider the cyber security impact on safety.
- Include cyber security in your governance model in order to define liabilities.
- Ensure you consider cyber security in all stages of the life cycle of products and services.
- Consider network connectivity and interdependencies and cascading effects.
- Start reusing existing good practices from other sectors, for example for SCADA.

The goals of ENISA could be a useful reflection for the proposed railway cooperation mechanism:

- Raise the level of awareness on Infrastructure security in Europe.
- Support Private and Public Sector cooperation with focused studies and tools.
- Facilitate information exchange and collaboration.
- Foster the growth of communication networks and industry.
- Enable higher levels of security for Europe's Infrastructures.

[10] ENISA – European Agency for Network and Information Security https://www.enisa.europa.eu

[11] ENISA Reports
Airports - https://www.enisa.europa.eu/air
Road - https://www.enisa.europa.eu/
SCADA - https://www.enisa.europa.eu/scada

11. Perspectives from a European railway operator: "Trains as data centres – protecting train IT as a cyber-crime target".

Gertjan Tamis, Information Security Officer, NS, provided cyber security perspectives from a European railway operator emphasising Train IT. Mr Tamis emphasised how NS started with practical solutions rather than policies. A train is conceived as a "data centre on wheels", connected to a network that coordinates other data centres on wheels. Threat modelling uses a risk-based approach, noting that both external hackers and insider threats can challenge passenger wi-fi, comfort IT, and train IT. These are points of interest to be protected, and are connected via networks, so can provide routes to other systems and processes.

Prevention is the key, and relies on careful management of traffic to ensure nothing can happen that should not. To achieve that, certain challenges must be faced:

Train suppliers should collaborate on cyber security:

- Include security requirements in RFI and RFP (request for information / proposals).
- Assist in interpretation of requirements.

Continuous communication and open exchange of information.

Create a common understanding of risks using a standard process covering:

- Business Impact Analysis.
- Threat and Vulnerability analysis.
- Risk Determination.
- Selection and implementation of controls.
- Implementation testing for security.

Lessons from practice at NS also indicate a need to:

- Specify Information Security Requirements beforehand.
- Protect all software (logical and physical) up to current levels of security standards.
- Include physical security as an important aspect (safety versus cyber).
- Ensure train builders comply on process level. It is harder to improve hardware level when buying off-the-shelf trains.
- Define an internal process to manage residual risk including stakeholders and ownership.

NS experience demonstrates that Information technology enables new business and operational models. Information security for Train IT is quite new but is key in keeping trains safe in the (very) near future. Threat analysis provides a good basis for mitigating risks efficiently. Close co-operation is needed (Rail Operators; Suppliers; Maintenance Companies; Regulators).

While many of these messages emphasise Train IT, they can be generalised to the wider networks to which trains are connected, and on which they depend.

12. Lessons learned from EU projects SECRET and CYRAIL: "Rail as critical infrastructure requires strong projects to protect it".

Marie-Hélène Bonneau, Senior Security Advisor, UIC (International Union of Railways), shared some lessons learned from EU-funded projects SECRET and CYRAIL.
Mme Bonneau outlined UIC activities in general and in relation to cyber security, including forthcoming conferences.

Rail is identified as a critical infrastructure that is becoming more connected and open, interoperable and harmonized. Threats (both human and technology) are emerging and adapting faster than traditional security can adapt.

The SECRET Project addressed Electro Magnetic attacks (EM) that can jam electronic transmissions, or even damage electronic systems. SECRET investigated threat scenarios, consequences, prevention and recovery solutions. The public white paper produced over 40 recommendations and was supplied in hard copy at the conference and can be downloaded[12].

CYRAIL[13] aims to deliver a cyber security assessment of railways, including operational scenarios, security assessment, threat analysis, attack detection, early warning, mitigation and countermeasures, as well as protection profiles. The early work will focus on signalling and communication systems, and will deliver an assessment methodology based on ISO 62443[14] (although this has many limitations except where it applies to isolated products).
The links to these projects (below) provide access to results and participants.

[12] SECRET project recommendations on EM attacks - http://www.secret-project.eu
[13] CYRAIL – http://www.cyrail.eu
[14] ISO 62443 - https://webstore.iec.ch/publication/7029 Industrial communication networks system security

13. Perspectives of a railway infrastructure manager: "Extensive premises, public accessibility – DB managing security risks"

Christian Schlehuber, IT Security, CCS, DB NETZ, provided practical perspectives from the railway Infrastructure Manager (IM). DB owns the largest business premises in Germany, and most of it is publicly accessible, and so the challenge for security is immense. For this reason, there is strong emphasis on security standards, including:

EN 50126[15] (Reliability, Availability, Maintainability, Safety – RAMS)
EN 50128[16] (Communication and Signalling)
EN 50159[17] (Software for safety systems) . . . etc.

Railway transport significantly contributes to society's mobility, and also to its economy - business staff and goods move by rail. The railway is a Critical Infrastructure, and in Germany the TEN-T Corridors are categorised as critical because failures would disrupt public safety and security, and would cause supply shortages.

The impact of the NIS directive was presented and shown to involve costs and efforts for a wide network of key actors supporting railway transport (components, systems, services). Having a common approach would help reduce this impact. However, changes to laws and regulations may take significant time.

Herr Schlehuber emphasised that operationally, safety relies on specific elements: Secure asset and configuration management; Physical access detection; Data Filtering; Data logging and aggregation; Reaction to critical events; Authentication and key exchange.

Security-Applied Design in the wider systems architecture is critical since vulnerabilities can be found in any segment or component.

Specific challenges to be faced include:

- Vulnerability Analysis and recommendations
    - Is knowledge about systems available?
    - Can Recommendations be implemented?
- Preventive Vulnerability Scanning
    - Is my system capable of a scan?
- Penetration Testing
    - Will the test result in outages?
- Staff Training and Awareness
    - Can staff understand cyber security?
- Forensic Analysis versus Fast Recovery

[15] EN 50126 – Railways applications: RAMS - Reliability, availability, maintainability and safety
https://shop.bsigroup.com/ProductDetail/?pid=000000000030228795
[16] EN 50128 – Railways applications: Communications and Signalling
https://shop.bsigroup.com/ProductDetail?pid=000000000030299071
[17] EN 50159 – Railway applications: Safety-related communication in transmission systems
https://shop.bsigroup.com/ProductDetail?pid=000000000030202175

Despite success at DB in addressing cyber security, duplication of efforts was observed: Safety and Security Departments worked in parallel with minimum interaction; Safety and Security performed their own analyses, estimated impacts and derived requirements. Cooperation and open exchange can reduce efforts and cost, as well as ensuring that nothing is overlooked, and that a common approach is achieved.

14. The telecommunications view: “Risk management depends on agility”.

Mr Guus van Es, General Manager BT Consulting, shared the Telco perspective on cyber security. Mr van Es summarised the BT position on cyber security, addressing Internet of Things (in Trains), Digitalization, Cyber, Big Data and analytics Compliance, among other technical aspects relevant to cyber security.

An overview of risk quantification was presented and shown to be key to cyber security strategy. It was shown how numerous companies’ cyber journey may start with denial (e.g. “not my problem”), but soon moves to worry (relevant news awakens), through learning, to then achieving a sound approach.

Cyber security is a business risk because it arises from IT improvements or changes that provide new attack opportunities. Continued innovation will ensure continued risk, and so we must continually evolve our approach. As a sector, Rail needs to understand the need to collaborate (reduce efforts, costs, and risks by sharing), and to follow leading standards and practices.

Cyber threats demand risk management, so we need to consult with practitioners, and should learn lessons about agility, even in policy making.

15. The IT provider view: “Understand vulnerability and develop avoidance and mitigation strategies”.

Romolo Buonfiglio, Senior Executive, Information Security, Almaviva, presented some perspectives from a railway IT provider.
As a leading IT provider, Almaviva supports passenger and freight transport operators, infrastructure managers, port authorities, local authorities engaged in developing and managing local integrated passenger mobility systems and services, as well as “last mile” logistics providers. In all areas, the key issues remain the same – understanding vulnerability, developing avoidance and mitigation strategies, remaining up to date on new threats and challenges as they emerge.

The cited Gartner report[18] shows ~ 7% CAGR spend on Cyber Security. Some case study examples were provided, including mobile fraud as well as methods for intelligence and analytics, each providing examples applicable to railway considerations and highly relevant to the idea of sharing experience and solutions.

[18] GARTNER prediction cyber security spend - http://www.gartner.com/newsroom/id/3784965

16. Second panel discussion: “The need for co-ordinated action”.

The afternoon panel discussion emphasised understanding how railways can benefit from the outputs of the many activities described, especially CYRAIL and Shift2Rail, and it was noted that projects like CYRAIL deliver outputs via Shift2Rail who will make them available to EU Railways in general.

Broad discussion also focused the need for coordinated action and sharing to ensure the many different roles and concerns are interconnected meaningfully.

In response to that, it was questioned how EU Railways could benefit from the idea of realistic field exercises, such as those presented by Mme Bonneau, and the panel indicated a range of activities already in place to support such exercises.

Furthermore, it was emphasised that we need some way to get a critical mass of RU/IM and Support Service involvement to make a really meaningful Europe-wide exercise that could convince Railways of the way ahead, and so the role of the Rail ISAC could consider how to enrich community knowledge by this and other means.

17. Closing keynote address: "Achieving an EURail-ISAC, without replication or over-regulation….".

Carlo Borghini, Executive Director of Shift2Rail, provided a keynote closure by addressing the panel debates. Sgnr Borghini noted that we are in a sector whose nature, whose IT, and whose services are evolving rapidly with innovations in many quarters.

Shift2Rail was illustrated as a public-private partnership R&I platform for railways working together to drive innovation till 2024. User-centred mobility is emphasised as a priority – putting the user first.

The main conclusions are that advancement starts at the top (cyber hygiene[19]); done by design; moving from behind to the leading edge; building trust and cooperation within the "railway intelligence community" together with those who can bring outside expertise.

Progress towards a Rail ISAC must define objectives, participation, exchange of information (including with CSIRT/CERT), events reporting, solutions, working together, etc. . . . but not by over-regulation.

Sgnr Borghini concluded that from this very constructive conference we must take away the messages on how to collaborate together in practical ways, reducing replication and divergence, sharing innovation in combatting cyber threats, making Railways safer.

[19] Cyber Hygiene definition and profile - https://en.wikipedia.org/wiki/Cyber_hygiene

18. The Way Forward: "Establishing a European Railway ISAC based on a common understanding"

The very positive participation and contributions at this conference indicate that cooperation between key actors in European Railways to address cyber security is now a work in progress. The supportive and positive orientation of both speakers and participants indicates good prospects for collaboration of the supporting Railway Organisations, Agencies, and European Commission DGs. Based on the sharing of understanding, and the complementary perspectives on objectives and opportunities, a draft discussion paper will be tabled in support of planning for a future Rail ISAC.

The conference has confirmed a common understanding based on recent EU law:

- The Directive on security of network and information systems (the NIS Directive[20]) was adopted by the European Parliament on 6 July 2016, and entered into force in August 2016. Member States were provided 21 months to transpose the Directive into national law and 6 months more to identify "operators of essential services".
- The NIS Directive ensures that Member States will designate National CSIRTs (Computer Security Incident Response Teams). These are also named in some Member States as CERTs (Computer Emergency Response Teams).
- The Directive creates a European cooperation group (EU CSIRTs Network) supported by ENISA (European Network and Information Security Agency).
- The NIS Directive emphasises the need for "operators of essential services" such as Rail, and their digital service providers, to collectively take appropriate security measures and to notify serious incidents to the relevant authority.
- Rail Transport (Infrastructure Managers, Railway Undertakings and supporting organisations including digital service organisations) provide essential services across Europe, and is cross-border in nature, requiring collaboration to inform each other of threats and incidents, as well as best practice in cyber security.
- European essential service operators are beginning to adopt the ISAC model[21] - "*sectorial member-driven organisations organised to collect, analyse and disseminate information on cyber-threats, and to help critical infrastructure owners and operators to protect facilities, staff and customers from cyber threats*" - the objective is to organise, not to regulate or control information.

In response to the above statement of common understanding, made evident in the conference, some potential features of a Rail ISAC are identified in the presentations and discussions, and will be taken into account as the Railway sector progresses this debate.

. .

[20] NIS Directive http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG
[21] ISAC Model from USA https://www.nationalisacs.org

19. Annexe - Conference Evaluation Summary – Consensus

The conference attracted 120 participants who provide a very good cross sector representation of European Railways, including IMs, RUs, IT expertise, and Security.

A total of 30 participants provided a completed feedback form. This 25% response rate (1 in 4) is very good compared with common reports suggesting around 10% average in such circumstances, and 20% being good. We can therefore be confident that we have a reasonable sample of opinion and experience. Reported ratings use a scale of 1-6.

19.1. Event Logistics

Event logistics (questions 1 to 3) were rated very highly, with no negative comments. The venue and overall arrangements were very positively appreciated by all.

Note1. no respondents scored below 4, which is very positive.

Event Logistics	score 6	score 5	score 4	average
Q1. Overall management and logistics	18	10	2	5.53
Q2. The venue and facilities	11	17	2	5.30
Q3. Hospitality and meals etc.	15	13	2	5.43

19.2. Programme, Speakers and Presentations

Respondents showed a high appreciation of speakers and programme overall.

Note2. some respondents ticked several values to show a range – the average is taken.

Programme, Speakers and Presentations	score 6	score 5	score 4	average
Q4. Content and relevance of presentations.	6	16	8	4.93
Q5. Quality of speakers overall.	5	18	7	4.93
Q6. Satisfaction with overall programme.	7	16	7	5.00

19.3. Appreciation of Good and Useful Speakers

Many speakers were identified (Q7) as particularly “good” speakers, and respondents also rated (Q8) how “useful” the presentations were, from a personal and professional perspective (useful to me and my work).

It was noted that not all “good” speakers were also marked as “useful” speakers.

Results showed a consistent preference for practical presentations (“how to”, cases, regulations, practical advice, actions of interest).

Some of the presentations rated as less useful (Q9) at a practical level were nonetheless very interesting in providing participants with wider perspectives on cyber security issues.

It is worth bearing in mind that every speaker was identified as positive and useful for a section of the audience, and so a message for future events may be about having a good mix to ensure coverage.

19.4. Areas for Future Coverage

Participants were asked about coverage of topics not yet well covered in the railway community, and/or needing coverage in the future (Q10/Q13).

The main stated topics were:

- Practical cybersecurity solutions.
- Business continuity management.
- Threat and risk management.
- Science and research.
- Practical arrangements for exchange of cyber info (ISAC).
- Examples of Cyber security / Practical cases.
- European Rationale.
- Practical "how to" for cybersecurity in Railways.
- Securing messaging between service operators.
- Strategic plans.
- Technical security aspects.
- Implementation of security measures.
- Interoperability in Rail.
- Practical SCADA.
- Cloud.
- IoT in Transport.
- ERTMS evolution.
- IT Regulations.
- Radio.
- Industry who will build systems.

In conformation of the earlier emphasis on practical aspects (what to do), the statements here were also highly focused on practical matters.
One respondent summed it by stating “Examples of how Rail addresses Cyber Security were good, but we need more of these”.
As well as asking for more on Cybersecurity in detail (how to), there is emphasis on a range of both related and unrelated issues. It may therefore be possible to move away from a single themed conference to provide a range of topics of interest in future (mix).

19.5. Hit Rail Contribution

The Hit Rail contribution was very positively appreciated, including the good organisation of discussions on cyber security, coordination of railway actors to ensure involvement, and the provision of good speakers and moderation. There is a good expectation that Hit Rail might continue to support exchange of experience and learning between members of the European rail community in this manner.

19.6. Interests of Participants

The participants were asked why cyber security was of particular interest to them (Q12). This produced a range of statements that emphasise a range of challenges for people close to the practical side of railway IT. Participants stated, "I am":

- A digital Rail Specialist facing cyber security concerns.
- Implementing cybersecurity.
- Addressing cross-border and complex interconnectivity security issues.
- Working as architect for security solutions.
- Addressing cybersecurity governance.
- Running a security operations centre.
- Developing resilience to attack.
- Seeking trusted suppliers.
- Setting up a cybersecurity framework.
- Conducting risk assessment.
- Developing Risk Policy.
- Work in standardisation for cybersecurity.
- Reviewing risk in cybersecurity.
- Working on functional safety.
- Developing security for a new train.
- Responsible for IT Security and focusing cybersecurity.
- Providing Rail IT.
- Working in risk management.
- Managing cybersecurity into rolling stock (old and new).
- Advising railways on IT and security.
- Working on research in cybersecurity.

This range of personal and company interests really emphasises how cybersecurity is cross-cutting and raising concerns for professionals in many areas.

19.7. Support for a coordinating body for cyber security such as an EURail-ISAC

Concerning the ISAC question, and following the various presentations covering legal aspects, examples of other ISAC's, and various perspectives on collaboration/sharing, 16 of 25 respondents said Yes (= 64%) and agreed to cooperate in an ISAC.

Only three stated No (= 12%) and one of these said it was not within his job remit.

Therefore, there appears to be good support for coordination of sharing around cybersecurity, but it is also the case that not all participants are able to confirm their organisational orientation. Work will have to be done to better engage CISOs and other company actors who are closer to the question of exchange of experience and events concerning cybersecurity.