UIC Security Platform

Update on recent activities

UNECE Working Party on Rail Transport (SC.2) 72nd session
Geneva, 21-23.11.2018

Security Division
Bruno De Rosa
UIC Security Activities

Security Platform Activities

- Rail Security Hub
- Working Groups (Permanent, Temporary)
- TACT Toolbox
- Publications
- Workshops...

Permanent

Research Projects

Mid-term

UIC Network of Quick Responders

Short term
Network of Quick Responders

- **Goal:** Exchange fast information about arising security questions
- **Process:**
- **Timeline:**
  - app. 2 weeks – Responds from the network
  - app. 2 months – 1st technical position paper
  - If needed, further actions
# Network of Quick Responders

<table>
<thead>
<tr>
<th>Topic</th>
<th>Survey</th>
<th>Follow-up activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Awareness of radicalized employees</td>
<td>03/2017</td>
<td>06/2017: Dedicate Workshop during the Security Week</td>
</tr>
<tr>
<td>2. Use of Air Drones</td>
<td>05/2017</td>
<td>12/2017: Main focus of the WG Security Technologies with authorities and provider</td>
</tr>
<tr>
<td>3. Inspire Magazine</td>
<td>09/2017</td>
<td>On-going: Thematized within the WG SIA &amp; single exchange</td>
</tr>
<tr>
<td>4. Attacks against maintenance staff</td>
<td>09/2017</td>
<td>11/2017: Hand over to the Safety Unit for further actions</td>
</tr>
<tr>
<td>5. Anti-smoking policy at railway stations</td>
<td>10/2017</td>
<td>No further actions requested by the responders</td>
</tr>
<tr>
<td>6. Security of women in railway transport</td>
<td>02/2018</td>
<td>06/2018: Dedicated topic during the 2nd Awareness Day</td>
</tr>
<tr>
<td>7. Use of FFCCTV</td>
<td>04-05/2018</td>
<td>09/2018: Dedicated Workshop on the 12 September 2018, next planned in 02/2019</td>
</tr>
<tr>
<td>8. Aggression against ticket inspectors</td>
<td>06-07/2018</td>
<td>Integration in WG Human Factor under the umbrella “Security feeling in public transport” (focus customer and employees)</td>
</tr>
<tr>
<td>9. Mystery Customer</td>
<td>07/2018</td>
<td>Currently no further actions requested by the responders (topic memory)</td>
</tr>
<tr>
<td>10. Use of AED’s</td>
<td>09/2018</td>
<td>First half 2019: Organization of a dedicate workshop together with the safety unit</td>
</tr>
<tr>
<td>11. Use of body cameras</td>
<td>10-11/2018</td>
<td>In evaluation</td>
</tr>
<tr>
<td>13. CBRN</td>
<td>11-12/2018</td>
<td>In preparation</td>
</tr>
</tbody>
</table>
FFCCTV – follow up activities

**Date:** 12 September 2018 (Paris, France)

**Contents:**
- Test area setting
- Purpose
- Technical aspects
- Fleet
- Cooperation with law enforcements
- Trade unions
- Public reaction
- Experience
- Drawbacks / difficulties

**Outlook:** next meeting in February/March 2019
4th UIC Security Week
18 – 21 June in Paris, France

- Seminar on CBRNE terrorism
- Workshop on Cybersecurity
- 2nd UIC Security Awareness Day
- Workshop on BCM
- Interactive Session Security Hub

Conclusions available at: https://events.uic.org/uic-security-week-2018
14th UIC World Security Congress
16 – 18 October in Bled, Slovenia

- 15th October: Tunnel Safety and Security Workshop
- 16th October: Official opening session
- Technical sessions:
  - 1st session: Blackout Situation in Slovenia 2014
  - 2nd session: Ice storm and impact on railways
  - 3rd session: Blackout Situations. Railway experiences and challenges.
  - 4th session: Crisis Management
- Official closing session incl. UIC security actions, conclusion and next steps
- Conclusion: https://events.uic.org/14th-uic-world-security-congress-crisis-management-and-resilience
Crisis Management - Member request 2018

- **Crisis Communication**
  - Recommendations for the external and internal communication incl. key words, reaction times, design of websites, preparation of communication channels like a special hotline, use of social media
  - Date: 13 – 14.02.2018 in Paris

- **Business Continuity Management**
  - Recommendations for the framework of BCM and the close connection to CM incl. devising plans and strategies to continue business operations and recovering quickly and efficiently from different types of disruption
  - Date: 21.06.2018 in Paris

- **Blackout Situations**
  - Example: 12 May 2017 Cyberattack WannaCry – over 150 countries involved
  - Recommendations for the handling of (partially) blackout situations
  - Date: 16.-18.10.2018 in Slovenia

By the end of 2018 / beginning 2019, publication of recommendations for each topic in cooperation with UITP and COLPOFER.
CYbersecurity in the RAILway sector

- **Duration**: 1 Oct. 2016 - 30 Sept. 2018
- **Budget**: 1,5 M
- **Coordinator**: Evoleo Technologies
- **Consortium**: 6 Partners from 5 countries
Final Conference held in Paris at UIC Headquarters on September 18th, 2018

Project brochure publicly available online at: www.cyrail.eu
SHERPA - Shared and coHerent European Railway Protection Approach

- **Framework:** DG HOME call for proposal

- **Planning:**
  - 31/01/2018: submission of the proposal
  - June 2018 – October 2018: Signature of the GA
  - 13 November 2018: Kick off meeting in Paris

SHERPA is an European Funded Project selected in the framework of the call ISFP-2017-AG-PROTECT.

sherpa.uic.org
Structure of the project

Shared and coHerent European Railway Protection Approach

- **WP2 – Coherent approach for terrorist risk assessment and management - Lead: SNCB**
  
  **Objectives:** to achieve a comprehensive and consistent understanding of terrorism-related threats against railway stations and trains and thus to elaborate a coherent approach for terrorist risk assessment and management in the railway sector.

- **WP3 – Analysis of emerging terrorism-related threats against stations and trains - Lead: SNCF**
  
  **Objectives:** to identify and assess emerging threats - e.g. insider threats, misuse of commercial UAVs - potentially affecting stations and trains; to define and share an updated knowledge base on the matter; to identify requirements and priorities for industry, research and policy making bodies.

- **WP4 – Assessment of security solutions: technologies, procedures, legal and ethical aspects - Lead: PKP S.A. and DB AG**
  
  **Objectives:** building a common knowledge base - validated by users and external experts - featuring the most efficient solutions for protecting trains and stations; identifying the gaps to be fulfilled and the future needs for better securing stations and trains in accordance with business constraints.

- **WP5 – Practical tools for a common approach on raising awareness and improving security of stations and trains - Lead: FS Italiane**
  
  **Objectives:** designing and delivering practical tools aimed at fostering a common, effective approach to the protection of stations and trains from both already experienced and emerging security threats.

**SHERPA** is European Funded Project selected in the framework of the call ISFP-2017-AG-PROTECT.

sherpa.uic.org
UIC Rail Security Hub

**Secure** web platform, accessible to UIC Members and other eligible stakeholders with differentiated access levels.

**User-Friendly** content search and navigation with a clear browsing interface.

**Comprehensive** catalogue of hundreds of security solutions addressing both daily crime issues and emerging threats to the railway environment.

**Integrated** with all the UIC Security Division projects and tools such as the Network of Quick Responders and Training Awareness Communication Toolbox.

**Open** to interaction with and between users through comments, ratings and information sharing.

**Updated** permanently by UIC Security Division.
PHISHING / SPEAR PHISHING ATTACK SIMULATIONS TOWARDS EMPLOYEES FOR EDUCATIONAL PURPOSE

PHISHING TRAINING VIA SIMULATED ATTACKS, EDUCATIONAL PHISHING CAMPAIGNS TOWARDS STAFF, SIMULATED PHISHING CAMPAIGNS, EMAIL PHISHING ASSESSMENT, PHISHING ATTACK SIMULATION

0/5 (0 vote)

DESCRIPTION

THREAT DEFINITION

PHISHING is a fraud attempt aimed at obtaining sensitive information (e.g. company information) from potential victims and/or at causing disruption to an organization's business by sending deceptive emails impersonating apparently legitimate senders/sources. Usually phishing email campaigns target a large number of potential victims at the same time: for this reason, usually they present a lower level of sophistication than spear phishing attacks. The email content is typically aimed at:

- Harvesting information (company or personal passwords, credit card numbers, banking details) directing the victim to an apparently legitimate website where he is required to enter information;
- Taking control of the victim's device infecting it as soon as the link contained in the phishing email is clicked.
Thank you for your kind attention!

<table>
<thead>
<tr>
<th>UIC website (Security):</th>
<th><a href="http://www.uic.org/security">http://www.uic.org/security</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rail Security HUB:</td>
<td><a href="http://www.railsecurityhub.org">http://www.railsecurityhub.org</a></td>
</tr>
<tr>
<td>Online from January 2019</td>
<td></td>
</tr>
<tr>
<td>Contact:</td>
<td><a href="mailto:security@uic.org">security@uic.org</a></td>
</tr>
</tbody>
</table>