Written evidence submitted by Wahiba Erriadi, Dr Suresh Renukappa, Dr Subashini Suresh, and Luke Seabright, Faculty of Science and Engineering, University of Wolverhampton

Adapting Railway Sector to Repel Ransomware Cyber Threats

Executive Summary

- The number and severity of cyber threats continue to grow exponentially as the world becomes increasingly connected. While the proliferation of connected devices has created unprecedented productivity and efficiency gains, it has also exposed previously unreachable infrastructure systems to attack from a range of malicious groups with varying motivations. Infrastructure asset owners, planners, builders, and financiers routinely channel ample resources into mitigating any number of risks to an infrastructure asset. Yet, they rarely if ever place as much care into anticipating potential cybersecurity incidents.
- The oldest documented history of railway infrastructure in the World lies on Britain's landscape, connecting all the cities and towns together. With the interconnecting template already in place for Britain, there is an ever-growing requirement to maintain railway infrastructure assets to improve the longevity of all the different componentry, whilst keeping costs as low as possible, continuously improving sustainability. On top of such targets, the awareness of cybersecurity themes has also changed. Securing railway systems from cyber-attacks has become a central issue for practitioners and the public.
- Ransomware attacks have been spreading like wildfire and will worsen in the future. According to cybersecurity experts, ransomware frequently attacks government services, especially urban infrastructure like transportation services, emergency services, traffic light management, CCTV, and railway equipment. As this new digitalised infrastructure is connected to sensors and 5G Internet of Things (IoT) services, ransomware attacks could destroy the infrastructure of a whole 5G-enabled smart city.

- The digitisation of the existing and newly created infrastructure has recently received much attention due to technological developments. The railway is among the most crucial infrastructure, and its security is just as critical as other essential infrastructure. The digitisation of rail systems is yielding unprecedented efficiency gains and customer service improvements. Nevertheless, this digitisation comes with increased connectivity, and the extended air-gapped rail networks are now exposed to the internet through IT networks. Efficient railways need to report information constantly. Hence, data should flow efficiently while rigorously protecting vital networks with the same rigour and thoroughness applied to the design, development and maintenance of safety systems.

Written evidence

- Evidence is provided by conducting semi-structured interviews with 25 railways professionals including Chief Information Officers, security directors, site managers, testers in charge, and rail engineers. They were enquired about their opinion regarding

the ransomware attacks, the cybersecurity systems, and what they think is needed to protect their companies from cyber breaches.

- Participants indicated that ransomware is a major threat and that the railway's systems need urgent security measures and defensive controls. A ransomware attack cannot only harm the organisation's ability to provide services but also its reputation. This was cited by 35% of interviewees. The UK Office of Rail and Road should regulate and design a secure and safe railway system guide to tackle cybercrimes efficiently. Although, the existing railway network safety measures may prove to be some protection against cyber threats, it is unlikely that they can fully mitigate all types of ransomware attacks.

- The UK government is advising companies on the ransomware attacks through direct communications with designated contacts and supporting them by responding to incidents. Furthermore, it is also helping to share the best practice through informing and supporting networks as well as giving a higher priority to cyber security protection.

- The scarce public sector IT budgets make networks less secure against attacks. Furthermore, since the local governments pay the ransom to unlock the network and resume services, this makes them easy and prime targets for extortion of funds and encourages criminality.

- When discussing with the participants, only 8% disagreed that their organisations were poor at preventing the damage that attackers could cause inside their networks. They have stated that their companies impose compulsory cyber-security training. Employees need to have a cyber-pass by completing all the cyber modules and passing a test at the end of the training.

- As a good practice, organisations should follow the National Cyber Security Center's advice that offers guidance and best practices to adopt when a cyber security attack occurs. Also, a regular threat analysis that considers internal and external security threats are recommended. Besides, defence in depth, where cyber security should be implemented in layers using a variety of solutions to provide monitoring and defence across and throughout the organisation, should be implemented.

- Addressing cybersecurity breaches at the earliest stage of any project will help prevent a ransomware attack. Some participants proposed some solutions as primary protection from physical attack - this protection by limiting access to equipment to only trusted maintainers and using a secure locking system for equipment rooms, equipment cabinet's rooms, rolling stocks, and communications cables and ports. The participants also advised the railway organisations to adopt good security management practices like ensuring that the login credentials have a complex password and applying multi-factor authentication to the employee's account.

- Rail under-reporting of cyber-attacks was identified as a security issue to consider. Although the number of reported cyber-attacks has stayed relatively constant over the years, some less cyber-mature organisations may be underreporting threats. The latter has pushed a significant number of participants to state that not reporting a cyber

security incident can lead to what may seem to be a non-loss scenario developing into a major problem if it needs to be adequately investigated.

- 54% of the interviewees suggested that the employees within the company, especially the internal cyber ones, should be thoroughly trained and have sufficient knowledge to handle the possibility that their company could be the target of a ransomware attack. They must take all reasonable precautions to prevent this from happening. Additionally, they should have a ready strategy to restore the network in the unfortunate case of an occurrence, preferably without paying a ransom.

- According to 87% of the interviewees, networks must be segmented to prevent attackers from using single devices to compromise the whole network. Micro-segmentation, a network security technique that allows security planners to reasonably divide the data centre into separate security segments down to the individual workload level, can give better control and contain the ransomware attack. Participant also advised having backup data by adding backup offline cold storage, taking majors, and changing passwords.

- Participants also urged the organisations to do a test mode as an exercise to know how long it will take the organisation to get its data back when an attack occurs. Only by making a ransomware test and inventing real scenarios will the executives be aware of how their team will digest and proceed in case of a real attack and report the basics.

- Significant ransomware cyber-attack on the IT systems of Italian State Railways and Italian Rail Network delayed ticket sales at stations, passenger information displays, and affected tablets used by railway workers. As a precaution, Trenitalia shutdown several of its IT services, including ticket sales at stations. However, customers were still able to purchase tickets online. The conductor permitted passengers unable to purchase tickets without incurring any fees.

- It is recommend that railway infrastructure asset owners and operators must first understand how old vulnerabilities will affect new technology and then develop integrated cybersecurity plans to apply the appropriate level of protection to their entire technology environment. The result will be safer and more resilient connected infrastructure delivering reliable services to customers for years to come.

- When considering digitised railway sector, owners typically focus their energies on envisioning the improvements in efficiency and customer experience that can be realised by new technologies. Cyber attackers, on the other hand, focus on uncovering the ways that new technology use cases rehash the same weaknesses and vulnerabilities of the old. Indeed, the problems faced by cybersecurity professionals. To build adequate defences, railway infrastructure assets owners and operators should start by assuming that a cyberattack is imminent. Then they must build a unified, integrated cyber defence that best protects all relevant infrastructure assets. By starting with an assumption that a future cyberattack will degrade, disable, or destroy key railway infrastructure functionality, owners and contractors can take action early to build resilience into their systems. When planning incident response, leaders should

look beyond the railway infrastructure sector for lessons learned from cyber incidents that caused outages in other sectors of the economy. While the technology components deployed in the IT and infrastructure environments may differ significantly in their purpose and complexity, railway infrastructure asset management is vulnerable to the same risks when connected to the internet.

- Railway infrastructure groups need to get creative with where to look for cybersecurity talent. Selection and training of an incident response team before an incident occurs is key. To sustain the mind-set shift, asset owners must integrate cyber resilience metrics into their regular performance measurement programs.

15 December 2022