Developing Cyber Resilience Together:

Industry Cooperation for a More Secure Railway

Alexander Patton, BEng MIET AMIRSE, Siemens Mobility (UK)

SUMMARY

Railway digitalisation is rapidly introducing commercial information technologies to signalling and train control systems. While this provides for significant opportunities, it introduces new risks. The security risks posed by digitalisation are unique because of the increased exposure to, and/or magnified impact of, a cyber-attack. In response, governments are now regulating for the rail industry to comprehensively manage the cyber security of essential railway systems.

The signalling industry is still in the early stages of addressing these risks, and stakeholders are at varying levels of maturity. Currently, signalling asset owners take different approaches to procurement. Individual system suppliers consider security architecture within their own limited scope. Vendors build products to varying levels of security and sometimes with incompatible technologies. When security functionality does finally make it to the railway, it can become obsolete long before the end of the system lifespan.

To efficiently and effectively manage security risk across the railway, stakeholders must work together to overcome this maturity gap. Like has been done with safety, the industry needs to collaborate on a common approach, agree clearly defined baselines and create standard security architecture. To achieve this, stakeholders will need to overcome challenges including protecting one's intellectual property and commercial position while openly cooperating on cyber security. This paper examines why industry cooperation is an essential part of building a more secure and resilient railway and identifies challenges to implementing such cooperation.

---

*"Cyber systems and procedures adopted on the GB rail network should be designed, operated and maintained by **the railway industry as a whole**, to provide **resilience against malicious attack**."*

-UK Department for Transport, 2016

---

1 INTRODUCTION

1.1 Background

Shortly after ASPECT 2017, the industrial control systems (ICS) community received a stark reminder of the cyber threat to critical infrastructure. An energy plant in Saudi Arabia had been shut down by malware. Except, this malware was different: It had successfully infected the SIL-rated Safety Instrumented System and attempted to cause a wrong-side failure. All that stood between the plant and violent tragedy were a couple of small coding mistakes on the part of the attackers. [1]

Furthermore, targeted attacks on critical infrastructure are not the only concern. Systems anywhere from the National Health Service in England to the Deutsche Bahn in Germany have become collateral damage in generic cyber-attacks such as WannaCry. Even now, many signalling and rail SCADA systems are still unsecured against similar "critical" ranked vulnerabilities.

As cyber threats continue to grow, governments are beginning to introduce security regulations that impact the signalling and train control industry. A good example is the European Union's Network and Information Systems (NIS) Directive – the world's first inter-governmental initiative on cyber security – which came into effect in May 2018. It places legal obligations on the operators of essential services, including railways, to address cyber security concerns.

In the United Kingdom, the four objectives of compliance with the NIS Regulations 2018 [2] are defined by the National Cyber Security Centre (NCSC) to be:

A. Managing Security Risk;
B. Protecting Systems Against Cyber Attack;
C. Detecting Cyber Security Events;
D. Minimising the Impact of Cyber Security Incidents.

NIS Indicators of Good Practice help determine whether an operator is working toward the objectives. Non-compliance penalties are in excess of USD$20 million.

Historically, operators and suppliers of signalling and train control systems have not emphasised cyber security in risk management and system design. NIS is seen as a game changer within rail cyber security circles. It requires an industry with limited cyber maturity to take a deep look at security risk, including threats to system resilience from cyber-attack, and challenge past assumptions. Notably, it not only affects newly deployed systems, but also requires operators, to an extent reasonably practicable, to protect all existing systems.

The industry must now make a brisk stride towards security maturity. This is necessary not only for the sake of compliance, but to mitigate the impact of an inevitable future cyber-attack on the railway. The answer cannot come from one operator alone or even a group of operators. Cooperation across the signalling supply chain is essential.

1.2 Aim

This paper aims to demonstrate how close industry cooperation on cyber security is essential while highlighting the challenges faced.

1.3 Method

This paper examines how stakeholders support the four objectives of NIS compliance during procurement, commissioning and operation of a signalling and train control solution. While written from a UK perspective, it should be applicable across other EU member states and relevant worldwide.

2 OBJECTIVE A: MANAGING SECURITY RISK

Overall responsibility for the security of a specific railway system lies with the operator, as made clear by NIS. However, the operator relies heavily on suppliers to support NIS compliance by providing security services and technical capabilities throughout the signalling system lifecycle. Furthermore, system suppliers often rely on additional product vendors, who in turn may rely on generic software vendors. For this reason, it is essential that all stakeholders partake in the security risk management process.

2.1 Defining Initial Security Requirements

2.1.1 Why Industry Cooperation is Needed

When the operator seeks to procure rail automation service such as the provision of a new signalling system, it carries out a procurement process to select a supplier. They primarily consider price, whole life cost and the proposed solution's compliance with high-level requirements supporting the objective to transport passengers and freight. However, recent emphasis on cyber security now forces operators to ensure that any procured solution will be suitably secure.

One of the earliest stages of the security lifecycle is defining initial security requirements (often called "security controls") for the purpose of system procurement.

NIS Good Practice Indicator A4: *You can clearly express the security needs you place on suppliers in ways that are mutually understood and are laid in contracts.*

In the past two to three years, many operators have found themselves procuring signalling systems within this new environment for the first time. Lack of maturity has been an issue affecting all stakeholders, operators and suppliers alike, large and small. Operators have limited experience managing cyber security, and suppliers are still working to overcome the fact that most railway technologies were never architected to prioritise security.

Early such procurements emphasising security have raised concerns around this maturity issue. Some have not put forward any specific security requirements. Instead, the operator has relied on the winning supplier to fill the role of security consultant. Such procurements typically used a pre-qualification questionnaire to try and mitigate risk of selecting a supplier whose own security experience may be insufficient.

While this approach may yield a collaborative relationship between the operator and winning supplier, its success is limited by a lack of opportunity for wider cooperation. With this approach, the operator and solution supplier effectively go into contract without a picture of the security risks and potential costs. There is weak assurance that the successful supplier's proposed solution will be found fit for purpose from a security perspective. Many change orders could be necessary, driving the ultimate cost higher. Furthermore, the operator may not benefit from a comparison of unique benefits of different suppliers' proposed solutions such as automation of security administration.

Some other operators have preferred to maintain a high level of direct control over the security solution and developed comprehensive requirements before putting a project to tender. These requirements have often been drafted with the support of independent security consultants. Such an approach improved upon earlier examples by clearly establishing to potential suppliers the operator's expectations. This can allow compliant solutions to be compared like-for-like without further concern around security.

However, the prescriptive nature of such requirements can force the application of countermeasures that may not provide the same risk mitigation cost-to-benefit ratio across all proposed solutions. Either way, when requirements can be considered by a wider industry group pre-contract, these issues fall away.

Current good practice is for the operator to create, before any procurement, a generic high-level system-of-systems architecture and partition it into security zones and conduits based on criticality and function. They then perform an initial security risk assessment (SRA) on each zone. To ensure that appropriate requirements are set, the operator refers to a defined standard, which is most often the IEC 62443-3-3 international standard for ICS security controls. This standard defines four Security Levels that act as baseline control sets. The operator selects the Security Level to apply to each zone based on the magnitude of risk mitigation required. Examples of this currently exist, such as the UK Digital Railway Programme's system-of-systems security risk assessment.

However, good practice is not infallible. Without the input of suppliers and wider stakeholders, the accuracy with which appropriate Security Levels are selected suffers, frustrating procurement and driving up cost. Industry standard system-of-systems architectures should act as a forum for discussion around cyber security requirements.

2.1.2 How Industry Cooperation Can Be Implemented

Much of the current challenge around tendering and the early security requirements stages could be alleviated by proactive engagement within the supply chain. Long before operators put new railway systems to tender, industry stakeholders should explore the topic collaboratively. Because rail industry security maturity is still developing, we are in the stages where such industry collaboration presents a high level of opportunity. The quicker the industry builds compatible roadmaps for addressing cyber security challenges, the quicker secure railway technology will be normalised.

---

*"The task **to ensure security of the system cannot be successfully performed by the operator itself**, it is an exercise to which **different roles and parties must contribute** in order to be successful - customers, suppliers and assessment bodies."*

- Norbert Howe FIRSE, IRSE International Technical Committee [3]

Cooperation starts with engaging a full breadth of stakeholders in the initial system-of-systems SRA. Approaching this collaboratively, by inviting representatives of major suppliers to participate in industry wide SRAs of standard systems would ensure that better security requirements are in place at the project tender stage. It would also give suppliers better direction on where they should steer their product and solution security roadmaps. As standard

signalling architecture projects such as EULYNX progress, an industry collaborative SRA should be a serious consideration.

Ultimately, by working together, suppliers and manufacturers can build ambitious roadmaps to deliver more secure products and solutions, and the procurement process for these ambitious solutions can be less risky.

2.1.3 Challenges Posed by Industry Cooperation

In pursuing the benefits of better industry cooperation and collaboration, the challenges must be recognised.

Effective cyber security is, particularly when its impact on safety is considered, a basic prerequisite for the railway to function. Security immaturity of one party impacts the whole industry, so it makes since for the industry to pool its experience to overcome this. Yet, particularly on the supplier side, commercial concerns quickly flare up when multiple vendors are placed together in a workshop to reveal potential vulnerabilities and weaknesses of key products and solutions. There is a risk that such information could be exploited in future tenders to imply, rightly or wrongly, that their solution is superior to the competitor's.

2.2 Defining Detailed Security Requirements

2.2.1 Why Industry Cooperation is Needed

Once the procurement stage is finished, a supplier is contracted to design and deliver the system. Because a railway is a system-of-systems, there may be a signalling supplier, traffic management supplier, telecoms supplier and other relevant system suppliers. Suppliers must conduct a detailed security risk assessment on their planned solution to determine what security controls are required in practice.

Modern signalling and train control systems feature digital interfaces between many subsystems comprised of intelligent electronic devices. Inevitably, the different systems supplied will have the potential to impact each other from a security perspective. A signalling system may interface with an adjacent signalling system. A traffic management system may interface with the operator's wider enterprise networks and, in turn, public networks. That same traffic management system may interface with the signalling system.

For the sake of managing security risk, suppliers need to first understand the level of trust they can place in the other systems. At one level, there may be trust concerns between two systems developed to differing security requirements. Importantly, two different systems often operate in different environments and have differing exposure levels to attack. Suppliers also need to have a common understanding of interfaces between systems in order to effectively risk assess them. It's essential that the party acting as overall system integrator facilitates cooperation amongst stakeholders.

2.2.2 How Industry Cooperation Can Be Implemented

Suppliers for each system should have a broad and inclusive guest list for their respective SRA. They should invite key stakeholders. In addition to interfacing system suppliers, the operator has the best view of how a system will be used in operation and individual product manufacturers have the best understanding of low-level technical details that may impact system security. Additionally, there are likely parties other than the supplier that best understand the threats existing in the environment of the system under consideration. The operator is a good stakeholder to contribute in this regard, but collaboration with other stakeholders such as the railway police force may lead to a more robust risk assessment.

An SRA often identifies security risks that could be addressed in different ways by different stakeholders. When stakeholders engage cooperatively, the best solution can be found. For example, a signalling system SRA may reveal that the highest risk of a hacker impacting the railway is at trackside equipment buildings. From the supplier's perspective, this could be mitigated by developing new, potentially expensive, technical countermeasures for trackside equipment (e.g. cryptographic authentication). However, the operator may be able to mitigate the risk by instead changing its own physical access control policy or process.

2.2.3 Challenges Posed by Industry Cooperation

The challenges posed are largely the same as with defining the initial security requirements. Stakeholders may treat security weaknesses as commercially sensitive, which can hinder the effectiveness of collaborative risk assessment.

An additional noteworthy challenge is finding the right balance between not inviting enough stakeholders and inviting too many. The former can result in a risk assessment that lacks robustness, while the latter can result in the cliché “death by committee”.

3 OBJECTIVE B: PROTECTING SYSTEMS AGAINST CYBER ATTACK

3.1 Designing Countermeasures

Upon completing a detailed risk assessment and defining detailed security requirements to mitigate security risks, the system supplier must translate these requirements into a security design made up of countermeasures. Countermeasures are technical implementations that protect the system against cyber-attack. Like with other technologies, there is often a need for designs to be compatible or interoperable.

3.1.1 Why Industry Cooperation is Needed

There are many examples of security requirements applied to signalling systems and countermeasures that are used to address them. User access control is one common requirement. The requirement is generally that human users must identify themselves to the system and authenticate that they are who they say they are. A countermeasure that works to address this requirement is an Identity and Access Management System (IAMS). This is a server that maintains the identities and credentials (e.g. password; PIN number) of users. It interfaces with computer clients such as signalling workstations to authenticate a login.

Realistically, an operator is unlikely to want to manage users individually for each of their railway operations and control subsystems. Equally, their users will not want multiple different sets of credentials. There is a demand for stakeholders to integrate many of their cyber security systems in order to provide features like Single Sign-On.

This demand is by no means limited to user access management. The root of any security system is trust. When users and devices interact, they need assurance that the other party is genuine and that messages exchanged are not corrupted in some way. When a system is wholly contained within a controlled environment, this trust is inherent. The reality is that most environments are not perfectly controlled, and the railway is no exception.

> ***Rail Code of Practice for Security-Informed Safety:*** *“Data received from an external source should be checked for authenticity. Data received from an internal source should also be checked for authenticity unless it can be shown that the internal data link cannot be accessed …* ***To ensure authenticity, the use of cryptographic techniques is recommended****”*

Early digital railway systems assumed trust and relied only on the validity of safety checksums to authenticate. Safety assurance functionality is designed to safeguard against accidental violations of fidelity, for example, a mistake made by an engineer. However, as the risk to railway systems from intentional, malicious violations increases, security functionality becomes necessary. And since the dawn of secure communications, the most important feature has always been a secret key- perhaps a physical key, a cypher or, as used in the modern world, a number/passcode that can be used with a cryptographic formula. These can be used to prove the identity of the author and prevent manipulation of a message (known as ‘signing’) or to ensure only the intended recipient can read a message (known as ‘encrypting’).

Communications are not the only element which are recommended to be protected by a cryptographic signature. Device firmware could be tampered with in the supply chain, causing a rogue device to be introduced to the system. A vendor signing the firmware such that an operator’s system can confirm the genuine status of the device protects against this.

Devices from different vendors need to be interoperable to support the rail industry’s ongoing strategy set out by collaborative efforts such as EULYNX. For this to be the case, there are fundamental questions the industry must answer such as the cryptography architecture to be used, how cryptographic keys will be managed, etc.

3.1.2 How Industry Cooperation Can Be Implemented

The good news is that as we continue to use more commercial off the shelf (COTS) technologies in our systems, a large amount of standardisation has been done already by the wider IT industry. There are many standard secure architectures and interfaces that can be used in digital railway systems. The industry should work to agree which standards to adopt, and fortunately, we have Shift2Rail and other technical bodies who are considering such things.

When it comes to user access management, operators can run a single directory service such as Microsoft Active Directory and then specify that all stakeholders must interface with it. The industry could agree a common protocol for user access management interfaces like LDAP.

Regarding the more fundamental question of how to address trust: Looking at existing cooperative efforts, the ERTMS Euroradio standard uses what are called 'pre-shared' keys. Parties must be privy to a common secret key. It works well for legacy hardware. Taxing calculations required to create the key can be performed off-device. However, keys must be manually distributed for every piece of hardware. A compromise of the central key store would have a catastrophic impact to rail operations. The alternative is Public Key Infrastructure (PKI). Each device has a publicly shared key and a secret private key. Any message signed by the private key can be mathematically validated by the public key. Any message encrypted by the public key can only be read with the private key. This mathematical concept is well documented by the security industry for lay readers. Devices must perform intensive calculations to generate these keys, however the process is decentralised, allowing trust to be peer-to-peer. The use of PKI is scalable, both within systems and across systems of systems. For this reason, it offers a great opportunity for building trust between systems from different vendors across a national or even internationally interconnected railway network.

NIS Good Practice B2b: *You perform **certificate-based device identity management** and only allow known devices to access essential services.*

Of course, the technical reality is more complex. The public keys themselves, floating around in a system, need to be trusted somehow. Each public key needs to be signed by some universally trusted computer (a "trust anchor" or "certificate authority") that has a minimum risk of being compromised and whose own public key is well recognised.

Assuming appropriate cryptographic strength is used, and best practice is followed, PKI effectively extends the level of security afforded by the controlled environment of the certificate authority to devices out in the field. However, maintaining the security of a certificate authority can be expensive. Organisations are known to spend over £1 million / year (€1.2m, USD$1.3m). Furthermore, the ability to guarantee trust within a static system alone is not enough. Trust must flow through the entire supply chain.

As of June 2019, there is not yet a common industry approach to this issue. However, one potential architecture that could facilitate a high level of cyber security interoperability between vendors and operators using existing IT standards is given in Figure 1.

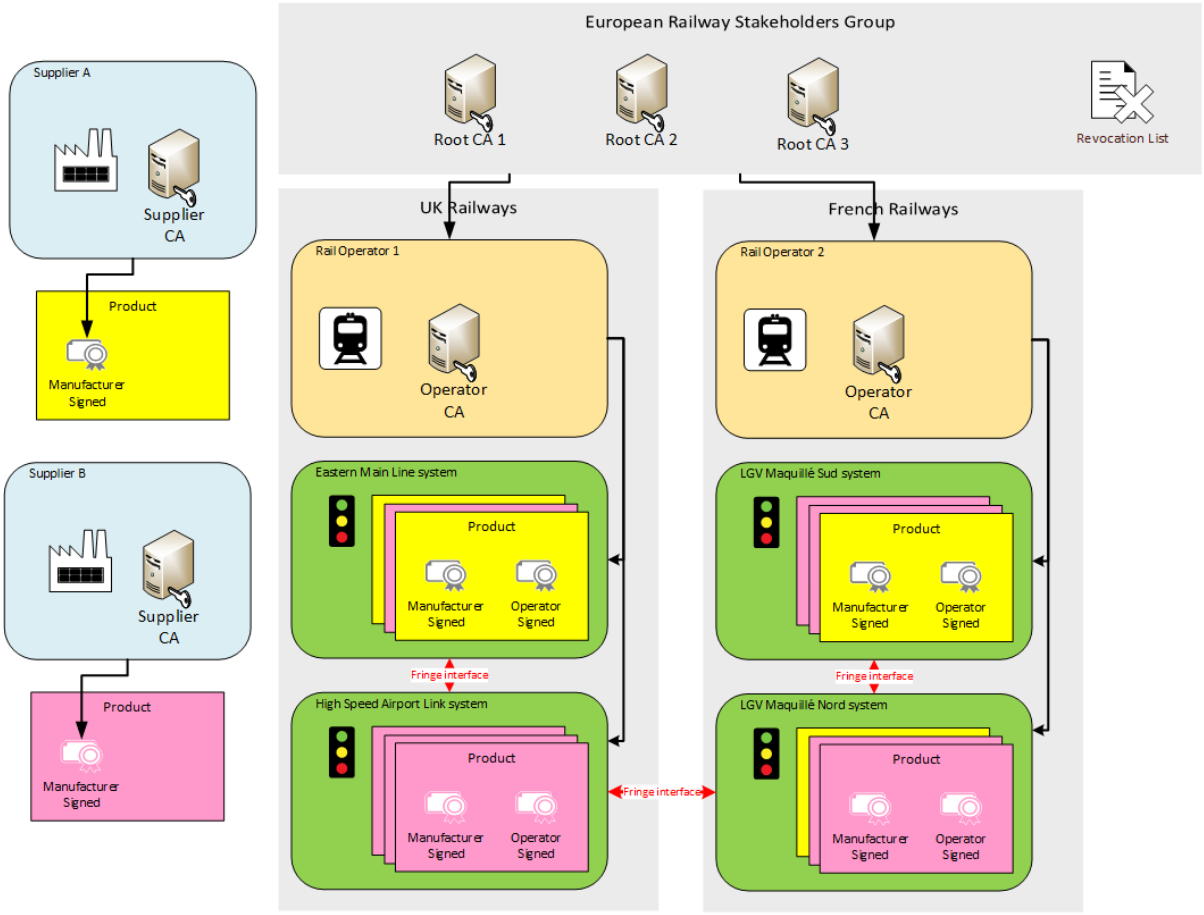

Figure 1: Potential Trust Architecture for Interoperable and Secure Railways

The aim of this architecture is to facilitate trust between railway stakeholders without introducing mission critical interfaces, single points of failure or an unbalanced responsibility/financial burden on any party.

In the architecture presented, each supplier publishes a public key. No system interface is required between railways and the manufacturer. Railway operators maintain a list of public keys from the manufacturers they choose to trust. When a device is connected to a railway system and presents a certificate signed by such a supplier key, the operator's CA grants an operator certificate to the device. This operator certificate allows the device's identity to be trusted by any other device within the system or wider national railway network

This can be extended between operators or national railway systems. With minimal effort, this can be achieved simply by two operators recognising the public keys of their respective Certificate Authorities. However, the risk of a system compromise needs to be managed. Should the private key of a device be compromised, the operator Certificate Authority (CA) must announce that its public key certificate is no longer valid. If the operator's CA private key is compromised- there is a serious problem. This could affect the entire national railway operations.

An alternative is direct cooperation between stakeholders. For example, a group of European railway stakeholders could operate a pool of highly secure Root CAs. If each operator is signed by multiple CAs, then one being compromised does not bring down the system. The signature of one of the other CAs would be enough to keep trust.

3.1.3 Challenges Posed by Industry Cooperation

As cross-industry collaborative efforts such as EULYNX continue to develop, we should expect to see such innovation in future. Of course, it cannot be expected that such a development will happen all at once in a 'big bang'. A strength of this approach is that it sits at a very high level architecturally and still allows for significant variation in application within each system. Notably, signalling system data networks can be zoned with different security requirements to allow legacy devices that do not fit in to this vision. Migration is feasible. Legacy systems can initially be segregated and then upgraded later.

The establishment of common certificate exchange within the rail industry could lay the foundation for exchanging keys that facilitate cryptographic protection of communications. However, the industry, as a whole, must answer some technical questions.

What method and strength of cryptography should be used? How should the need, over time, for increasing cryptographic strength be managed? Experience with ERTMS has shown that the long lifecycle for railway technology does not play well with the rapid evolution of IT and cyber security. Researchers at the Universities of Birmingham and Radboud have demonstrated weaknesses in the Euroradio protocol's message authentication code (MAC or "signature") and commented that a brute force attack will likely be feasible within the next ten years. [4]

The cost of retrospectively upgrading a system of such scale is immense. Furthermore, it cannot be done in a single sweep, and inter-compatibility must be maintained. Each generation of cryptography requires not only new software, but new hardware capable of efficiently processing more intensive calculations.

In future, the industry might consider agreeing a constant rolling migration for security, with new hardware supporting the latest industry standard cryptography while also supporting older, weaker versions. Operators could then set deadlines by which time an older form of cryptography is no longer allowed to be used.

To facilitate this, safety and security should be kept separate, with safety messages packed within a standard secure IP packet frame such as Transport Layer Security (TLS) or Datagram TLS (DTLS).

3.2 Protecting Against Vulnerabilities

Security is not only designed into a system and forgotten. In the face of an ever-changing threat landscape, new vulnerabilities are periodically discovered. This requires ongoing management.

3.2.1 Why Industry Cooperation is Needed

NIS Good Practice B4d: *You regularly test to fully understand the vulnerabilities of the networks and information systems that support your essential service.*

NIS good practice puts the onus on operators to test systems for security vulnerabilities on an ongoing basis. From a technical perspective, the supplier is usually in the best place to lead this, particularly if a vulnerability is found and a security patch needs to be developed for a product. However, it is the very issue of security patches that causes problems demanding industry cooperation.

Because this is a safety critical industry, any change affecting a safety-related or safety-critical component requires significant product approval efforts. This is time consuming and costly. Thus, safety discourages the application of security updates. Yet, the security risk posed by not applying a patch could negatively impact safety. This is a catch-22 scenario that operators and suppliers must work together to resolve.

3.2.2 How Industry Cooperation Can Be Implemented

One potential cooperative resolution is for vendors to consider how to partition their product designs into safety-critical and non-safety-critical elements (e.g. separate processors). Operators should consider flexible and pragmatic approaches to the approval of security patches that only affect the non-safety critical element of a product that otherwise appears to be a single component.

The already accepted argument that IP networking equipment is not safety-related is similar.

3.2.3 Challenges Posed by Industry Cooperation

The primary challenge posed here is convincing stakeholders to accept changes to established and proven safety processes. Furthermore, integration testing of security patches developed by the supplier for operators presents other challenges. The operator needs to consider whether it has the capability to do this independently, or whether it should build a contractual relationship around the supplier maintaining a test rig with security test capabilities. Will operators need to maintain a rig for every bespoke instance of a single solution they sell? Are operators willing to accept patches from a generic rig?

4 OBJECTIVE C: DETECTING CYBER SECURITY EVENTS

4.1 Security Monitoring

While preventing cyber incidents is an important security objective, no countermeasures are perfect. Security monitoring supports the detection of cyber security events, which ultimately helps the operator respond before the impact increases.

4.1.1 Why Industry Cooperation is Needed

NIS demands an operator to continuously monitor systems for suspicious security events. This first requires that vendors and suppliers commit to all products generating relevant security event logs that can be aggregated for analysis. The operator must consider whether to have a single system that aggregates security logs from all suppliers' systems and does intelligent analysis itself, or whether each supplier is better positioned to provide individual security event management systems.

While significant automation and artificial intelligence can be deployed in this process, a 24-hour expert staffed Cyber Security Operations Centre (CSOC) is ideal for systems that demand a high level of resilience. This is particularly the case where systems have lower trust interfaces such as traffic management systems.

NIS Good Practice C1e: *You have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance. Monitoring staff have knowledge of the essential services they need to protect.*

Realistically, the scale of railway operations at which this becomes cost effective is enormous. For this reason, the industry must address how economy of scale can be leveraged.

4.1.2 How Industry Cooperation Can Be Implemented

An operator could operate a unified security event management system at their CSOC and place a contractual requirement on suppliers to support the development of rules for processing their respective log data streams. The supplier would also support the testing, but this would be led by the operator. Likely, the operator would contract out to a Security Information and Event Management vendor.

Larger national operators may find economy with an in-house CSOC covering both rail operation systems and enterprise systems. However, smaller operators could still benefit from the resilience provided by a CSOC if solution suppliers were to provide CSOC-as-a-service from a global centre covering many clients.

4.1.3 Challenges Posed by Industry Cooperation

Security monitoring systems can return a high number of false positives in the first months of operation. It may be challenge working with many different stakeholders to alleviate teething issues with a unified system.

5 OBJECTIVE D: MINIMISING THE IMPACT OF CYBER SECURITY INCIDENTS

5.1 Incident Response

The final key element to NIS compliance and cyber resilience is to minimise the impact of incidents by rapidly recovering from them and then building upon lessons learned.

5.1.1 Why Industry Cooperation is Needed

While cyber incident response should (hopefully) not need to be a common occurrence, when it arises, it plays a critical role in resilience. The operator needs to understand the nature of the attack and needs to understand what it can and cannot do to execute the first and most important step: Containing the incident and maintaining operations. With the wrong actions, it's possible to make a bad situation worse. The response needs to be swift and well organised.

It is worth noting that the reputation of all stakeholders is impacted by a security incident. All stakeholders will have a strong vested interest in the incident response and recovery, even when not contractually obliged.

5.1.2 How Industry Cooperation Can Be Implemented

To ensure any response is well organised, the operator or lead partner in a railway upgrade can involve all stakeholders in the creation of a Cyber Security Incident Response and Recovery Plan. Stakeholders should work together in rehearsing the incident response process periodically.

There is potential as well for members of the security operations team to cooperate with the project security testing team to experience how security monitoring systems function in the event of a simulated security incident.

Post commissioning, the operator may not have a member of staff with both cyber security expertise and intimate knowledge of the components of the system, so a potential solution is for the supplier to send such a person within a contracted time after an incident. This helps benefit from economy of scale.

5.1.3 Challenges Posed by Industry Cooperation

Security monitoring staff in the operator organisation may have security expertise, but because they must focus on a broad range of systems including enterprise networks, they will lack signalling system knowledge. Maintainers may understand signalling systems, but they are unlikely to have advanced security expertise. Therefore, it is good to have a signalling security specialist in the event of an incident. However, it is very expensive to have such a resource constantly on standby– even with economy of scale (though this too is difficult due to the global geographic spread of rail systems). A major security incident is rare but requires quick response. The operator and supplier have to work together to find a reasonable balance from a commercial perspective.

6 CONCLUSION

Cyber-attack poses an increasing threat to railway resilience. Attacks witnessed in sister industries, on products and solutions not very different to our own, demonstrate this. Furthermore, with increasing use of COTS technologies, the railway can become collateral damage in generic cyber-attacks targeted elsewhere.

The EU's NIS directive is driving a rapid growth of security emphasis in signalling and train control projects in Europe, and there are similar trends elsewhere. This change is raising a large number of questions in an industry historically lacking in cyber security maturity.

By building industry cooperation across the four objectives of NIS, the industry can collectively build this maturity. But this includes cooperation between suppliers regarding issues that may be considered commercially sensitive. Thus, industry stakeholders should seek to understand how to be more open with others.

7 REFERENCES

[1] S. Gibbs, “Triton: hackers take out safety systems in 'watershed' attack on energy plant,” 15 December 2017. [Online]. Available: https://www.theguardian.com/technology/2017/dec/15/triton-hackers-malware-attack-safety-systems-energy-plant. [Accessed 29 May 2019].

[2] HM Government, *The Network and Information Systems Regulations 2018,* London: Her Majesty’s Stationery Office, 2018.

[3] N. Howe, “Cybersecurity in railway signalling systems,” no. 236, 2017.

[4] T. Chothia, M. Ordean, J. de Ruiter and R. J. Thomas, “An Attack Against Message Authentication in the ERTMS Train to Trackside Communication Protocols,” in *2017 ACM on Asia Conference on Computer and Communications Security*, Abu Dhabi, 2017.