INTRODUCTION TO NIS

An Introduction to NIS for Train Operating Companies

As railways adopt more automated, wireless and connected technologies, their most safety-critical assets have become exposed to new and more dangerous types of cyber-attack. Train attacks are no longer science fiction. In early May of last year, the world was rocked by the WannaCry cyber-attack, which affected more than 200,000 victims and spread to over 150 countries. Computers had essentially been taken hostage by ransomware, and users were asked to pay up in the form of bitcoin. Law enforcement agencies, health services, telecommunication networks, universities, businesses, and railway systems were all affected by the attack. Estimates of the total damage ranged from hundreds of millions to billions of dollars. Experts said at the time that the next kind of attacks we will see will target critical infrastructure in the form of electrical networks, water companies, and transportation systems. The European Union had pre-empted this in 2016 when it brought out the EU Directive on Network and Information Systems (NIS) security. NIS addressed the cyber security needs of companies delivering operational services through harnessing ICT. It was made UK law in May.

The purpose of this paper is to demonstrate how and why the NIS regulations can be put into force by UK's Train Operating Companies. Its scope includes the guidance given by the UK National Cyber Security Centre and a discussion on what constitutes an essential service in terms of NIS relevance to train operating companies.

Joe Ferguson
Il7 Security Ltd

Information Technology increasingly underlies the successful delivery of train services. It is critical to signalling, interlocking, train and station management. Rostering of crew, rolling stock and fleet management are heavily dependent on IT systems and the communications glue that keeps them together. Our latest trains depend on mobile communications and on-board computers for regulation and movement authority. Train maintenance is finely tuned, and delivery of refurbished stock is precise and reliant on data availability and timing. Train planning is an art form underlain with science and technology and timetables…well can I say more. Getting correct information to our passengers is complex and technology driven.

Modern rail command centres use wireless connections to control activities, monitoring train speeds or regulating traffic signals. These wireless signals can expose a network's vulnerabilities and leave the infrastructure wide open for attack. Train networks use Wi-Fi connections to control critical components of the train, like brakes and doors. Attackers can find ways to access the wireless network to send commands to those components and change the behaviour of the train. Once attackers succeed in breaching a network to gather information, they can attack the physical elements of the network. They might change the controls on the train or could even access commands in order to derail the train. These kinds of attacks are termed 'simple' by dark net terms, and once a system is breached it's just a matter of deciding what commands a malicious actor wants to send. While current concerns concentrate on cyber-attacks aimed at corporate ICT infrastructure, systems and applications, the most dangerous attacks would be those aimed at systems 'in-flight'. A similar detect-and-resist approach is needed.

The threat landscape isn't that far-fetched. In the WannaCry attacks, Germany's rail network, Deutsche Bahn, was incapacitated by its ticketing and information systems going down. It is rumoured that cyber-insurgents from the middle east, aggrieved by German foreign policy, are already targeting Deutsche Bahn’s European Train Control System (ETCS). San Francisco’s subway services were recently the target of a cyber-attack which resulted in the hackers taking control of 2,112 out of 8,500 devices, shutting down workstations, ticket machines and computers. The hackers demanded a ransom of around $73,000, and the loss in revenue amounted to around $559,000 per day. A study by cyber security experts Raytheon and Ponemon claims that 66% of organisations are not ready to address security issues for remote assets.

Failure of ICT brings operational consequences, financial loss, and reputational downfall. Moreover, failure to deliver results in hardship for our customers – they are late home, late to work, late to meetings, rendezvous and dinner dates. Or they make do with cramped accommodation after trains are cancelled. Train failure reduces our customers quality of life, not to mention the clear safety imperative. Cyber vulnerabilities will surely cause our service mission to become compromised and leave our business open to intense scrutiny.

Being joined-up-digital, as train operating companies are nowadays, presents many challenges, not least because we occupy a place in the Internet of Things (IoT). Transport played a major part in the industrial revolution and it is now part of IoT, the “fourth industrial revolution”. The internet provides a vastly increased attack surface which requires us to consider our approaches to protection and crime prevention. These are very different challenges to physical security, preventing criminal access to our railway assets. The assets we possess and need to protect now are information assets, the data that allows us to move trains and the systems and applications that process and convey that data. Data volumes are proliferating: data velocities are accelerating, and data is generated and stored in complex and virtualised ways. The need for bandwidth and media to consume bandwidth are growing at our stations, our depots and our offices. The need to protect the Confidentiality, Integrity and Availability of our information Assets in this IoT, digital world, as it clashes with the increasingly competitive, increasingly scrutinised, hard pressed railway world is paramount.

Alex Cowan, CEO of transport cyber defence experts, Razor Secure, has warned rail, aviation and car manufacturers and operators that many more attacks on their distributed IT assets and networks can be expected in the coming year. Cowan has described how cyber-attacks on transport networks are an ever-increasing threat to the safety of passengers. Security vulnerabilities exist in the most unlikely places throughout all transports networks and since these networks are by definition on the move and distributed, they can be much harder to protect. They are characterised by weakness. Attacks on ‘non-critical’ networks, such as entertainment systems or passengers Wi-Fi may seem no more than inconvenient at the time but they can be a path to much greater access for the hacker to more automated, wireless and connected technologies their most safety-critical assets have become exposed to new and more dangerous types of cyber-attacks. These attacks can threaten passenger safety, disrupt service, and cause severe economic damage. Legacy components and many communication protocols throughout the railway industry were never designed with cybersecurity in mind and are in critical need of the new kind of network protection.

For hundreds of millions of train and metro passengers around the world, the need for a more robust network security has never been more critical.

Added to this is the global threat. The international threat to cyber security has never been less obvious, less publicised, or less real. The Russians' attack seems relentless – distortion and disruption of national transport will soon be on their radar, even if it hasn't been already, for a long time. How better to embarrass a government, to injure a National Economy, than attack its service economy, workers commuting into the City of London? Perhaps the attack motives are more direct, involving terrorism and major threat-to-life.

On May 10th the Network and Information Systems Regulations (NIS-R) came into law. This follows the EU NIS Directive of 2016, applicable to all member states. The aim of the directive is to ensure that organisations within those vital sectors of our economy are effectively managing the security of their network and information systems. Organisations within those sectors that are identified as "Operators of Essential Services (OES)" and will have to:

- take appropriate and proportionate technical and organisational measures to manage the security of their network and information systems (including managing cyber security risks and broader security and resilience risks to network and information systems);
- take appropriate measures to prevent and minimise the impact of incidents affecting the security of their network and information systems; and
- notify the relevant authority of any incidents affecting network and information systems which have a significant impact on the continuity of the essential service they provide.

The NIS Regulations apply to the sectors for energy, health, water, transport and digital infrastructure.

Main Players in NIS

National Cyber Security Centre

The National Cyber Security Centre (NCSC) performs two roles under NIS as well a third role for UL Plc. The roles under the NIS regulations are:

- Single Point of Contact (SPOC).
- Cyber Security Incident Response Team (CSIRT).

The NCSC is recognised as the Technical Authority on cyber for the UK. It is advisory and non-regulatory providing cohesion and authoritative competence in guiding both public and private sectors as well as government in the appliance of cyber security. It also provides a central role on sharing information through the Cyber Information Sharing Partnership (CiSP).

Competent Authorities

The regulatory role under NIS is given to what it defines as Competent Authorities (CA). These are the regulatory bodies, the agencies or government departments, that act as guardians of standards for particular industries. So, for water it is Ofwat and for gas and electricity it is Ofgem. Not surprisingly, or transport it is the Department for Transport (DfT). The CA is responsible for interpreting NIS in the context of the industry it is regulating. It will challenge the OES to identify and protect its essential services. It will produce an audit plan and audit each OES as it determines fit. It will liaise with NCSC in its interpretation of appropriate and proportionate control and expected outcomes. The CA will interpret the regulations to define reportable incidents and expect compliance. They are also responsible for fines which could be up to £17 Million[1] See the guidance from the NCSC to Competent Authorities.

Operators of Essential Services - Train Operating Companies

A Train Operating Company (TOC) is an OES and must conform to the NIS Regulations. Conformance provides a mainstay of TOC assurance to DfT as the Competent Authority, that the management of risk is appropriate and proportionate. This conformance should be regarded as a key project for any TOC. The TOC needs to demonstrate that:

> “The organisation understands, documents and manages access to systems and functions supporting the delivery of essential services. Users (or automated functions) that can access data or services are appropriately verified, authenticated and authorised.”

Essential Services

Defining these Essential Services is key to the focus an OES might lend to gaining compliance to NIS. For a TOC, essential services are those that ensure operational delivery targets are met, that trains run to schedule, within the defined safety and quality parameters, and that disruption and unnecessary delays are avoided. There are certain thresholds now given by the DfT for TOCs running more than 500 services a day which roughly equate to a 20% of these being disrupted requiring notification and reasons reported within 72 hours. Investigating the incident that occurred on July 5th. There was a loss of signalling between Selhurst and Balham which had a substantial impact on train services that day which was reported on BBC News. GTR (mainly on Southern) had 978 full cancellations and 248 part cancellations and was therefore in breach of NIS. DfT say both Network Rail and GTR should have reported this as an incident but neither did. Obviously signalling is a critical component to train management but was there a failure of another system that contributed to the outage? And was this a failure in technology, procedure or a breach of physical or personal security. Subsequent investigations into timetable and signal failures do not dig deep enough into the critical components underlying essential services.

One could interpret DfT guidance to mean that only services, the absence of which might cause a 20% outage in a day, should be protected. This would ignore common sense. There are a host of complimentary services that bring train operations together. One could suggest that the only service to cause a 20% outage would be a failure of the train or a failure of signalling. Signalling might be thought of as out of

[1] DfT have explained that the EU Directive merely followed GDPR in coming to this figure and it does not represent any academic measurement of incentive punishment regarding compliance. Philosophically, it is a ceiling unlikely to be reached unless there is some woeful incompetence or wilful disobedience.

control of the TOC, being the responsibility of Network Rail. But the failure to receive the signal or act correctly might be regarded as the responsibility of the TOC.

All trains have management systems and means of communications to the “shore” -it is not just the signalling. Once a train has signal – movement authority – it must transfer this to the propulsion, traction, brakes, and yes, the opening and locking of doors. These are controlled by the Train Control Management System (TCMS). The TCMS often taken for granted and overlooked is a critical part of train management. Because it’s taken for granted one might pause here to consider how vulnerable it is to physical intrusion – every coach has a server to support TCMS functionality and these are accessible via the ‘t-key’ – and they also have open service ports. They are all connected via a communications bus. There is also the Main Communications Gateway (MCG) through which the train communicates to the outside world. An attacker could disable train operations through these. One can see there are many in-flight essential services.

Bearing this in mind, and the TOC’s responsibility for operations and delivery as well as compliance, cyber security is aimed at the management of risk in the face of an increasing threat and there are many ways a third party might attack service. The financial risks a TOC faces are to its business; its income flow and the penalty fines it might occur (outside of NIS compliance) for delays and disruption or cancellations. There is the knock-on operational risk of having to re-schedule, re-roster staff and rolling-stock and all the resources this takes. Added to this are the reputational risks, the adverse reports in the papers and how this is interpreted in the press and social media. There are many reasons for defining services as “essential’ outside of just those that cause “reportable incidents” in the eyes of NIS.

There is also the question of the impact of those risks or the target of the threats. A little diversion to GDPR as these regulations coincided with NIS and in some ways have been treated with similar distinction – hence the fines and reporting allowance which are not entirely equivocal. GDPR is about the protection of personal data and its availability to the citizen. Confidentiality is prime with integrity and availability important but maybe not critical issues. With essential services, Availability becomes prime. However, Confidentiality cannot be ignored as access to detail on how a service is provided, technical detail on how it works, could make it vulnerable to attack. Similarly, customer information services might be attacked subtlety – not obviously as this would result in immediate reaction – enough to cause disruption. This might not result in a 20% NIS threshold being breached but might have significant reputational impact. On a sliding scale therefore, of the panoply of services the TOC delivers, it is obliged to protect not only Availability but also Confidentiality and Integrity.

The most important service, the one that if successfully attacked, might lead to delay and disruption is the movement authority, train regulation, so stop, start and speed. All these are safety related as well as able to cause disruption and are reliant on cooperation and collaboration between the TOCs and Network Rail. Similarly, the tactical management of train movement during the day is essential to performance and is a collaborative effort utilising applications and information sources from various interfaces. Allied to train management is station and platform management and there are a number of contributing services to the on-going administration of a station.

One of the most frequent causes of individual train delay is crew non-availability. Crew rostering is absolutely vital to consistent delivery of service. While crew planning can be seen as a background task, substitutions on the fly are necessary if trains are not to be taken out of service.

Underlying these critical services are important ones whose absence would cause disruption, the severity of which would be dependent on the length of outage, how long the service was not available. These include train planning, train maintenance and HR services. These could realistically be determined "important" rather than "critical". Another differentiator between important and critical is whether one medium of information exchange might be substituted for another. This might be in terms of radio / telephone rather than an email or signal. CCTV imagery for station management might be substituted by extra manpower – however there have been many occasions when stations have been closed because of the CCTV not working, so should CCTV be regarded as essential? Similarly, the original advice from DfT as to how to interpret "essential" was to exclude business systems, ICT, and to concentrate on the IT systems (applications) that supported front-line services. But then one hears of drivers refusing to commence a journey because they have no hard copy of the 'train plan' because of an IT/printer failure. Similarly, the underlying infrastructure, the hardware platforms, operating systems and communications media, be it video, Wi-Fi, LAN or WAN need to be regarded as 'essential' and downgraded from 'critical' to 'important' by providing resilience and alternatives.

There are two distinctions that are to be made. Critical services are vital to operational performance and the absence of ICT to support them needs to be avoided by compliance with NIS guidance. Important services become critical over time through aggregation and aggravation as well as depletion of alternatives. Key words in NIS guidance are 'proportionate' and 'appropriate'. NIS guidance to protect these critical and important services is to apply the applicable controls in a proportionate and appropriate manner. To make judgements, the Competent Authorities and Operators of Essential Services have received guidance from the UK Cyber Technical Authority, NCSC.

The NCSC Cyber Assurance Framework

The CAF is the means to demonstrate assurance to the Competent Authority that the operating company is applying 'applicable' best practice in *a proportionate and appropriate manner.* It is not a check-list but a series of principles that need to be addressed in a way that best suits the business while satisfying the CA that due attention is being made to the cyber threat at large. The CAF as a whole is an "indicator" of cyber health and maturity and allows a judgement to be made.

It is worth noting that the 14 principles presented in the CAF address the top-level descriptors of cyber-defence, namely Security Management, Threat Protection, Threat Detection and Response. Below the principles are some 30 aspired "outcomes and within these are spread some 177 indicators of 'good practice'. Not all the indicators need to be satisfied, only those that are applicable and where the targeted threat is not mitigated elsewhere. The 14 principles are divided accordingly:

Security Management:	Governance, Risk, Assets and Supply Chain Management
Threat Protection:	Services, Access, Data, Systems, Resilience, Users
Threat Detection	Protective Monitoring, Event & Anomaly Detection
Response	Incident Management, Lessons Learn

Approach

The CAF, as described, in guidance not just a check list for compliance. The check list approach is good for auditors and the quick and easy approach is to target those items that are easiest – "the low hanging fruit", the so-called easy controls such as acceptable use policies or introducing complex passwords. But there are no easily achieved outcomes, they all require planning, implementation and documentation. If serious about cyber security and combatting the threats, best target the "crocodiles nearest the canoe – if legacy applications exist or servers are unpatched, these are vulnerable and need protecting. Locking down platforms, introducing intrusion prevention, firewalls and event monitoring are primary foci if not already addressed. And then back to the checklist. The CA is responsible for issuing a checklist of CAF based indicators of best practice and these can be used for a gap analysis.

Planning

Unless the margin in the gap analysis is small, a plan will be needed – this is the only way to get management buy-in and the necessary resource. Start with the buy-in as principle A1 requires Governance and while this involves presentations, Board level sponsorship and activity are pre-requisite. Buy-in will see signatures against all the NIS based policies that will need to be written. The plan should involve writing the policies based on the outcomes required in the CAF then executing the activities that will achieve these outcomes. Some activities will be longer and more complex than others, so for instance if currently there is no protective monitoring, a Security Incident & Event Management (SIEM) system will need to be procured to satisfy principles C1 and C2 – all procurement exercises take time and implementing a SIEM with corresponding resources and procedures is a comparatively challenging exercise. Similarly, a corporate Cyber Awareness Programme (CAP) is going to be a resource demanding challenge if it is to satisfy principle B6. Through planning, measures necessary to counter the cyber threat, and being able to review these, getting approval from the operating board, an auditable, acceptable, NIS compliant cyber security platform, can be achieved.

ISO/IEC 27001:2013

Response, that is, principles D1 and D2, Incident Handling and Lessons Learn are best achieved if one embraces the 'continuous improvement' manta from ISO 27001. Common to all ISO standards 27001 incorporates the Plan-Do-Check-Act model. To follow this advice, it is best to align oneself completely to the standard. Due to legacy conditions of railways it may be impossible to achieve certifiable compliance across the TOC, but the scope may be limited to the ICT department. This would be the 'scope' of the Information Security Management System (ISMS). It would include the Personal, Procedural, Physical and Technical (P3T) controls needed to counter cyber threat and the project organisation to implement and maintain the veracity and legitimacy of these controls. Implementation and maintenance could be governed by a Cyber Security Working Group (CSWG), convened of stakeholders and implementers. These would deliberate upon and manage change as well as response to incidents, learning and remedial action. Changes would be based on applicability, appropriateness and proportionality. ISO 27001 itself comes with a checklist in Annex A with some 121 controls with considerable if not total overlap to the CAF outcomes and indicators of good practice. The CSWG should manage the CAF based gap analysis and a risk register of cyber issues to be addressed.

Conclusion

Train Operating Companies are under threat of cyber-attack. Across the railway industry we rely on constant internet access, and connectivity has become vital to many core business functions. What's more, with the growth of the Internet of Things, more devices than ever are at risk of malicious attacks. In the railway industry there are also the specific challenges of remote and small-scale networks – for example on rolling stock itself – that are difficult to secure. Hackers are continually finding new systems that lack sufficient security, and as the San Francisco incident demonstrates, it is just a matter of time before an unsecure system is exploited – and sometimes at great cost ; many companies across the transport industry are unprepared for the cyber security challenges of today.

The need for TOC ICT infrastructure to be secure from cyber-attack is now apparent to all. The need to implement measures leading to the outcomes and able to demonstrate positive indicators of good practice is not only achievable but auditable and even more significantly law. The guidance given by NCSC should be consumed voraciously and with alacrity if we TOCs are going to avoid cyber incursion and/or major incident.

DfT guidance and the subsequent protection to essential services must be extended beyond the boundaries of the terrestrial ICT real-estate and onto the rolling stock itself. This will require collaboration with the suppliers, Rosco's and operators as well as the authorities. There are physical means of protecting ICT assets on board the train. There is resilience and encryption as measures to protect the CIA of data processed and transmitted throughout the train. This however does not fulfil the needs of the NISC CAF which calls for monitoring, event detection and response. To satisfy these needs TOCS need to adopt in-flight intrusion detection and recording.

Joe Ferguson
CCP, M.Inst.ISSP, SIRA
Risk Analyst, Cyber Consultant
Project Manager Thameslink Assurance (NIS)
Joe.ferguson@GTrailway.com
0044 (0) 7817689081
www.il7security.com