`See It, Say it, Sorted' or in Cyber (See IT! Say IT! Sort IT!)

British Train Operating Companies (TOCs) are presented with a massive opportunity to get their cyber technology right. The EU saw the need for information security to boost safety and delivery of operating essential services. Essential Services contribute to the critical national infrastructure – in terms of importance, transport is the bloodstream of UK Plc. The EU put their vision into the European Regulations of Network and Information Services (NIS) in 2016. By May 2018, information security compliance was British Law. The NIS Law covered transport as well as other essential facilities such as the provision of gas, electricity, drinking water and Internet bandwidth. It recognised that without information security there can be no guarantee these essential services would be delivered. But has compliance been achieved since then, has it been "sorted"? Current evidence suggests the journey has some way to go, certainly with Train Operating Companies.

Increasingly this nation's essential services are under cyber threat. The threat landscape is examined in many articles – a fair rendition can be seen at https://www.il7security.com/. Foreign Intelligence Services, Terrorists, and criminal gangs in their thrall, have most to gain by disrupting the economies of western nations and the reputation of their governments. Imagine the effect on London of closing the tube or commuter arteries for any significant time. The NIS Act of May 2018 recognised this and appointed the Department for Transport (DfT) as the "Competent Authority" to regulate compliance and to oversee the improvement of information security in aviation, maritime and heavy rail. The UK "Technical Authority", the National Cyber Security Centre (NCSC) set out a framework to evaluate compliance with NIS. The Cyber Assurance Framework (CAF) set out achievable targets in areas of asset and access management, security awareness, monitoring and incident management. Failure to comply with these targets is actually in conflict with NIS and therefore against the law. Failure is subject to a high penalty – up to a £17 Million fine. But we are not quite there yet. There is a huge opportunity for operating companies, TOCs to use the guidance for their own good. Unfortunately, while the EU saw the problem, and the UK said what to do about it, it still 'aint sorted' ! Why is this and what are the consequences? Turn those consequences on their head and the TOCs are presented with a great opportunity.

So, why hasn't it happened yet? Is there an opportunity to get it right? Well, from the start, the government has not quite addressed the problem. It's a question of priorities. Since 2016, the year the EU came out with NIS, UK government has prioritised Brexit. By the time NIS became British law, Chris Grayling, a myopic of failure in all he has overseen, was in charge of the DfT and, of course, 2018 was the year of his disastrous timetable failure. The DfT, charged with being the 'Competent Authority' have failed to lead. Instead of being the 'elephant in the room' when it comes to regulation, they have made it all too easy for the TOCs to take their time, to be slow investing to protect themselves, in meeting regulatory targets. This is not the fault of the civil servants; they just have not been given the power to be authorative. This Conservative government fails to see privatisation as part of the problem. They believe in the policy and after nine years of Conservative mismanagement, this is just another case of implementing a European initiative incorrectly. This does not mean that railway people can't re-assume the initiative for the good of the UK.

The DfT requested the TOCs to submit compliance statements against the NCSC CAF requirements by end-March 2019, a full ten months after the Law was introduced. There

were some 70 CAFs submitted and under-resourcing meant NCSC had to step in and help. The CAFs were returned with comments from NCSC early this month. The appraisal was judged on non-compliance (RED), part-compliance (AMBER) and full compliance (GREEN). Needless to say, most submissions will be returned with more RED and AMBER judgements than green. Of approximately 170 'indicators of good practice' NCSC don't expect to find any to be anywhere near perfect. So, are all the rail companies operating outside the law? DfT have given them another twelve months to get things right so presumably not. It may be another 12 months down the line before this problem is addressed or as the railways need to - see it, say it, sorted. And even then, the DfT is only looking for AMBER in most of the CAF principles and not even that in some.

Perhaps what is needed is a further look at what is making it so hard for the operating companies to comply with regulation. For government organisations, compliance with information security policies is mandatory. The train operating companies are private entities but while they provide essential services to UK Plc, some of DfT lenience lies in recognising this. The policy of enabling the provision of essential services to the lowest bidder, the competition of the franchise system, might be the real cause of the problem. Many of the TOCs are owned by foreign conglomerates or large bus companies. They have diverse histories and operating constraints. Have they really got board-room commitment to long term investment in IT infrastructure that can be removed from them in the next round of short-term franchise negotiation and allotment? The cheapest bidder may not have the funds to make the investment. We see franchise decisions based on capped fares or payments to keep pension funds afloat. The shareholders of those conglomerates or holding companies may not have envisaged the NIS commitment just around the corner when they bid for an operating license just a few years before NIS. Conversely what incentive is there for Virgin, 49% owned by Stagecoach, to invest in its infrastructure when the DfT have revoked their ability to compete for the franchise they have held for ten years? Maybe NIS compliance might be built into the franchise competition with compliance rewarded and DfT seen as incentivising the implementation of best practice.

The IT systems that need to be managed to 'best practice' are those involved in getting the trains to run on time, to keep UK Plc productive. Clearly these include getting the people who drive and service the trains and stations in the right place, in the right quantity at the right time. So, the IT used for 'rostering' is essential. Also, essential, even critical to avoiding the delay and disruption to services, are the station management, the timetables, train maintenance and customer information systems. All rely on the communications and information systems, that NIS aims to protect. These systems need to have strong passwords, be configured correctly and free from physical or cyber-attack. They need to be operated by responsible people, trained and dedicated to the task, not easily influenced or susceptible to internet born social engineering, phishing or ransomware. Above all, these systems need to be monitored as much as any government system needs to be monitored. They are all vital to the running of UK Plc. Indeed, if one adds the safety factors involved, heavy rail, as well as aviation, maritime and for that matter any automated or semi-automated vehicle, needs to be monitored effectively and protectively. Good practices listed above are just a few of the indicators of best practice drawn up by the NCSC. Unfortunately, the networks and infrastructure are often shared with the parent company and the opportunities for attack are greater. Separation and protection, the implementation of focused security policy and procedure, take time and most importantly cost money – perhaps not budgeted for and

therefore only available at the expense of other priorities or through fare increase. This becomes a dilemma for the TOCs. It is not helped by the guidance given by DfT, who indicate that only disruption of service or delays to trains constituting 20% or normal service will attract penalty. The canny Finance Director, or controlling parent company, may argue that no IT system on its own, through its own failure, could cause 20% damage to services are in scope. And the DfT has allowed the TOCs to decide themselves what are critical or essential services. This is hardly conducive to clear incentivisation of 'good practice'.

Good practice might also extend to the Rolling Stock, the actual trains themselves. These are increasingly automated and semi-automated and, because of this, are susceptible to cyber-attack. There is even more confusion here. The first element of this confusion stems from the DfT not determining what is included as a critical or essential to the running of the train service. The second is the divergence between Operating Technology and Information Technology. The former is the responsibility, in TOCs at least, of the engineering department, the latter the IT department and it is only the latter that has been subjugated to years of cyber awareness. Engineering, quite rightly it seems to them, regard the computer and network on board a train as just another functional component that makes the train start, stop, go faster, slower, monitors its importance, and of course, opens the doors on the right side of the train at the station – everything that a train needs to do. They see a train as a closed unit, not as one more thing in the Internet of Things. That's why they do not see the cyber threat. That's why DfT received hardly any in-flight systems when they asked TOCs for a list of "essential services" – the TOCs did not see its rolling stock as in 'scope' as they did not see the cyber threat.

The cyber threat to trains comes from their increased connectivity, not only to the controllers that regulate their speed and direction but also internally where the on-board networks are connected, not only to the systems that operate the brakes, the traction and the doors opening. There are the on-board Wi-Fi comms, operational for Driver-to-shore communications and to relay real-time performance and maintenance issues, but also for entertainment, customer Wi-Fi and CCTV and for passenger information systems. The latter connect to the internet and are not monitored for cyber or physical attack. There needs to be strong interconnect between the IT department, who should have been looking at cyber for years and Engineering who could now be facing the biggest problems to safety from cyber.

Perhaps the biggest problem and another source of confusion is the in-flight regulation. Regulation controls the trains' speed and can be consumed from balises on the trackside, can be operated through manual over-ride, or increasingly through the operation of the European Rail Train Management System (ERTMS). The latter utilises GSM-R, a form of mobile communications between a Radio Block Centre, normally operated by Network Rail, and an on-board computer. Unfortunately, this communication is reliant on G3 or even G2 (note that the 'real-world' is already moving to G5) and an old style of encryption called triple DES. The communications stream has been hacked by Birmingham University and their methods of duplicating the encryption key published on the internet over twelve months ago. Once hacked a disruptive influence might introduce malware or worse to the regulation/ movement authority. In addition to this, jammers, cheaply available over the internet might disrupt service.

The computers on trains are not effectively protected even from physical attack and malevolent code might be introduced through removable media (USB etc.) as well as communications signals. Recent attacks on trains in Germany are cited as proof of vulnerability here. There are huge opportunities for TOCs, perhaps led by DfT, to address this problem, updating the signalling, physically protecting its systems or simply monitoring those systems for anomalies that might indicate a cyber-attack build up. Further confusion lies with shared or ignored responsibilities. Is it the train / computer manufacturer obliged to maintain the security and integrity of the systems supplied? Is it for the "Roscos" – these are the owners of most trains in this category who lease the trains to the TOCs or is it the Train Operating Companies themselves? Part of this question is how much responsibility lies with Network Rail who are responsible for sending the 'movement authority' as part of the regulation. NR themselves come under NIS scrutiny but it is not apparent that they have included regulation in their list of 'essential services'. This might be perhaps because DfT have not mandated this and disagreements exist as to whether is would disrupt more than 20% of service. To be fair, DfT do want NIS submissions based on what is considered essential not just whether it meets the 20% threshold though it is a very subjective decision for the TOCs to make. It may not disrupt >20% but one train derailed is a percentage too much.

The TOCs have been presented (for free) with a very comprehensive set of 'indicators of good practice' in the NCSC Cyber Assurance Framework. Compliance should not be seen as a mandatory duty of the TOCs but a blatant opportunity to lead. Compliance, or more importantly – getting IT (cyber) right - should be seen as a key differentiator when negotiating a new franchise and the DfT should make it very clear how competitors will be judged. Yes, investment in rolling stock, past records of meeting service requirements, good conduct in meeting staff (e,g. pension) obligations should all be taken into account. So too must be a recognition of and commitment to, Information and Operational Technology Security. Add this to the fact that information assurance also demonstrate commitment to protecting personal information a big GDPR plus!

Compliance with the NIS regulations is not the only way these obligations can be demonstrated. One of the NCSC CAF requirements is for the Operator of an Essential Service (OES) to conduct a risk assessment on those critical and essential services identified. Risk assessments should be carried out by a professional analyst and for assurance purposes should follow a common method. Typically, a method aligned to international standards[1] would consider threats – the source for threat motivation as well as the capability and opportunity of someone or thing in place to activate that threat. These threats would take into account any demonstrable vulnerabilities and factor these with the impact or consequence of a realised threat to operations, finance, personal distress, corporate reputation and legal compliance issues. Risk could then be evaluated against the business opportunity and if necessary, applicable controls could be put in place. By utilising the NIS Risk Assessment approach TOCs can identify those controls that are appropriate and proportionate to their needs and make a well-structured case for only applying those controls applicable to the evaluated, even prioritised risk. They have the whole plethora of 'indicators of good practice' to choose from and may select pragmatic, affordable options over a gilt-

[1] For example - ISO 31000 (2009), ISO /IEC 27001:201 ISO 27005:2018, NIST 800-30 Rev 1 (2012) Reference Chris Hodson Cyber Risk Management.

edged 100% compliance. In the first instance a documented risk workshop is recommended to align the aspirations of the stakeholders with the regulators.

With such a practical approach, TOCs can exploit NIS regulations and utilise 'free' NCSC advice on best practice to maximise benefits from information technology even in operations. This will generate the greatest revenues whilst delivering optimum services to their customers. The benefits far outweigh the tribulations of instigating a project to develop control over the IT function. Risk Assessments can cover both information and operational technology and focus on the cyber threats undoubtably looming. The positive benefits include: More Passengers: Less Delays: Less Disruption: Less Penalties: Fuel Maximisation: Staff utility optimisation: Minimising Maintenance overheads: Better Industrial relations. By taking the NIS Regulations to their heart, TOCs can take back control and run efficient services to the delight of workers, managers, shareholders and customers. A TOC should not be inhibited by the variations in the ambitions of its parent company, be it a foreign operator or international bus company – it should be driven by its ambition to deliver a train service. Rail Employees live by their commitment to the railway, putting customer service and safety first. NIS can help them do it despite franchisation and private, foreign, conglomerate ownership. The alternative to embracing NIS may be to take away these inhibitors and take the Railway back into public ownership. As they say in the industry, there is no right way, no wrong way, only a railway! The gaps left by the poor management of NIS by the so called 'competent authority' can be filled to the advantage of the Operators of Essential Services, the Train Operating Companies, and the UK need not lag behind the EU in implementing best practice. Its up to the TOCs to See It Say IT Sort IT. What to see is the cyber threat, what to say is that it threatens IT and OT, and how to sort it is a meeting of minds between IT and Engineering and the DfT being a positive contributor, not just the Elephant in the room and certainly not the 'pussy in the corner'.

Joe Ferguson, IL7 Security[2], working with Whiteflare.

[2] https://www.il7security.com/ http://whiteflare.co.uk/