Pride Security
A Pride Solutions Derby Ltd Brand

Developing A Fleet Cyber Security Framework

A Guide For Railway Undertakings

Presented by
Lee Clough

Developing A Fleet Cyber Security Framework

A Guide for Railway Undertakings

Pride Security

Executive Summary

The digital transformation of the railway industry has undoubtedly brought about new opportunities for improvements in operational efficiency, safety, and passenger experience. But it has also introduced a host of cyber risks that are previously unknown to the industry and simply can't be ignored.

Today's trains are essentially sophisticated, networked computers on wheels, and protecting them requires a solid and comprehensive cyber security strategy. That's where this Fleet Cyber Security Framework comes in—it's designed to help railway undertakings build a proactive, resilient approach to managing cyber threats.

This manual isn't just about organisations meeting compliance requirements or ticking boxes. It's a practical guide that discusses strategies to secure critical fleet systems, protect passengers, and ensure the smooth operation of rail services.

In recognising that cyber security can often seem overwhelming, especially with complex regulations and evolving threats, the guidance looks to provide structure, clarity and direction for both technical and non-technical leaders in the rail industry.

This guide covers all the key points a railway undertaking needs to work on to get started, from understanding the current regulatory landscape, to improving audit capabilities and implementing a comprehensive cyber security policy.

We look at how to integrate cyber security measures seamlessly into existing safety management systems, ensuring that digital safety becomes an extension of the physical safety culture already ingrained in the rail industry.

A successful fleet cyber security framework is more than just a set of technical controls—it's a mindset that weaves security into every part of fleet operations.

This guide promotes a proactive, risk-based approach that prioritizes regular assessment, continuous improvement, and strong communication between teams. In breeding a culture where everyone understands that cyber security is their responsibility, we create a workforce that protects digital systems and knows that it is just as crucial as maintaining physical safety.

Developing A Fleet Cyber Security Framework

A Guide for Railway Undertakings

Pride Security

Contents

Developing A Fleet Cyber Security Framework

A Guide for Railway Undertakings

Pride Security

Introduction

The last 10 years in the rail industry has seen a marked increase in the complexity of digital systems used in modern train operations. As more advanced digital systems become part of everyday rail fleets, the inherent risk of cyber threats embeds itself. It has become critical for railway undertakings to develop robust cyber security strategies that safeguards their entire fleet.

The level of regulation and compliance work required in the industry on a day-to-day basis is no revelation to those who must follow it. Applying the necessary due diligence to fleet operations, security and safety is a legal mandate that we all must follow.

To meet the needed levels of due diligence, railway organisations are required to develop a framework of policies, procedures and processes that, when combined, act as a roadmap, guiding companies through the process of spotting potential risks, evaluating their impact, and putting measures in place to limit damage.

This document is designed to be a practical guide for railway executives and engineering teams who need to build a solid cyber security plan. It'll help them understand the current state of digital safety in the rail sector, highlight areas that might be vulnerable, and outline specific steps to create a secure and resilient environment for connected train systems.

The key topics in the report include:

Understanding the Regulatory Landscape
An overview of key regulations and industry standards, such as EN 50129:2018 and the Railways and Other Guided Transport Systems (Safety) Regulations (ROGS). These rules stress the importance of staying ahead of potential cyber threats, especially in areas where passenger safety is concerned.

Evaluating the Cyber Threats
As discussed above, assessing, controlling and documenting risk is not new to the railway. However, the processes required for assessing cyber security risk differ from the processes used to calculate electro-mechanical risks for example. quantifying and mitigating these risks is a dynamic process that will require old methods to be amended and improved to ensure that emerging threat and risk is documented and controlled adequately.

Building a Strong Security Plan
A cyber security framework is not just about how we detect and prevent a cyber security incident. It is as much about creating the capability to respond robustly if an attack occurs. We look at this in some detail and provide practical advice on structuring a security plan that not only responds to incidents but also focuses on regular monitoring and long-term risk management.

Merging Cyber Security with Safety Protocols
Finally, the difficulties associated with blending new digital safety measures into existing safety management systems are not to be underestimated. A well-developed cyber security framework must ensure that the protection of digital systems goes together with already established physical safety practices. The aim of the framework is to complement the way the railway works, not frustrate it.

By incorporating the suggestions in this guide, railway undertakings can build a more resilient system that's better equipped to tackle the challenges of an increasingly digital world. The aim of the framework is to protect not just the technology, but also the people who rely on these systems every day.

Existing standards & legal obligations

Railway undertakings in the UK are subject to a complex web of laws, regulations, and standards that govern both safety and security aspects of their operations. The increasing digitalisation of railway systems has led to a greater focus on cyber security, which is now recognized as a critical component of overall railway safety.

Key Legislation and Regulations

The Network and Information Systems (NIS) Regulations 2018: These regulations require 'operators of essential services' (including many rail operators) to implement appropriate and proportionate security measures to manage risks to their network and information systems [1][2]. The NIS Regulations are particularly significant for cyber security, as they mandate a proactive approach to protecting critical infrastructure.

Railways Act 1993: Under Section 119, the Secretary of State has the power to issue security instructions to protect relevant assets within Great Britain against acts of violence [1]. This can include cyber-attacks that could potentially lead to physical harm or disruption of services.

The Railways and Other Guided Transport Systems (Safety) Regulations (ROGS): While primarily focused on safety, these regulations are relevant to cyber security as they require rail operators to implement safety management systems. Given that cyber vulnerabilities can lead to safety hazards, addressing cyber security is implicit in complying with ROGS [1].

The Railways (Interoperability) Regulations 2011 (RIR 2011): These regulations incorporate European standards that increasingly include cyber security considerations, especially for new or significantly altered subsystems.

Standards and Guidance

EN 50129:2018: This standard requires safety cases to describe how systems are protected from unauthorized access, including evaluation of IT security threats that could affect safety-related functions [1].

PD CLC/TS 50701:2021: This new cybersecurity standard for railways aims to ensure that Reliability, Availability, Maintainability, and Safety (RAMS) characteristics of railway systems cannot be compromised by intentional attacks [1].

Department for Transport (DfT) Guidance on Rail Cyber Security: This guidance emphasizes that safety claims must be informed by security considerations, and failure to secure systems might contravene regulatory safety requirements [1].

NCSC Cyber Assessment Framework (CAF): Published by the National Cyber Security Centre (NCSC), the CAF provides guidelines for assessing cyber security in critical sectors, including rail. It outlines 14 principles across four objectives: managing security risk, protecting against cyber-attacks, detecting cyber security events, and minimizing the impact of incidents [2].

Compliance and Enforcement

Railway undertakings must comply with these regulations and standards to:

1. Ensure the safety and security of their operations and assets.
2. Maintain their operating licenses and safety certificates.
3. Avoid potential financial penalties, which in the UK can be up to £17 million for non-compliance with NIS Regulations [2].
4. Meet the expectations of regulators, including the Office of Rail and Road (ORR) and the Department for Transport.

Implications for Cyber Security Frameworks

In developing a cyber security framework for railway fleets, undertakings must:

1. Implement comprehensive risk assessment and management processes.
2. Establish robust security measures to protect against cyber-attacks.
3. Develop detection capabilities to identify potential security events early.
4. Create incident response and recovery plans to minimize the impact of cyber incidents.
5. Ensure that cyber security considerations are integrated into safety management systems.
6. Provide regular training and awareness programs for staff.
7. Conduct ongoing monitoring and reporting to demonstrate compliance.

Merging all the incredibly complex requirements above into a framework of policies, processes and procedures is no small undertaking and not one that should be taken too lightly. Further into the report, we delve deeper into some of the elements of the framework that are needed to support a railway undertaking with their cyber operations.

Pride Security

Fleet Cyber Security Policy

A Fleet Cyber Security Policy isn't just another document on the shelf—it's the playbook that guides a railway organization's efforts to protect its trains and digital systems from cyber threats. Think of it as the backbone of any robust cyber security framework.

A robust policy sets the direction on how the company approaches security across its fleet operations and maintenance. The policy ensures everyone— at all levels of the organisation —are on the same page when it comes to safeguarding these critical assets.

A good policy does a few crucial things: it guards against unauthorised access and data breaches, keeps trains running smoothly, and ensures that the organisation meets all the necessary laws and regulations. It also goes a long way in reducing financial losses and keeping the company's reputation intact if something does go wrong.

All that sounds great, but if you are a railway undertaking with no cyber security infrastructure in place for your fleet, what should a Fleet Cyber Security Policy look like? Well, for starters, it needs to clearly define its Scope and Applicability—spelling out exactly which systems, equipment, and people are covered.

Next, it should lay out Roles and Responsibilities for the key stakeholders, mapping out who is responsible, accountable, consulted with and kept informed of what when it comes to cyber security. This structure should extend all the way from the executive branch, all the way down to the teams handling business-as-usual operations.

As the railway is already aware of, Risk Assessment and Management is critical to all activity. Any decision made that affects the fleet, operational safety or passenger interactions must be documented and defensible. This involves setting up processes for spotting potential security risks as quickly as practicable and figuring out how to deal with them. And, of course, a big part of this is Access Control—setting strict rules for who gets access to these systems and how that access is managed and monitored.

Keeping track of what's part of your digital ecosystem is just as important. That's where Asset Management comes in—keeping a detailed inventory of every piece of hardware, software, and data associated with the fleet. And when it comes to

responding to cyber incidents, a good policy will have a clear set of guidelines for Incident Response so the team knows exactly what to do if a security threat pops up.

Don't forget about the people. Training and Awareness programs are a must to make sure that staff at all levels understand the importance of cyber security and know how to contribute. But the policy can't just stop at the front door—Supplier Management is crucial too. After all, a third-party vendor carries, and brings with them, their own operational risks, so it's essential to set security expectations for them as well.

And let's not overlook Compliance and Auditing. A policy needs to include steps for regular reviews to ensure everyone is sticking to the plan and meeting industry standards. Lastly, to keep operations running smoothly even in the face of a cyber-attack, you'll need Business Continuity provisions—detailed plans for keeping things on track if something goes awry.

To be effective, a Fleet Cyber Security Policy can't be a "set it and forget it" document. It should live and breathe within the business. Executive level buy-in is crucial, integrating seamlessly with existing safety management systems and IT security policies.

The whole policy must be regularly updated to reflect the latest threats and tech developments. Just as importantly, it should outline what happens if someone breaks the rules and how those breaches will be handled.

A well-structured policy sends a clear message: the company is serious about cyber security, meeting all regulatory requirements, and committed to keeping its operations safe and reliable. By putting such a policy into action and ensuring everyone adheres to it, the organization can significantly reduce the chances of a cyber-attack, protect its reputation, and even minimize legal exposure.

In today's fast-evolving digital world, having a strong Fleet Cyber Security Policy isn't just good practice—it's a necessity for any railway company that wants to stay ahead of potential threats and keep its trains running safely and efficiently.

Fleet Cyber Incident Response Plan

A Fleet Cyber Incident Response Plan isn't just a box-ticking exercise—it's a vital piece of a railway company's broader cyber security strategy. This plan spells out who does what, how they communicate, and the exact steps to take if something goes wrong with the digital systems controlling the trains. Being able to respond quickly and efficiently to a cyber threat isn't just about avoiding inconvenience; it's crucial for keeping services running and, more importantly, for ensuring the safety of passengers, staff, and critical infrastructure—the absolute top priority for any railway operation.

Having a comprehensive response plan in place also means meeting regulatory obligations, like those outlined in the NIS Directive & ROGS. These obstacles aren't just bureaucratic hurdles—they exist to make sure operators are taking all the right steps to protect their fleets and their organisations - also known as applying adequate 'Due Diligence'. When a railway company can show they've done their due diligence and are fully prepared for cyber incidents, it sends a powerful message to regulators and the public alike.

It's essential to remember that railways don't just run trains; they serve the public. And that service comes with a responsibility to show they're taking safety and security seriously. A solid response plan proves they've thought things through and taken every reasonable precaution to keep people safe. It's not just about following the law; it's about demonstrating a commitment to public trust.

Handling cyber incidents effectively also has a big impact on how the organisation is viewed and regarded by the public with whom they serve. A well-executed response to an attack shows the world that the organisation is both prepared, and competent, reducing any potential reputational fallout. It can also help keep disruption to a minimum, limit data loss, and control legal liability in the event of a cyber-attack. All this before we consider the financial damages that can come with a poorly managed response to a cyber-attack- critical when the potential fines for failing to apply correct due diligence could be 17% of an organisation's turnover.

The Multi-Purpose Role of a Response Plan

The Fleet Cyber Incident Response Plan does more than just dictate the process operational decisions are made against during a crisis.

First, it acts as a response method for the team, with clear, step-by-step instructions so everyone knows exactly what to do in a cyber emergency. Next, it lays out a communication strategy, making sure that everyone—from internal teams to external regulators and law enforcement—stays in the loop. It's also a training tool, providing the foundation for regular drills and simulations so staff get comfortable with their roles long before a real crisis hits. Finally, the plan helps the organisation improve its cyber security approach for future attacks through detailed post-incident analysis of previous attacks.

What Should a Response Plan Aim to Achieve?

Any incident response plan worth its salt has a few core goals: Identify, Protect, Detect, Respond, & Recover. These aim to quickly identify an emerging vulnerability, protect the systems against vulnerabilities being exploited, detect any new attacks, contain any threat, keep essential services running, protect sensitive information, preserve digital evidence for forensic purposes, and ensure clear communication with stakeholders throughout the process.

Following these incident response steps means the organisation is not just reacting to an incident, but proactively managing it in a way that limits the impact and reassures the public, and regulatory bodies, that everything is under control.

Key Elements of a Strong Incident Response Plan

Building an effective response plan means covering a lot of bases. It needs a solid incident classification system to distinguish between minor blips and full-blown crises, a clearly defined response team structure with roles and responsibilities laid out, and escalation procedures for when things need to be kicked up a notch. The plan should also include containment strategies, recovery procedures, and even pre-approved communication templates to keep everyone aligned. And don't forget the regulatory reporting guidelines—having these built into the plan ensures compliance is automatic, even in high-pressure situations.

Implementing the Plan Effectively

To really make it work, a Fleet Cyber Incident Response Plan must be more than just words on paper. It needs to be updated regularly to keep up with new technology and evolving cyber threats. It should be backed up by ongoing training and simulation exercises that give the team hands-on experience. Plus, it must integrate smoothly with the company's wider business continuity and disaster recovery strategies. Building strong connections with external cyber security experts and law enforcement can also be a game-changer, making sure help is on hand when it's needed most.

By investing the time and effort to build a thorough incident response plan, railway companies aren't just ticking a box—they're enhancing their resilience, protecting critical infrastructure, and maintaining public trust in an increasingly digital world.

Pride Security

Engineering Change Management

The last 10 years completely transformed how railways operate. New, digitally connected fleets bring a level of efficiency and connectivity that drives huge improvements in reliability and maintainability. But this shift also comes with a new set of cyber security risks that railway companies simply can't afford to ignore. This report explores why a solid cyber security framework is now essential, outlining strategies to keep passengers, and rolling stock systems safe from the latest cyber threats while maintaining smooth operations, meeting regulations, and keeping public trust intact.

Railway networks have some unique challenges when it comes to cyber security. These systems aren't just complex; they often rely on outdated technology and are critical to national infrastructure. That's why this report lays out a big-picture view of what an effective Fleet Cyber Security Framework should look like, covering several key areas:

First up, the Regulatory Landscape. Railways have a host of standards and legal requirements to juggle—everything from NIS Regulations to the Railways Act, and the industry's own set of safety rules. Getting it right means knowing the rules inside out.

Next, there's the Fleet Cyber Security Policy—think of it as the backbone of your security setup. This policy is your organization's game plan for keeping all digital systems and rolling stock secure against cyber-attacks.

Another crucial element is Incident Response Planning. If a breach happens, you need a solid plan to jump into action fast and minimize damage. Having a response plan in place is like having a fire extinguisher—you hope you won't need it, but it's a lifesaver when you do.

Of course, you can't forget Engineering Change Management. This means tweaking the way you handle changes to the fleet to factor in potential cyber risks. Every modification completed should be subject to a thorough review to catch any new vulnerabilities that might crop up and to keep cyber risk profiles relevant.

Then there's Risk Assessment and Management, which is all about evaluating potential weak spots and figuring out how to shore them up before hackers can exploit them.

Asset Management and Inventory is another must-have. Keeping a real-time, accurate inventory of all digital assets related to the fleet gives you the visibility you need to stay one step ahead of threats.

You'll also want to invest in Training and Competency Programs for everyone involved. Ensuring that staff—from top management to frontline operators—understand cyber security isn't just a "nice to have"; it's a necessity.

Lastly, Supply Chain Security and Continuous Improvement are about thinking beyond your own systems. Suppliers, vendors, and third parties can be entry points for cyber-attacks, so it's crucial to keep a close eye on them. And just like in any security setup, there's always room for improvement—constantly refining your approach will keep you prepared for whatever comes next.

By breaking down these areas, this report aims to give railway companies a clear idea of what a solid cyber security setup should include. It's not just about protecting the nuts and bolts of your infrastructure but also about ensuring your entire operation runs safely, complies with regulations, and reassures the public that rail services can be trusted.

As cyber criminals get savvier, rolling out a structured Fleet Cyber Security Framework isn't just a good idea—it's a must-have for any railway organization that wants to stay ahead of the curve. This guide offers a roadmap to navigating the often-murky waters of cyber security in fleet management, packed with actionable insights and recommendations for boosting your cyber defences.

Pride Security

Whole Life Maintenance Planning

Traditionally within the railway, vehicles are purchased, designed and built to last for a specified design life (typically 30 years). Over that period, the unit is scheduled to undergo routine and scheduled maintenance from regular servicing of drivetrain equipment to half-life interior upgrades and corrosion workstreams.

Typically, the equipment within sub-systems is not expected to be upgraded very often, and indeed for most of the non-consumable equipment on board a vehicle, it is expected it will last and function for the design life of the vehicle.

Usually, this would not present a problem as, once risk assessed as suitable to be installed to a vehicle, the systems are generally fit and forget. The electro-mechanical risk does not really change for products installed to trains, so the only issue arises around unexpected failures, which are dealt with by simply repairing or replacing the failed component.

Whilst this process has served the railway well for many years, unfortunately that approach may no longer be adequate when designing and installing digital infrastructure. The hardware within a digitally connected device, whilst deemed secure on the day of assessment/installation, can be a source of vulnerability within a network immediately after installation.

This is because the hardware, software and firmware used within the device will also be used in other digital systems. Vulnerabilities may have been identified and logged with their OEMs, but not identified by the OEM of rail equipment.

As part of their whole-life maintenance planning activities for vehicles. Railway vehicle owning companies, as well as railway operating companies and third party OEMs, now have an obligation to review the position of their digital infrastructure and ensure the maintenance schedule accounts for these dynamic risks and has steps to identify, patch, and renew equipment that has been subjected to vulnerabilities, no matter the frequency at which those vulnerabilities are found.

Now, nobody expects these systems to be assessed constantly, and upgraded every single time any possible vulnerability is identified. The agreed procurement contracts for the equipment should include necessary patching and security update support for a determined period beyond the normal warranty of the hardware.

Likewise, the scheduled maintenance plan for the vehicles should account for the need to routinely reassess the hardware, software and firmware against known lists of vulnerabilities and enact any known fixes for these vulnerabilities.

Where vulnerabilities are identified, but no known fix exists, it may be suitable to either live with the risk if it is sufficiently low, or to put in place additional mitigation activities using other means to lower the likelihood of a vulnerability being exploited.

This is achieved through continuous, dynamic risk assessment of digital systems on a regular basis to ensure that all known risks are known, understood, mitigated and documented correctly.

Pride Security

Fleet Cyber Risk Assessment

When it comes to securing a railway fleet, conducting a cyber security risk assessment isn't just a checkbox—it's a must-have for any organisation serious about protecting its assets. It's a step-by-step way to pinpoint potential cyber threats and vulnerabilities that are unique to the complex systems onboard modern trains.

How Often Should Risk Assessments Be Done?

As discussed, unlike electro-mechanical risks which remain broadly static and defined, cyber security risks are dynamic and change on a regular basis as new vulnerabilities are identified and threat actors learn to use them. To keep up with such a dynamic risk profile, detailed risk assessments are required at the outset, along with periodic revisits to ensure the risk assessment remains accurate.

Here's how we recommend scheduling the reviews:

Annual Detailed Assessments: These yearly reviews should aim to take a deep dive into the risk profile of the whole fleet.

Quarterly Check-ins: These much shorter, quarterly reviews have the objective of identifying if any major changes (like new threats or company changes) have popped up that deviates the risk rating from the recorded level.

Ad-Hoc Reviews: Whenever you make big changes—such as rolling out new trains, deploying software updates, or responding to a cyber incident—conduct a fresh assessment.

The Risk Assessment Journey

Think of the risk assessment as a map, guiding you through several key steps. The first step is to take a step back and evaluate the extent of your infrastructure. List every single digital asset in your fleet, from onboard systems to the networks they connect to.

Once you have visibility of the whole infrastructure, you can quantify the threats. Categorising the risk and threat is achieved using both industry knowledge and past similar incidents.

Once you have defined the threat landscape and you understand the different ways your systems could be compromised, you are able to identify weak points in your current systems and practices that could be targeted.

So now you have the lay of the land, you know what your attack surface looks like, you have the knowledge about possible vulnerabilities and where the weak spots may be in your systems. The next step is to understand what the potential impact would be for each threat. The impact is the fallout if these threats were to succeed—what's at stake for safety, operations, finances, or reputation? This would be scored on a matrix from minimal impact to catastrophic and be given a numerical score.

Understanding the impact is only one part of the equation though, and without knowing how likely a particular scenario is to occur, the impact does not mean much in real terms.

Traditionally in the railway, we would draw on service experience to quantify the likelihood of a scenario occurring. That is to say, if a fleet of 10 trains has been operating for 10 years, there are 100 operational years to draw from. If a particular scenario occurred only once in that time, then the likelihood would have a rating of 0.01.

The difference with cyber risk, however, is years of service for the fleet or product count for nothing. Likelihood is instead calculated based on the ease of execution and the levels of access required. It may be more appropriate to replace likelihood with the CVSS score if one is available.

Finally, to obtain the overall risk rating, just as in the normal process for calculating risk, we multiply the potential impact and likelihood scores to figure out the overall risk for each scenario. This will give you a final risk rating and decide how tolerable the risk is to the organisation.

Keeping a dynamic risk register live and up to date is critical to your ongoing game plan. It's not just a list; it's a live document that evolves as your fleet and the cyber landscape change.

Developing A Fleet Cyber Security Framework

A Guide for Railway Undertakings

Pride Security

Railway Fleets Railway systems are a unique beast. When assessing risks, keep these points in mind:

- Pay extra attention to safety-critical systems that could impact train operations if compromised.
- Watch out for interoperability risks at the points where different systems connect, whether that's within your fleet or with external partners.
- Don't ignore legacy systems—older technology can be surprisingly vulnerable.
- Be aware of supply chain risks, especially with third-party suppliers and maintenance providers.

By keeping your risk assessment process agile and thorough, you'll be better equipped to handle whatever cyber threats come your way—ultimately making your fleet more secure and resilient.

Software Control

Let's be real—modern trains are basically computers on wheels. Just like the sophisticated systems you'd find in a high-tech factory or a power plant, today's trains are run by software that controls everything—from how many doors open on each side, to the temperature in every passenger car, and a ton of other critical operations.

This digital transformation is amazing for efficiency and passenger experience, but it's also a bit of a cybersecurity nightmare. Unlike updating an app on your phone, every single software change in a train system, no matter how small, can have a massive impact on safety and operations.

Making Sure Updates are Safe: It's More Than Just Clicking 'Install'
Let's be honest—would you feel comfortable riding a train if you knew they just threw in some new software without thoroughly checking it first? Of course not! That's why we test every update to the nth degree before it goes anywhere near an operational train.

Here's how we make sure everything is safe:

- Dig deep into what's changed—and I mean every tiny detail. We need to know what exactly has changed, why, and exactly how we should be expecting the applicable system to behave with the new software.
- All software updates with the slightest potential to affect the correct operation of the train MUST be tested on 'Train-Zero' (a virtual train that matches the exact configuration of the train) until we're sure it's rock-solid. If testing in Train-Zero is not appropriate for the update, restrictive and controlled testing and deployment of the software should be carried out on the fleet to assess compatibility and performance.
- Document everything—yes, every test, every result, as if safety depends on it (because in many cases, it does).
- Have a rollback plan—so if something goes sideways, we can quickly put things back to the way they were.

Change Management: Not Just Bureaucratic Boredom

As we discussed in the Engineering Change section, managing, assessing and controlling risks using the engineering change process is nothing new to the railway. As is the case for all changes we make to a train, when it comes to train software, it's a crucial safety net. Every single update—no matter how tiny—needs to jump through the hoops.

Thorough risk assessments to understand what could go wrong, using input from the right experts who know the system inside and out, allows fleet management teams to identify and address potential problems before they turn into real-world headaches. Keeping a detailed record of every step, so we always know what's been done and why, will make any incident response smoother as those records may contain the answer to how to stop an attack.

Post-Update: The Work Isn't Over Yet

Once the new software is in, we don't just sit back and relax. We've got to monitor the system for any strange behaviour. Just because the software releases tell us it passed quality control testing, we cannot just take this as gospel. We need to validate that the train systems perform as expected.

This is best achieved by requesting and listening to feedback from the people who are using the trains, such as drivers, maintenance staff and customer feedback, and by being ready to quickly address any arising issues.

By taking software control this seriously, we're not just following some checklist—we're actively making railways safer and more reliable. It's a constant balancing act between embracing new technology and not dropping the ball on safety. But hey, that's what makes this work so rewarding, right?

Pride Security

Training and Competency

In safety driven industries such as the railway, managing and enforcing training and competency standards is a mandatory requirement to demonstrate that the people making decisions and carrying out work on safety critical systems possess the correct levels of knowledge and skills to carry out the work competently.

Traditionally, rail vehicles have been managed by electro-mechanically trained engineers who understand the way their trains are designed, built and operate better than anyone. They are highly trained artisans of engineering that is for sure, but in this new world of connected vehicles, this is no longer enough.

For any fleet cyber security framework to be successful, it is critical that railway undertakings fully understand the skills and capabilities they need within their teams to be able to manage the digital systems, and associated risks, correctly.

Fleet engineering teams must have capabilities in assessing digital information and performance to be able to adequately assess risk. This means that someone managing the day-to-day engineering and performance of a modern fleet must be able to interpret network information, understand how different digital Operational Technology (OT) systems communicate using protocols such as TCP/IP, CANBUS and MODBUS systems. They must be able to read, understand, interpret and use Common Vulnerability & Exploit (CVE) information to be able to assess risk, how to respond to potential attacks and be able to use all this information to determine how the trains performance may be affected in the event of a cyber-attack. Oh - and they must be able to do all this on the fly.

Even outside of the hyper detailed understanding required of fleet management teams, there must be a good level of awareness of cyber risks, and the indicators of cyber-attacks, within your operations and maintenance teams, with robust reporting systems in place for this information to be communicated clearly and concisely back to the fleet management teams. This awareness breeds a security first culture and gets people questioning whether it is possible that a malfunction or degraded performance within a system could be a cyber-attack.

As such, for a railway undertaking to be successful in deploying supporting their fleets cyber security posture, they must update their training and competency standards to ensure that different staff are trained and knowledgeable in the

relevant areas for them to complete their role without potentially adding to the risk profile of the fleet.

Consider training your staff in the following areas:

- Fleet Management Teams:
  - Introduction to Operational Technology Security
  - OT Communication Protocols (SCADA, CANBUS, MODBUS)
  - Introduction to Cyber Risk Management
  - Software Control Courses
  - Cyber Risk Assessment

- Maintenance Teams
  - Introduction to Operational Technology Security
  - OT Communication Protocols (SCADA, CANBUS, MODBUS)
  - Cyber Security Awareness Training
  - Introduction to Social Engineering

- Operational Teams
  - Cyber Security Awareness Training
  - Introduction to Social Engineering

The importance of training and preparing staff, and the benefits repaid in the event of an attack cannot be overstated. The more knowledge, training and skills you can build into teams, the smoother and more robust a security posture a railway undertaking can develop, and the more effective any response efforts will be.

Supply Chain Control

When it comes to railway undertakings taking steps to keep fleets secure, managing third-party suppliers is just as crucial as maintaining their own cybersecurity practices. The reality is, as rail systems get more tech-savvy and interconnected, it's not just your own defences that have to be considered. If one of your suppliers has a weak spot, it could end up becoming your problem.

Why Supplier Management Matters for Fleet Security

Having a strong relationship with your suppliers isn't just a "nice-to-have"; it's a must. Without a clear plan for managing them, you're basically leaving yourself open to trouble. It's not hard to see how things can go wrong: If you don't have a firm grip on who's responsible for what, vulnerabilities can slip through the cracks. Here's where some extra attention can go a long way:

Setting the Right Expectations

If contracts don't clearly lay out who's on the hook for security, things get messy fast. When everyone's not on the same page, security gaps pop up, and suddenly, you're dealing with unexpected headaches. The key is to spell things out from the start. What exactly does security mean for this project? Who's going to keep it up to date? These details can make or break your defences.

Smart Procurement Practices

When you're picking suppliers, it's not just about finding someone who can deliver on time and at the right price. Security must be part of that equation too. Weak standards in procurement can bring in systems that are already flawed, putting you at risk before you've even begun. Make sure cybersecurity criteria are baked into your selection process and that suppliers can prove they're serious about it.

Keeping Tabs with Regular Checkups

A lot of people forget this step: checking in regularly. Even if you've started on the right foot, you need to keep up with routine audits to ensure that everyone's still following through on their promises. These check-ins should do more than just tick boxes—they should dig into whether suppliers are sticking to agreed standards and catch any issues before they snowball.

Long-Term Support from OEMs

Then there's the role of Original Equipment Manufacturers (OEMs). Just because they handed over a system that works, and is secure on day one, that does not mean it will remain secure forever. If suppliers are not consistently testing and patching vulnerabilities in their products, your fleet could be exposed to new threats. It's essential to lay out how long they're going to support the system and ensure updates come regularly.

When you consider all the above, neglecting supplier management can lead to a cascade of problems:

- Ongoing Weak Spots: Vulnerabilities that aren't caught early can stick around and become much harder (and costlier) to fix later.
- Bigger Attack Surface: Every unsecured connection or system from a third party is like leaving a window open for cybercriminals.
- Regulatory Issues: Falling short on supplier security can mean you're not meeting industry regulations, which could lead to fines or worse.
- Operational Disruptions: If a supplier's system goes down or is compromised, it can throw your whole operation off, affecting schedules and safety.
- Security Gaps Over Time: With trains and systems in use for decades, you need long-term plans for updates. If you're not on the same page about that from the start, things can get tricky years down the road.

It is critical that rolling stock organisations work closely with suppliers to keep pace with new threats and changes. Ensure they have solid plans for handling incidents and disclosing vulnerabilities.

When you put these pieces in place, you're not just ticking off a compliance box—you're building a stronger, more secure network that can handle whatever comes its way.

Pride Security

Document and Record Control

Now this section is one of the most crucial. This is not the same as the documenting and recording themes we have discussed throughout each section of this manual – though they would be subject to the theme of this section.

This refers to the security of maintenance documentation and records. Historically, a trains maintenance manual or details of the maintenance records were of little use to anyone outside of the vehicle owners, operators and maintainers. For those of you in the know, they were more akin to a Haynes manual for what maintenance should be done when and how.

With our latest generation of modern fleets, however, this is not the case. The maintenance manuals and records likely now contain sensitive information such as IP addresses, network architecture information and, potentially, administrator credentials for systems.

This information, in the hands of an adversary, could be seen as a playbook for exactly how to gain administrator level access to systems on board the train, and how to compromise safety critical systems or disrupt train operations.

For any cyber security strategy to be successful, this information must now be treated as strictly confidential. Access to the documentation must be kept to a need-to-know basis. Ideally the documentation will be permanently retained within secured digital systems, with the printing and distribution of the documentation either restricted, or heavily audited to highlight the user that carried out each action.

Any rolling stock organisation who manages these documentations must ensure they are using robust data-loss prevention systems and strategies to minimise the likelihood of data being exfiltrated from the organisation. This should also be documented as a risk within the wider organisation's cyber security risk assessment.

Likewise, a railway undertakings, along with OEMs and suppliers may want to consider deploying systems that scan both the clear-web and the dark-web for documentation being available at sources not controlled by the organisation. In the event of this happening, then the cyber security policy must treat this as a cyber-attack, and the framework must be robust enough to take corrective action.

Audits & Non Conformance

When it comes to cybersecurity in railway operations, having both internal and external audits isn't just a good practice—it's essential. These audits are like regular check-ups for your security systems, making sure everything is running smoothly and that no critical issues are slipping through the cracks.

Internal audits are all about taking a close, ongoing look at how well your organisation is sticking to its cybersecurity policies and procedures. They offer a few big advantages:

- Regular Check-Ins: Because they're done in-house, internal audits can happen more frequently, making it easier to catch issues before they become big problems. Regular interaction between audit teams and internal business-as-usual teams reduces friction and makes it fell less intrusive.

- Deep Understanding: Since internal auditors know the organisation's structures and processes better than external audit organisations, they can identify smaller, more nuanced issues that might escape an outsider's notice.

- Quick Fixes: When problems are spotted, they can be acted on fast, keeping disruptions to a minimum.

- Budget-Friendly: Robust audits underpin internal readiness. This reduces an organisations reliance on bringing in outside help every time there is an issue, reducing budgetary burdens.

External audits, on the other hand, are like bringing in an outsider's perspective—a fresh set of eyes. An external team can catch deficiencies that are baked into your processes, that internal teams might overlook just because they're too close to the problem. These teams of auditors are also a great tool for demonstrating due diligence to standards and regulations. External auditors work with different companies, so they can offer tips and strategies based on what's working elsewhere.

Through their work across multiple industries, it is also important to remember that external auditors often bring tools and expertise that aren't always available in-house, adding another layer of scrutiny.

Keeping an Eye on Third-Party Suppliers

As discussed in the last section, with rail systems relying on a web of third-party suppliers and OEMs, auditing compliance of their cybersecurity practices is crucial to a successful cyber security strategy. Weak compliance inside suppliers can unwittingly introduce vulnerabilities to your organisation, so regular audits are a must to ensure they're doing their part.

Some of the things you should be auditing include emerging supply chain risks through regular audits to help identify any potential vulnerabilities coming from third-party suppliers, whether it's outdated software or lax security protocols. You should also be assessing contract compliance through your audits. You want to make sure suppliers are living up to the cybersecurity terms they agreed to in their contracts so that you inherit the minimum levels of unknown, unquantified risk.

Audits can be a chance to get everyone on the same page, helping suppliers understand what's expected of them and how to align with your standards.

Recording Non-Conformances

Keeping meticulous records of any non-conformances—that is, instances where something isn't meeting the standard—is key and here's why. Thorough documentation helps track issues and what was done to resolve them. Over time, these records can highlight recurring problems that might need a bigger, more systematic fix. When there's a clear record, it's easier to hold the right people accountable for addressing issues and, when the day comes that a regulator wants to see how an organisation is managing risks, these records show that they are proactive and on top of things.

Feeding Back into Risk Management

All that is great, however simply identifying problems isn't enough. The insights from these audits need to be fed back into your overall risk management strategy. Each time a new issue is identified, it should force the organisation to consider how it changes the fleets overall risk profile.

This constant feedback loop helps keep your cybersecurity framework flexible and responsive to new challenges. The next challenge is prioritising fixes. Knowing which issues are the most serious allows you to tackle them in the right order. If you notice a pattern of similar problems cropping up, it's a sign to implement broader changes to keep them from happening again.

In the end, a strong mix of internal and external audits, along with careful attention to third-party suppliers, forms the lifeblood of a strong cybersecurity framework. By diligently tracking non-conformances and feeding this information back into your risk reviews, you can stay ahead of the curve. This not only strengthens your security setup but also shows regulators and stakeholders that you're serious about keeping things secure and compliant.

Pride Security

Cyber Security Testing & Vulnerability Management

The final piece in our cyber security framework puzzle is the testing of security systems, response processes and hunting for vulnerabilities. This regimen of testing will provide robust insights into how capable the organisation is in identifying, detecting, protecting and responding to incidents on their fleet.

In today's constantly changing cyber landscape, having a solid testing strategy isn't just a good idea—it's essential if you want to keep your railway fleet systems secure and running smoothly. Regular, thorough testing lets you catch potential weaknesses before anyone else does, makes sure your existing defences are holding up, and gets your team ready to handle any security threats that come your way.

Penetration testing, or "pen testing" as it's often called, is about taking the offensive role of a hacker and trying to find weaknesses in your systems, networks, and applications. When it comes to railways, this type of testing is a must. It helps spot holes in both the digital controls and the physical systems that keep trains operating safely.

You can uncover new vulnerabilities that might have been accidentally introduced through software updates or recent system changes.
Plus, it's a great way to see if your fleet can withstand some of the latest attack methods used by hackers today.
The ideal setup? Pen testing should be done at least once a year, or every time you make a significant change to your systems.

Physical Security Testing: Protecting the Perimeter
It's easy to focus on digital security, but if someone can get their hands on your physical equipment, all your cybersecurity might not matter. That's why it's important to test the physical security of your fleet's systems, which means:

Checking how secure your maintenance facilities are, since that's where someone could access your fleet's systems directly.
Testing access controls for onboard equipment and sensitive areas.
Making sure things like wireless access points aren't easy entry points for an attacker.
In short, these tests make sure that even if someone tried to get into your critical systems physically, they'd hit a wall.

Incident Response Testing: Being Ready for the Worst
No security system is 100% foolproof. That's why it's crucial to practice what happens if things go wrong. Incident response testing is all about running through simulated attack scenarios to see how prepared your team is to respond. This kind of testing involves:

Playing out different types of cyber-attacks and watching how your team handles them.
Checking how well your communication channels work when everyone's scrambling to respond.
Assessing whether your team can contain the damage and get back on track quickly.
Regular practice drills like these help everyone know their roles and iron out any issues before a real crisis hits.

On top of internal testing, it's a good idea to bring in an outside party to make sure you're meeting industry standards. This type of external compliance testing focuses on verifying that you're following regulations like IEC 62443 for industrial control systems and making sure your data practices comply with laws like GDPR. Having an independent group take a look gives you an unbiased view of where you stand and can reveal areas your internal team might have missed.

Putting a strong testing plan in place comes with a ton of benefits. Regular testing means you're identifying and fixing weaknesses before an attacker can take advantage of them. Every test teaches you something new, helping you fine-tune your defences. It's a solid way to show that you're complying with all the industry rules and standards.

Knowing that you've put your systems through the wringer builds confidence among passengers, regulators, and partners. It demonstrates your continuous commitment to maintaining high standards of security, safety and compliance.

In the end, having a strong testing strategy is more than just a box to tick—it's a necessity for keeping today's railway systems safe and reliable. In taking the time to run regular tests that push your defences to the limit, you're not only protecting your fleet but also making sure you're ready for whatever cyber threats come your way.

Conclusion

This manual has covered a lot of ground, and there is no doubt that there will be some information overload. It is important to remember this is only a high level guide to a rolling stock cyber security framework and it by no means touches on every facet that would be required in all organisations.

When the time comes to implement a similar policy in their own organisation, readers would do well to take their time, revisit topics multiple times and understand in detail what is required of them and how the principles of this document can be best applied to their organisation.

Putting together a solid Fleet Cyber Security Framework isn't just a nice-to-have anymore—it's something that every railway operator must take seriously these days.

With modern rail systems becoming more and more connected, even small weaknesses can lead to big problems, both for safety and keeping things running smoothly. This guide laid out the key pieces needed to build a strong defence, like setting up clear policies and making risk management and testing part of your everyday routine.

But there's more to it than just locking down the tech. It's about taking a systematic approach to wholistic security. An organisation should be looking out for the people who count on these systems every single day.

By weaving cybersecurity into existing safety protocols, staying one step ahead of digital threats, and training their staff to respond effectively to them, railway undertakings can handle whatever new risks pop up. This approach helps organisations meet all the necessary regulatory obligations, demonstrating to passengers, regulators and stakeholders that safety is front and foremost, with sufficient due diligence being applied.

At its core, the framework we outline in this manual is about creating a resilient system—a setup where safety, reliability, and security are all working together. That means building a culture where everyone, from the top executives to the folks on the ground, understands the importance of cybersecurity. And it's not just about what's happening inside your own organization. It's also about making sure that third-party suppliers and maintenance crews are on the same page because their security practices can impact yours, too.

Of course, rolling out these strategies isn't going to happen overnight. It's a long-term commitment that requires investment in training, technology, and a mindset that's always ready to adapt. The railway industry is standing at the precipice between traditional ways of working, and cutting-edge technology, and building a security-first mindset is the only way to keep moving forward.

References

[1] https://www.npsa.gov.uk/system/files/documents/rail-code-practice-security-informed-safety.pdf

[2] https://www.razorsecure.com/post/nis-regulation-rail-cyber-security

[3] https://www.dnv.com/cybersecurity/services/cyber-security-testing-and-verification/

[4] https://www.rock.co.uk/insights/cyber-security-risk-assessment-guide/

[5] https://hyperproof.io/resource/cybersecurity-risk-management-process/

[6] https://www.mdpi.com/1424-8220/23/10/4979?type=check_update&version=2

[7] https://www.sae.org/publications/technical-papers/content/2017-01-1655/

[8] https://www.aqmd.gov/docs/default-source/Agendas/gov/2012/engineering_change_forms_0-2.pdf