PROTECT

Case Study

# : Northern

## Implementing first class cybersecurity in the rail sector

_enabling a trusted future

# At a glance

| | |
|---|---|
| **Customer** | Northern Trains Ltd (Northern) |
| **Industry** | Transportation & Smart Mobility |
| **Key Challenges** | • Increasing awareness of cybersecurity risks<br>• Implementing a cybersecurity strategy |
| **The solution** | • Vulnerability Assessments<br>• Penetration Testing |
| **Benefits** | • Increased cyber awareness<br>• Detailed understanding of position and vulnerabilities<br>• A proactive and continuous improvement approach |

## Rail operations have evolved significantly in recent years. As a result, cyber security has become a growing source of concern in the rail sector.

Once entirely disconnected, IT and OT are increasingly converging on trains. This carries countless benefits for both passengers and operators, from providing passenger Wi-Fi access, to seat reservations, train management systems, driver advisory systems and real-time fleet tracking. However, these technical advances can introduce new cyber vulnerabilities.

In addition to modern, connected OT infrastructures, train operators must also manage threats from legacy systems, the wider rail supply chain, and commercial off-the-shelf products. That's no easy feat.

## What are the rail sector's key cyber security challenges?

Though rail is part of each country's critical infrastructure, cyber security is a relatively new consideration in the sector. This has several implications. Firstly, **there's an overall lack of cyber maturity**. For aerospace and defence organisations, building cyber security into moving platforms has long been a priority. This simply isn't the case for rail. As highly connected OT is still an emerging phenomenon, there's a low level of maturity throughout the sector, compared to other industries.

Secondly, **budgets are limited**. Unfortunately, it often takes a successful breach for cyber security to become an organisational priority. Since the rail sector hasn't yet suffered a high-profile attack, the threat often doesn't feel as tangible as it does in other sectors. This means cyber security budgets in the sector tend to be limited, with cyber teams treading a tightrope between cost and risk.

The above challenges are further compounded by the fact that the **responsibility for cyber security is often shared** between various sector stakeholders. They typically include rolling stock owners, infrastructure managers, train operators, train manufacturers, government departments and more.

# Northern Trains – cybersecurity transformation delivered right on schedule

## Airbus Protect has a long working relationship with Northern Trains Limited (Northern).

Together with Airbus Protect and its partners, Northern has kickstarted a sector-leading cyber security programme over the last two years. This is how its journey has progressed so far.

### About Northern

Northern is a publicly owned train operator that serves over 500 stations in the North of England.

It operates 380 trains over 3,000 kilometres and runs nearly 2,000 services a day.

Pre-pandemic, Northern moved more people annually than Heathrow Airport (108 to 110 million), with over a quarter of a million passenger journeys taking place daily.

# Where it started

**“It all started in 2015, when David Cameron [former UK prime minister] said all trains should be equipped with Wi-Fi,” says digital trains system manager, Marc Silverwood. “At that stage, we weren’t sure of what we needed to protect, what was critical and what wasn’t.”**

After this, the Northern team equipped its fleet with Wi-Fi, but there was little else in terms of digital systems. It took until 2019, when a new fleet of the latest generation, high-speed CAF trains ordered in 2016 started to be delivered, for the operator to begin rolling out its ‘**digital trains**’ programme in earnest.

The first step was to make the Northern board **aware of potential cyber risks** and convince them that cyber security was worth investing in. Together with Airbus Protect, Northern essentially attacked its own systems, as well as conducting a **vulnerability assessment** and reviewing trains’ IT and OT vulnerabilities, before delivering the findings in a unique risk report.

**“We discussed with Airbus how we could bring threats and risk vectors to life, because the realisation just wasn’t there,” says Silverwood. “The Airbus Protect team helped us to explain threats in a language that our board could understand. They were integral throughout key meetings, presentations and calls. Airbus was able to talk us through exactly what had happened, why it happened, but more importantly, how we fix it.”**

This provided clear and actionable guidance on the steps Northern needed to take to address the most pressing security issues and kickstart its journey to becoming an industry leader.

# Where we are now

Two years later and Northern has powered on to become a leading train operator in terms of cyber maturity. On the technical side, it now has **monitoring systems** in place that provide visibility into the type and quantity of attacks. Silverwood and his team can now spot patterns and trends, such as which routes and locations generate the most cyber activity, and how threats tend to manifest themselves.

**"Two years ago, we didn't monitor attacks on trains because we didn't have any controls in place. Now, we check and record everything. Ransomware is a big concern everywhere right now. It affects industrial control systems like trains as much as it does commercial systems, so that's a threat that has increased."**

Aside from the technology, a major change Northern has made over the last two years is implementing **security by design principles** into the key areas it has control over. From an operational perspective, this shift has centred around making physical security improvements to train design.

Changes have ranged from the simple – like adding new secure key locks in places where they never used to be, or removing publicly accessible network ports – to the complicated, such as redesigning trains so key pieces of kit, such as network switches, are much harder to access. Whatever the physical change, the goal is always the same – to make it as difficult as possible for hackers to access potential entry points. And, as Silverwood explains, it's been a case of making **incremental improvements** as part of a wider mindset shift.

**"Even on newer trains, there wasn't really a focus on physical security. You could simply walk into a toilet, lift up the mirror and there's a network port access point. So, we now hide these things. These days, it would be hard for someone to access the network switch – because it's ten foot in the air and behind a panel that requires four people to remove."**

**"On most of our trains you've now got to unbolt seats to get things out. These little things, even if it's just a new lock, all add together and put more and more potential hackers off. We've purposefully made it really inconvenient for them. The whole design culture from a physical aspect has changed quite dramatically."**

And the journey has been a valuable **collaborative experience** for both parties. Airbus Protect and Northern have been able to share learnings, guide each other through new processes and exchange ideas drawn from different industries.

**"It's very much a mutual learning process and obviously the relationship is very strong. We've gone from the steam age to the modern age within two years. It's been a dramatic change, but our cyber security journey is still evolving," adds Silverwood.**

# What’s next?

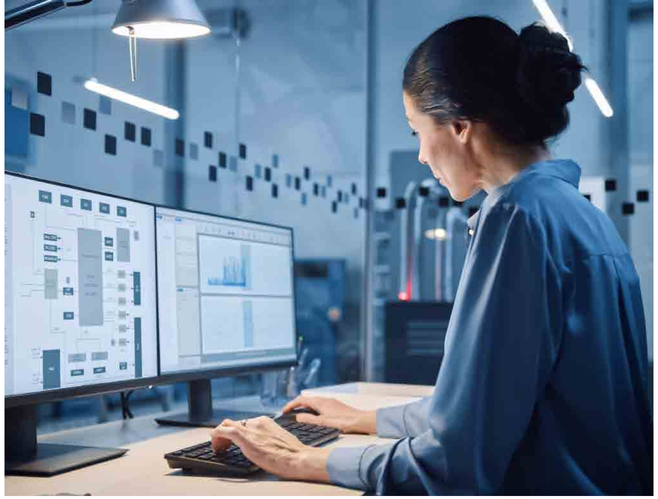
Northern has come a long way in the last few years, establishing itself as a sector leader in OT security. However, it’s not ready to stand still. The operator how has a five-to-ten-year cyber plan in place, involving further testing to gauge the effectiveness of new and existing measures.

But it’s not just about technology. As well as ensuring the right systems are in place, a core focus will be on driving a culture of cyber security across the organisation.

From implementing simple security practices – whether that’s never sharing passwords or using a VPN on public Wi-Fi networks – to fostering awareness of new regulations, one of Silverwood’s key priorities will be to establish a culture that puts cyber security at the core of all operational and engineering decisions. This will ensure that people are more in-tune with the various risks involved.

**“Awareness is still a big challenge. We need to keep driving awareness, so that people know the reasons behind all of this,” he explains. “The cultural element is massive. The more we can get the message out there that cyber is a very real threat, the more we can change people’s mindsets and help them understand what cyber means to them.”**

# Key takeaways



Ultimately, ensuring cyber security in the rail sector is still very much a work in progress – both for Northern and the sector as a whole.

**“When it comes to IT/OT cyber security, there’s a lot of realisations yet to happen in the wider rail industry. It’s something that still has to be learned by a lot of train companies, so convincing the people with the chequebook that this is a risk that should be addressed is still a challenge.”**

Rail operators must be prepared to take a proactive approach to cyber security. Continuously staying one step ahead of attackers is impossible, so the focus should be on response and recovery. That way, when the inevitable happens, there will be a system in place to address it.

**Rail operators that prepare themselves for all eventualities, implementing both the right technologies and selecting the right partner to guide them on their journey, will be the ones best placed to tackle the cyber threats of today and tomorrow.**

Bringing together outstanding expertise in safety, cybersecurity and sustainability; Airbus Protect is a European leader in risk management.

## Our cybersecurity offerings mentioned in this case study

### Consulting Services

Protect your organisation by improving your corporate governance and security posture with our expert IT/OT consulting services.

### Vulnerability Assessments

Reveal your organisations true cyber maturity by uncovering hidden vulnerabilities and understanding potential system exploits.

### Vulnerability Management

Our expert teams provide passive and active remote scanning capabilities. We combine Airbus Protect's decades of cyber experience with industry standard methodology to prioritise vulnerabilities and build effective remediation plans.

**Contact Us**

protect@airbus.com

## Discover more case studies on our website

www.protect.airbus.com

AIRBUS

**Airbus Protect, 31700 Blagnac, France**

**www.protect.airbus.com**