FoxGuard Solutions®

Railway Cybersecurity

The Pressing Need and Where to Start

Your computer has been encrypted!

The hard disks of your computer have been encrypted with a military grade encryption algorythm. It's impossible to recover your data without a special key. You should immediately purchase this key and decifer all your data.

Your data will be erased in:

06 days 08:51:43

As the rail industry continues to embrace new digital technologies, it is also exposing itself to the security risks that come along with operating in such an environment, writes George Ifebuzo, Sales Director at FoxGuard Solutions, a wholly owned subsidiary of Framatome.

When we travel, we're focused on getting to our destination safely and on time. The average passenger doesn't give much thought to cybersecurity when they jump on a train; however, it has more of an impact on their daily journey than they realise.

As a passenger, it is easy to overlook the risks associated with modern conveniences provided by digital technology. Tickets can be purchased online before arrival, eliminating the need to stand in line. Apps provide real-time tracking of schedules, automatically notifying passengers of delays and preventing long waits at stations. But as the rail industry continues to embrace new digital technologies, it also exposes itself to the security risks that come along with operating in such an environment. Cyberattacks designed to disrupt travel, gain access to protected data, or encrypt files to hold as ransom, have now become a very real threat. Protecting the rail industry's IT/OT infrastructure is now more important than ever.

In recent years, a number of cyberattacks on transport networks have made headlines, including **Anonymous' 2018 attack on San Francisco's Bay Area Rapid Transit (BART) network website**, where hackers stole and published the contact details of over 2,000 BART customers.

We've also seen the **SamSam ransomware shut down back-end operations at the Colorado Department of Transport (CDOT) for a full month**, at a cost of 1.5 million USD to the department. Later the same year **Southeastern Pennsylvania Transportation Authority (SEPTA)** suffered a malware attack compromising real-time travel information, payroll and company email systems. This resulted in months of recovery efforts for SEPTA and a year's worth of free credit monitoring for employees.

While these examples all come from the United States, the rest of the world isn't immune. A global **trojan attack took control of Deutsche Bahn's (DB) passenger information** screens, replacing train schedules with ransom requests demanding 300 bitcoin.

Money, however, is not the only reason hackers would want to target railways. Political motivators were behind the Belarus Railway hack earlier this year when a group called Cyberpartisans encrypted servers and databases to disrupt operations in hopes of preventing the advancement of Russian troops into Ukraine. This attack temporarily prevented **Belarusian Railways from issuing electronic travel documents**.

Cybersecurity Standards and Regulations

As cybercriminals focus more on the rail industry, new regulations are being introduced that require the implementation of a more robust and proactive defensive strategy. Regulatory guidance and industry standards provide valuable frameworks that can help an organisation design, develop, implement and monitor an effective cyber programme.

In the European Union, these include TS 50701 and IEC 62443, which the United States' Transportation Security Administration (TSA) used as a blueprint when developing its own regulations last year.

Standards and regulations are a good starting point for the development of strategy and provide an organisation with useful guidelines for creating their cybersecurity roadmap. While companies must remain compliant with industry regulations, the cybersecurity mission doesn't stop when the audit box is checked. Compliance doesn't necessarily equal security; there is much more that can and should be done.

Develop and Sustain a Culture of Cybersecurity

Cybersecurity should not be something done in addition to your daily job. It should be engrained in how the job is done, which requires a culture of cybersecurity to be developed within an organisation. It's a team sport, and everyone has their role to play, but for this change in culture to set in there must be buy-in from leadership. A good cybersecurity culture starts at the top.

Executive boards need to instil a sense of urgency, prioritise budgets and make time for cybersecurity projects and reviews. While important to the success of the programme, these are only the first steps.

For a well-rounded cybersecurity culture to exist, companies should not only focus on the technical element of cybersecurity but must focus on the human element as well. A strong human firewall is the first line of defence against cyber attacks.

We would like to believe that hacking is a complex elaborate game, but the truth is that most breaches occur because of human error due to a lack of cybersecurity awareness. Ensuring employees are properly trained to identify risks and how to prevent them, along with reinforcing best practices and securing behaviours, creates a security-first mindset, which is a key element in creating a secure environment. When it comes to cybersecurity, prevention is key.

Hackers will exploit even the smallest weaknesses; a robust, well-rounded security programme is a must.

Where to Start?

With a variety of infrastructure and assets in multiple locations spread across a vast area, ensuring cybersecurity can be highly challenging for transport networks.

The first question I always ask customers is, what's critical to your organisation, because the first step in developing a security strategy is knowing what needs to be protected.

With that information in hand, a cybersecurity vulnerability assessment is performed to understand the overall attack surface, and threat vectors that pose the greatest risk to the environment. This assessment, followed by a comprehensive review of company policy and procedures, helps establish a baseline of an organisation's overall security posture.

From the baseline, a gap analysis is created that outlines the difference between where you are currently, and where you need to be to align with industry regulations and standards.

Once you have a clear picture of what assets are at risk, a cyber risk mitigation strategy is created to address immediate needs, along with a cybersecurity roadmap to guide your company towards a more secure future.

Expert Support for Your Cybersecurity Journey

Taking the first step in cybersecurity can be overwhelming but having the right partner to support you can make all the difference.

FoxGuard has been providing cybersecurity solutions and supporting critical infrastructure for over 40 years. Together with Framatome, our parent company, who has extensive experience in cybersecurity across nuclear and non-nuclear industries, we have teams of experts across both Europe and the United States to help assess your cybersecurity posture and mitigate any weakness you may have.

The reality is, cybersecurity is not a destination, it's a journey where the road is constantly changing. New vulnerabilities create new threats, technology evolves, environments change and we must evolve and change with them. The moment we believe we are secure and become complacent, we open the door to additional risk. FoxGuard can help you break down and prioritise the steps needed to develop and maintain your cybersecurity programme and provide expert support along the way.

Check out **foxguardsolutions.com/transportation-rail/** to find out more.

George Ifebuzo

Director of Sales

gifebuzo@foxguardsolutions.com

+1 704 330 3521