Ensuring the Security of Transport is Not Just a Priority; it's an Imperative.

In an interconnected world where digital innovation propels the future of transport, robot security measures will guarantee the foundation for safeguarding public safety, maintaining critical services for the public, and upholding the resilience of many other infrastructures.

The Transport Sector

The transport sector encompasses a wide array of modes of transportation. Modern civilisation relies heavily on road and aviation transport for passenger and freight movements. Many countries have well-developed railway networks that provide high-speed rail services and regional train routes. Maritime is another mode of transport that leverages seaports to facilitate trade and transportation, including container shipping. The transport sector ultimately serves as the lifeblood of modern societies, ensuring the seamless movement of key assets (people and goods).

Securing organisations from all avenues within the transportation sector involves addressing a multitude of challenges specific to each mode of transport while also considering the overarching need for resilience against cyber threats that are common to the sector as a whole.

Security Challenges in Transport

There are many challenges that exist pertaining to the transport sector. Congestion is a common one, particularly in major cities. Another challenge relates to investments in infrastructure, which aim to enhance connectivity, reliability, and safety across various modes of transport. One such example is smart transport, where technologies such as smart ticketing systems and real-time tracking can contribute to these benefits.

In the UK alone, transport is one of 13 critical national infrastructure sectors, which is vital to ensure the normal functioning of the entire country. As transportation becomes more interconnected and reliant on digital infrastructure and technologies, the need for robust cybersecurity measures becomes paramount to safeguard operations, protect passenger safety and defend the overall resilience of the sector to mitigate disruptions to critical services.

In 2018, British Airways suffered a large data breach of personal and financial information for hundreds of thousands of customers, resulting in a large financial penalty. It is one real-world example of where poor decision-making around sensitive information can have an impact on people's lives.

In 2022, the transport sector observed a 25% increase in monthly cyber incidents affecting the sector compared to the previous year. With an ever-growing threat landscape that constantly increases in both complexity and scale, there is no doubt activity will rise further.

Transport and IoT

The Internet of Things (IoT) essentially involves devices that are connected/networked.

While many different use cases exist for IoT devices in the transport sector, one key reason is cost efficiency. For example, railway systems leverage vibration and temperature sensors to aid in predictive maintenance of monitoring carriage fleet diagnostics and rapid notification of safety hazards.

However, the rapid integration of IoT devices in the transport sector raises security concerns. Manufacturers of IoT devices tend to prioritise functionality over security, using unsecured or non-standard communication and encryption protocols or default passwords that are very easy to crack, increasing the risk of IoT-based vulnerabilities that can impact transport safety.

Asset Management

It is tricky to manage a large collection of assets in many cases. However, the complex ecology of transport technology ecosystems makes this more difficult.

For example, the average airport may employ hundreds of networking devices, such as firewalls and switches running bespoke applications. Furthermore, the hardware and software embedded into the complex supply chains that transport services rely on typically come from a diverse set of manufacturers and suppliers. Tracking the location and status of all software and hardware assets is no small task, with one vulnerability in a single asset that is unpatched potentially able to cause a cascading effect that can lead to a significant data breach or operational safety hazard.

Strategies for Improving Operational Resilience and Security Posture in the Transport Sector

From air to road to maritime, there are some bespoke differences in terms of strategic placement of technologies to protect operational resilience and, ultimately, the safety of the transport sector and its entities.

Sapphire's suite of security solutions can help companies in the transport sector thrive in modern, digital ecosystems.

Network Segmentation

In the transport sector, we can observe an increase in IT/OT convergence and partitioning critical networks into segments and zones can help contain disruptive attacks in specific areas. This can harden the most critical operational systems against attackers who try to cross boundaries from IT into OT, protecting operational safety. Sapphire's consultants, who specialise in both IT and OT, can help guide you in protecting your networks and ensuring your transport architecture remains resilient and robust to attacks while ensuring your operations remain efficient.

Security Awareness Training

Implementing cybersecurity awareness and training programs for all employees, including non-technical staff, can help address common pitfalls in security knowledge. Sapphire can help tailor training programs to create a safety-first culture, reduce risks from low-hanging fruit attacks and ensure everyone knows the role they play in protecting the organisation against cyber-attacks.

Security Testing and Assessment

The complexity of transport technology environments makes penetration testing and vulnerability assessments a necessary tool to implement. These tests look for exploitable vulnerabilities in your networks, protocols, devices,

and applications and provide knowledge of where the weak spots are and how they can be remedied.

Sapphire's certified penetration tests and vulnerability analysis can provide visibility into the current threat posed to your risk and security management systems. Benefit from access to Sapphire's streamlined reporting, collaboration, and management portal for all testing activities end-to-end.

Securing Operational Technology (OT)

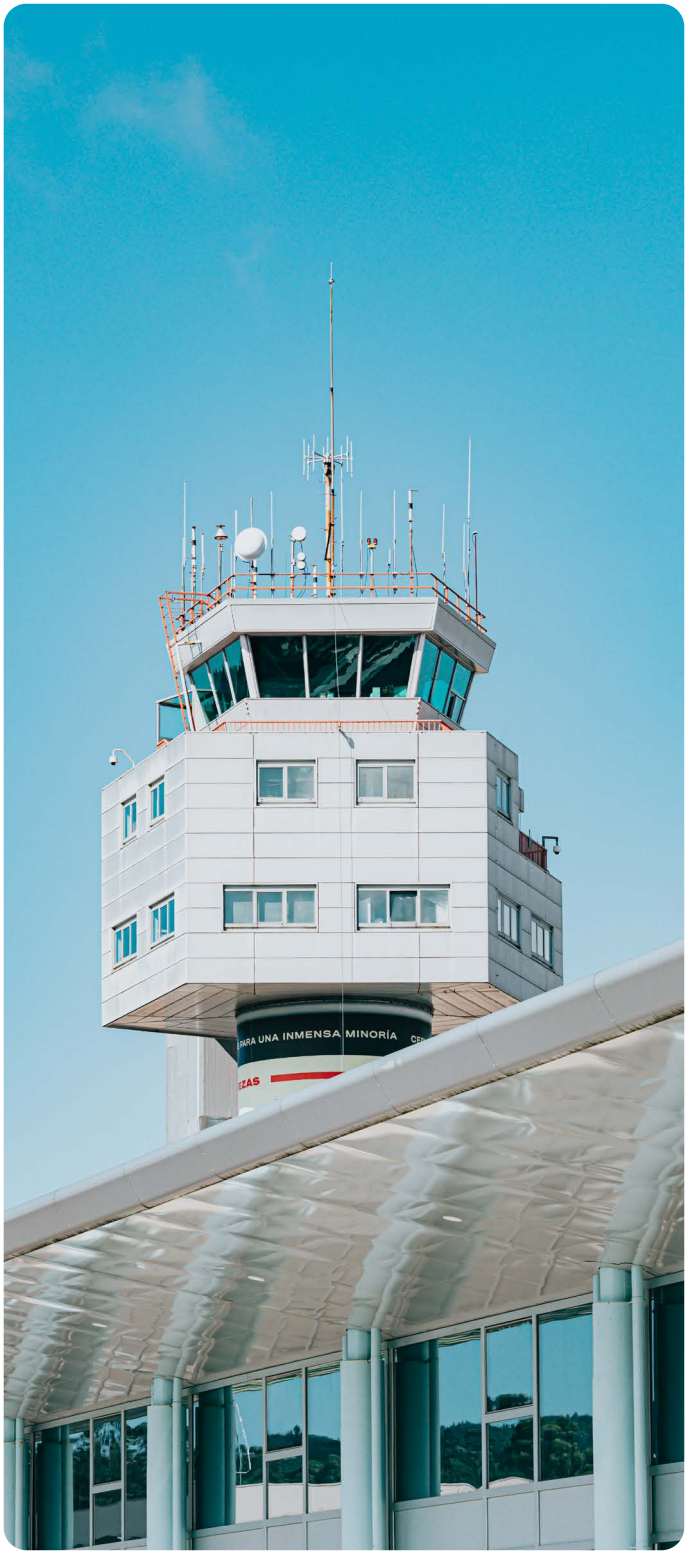
Not all attacks target your computer systems, but attacks may directly target your physical transport infrastructure, which can quickly damage your critical services and further impact the entire sector.

Sapphire's OT capabilities can help you identify all your assets relating to critical physical infrastructure and identify potential weaknesses that can be remedied to ensure your physical infrastructure and systems are secured.

Asset and Patch Management

It is important that all assets in your environment are identifiable, categorised and managed. OT assets typically include a wide assortment of devices and systems, such as programmable logic controllers (PLCs), human-machine interfaces (HMIs), actuators, sensors, and other hardware and software that control and monitor your critical operational processes.

Sapphire's OT solutions can help you actively seek and identify devices in your OT environments and profile them so you can learn more about each of them. Creating a detailed inventory of your environments and continuously monitoring your critical assets is important.



To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

Sapphire's Service Offering

Service /Offering	Introductory	Foundations	Intermediate	Advanced
NCSC Guidelines	✓	✓	✓	✓
Standards Compliance Review	✓	✓	✓	✓
Gap Analysis	✓	✓	✓	✓
Security Improvement Planning	✓	✓	✓	✓
Security Awareness & Training	✓	✓	✓	✓
Procedure & Policy Review	✓	✓	✓	✓
Network Configuration Review	✓	✓	✓	✓
Firewall Security Checkup	✓	✓	✓	✓
Framework Review (CyberEssentials, GovAssure)		✓	✓	✓
Information Security Management		✓	✓	✓
Authentication Review		✓	✓	✓
Business Continuity Planning		✓	✓	✓
Disaster Recovery Planning		✓	✓	✓
Incident Response Planning		✓	✓	✓
IT/OT Asset Discovery		✓	✓	✓
Identity & Access Management Review		✓	✓	✓
Threat Assessment		✓	✓	✓
Penetration Testing		✓	✓	✓
Internal/External Audit		✓	✓	✓
Threat Intelligence			✓	✓
Vulnerability Management			✓	✓
Third-Party Risk Management			✓	✓
IT/OT Consultancy			✓	✓
MXDR & Endpoint Management				✓
CISO as a Service				✓
Red Teaming				✓
Breach Attack Simulation (BAS)				✓
SIEM & SOC Advisory Services				✓

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001