# CYBER RISK IN THE TRANSPORTATION INDUSTRY

## BE PREPARED

As transport operators digitalise their operational technology, the risk of a cyber-attack is elevated, and new architecture should be controlled and protected.

Transport networks have become increasingly digitalised, with a wide range of data flowing across systems, tracking and monitoring both digital and physical networks. As more devices and control systems are connected online, more vulnerabilities will appear, increasing the potential for disruption to physical assets.

No enterprise is completely immune to cyber-attacks, but a comprehensive proactive strategy can eliminate many threats.

These following solutions reduce the likelihood of disruptions resulting from cyber-attacks:

- Implementing a security best practice
- Establishing an effective risk governance structure in-line with other risk types and maintain board engagement
- Establishing a process to better understand the threats and risks to the organisation and enable the setting of risk appetite for cyber exposures.
- Establish incident-response capability with tested incident response plans to ensure that the impact of any cyber-attack is minimised.

## KEY CYBER RISKS

- Physical asset damage and associated loss of use.
- Unavailability of IT systems and networks.
- Loss or deletion of data.
- Data corruption or loss of data integrity.
- Data breach leading to the compromise of third-party confidential information, including personal data.
- Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information.
- Extortion demands to cease a cyber-attack.
- Direct financial loss as a result of theft.
- Damage to reputation

**SOLUTIONS...**
**DEFINED, DESIGNED & DELIVERED**

ISO SYSTEMS UK
Intelligent Management Systems
Practical • Simple • Flexible

www.isosystems.org.uk

# CYBER RISK – A PERVASIVE & GLOBAL RISK

*As cyber technology becomes more sophisticated, the threat from attack is moving from data breaches to interrupting physical critical infrastructure, exposing transport operators to economic and reputational damage.*

The sophistication and frequency of cyber-attacks is on the rise and the risk to business in the UK and globally is growing. A total of 81% of large businesses and 60% of small businesses suffered a cyber security breach in the past year, and the average cost of breaches to business has nearly doubled since 2013. £600,000 –£1.15million is the averaged cost to a large organisation, average cost up from £450 - £850 a year ago.

The growth of the internet has driven the rapid development of cyber-crime. Put into context, in less than 15 years, the number of global web users has increased from 16 million in 1995 to more than 1.7 billion today. By 2015, there were more interconnected devices on the planet than human beings.

Awareness of the threat and the potential repercussions has reached the boardroom, with cyber risk and risk to critical infrastructure featuring in the top five concerns in the World Economic Forum's *Global Risks* report.

Shareholders and customers therefore possess an expectation that organisations will have undertaken a thorough evaluation of cyber risks that may impact the business.

The damage that cyber events can pose to a company's profits, reputation, brand, competitive position, and even operational ability is potentially vast; however, many companies remain underprepared. Companies must understand the risks they face and put into place robust systems to limit the impact on the business.

**116** TARGETED GLOBAL ATTACKS PER DAY[1]

**40%** OF ALL DATA BREACHES ARE CAUSED BY HACKERS[1]

ISO SYSTEMS UK
Intelligent Management Systems
Practical • Simple • Flexible

www.isosystems.org.uk

# WHY IS THE TRANSPORT SECTOR PARTICULARLY VULNERABLE?

Transport networks have become increasingly digital, with a wide range of data flowing across systems, racking, and monitoring both digital and physical networks. As more devices and control systems are connected online, more vulnerabilities will appear, increasing the potential for disruption to physical assets.

Advances in electronic platforms and communications introduced across electronic and physical networks have meant that the potential to detect becomes a challenge, and the potential to disrupt a serious concern. Electronic data can now:

- Track the location, status, and condition of physical assets and associated infrastructure.
- Monitor emerging weather-related risks, landslides, ash clouds, and other extreme weather.

Companies that have interconnected data systems flowing throughout the value chain are particularly vulnerable. Rail infrastructure owners and operators, airlines and airport infrastructure, logistics operators, and automotive suppliers all face the possibility of a cyber-attack interrupting physical networks and causing significant disruption.

## THE INDUSTRY VIEW

In the aviation industry, technical advances in navigation systems and airframe design have reduced the chances of an accident; however, the increasing reliance on computers poses a different kind of threat.

As aircraft move ever closer to becoming fully e-enabled and automation increases, pilot practices and training will need to adapt in the event of system failure or security breach.

In July 2013, passport control systems at the departure terminals at Istanbul Atatürk and Sabiha Gökçen airports were interrupted by a cyber-attack. Passengers were delayed at the point of entry and exit and flights were delayed for many hours.

In light of the more sophisticated risk, the International Air Transport Association recognises the potential threat and has been working to improve cyber security, recently launching a toolkit to help airlines assess and mitigate risks in their information technology (IT) systems.

In the logistics industry, cyber security is more crucial to resilience and safety than to the protection of customer data. The vast quantities of data exchanged across networks to transport goods in a supply chain leave the sector particularly vulnerable.

The more frequent use of goods tracking systems and real-time control applications with web interfaces also opens up a growing number of weak points to be managed across a large supplier base.

The rail industry also relies heavily on IT and automation. These systems:

- Control train movement.
- Deliver power to the network.
- Control signalling infrastructure.
- Report on the condition of the rolling stock and associated infrastructure.
- Support operational planning and timetabling.

As a provider of critical national infrastructure, the rail industry – in the same way as the airline industry – may be targeted by political groups intent on causing disruption, in addition to amateur hackers, organised criminals, and/or disgruntled employees.

As the rail industry adapts and becomes increasingly dependent on electronic sensors and network technologies, new vulnerabilities to physical networks are presenting themselves.

This was seen in a case in Lodz, Poland, where a 14-year-old modified a TV remote control so that it could be used to change track points. The teenager broke into a number of tram depots to gather the information needed to build the device, which turned the tram system in Lodz into his own personal train set. As a result, four vehicles were derailed injuring twelve people.

# THE THREAT ENVIRONMENT

The cost of cyber-crime can be vast, potentially inflicting damage to a company's profits, reputation and brand, and operational effectiveness. Understanding the types of threat is critical to mitigating the risk.

## CRIMINAL

Hacking has become a mainstream activity for organised criminals, who target the digital assets of an organisation that can be acquired or sold on, including:

- Personal information.
- Credit/debit card information.
- Held funds.
- Intellectual property.

## HACKTIVIST

Hacktivist groups represent a formidable foe due to the technical capability of the individuals involved, and can target organisations for a variety of reasons. Effects may be as a result of:

- Public support for a cause.
- The direct impact of core activity.
- Being a top corporate brand target.

## STATE

Nation states represent the most sophisticated and technically capable threat and those operating critical infrastructure or holding intellectual property that would benefit a key foreign national industry may be natural targets. Nation states purpose includes:

- Offensive capability.
- Espionage.
- The acquisition of trade secrets and other intellectual property.

## KEEPING PACE WITH ADVANCES IN TECHNOLOGY

As operational technology evolves, critical infrastructure operators will need to ensure that new architecture should not be deployed until it can be controlled and protected. As companies develop and modernise, they will be at risk of cyber attack[10]. Exercises such as upgrading existing legacy systems may result in sacrificing security.

## TERRORIST OR STATE

The ability to create physical outcomes through the remote hacking of critical infrastructure represents an appealing option for terrorist groups, and can result in:

- Disruption to critical infrastructure.
- Economic consequences.
- Loss of life.
- Damage to property.

## MALICE

Where technical ability and motive combine, those with ill-feelings towards an organisation are able to act maliciously by electronic means. A malicious cyber event may be as a result of:

- A disgruntled employee/customer.
- Proof of ability.
- Untargeted malicious code.
- Random selection.

## GOVERNMENT SUPPORT

The threat to critical infrastructure is one of the reasons why governments, and especially the UK Government, have acted to alert all commercial companies to the wider risks posed by a large-scale cyber attack. The UK National Security Strategy categorises cyber attacks as a tier-one threat to the country's national security (alongside international terrorism) highlighting the likelihood and impact of potential attacks.

The UK Government supports the growth of the cyber insurance market to improve how UK businesses manage cyber security risk, and believes the insurance industry has a strong role to play in helping firms outside of the critical national infrastructure to manage their cyber risks efficiently.

# MANAGING THE RISK

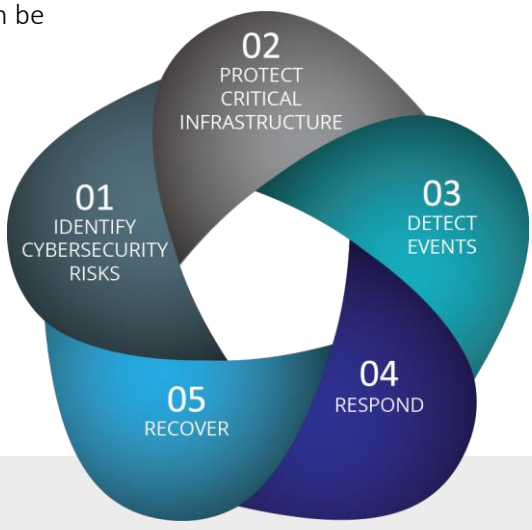
Organisations need to take preventive action to mitigate security risks. It is not just organisations with an internet presence that may have cyber and privacy exposures.

Essentially, any organisation will be exposed to cyber-related threats where they:

- Rely on computer networks and IT to secure sales and process transactions.
- Rely on IT to direct operations and run administrative functions.
- Rely on industrial control systems to automate physical processes.
- Store or process third-party confidential information, including personal data, on computer networks.
- Store and transmit sensitive corporate information that can be accessed over the internet (or intranet) by third parties.

The solution to these threats lies in:

- Implementing security best practice, which is in-line with applicable standards and guidance and continually reviewed and updated.
- Establish an effective risk governance structure in-line with other risk types and maintain board engagement.
- Establish a process to better understand the threats and risks to the organisation and enable the setting of risk appetite for cyber exposures.
- Establish incident-response capability with tested incident response plans to ensure that the impact of any cyber-attack is minimised.




## CONCLUSION

The digitalisation of transport systems connecting virtual and physical networks are increasing the amount of vulnerabilities within these essential systems. Combined with the challenge of upgrading existing legacy systems, it is only a matter of time before we see a significant event occur. No enterprise is completely immune to cyber-attacks, but a comprehensive proactive strategy can eliminate many threats.

ISO 27001

ISO 27701

CYBER ESSENTIALS

## SOLUTIONS...
## DEFINED, DESIGNED & DELIVERED


Scott Naisbett | ISMS Lead Implementer (CIS LI)

## CONTACT

E: scott@isosystems.org
M: 07813858310
W: www.isosystems.org.uk


**Amanda Jackson**
Director at Heritage Healthcare, Healthcare Manager, Home Care Recruitment, Operations Manager, Contracts and Tenders
March 20, 2020, Amanda was a client of Scott's

DCS&D Ltd T/A Heritage Healthcare would highly recommend ISO Systems UK Limited if they are considering implementing an Information Security Management System (ISMS). Their support has been crucial in the development of our ISMS System.

ISO Systems UK Ltd were professional in every way and they demonstrated their expertise and knowledge in all areas relating to our ISMS system and we found Scott Naisbett to be dedicated and hands-on, in tackling all stages of the project with professionalism. The attention to detail and wealth of information that Scott had, were tremendously valuable for us.

We could not have done it without him and would have no hesitation in recommending him to other Businesses.

Thank you for a superb job!

---

**Faye Smillie**
Accounts Manager at CAM-TEC SYSTEMS LTD
February 22, 2020, Faye was a client of Scott's

Scott is very knowledgeable in his field and works to a professionally high standard. A good communicator and a pleasure to deal with.

---

**Stuart Joyce**
Manager at Shildon Civic Hall
February 20, 2020, Stuart was a client of Scott's

Scott is a great guy to work with, very knowledgeable in his field & his attention to detail is second to none.

---

**Paul Thompson**
Director at Creative Audio Visual Ltd Excellence by Experience
June 26, 2019, Paul was a client of Scott's

I was overwhelmed by the work required to become GDPR compliant. There appeared to be so many elements to it and I did not know where to start let alone if it was even applicable to our business, as it turned out - it was! Scott suggested doing a needs analysis first to identify our priorities. His knowledge of GDPR immediately put me at ease and his logical, pragmatic approach made the task manageable. 8 weeks later and we now have a robust Personal Information Management System in place and Scott kindly set us up with a 12-month schedule to ensure it will be kept up to date and with minimal admin! Highly recommended!