Willis Towers Watson

Guide to the NIS Directive for transportation companies

The EU's Network and Information Security Directive (NISD): How should transportation companies respond?

It is predicted that cybercrime will cost the world over $6 trillion annually by 2021, up from $3 trillion in 2015. As transportation companies make rapid technological advances to remain competitive, they are increasingly exposed to costly attacks and network failures.

In response to this growing threat the European Parliament adopted the NISD which is aimed at promoting cross-border cooperation on cyber-security, and improving risk management practices. EU member states have till May 2018 to implement the Directive into national law.

The NISD…

- Applies to providers of **essential services** to customers based in the European Union
- Requires essential service providers to:
  - Introduce appropriate measures to **assess** and **prevent** risks
  - Ensure a level of **security** of network and information systems appropriate to the risks
  - Establish **response** strategies to **handle incidents** and **minimise** their impact
- Establishes Computer Security Incident Response Teams (CSIRTs) in member states
- Requires providers of essential services to notify CSIRTs promptly when a **significant** incident occurs. 'Significant' has not been fully defined but the number of affected users, duration of incident and geographic spread should all be considered
- Imposes obligations even when network and information systems are outsourced to third parties
- Allows authorities to demand information on the security of an organisation's network, such as documented security policies
- Gives authorities the power to make an essential service operator undertake a security audit
- Allows each EU member state to determine its own **effective**, **proportionate** and **dissuasive** penalties for infringement
- Has been committed for implementation in the UK, despite Brexit. The UK government recently announced it is considering fines of up to £17 million or 4% of global turnover

Are transportation companies covered by the NISD?

The NISD applies to all organisations that depend on network and information systems to provide services that are "**essential** for the maintenance of critical societal and/or economic activities."

Given their intimate ties to the global economy and ever increasing reliance on technology, many transportation companies will likely be defined as essential service providers across all EU states.

Where organisations provide both essential and non-essential services – such as **airports** who manage runways (essential) and retail (non-essential) – the security requirements will only apply to the essential service.

NISD definition of transport providers

- Air carriers (freight and passenger air transport)
- Maritime carriers (sea and coastal passenger water transport companies and sea and coastal freight water transport companies)
- Railways (infrastructure managers, integrated companies and railway transport operators)
- Airports
- Ports
- Traffic management control operators
- Auxiliary logistics services (warehousing and storage, cargo handling and other transportation support activities)

NISD, Annex 2

Is there overlap with the GDPR?

The EU's General Data Protection Regulation will also come into force in May 2018. While both pieces of legislation aim to strengthen cybersecurity, they deal with different subject matter.

Whereas the GDPR is concerned solely with personal data, the NISD covers any cyber incident that has a significant impact on the provision of services. However, it is possible that both personal data breaches and network disruptions will occur at the same time.

What are the issues for transportation companies?

Assess and prevent risks

Employees are your first line of defence against cyber risk; however they are also part of the risk. Employee negligence and malicious acts — including lost laptops, the accidental disclosure of information and actions of rogue employees — cause two-thirds of cyber breaches.

Transportation companies will need to measure the risks inherent in their employees' behaviours and determine how to lessen this risk and build a cyber smart workforce.

Ensuring security of systems

Due to the global nature of their physical and digital supply chains, transportation companies are often reliant on external networks and third parties. Cyber risks multiply for each partner taken on, for every alliance struck and for each link in the digital supply chain. Security measures must therefore be synchronised across this entire network.

Implementing robust security systems will require skilled workers, however nearly every EU member state is facing a shortage of IT and technology professionals. Transportation companies will have to identify emerging skills gaps and recruit key talent to build, lead and engage a cyber smart workforce. However competition will be stiff and not limited to transportation industry peers.

Handling incidents

As with security measures, transportation companies should ensure that business continuity plans are prepared for multiple network disruptions across the supply chain. Organisations that have a clearly defined recovery strategy are much more likely to overcome the initial crisis period and restore sustainable long-term operations.

Mandatory reporting of incidents will make it easier for traditional and social media channels to publicise perceived failings. Therefore companies must also be prepared to face the stark glare of media and customer scrutiny following an incident.

Opportunities of the NISD

While it may be easy to think of the NISD as yet another compliance burden, it should be viewed as a means by which to bring your organisation up to speed with the modern digital world. To harness NISD for business advantage:

- **Create a cyber resilient culture** so your employees feel prepared for future incidents
- **Enhance supply chain trust and resilience** by engaging 3rd party suppliers and customers in cybersecurity processes and business continuity measures
- **Approach cyber risk transfer analytically**. Cyber insurance is more than an add-on. It can provide assistance by demonstrating cyber resilience; restoring data, software and system functionality; covering the costs of regulatory investigations; defending third party cybersecurity claims; mitigating reputational damage; as well as covering breach response costs and network business interruption losses.

How Willis Towers Watson can help

For information on how Willis Towers Watson can help you **assess** your cyber risks, ensure **security** across your people and technology, and help you **recover** from cyber incidents please contact a member of our team.

Contacts

Mark Hue Williams
Head of Transportation Industry
+44 (0) 203 124 6123
Mark.Hue-Williams@willistowerswatson.com

Jamie Monck-Mason
Executive Director, Cyber & TMT
+44 (0) 203 124 7240
Jamie.Monck-Mason@willistowerswatson.com