Willis Towers Watson

The EU's Network and Information Security Directive (NISD)

How should the Energy and Natural Resources industry respond?

What is NISD, and how is it different to the General Data Protection Regulation (GDPR)?

European institutions and companies are increasingly targets of organised and sophisticated cyber-attacks, and it is estimated that these breaches result in losses of €260b – €340b annually[1].

In response, in July 2016 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 their national law.

The NISD…

- Applies to companies that provide 'essential' services to customers based in the European Union (EU)
- Establishes designated Computer Security Incident Response Teams (CSIRTs) in member states
- Requires operators of essential services to notify CSIRT authorities promptly if a significant incident occurs
- Asks essential service operators to demonstrate that they have:
  - systematically **assessed** security risks associated with their IT infrastructure
  - taken "appropriate and proportionate" measures to **prevent** these risks
  - established **response** strategies to minimise the impact of cyber-incidents to ensure service continuity
- Imposes these 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 set of penalties for infringement
- Has been committed for implementation in the UK by the current government, despite Brexit

While the NISD is designed to ensure the continuity of essential services for EU-based customers, the GDPR is a separate piece of legislation that aims to safeguard the personal data of EU citizens. They are best viewed as complementary pieces of legislation that will jointly form the bedrock for stronger cybersecurity and data management across the EU.

Why is it relevant to Energy and Natural Resources (ENR) companies?

Research conducted by the World Economic Council indicates that 80% of oil and gas companies saw an increase in the number of successful cyber-attacks in 2015[2]. The NISD recognises that most European ENR companies are likely to have better cyber-preparedness, but is designed to guard against similar outcomes. We believe that different EU states will apply this flexibility differently across the ENR value chain, depending on their unique national energy policy and infrastructure. For instance:

Upstream exploration and production (E&P) operators are likely to be considered essential service providers in EU states where E&P activities contribute significantly to government revenues, such as Norway and the UK.

Midstream pipeline and storage operators might be considered for inclusion under NISD in EU states which rely heavily on petroleum imports, such as Germany.

Electricity generation and transmission operators are likely to be deemed essential service providers across almost all EU states.

[1] http://www.bbc.co.uk/news/technology-35038424
[2] https://www.worldenergy.org/publications/2016/the-road-to-resilience-managing-cyber-risks/

What are the key challenges for ENR companies?

Assess

- ***Assessing*** security risks associated with IT infrastructure:
  - ***People challenges***: Our view is that the greatest challenge to cyber-security comes from within the organisation. Data collected from our insurance claims show that employees, either through negligence or malicious intent, account for two-thirds (66%) of cyber breaches[3]

Prevent

- Taking appropriate and proportionate measures to ***prevent*** these risks:
  - ***Skills shortages***: ENR companies are facing shortages of skilled technical workers - a trend which is expected to continue as staff retire. This means that learnings from past cyber breaches will begin to fade at the same time as the technical know-how to prevent future incidents reduces in supply. As they set priorities for their workforces, ENR companies could ensure that focusing on operations does not come at the expense of incident prevention
  - ***M&A impacts***: The ENR industry is highly deal-driven. The Oil and Gas sector alone saw close to 550 M&A deals worth about $250 billion in the 12 months ending June 2016[4]. Each deal brings with it the challenges of putting together a set of disparate IT systems, processes, strategies and cultures

Response

- Establishing ***response*** strategies to minimise the impact of cyber-incidents and ensuring service continuity:
  - ***Operational interconnectedness***: ENR company operations are deeply interconnected Outages in one part of the chain can rapidly result in a wave of impacts. For ENR companies to devise continuity plans covering just their asset footprints is inadequate. Plans must be Synchronised across a complex interconnected network

What can ENR companies do to strengthen their cyber-preparedness and reduce the risk of NISD non-compliance without impacting value creation in the organisation?

It is entirely likely that an incident causing a service outage will result in a data breach, doubly exposing a company to fines under both NISD and GDPR in addition to the monetary and reputational impact of the incident itself.

That said, while it may be easy to think of the NISD as yet another compliance burden, it should be viewed as an opportunity to revisit risk management practices across the organisation. A few measures that could be considered are:

- **Creating a risk-conscious culture across the organisation**. In our experience, large-scale cultural shift is possible if viewed as a journey rather than a project, starting with senior leadership and working its way down the organisational ranks
- **Thinking about cyber-risk and value together.** We believe a strong cyber-preparedness approach must be accompanied by a strong risk framework - one that does not constrict value-creating thinking at junior levels but elevates the risk profile decision to more senior levels
- **Thinking differently about incentivising risk management behaviours**. Many organisations view risk management as something their staff must do in the base case to perform their roles. In our view, there is merit in viewing a demonstrable commitment to good risk management as a behaviour that marks staff out as going over and above performance expectations, which could be reflected in their incentive programmes
- **Approaching cyber-risk transfer analytically, as an integral part of the overall insurance strategy.** Cyber-risk insurance has typically been bought as a standalone policy, or as an add-on to an existing insurance portfolio. We think the time is now right for ENR companies to assess cyber-risk transfer as a core part of the overall insurance strategy, seeking complementarity and synergies across the insurance portfolio

Contact
Thorsten Querfurt
Global Head of Natural Resources
+44 (0) 203 124 6236
Thorsten.Querfurt@WillisTowersWatson.com

Willis Limited, Registered number: 181116 England and Wales. Registered address: 51 Lime Street, London, EC3M 7DQ.
A Lloyd's Broker. Authorised and regulated by the Financial Conduct Authority

[3] https://www.willistowerswatson.com/en/press/2017/03/when-it-comes-to-cyber-risk-businesses-are-missing-the-human-touch
[4] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/energy-resources/us-energy-and-resources-oil-and-gas-m-n-a-report-2016.pdf