Cyber security remains in the public eye this year with multiple incidents and vulnerabilities reported. Energy companies are developing and updating their cyber security response plans to reflect the increased legal, operational and technical risks they are facing.

The evolution of the threat has not escaped the attention of governments around the world. 2018 will see the implementation of the Network and Information Security Directive (NISD) as well as the General Data Protection Regulation (GDPR) in the EU. The NISD, which is coming into force in May, will require energy companies to ensure that their network and information systems meet minimum standards of cyber security. In the UK, the National Cyber Security Centre (NCSC) has recently issued detailed guidance on the compliance requirements of NISD.

Cyber incidents: an increasing and evolving threat

There has been no let-up in the rate and seriousness of attacks. The energy sector is a particular target, as can be seen from the attack on Saudi Aramco in 2012, which resulted in the company’s systems being offline for 10 days, through to the recently discovered “Trisis” malware. The latter, reportedly created by nation state actors, seeks to disable safety measures built into industrial control systems manufactured by Schneider Electric and was discovered on such systems in a Middle Eastern petrochemical plant. It is believed to be the third publicly known attack on industrial control systems (the first two being the Stuxnet malware affecting nuclear centrifuges in Iran in 2010 and the attacks on the Ukrainian power grid in 2015).

The increasing interconnection of the energy sector is creating additional complexity in cyber security management, particularly through the challenges of managing cyber security risk in the supply chain. The digitisation of the sector including the increase in web-connected devices such as smart grids and smart meters and the growth of ‘internet of things’, whilst providing exciting innovation opportunities and increasing efficiency, is making it both more challenging and more important than ever to confront cyber security. The hack of a
telecommunications company providing smart-meter services to utilities in the Netherlands in 2012 demonstrates that, although the energy sector in the UK may be new to smart meters, hackers are not.

**Legal, regulatory and operational risks**

Businesses are increasingly faced with potential legal liabilities arising from cyber incidents. Liability to third parties can arise where attacks have either been made possible or been made worse, by a business’ negligent IT practices. Liability can arise either through tort law, where there are existing contractual obligations that have not been complied with, or through regulatory enforcement. Where operational security is compromised, there is also the risk of environmental damage, physical damage to property, and personal injury or loss of life.

Regulatory obligations often have a bearing on cyber security, such as the conditions imposed in licences granted by Ofgem in the UK for the transportation and supply of gas.

Under Section 9 of the Gas Act 1986 (applicable in Great Britain), gas transporters are required to develop and maintain an efficient and economical pipe-line system (and under the terms of the licence, gas transporters must have available resources to develop and maintain an efficient, co-ordinated and economical system of gas transportation). There is a similar obligation imposed on interconnector operators, under the terms of the interconnector operator licence. In light of recent cyber incidents and the significant risks posed to gas infrastructure, in order to discharge these absolute obligations energy companies will need to consider whether their cyber security management systems, including management of cyber security risk in their supply chains, are robust enough to detect, prevent and manage cyber security risk to enable the efficient operation of the system in the event of an attack.

In addition, the licences granted by Ofgem for the transportation and supply of gas reflect the interconnection of the gas supply and transportation sector placing obligations on gas shippers, suppliers and interconnector operators to share information with gas transporters for the purpose of enabling the transporter to draw-up plans for the safe, secure and efficient operation and development and maintenance of its pipe-line system. Further, gas shippers and transporters cannot pursue a course of conduct which is likely to prejudice the safe and efficient operation of transporters’ pipeline systems. These provisions require both a detailed consideration as to how different cyber security management systems interact with one another across a supply chain and promote information sharing of cyber security measures. Energy companies will also need to consider whether their actions prior to or during a cyber-attack could have any prejudicial effect on other market participants.

As a result of this, and in order to manage cyber risk more generally, energy sector businesses are updating their cyber incident response plans to reflect the need to consider the legal risks and obligations on the business when a cyber incident occurs as well as the technical issues that arise. They also are investing time and effort up front before incidents occur to speed up their ability to respond on the legal issues when faced with an incident.

Businesses’ IT and operational systems are increasingly integrated with those of other companies within their supply chain. This trend increases the attack surface for would-be hackers. Businesses are including cyber security terms in their contracts with their customers and suppliers to allocate responsibility for dealing with security, ensuring cooperation both before and after the event of an incident, and to ensure the position on liability is clear. We are already seeing cyber security becoming part of the procurement process for suppliers, significant cyber security schedules being included in contractual arrangements, as well as an increasing willingness on the part of customers and suppliers to negotiate such terms.

Businesses are increasingly recognising that merely allocating liability in contract for cyber security incidents is not enough – it is far better to engender the right cyber security behaviours of other parties in the supply chain in order to avoid incidents in the first place.

**New legislation**

Governments around the world are legislating new requirements for minimum standards of cyber security. In the EU, 2018 will see the GDPR and NISD enter into force. The GDPR enters into force on 25 May 2018. It imposes requirements on all companies processing personal data (including employee data) to ensure that the data is protected by adequate technical and organisational measures, taking into account industry best practice and the state of the art, as well as requiring the reporting of incidents within 72 hours.

The increasing interconnection of the energy sector is creating additional complexity in cyber security management, particularly through the challenges of managing cyber security risk in the supply chain.

The threat from cyber criminals, state actors and hacktivists is not going away: energy businesses in particular need to keep ahead of the curve.
The GDPR allows the imposition of significant fines for breaches of these obligations (up to 4% of global turnover).

The NISD is a more targeted piece of legislation, aimed at operators of ‘essential services’, a designation that will capture many energy companies. Electricity generators and transmitters and companies involved in oil and gas production and distribution all fall within the ambit of directive. The directive requires member states to introduce ‘appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems’, as well as reporting obligations when incidents occur. The directive mandates the imposition of ‘effective, proportionate and dissuasive’ sanctions for failure to implement appropriate standards and failure to report incidents – the same language as used in the GDPR.

In the UK the government has undertaken a consultation and draft implementing regulations are expected to be published shortly. The NCSC has issued guidance for operators of essential services that is expected to be adopted by the sectoral regulators when enforcing the requirements. Rather than taking a prescriptive rules-based approach the NCSC has adopted a principles based approach to cyber risk. The guidance requires a focus on four high level objectives, including managing risk, protecting against cyber-attacks, detecting attacks and minimising the impact of incidents. It sets 14 lower level principles to allow operators achieve these objectives. While much of the guidance is drawn from pre-existing industry best practice and existing NSCS advice, operators of essential services will need to ensure and demonstrate that their cyber security practices are compliant by May 2018 or face substantial fines.

The directive involves only a very rudimentary level of harmonisation, unlike the GDPR, so businesses with operations in multiple jurisdictions will inevitably have to become familiar with the differing local implementations. To date only a small number of states have implemented the directive; the initial deadline for implementation is 9 May 2018.

While the GDPR seeks to avoid multiple sanctions being imposed by different member states in respect of the same incident, the NISD could theoretically lead to liability in multiple jurisdictions and even dual liability where a cyber incident affects both an essential service and personal data for the purposes of the GDPR.

Other jurisdictions around the world are introducing similar legislation. Businesses will need to factor these new reporting obligations into their cyber response plans.

What does the future hold?

The 2015 cyber-attack that took down the Ukrainian power grid and the recent attack on a petrochemical plant has brought home how significantly the energy sector is being targeted by hackers. The threat from cyber criminals, state actors and hacktivists is not going away: energy businesses in particular need to keep ahead of the curve.

Businesses are including cyber security terms in their contracts with their customers and suppliers to allocate responsibility for dealing with security, ensuring cooperation both before and after the event of an incident, and to ensure the position on liability is clear.

Key contacts

Andrew Moir  
Partner  
+44 20 7466 2773  
andrew.moir@hsf.com

Silke Goldberg  
Partner  
+44 20 7466 2612  
silke.goldberg@hsf.com

Peter FitzPatrick  
Associate  
+44 20 7466 3711  
peter.fitzpatrick@hsf.com

Businesses are including cyber security terms in their contracts with their customers and suppliers to allocate responsibility for dealing with security, ensuring cooperation both before and after the event of an incident, and to ensure the position on liability is clear.