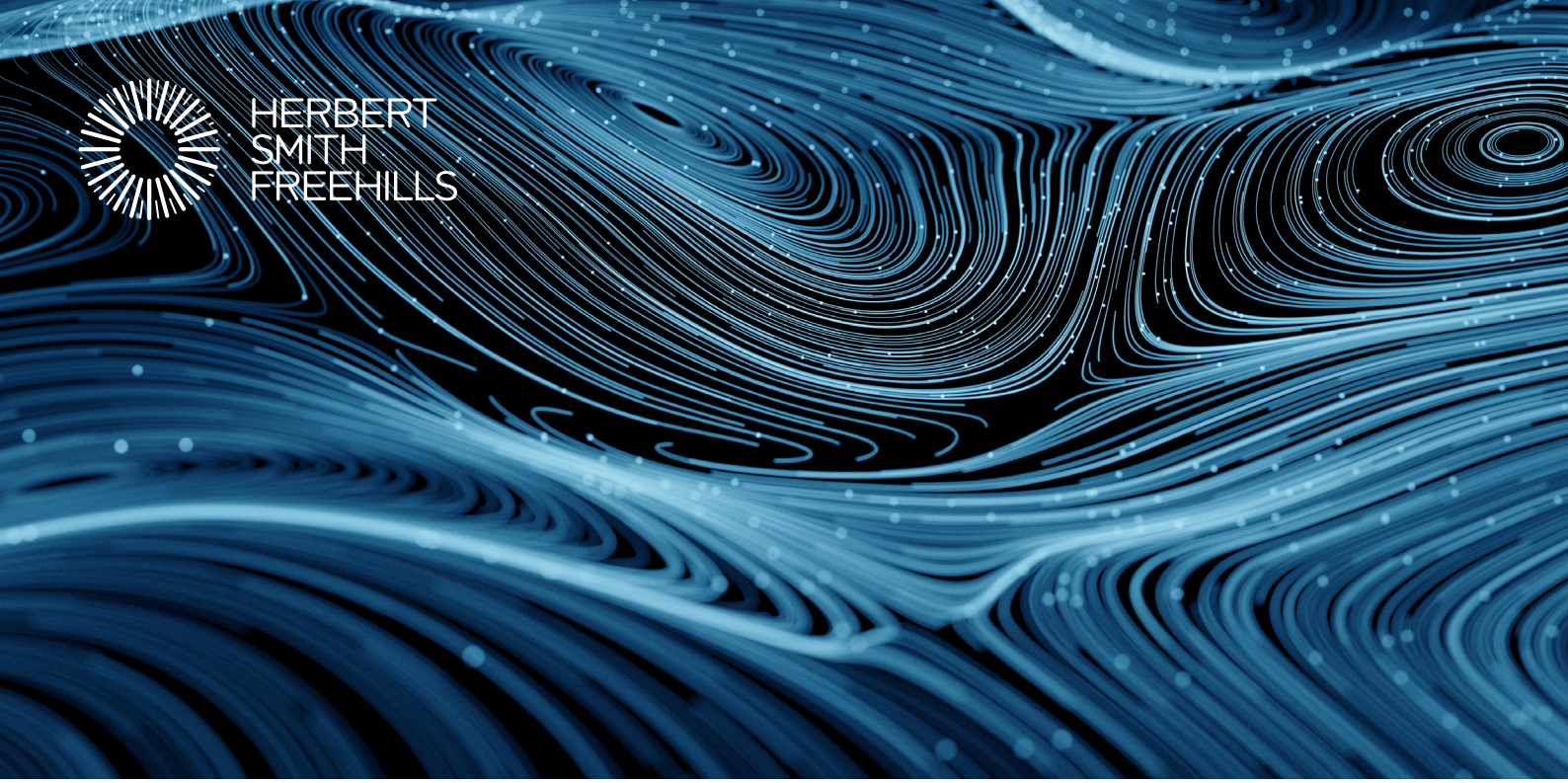

Managing cyber security risks in the telecommunications sector

Cyber security remains in the public eye with multiple incidents and vulnerabilities reported affecting telecoms companies. Telecoms companies need to continue to focus on the risks and consider updating their pro-active defence and cyber security response plans to reflect the increased legal, operational, technical and regulatory risks they are facing.

The evolution of the cyber threat has not escaped the attention of governments around the world. In 2018 the Network and Information Security Directive (**NISD**) as well as the General Data Protection Regulation (**GDPR**) will be implemented in the EU. The NISD, which is due to be implemented by May, will require operators of core "digital infrastructure" and certain "digital service providers" to ensure that their network and information systems meet minimum standards of cyber security.

Telecoms a target

There has been no let-up in the rate and seriousness of attacks in recent times. Telecoms companies, their core infrastructure and the large volumes of personal data they hold on subscribers, all represent an obvious target for malicious actors. Compared to other industries, telecoms companies are expected to be tech-savvy and often have a large consumer-facing footprint. This creates heightened reputational risks.

Telecoms companies face particular cyber security concerns as a result of their interconnected nature and the reliance upon international standards in their operations. For example, mobile telecommunications providers rely upon the Signalling System 7 (**SS7**) protocol, the standard by which telecoms companies interoperate globally to facilitate roaming and delivery of calls and texts. SS7 dates back to the 1970s and has been found to contain vulnerabilities that allow calls, texts and location information on handsets to be spied upon knowing only a subscriber's phone number. It also allows calls, texts and other content to be diverted away from a legitimate subscriber's handset to that of an attacker. For example, these vulnerabilities have recently been exploited in Germany by hackers to drain bank accounts by intercepting two factor-authentication SMS messages.

Internet routers – both routers used in the backbone of the Internet and end user (consumer) routers – have also been targets of cyber-attacks. Backbone routers process the data of multiple organisations simultaneously; in targeting these routers the hackers hope to compromise many organisations at once. Known issues with the BGP (Border Gateway Protocol), which is used by those routers to control routing of traffic on the internet, have been exploited to redirect traffic to bad actors. Home routers too, often those provided to customers by ISPs, have been an attractive target for hackers. The Mirai worm affected 100,000 UK Post Office broadband customers and 900,000 customers of Deutsche

Telecom, and was used to mount a distributed denial-of-service (DDoS) attack against core internet infrastructure provided by Dyn, which in turn resulted in outages across Twitter, Spotify, Netflix, Paypal and other services. The worm also disabled some subscribers' routers permanently (so-called "bricking") meaning they had to be physically replaced.

Many of these attacks present a unique challenge as protocols such as SS7 and BGP are defined by international standards and so require international cooperation to resolve the vulnerabilities. While these vulnerabilities remain unresolved, absent mitigating action, telecoms businesses are faced with potential legal liabilities arising from cyber incidents exploiting those vulnerabilities.

Liability to third parties can arise where attacks have either been made possible or been made worse, by the telecoms companies' IT practices. Liability can arise either through tort law, under existing contractual obligations that have not been complied with, or through regulatory enforcement. It is unlikely that liability will be avoided by merely pointing to the vulnerabilities in the standards themselves: despite the vulnerabilities themselves, there are steps that telecoms companies can take to mitigate the risks and protect their systems.

Telcos can expect increasing intervention from regulators and governments on cyber issues, including in relation to these protocol vulnerabilities, to the extent these or other cyber issues begin to compromise the integrity or privacy of communications networks. Telcos need to ensure that their pro-active defence and cyber incident response plans adequately address the legal and operational risks as well as the technical response to incidents.

New regulations

In the EU, 2018 will see the entry into force of two major pieces of legislation relevant to cyber security. The GDPR enters into force on 25 May 2018. It imposes requirements on all companies processing personal data (including employee and customer 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. It also requires the reporting of incidents within 72 hours. The GDPR allows the imposition of significant fines for breaches of these obligations (up to 4% of global turnover).

The NISD, a more targeted piece of legislation, is aimed at operators of "essential services" and certain "digital service providers". Relevantly to telecoms companies, "essential services" covers "digital infrastructure providers", specifically IXPs ("internet exchange points"), top-level domain (**TLD**) operators and DNS providers. Operators of online marketplaces, search engines and cloud services providers are also covered as "digital service providers".

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 in the affected sectors. 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. For digital service providers, the reporting obligations can also extend to data breaches, raising the spectre of a regulatory "double hit" under both the GDPR and NISD in respect of a single incident.

In the UK the government has undertaken a consultation[1] in relation to its implementation of NISD, which proposes fines of up to £17m. Draft implementing regulations are expected to be published shortly. The National Cyber Security Centre in the UK (which is part of GCHQ) has issued guidance[2] for digital infrastructure providers that is expected to be enforced by Ofcom (the nominated sectoral regulator). 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. Much emphasis is placed on managing supply chain risk. While much of the guidance is drawn from pre-existing industry best practice and existing NCSC advice, digital infrastructure providers will need to ensure and demonstrate that their cyber security practices are compliant by May 2018 or face substantial fines.

As a directive, the NISD is being independently implemented by each member state in the EU and is designed only to mandate a minimum level of cyber security. Telecoms 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.

Key contacts

Andrew Moir
T +44 20 7466 2773
M +44 780 9200434
andrew.moir@hsf.com

Peter FitzPatrick
T +44 20 7466 3711
M +44 7803 403 108
peter.fitzpatrick@hsf.com

Miriam Everett
T +44 20 7466 2378
M +44 7545 300 862
miriam.everett@hsf.com

Footnotes

1. https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive
2. https://www.ncsc.gov.uk/guidance/nis-guidance-collection