EU, Competition and Regulatory

December 2016

CYBER SECURITY – TIME TO CHANGE THE LOCKS?

The EU's Directive on Security of Network and Information Systems[1] (the NIS Directive) obliges Member States to improve national cyber security and reporting. In addition to obligations imposed on digital service providers, the NIS Directive also imposes obligations on businesses defined as "operators of essential services" which could include ports, terminals, airports and banks as well as other businesses in energy, transport, health, IT, telecommunications, water, food and finance.

When the NIS Directive is implemented (by 9 May 2018) these businesses must ensure that their security levels are adequate and must report serious cyber breaches to the relevant authorities. The NIS Directive aims to increase the security of network and information systems across Europe by improving cross-border cooperation and information exchange between EU Member States, thereby strengthening resilience to and improving response times in the event of a cyber incident. The UK already takes cyber security seriously. Its National Cyber Security Centre[2], which became operational in October 2016, provides guidance and assistance on cyber security to businesses and the National Crime Agency has a specially designated unit, the National Cyber Crime Unit[3], to respond to cyber crime.

What are Operators of Essential Services?

Operators of Essential Services (OESs) are operators which provide a service which is 'essential for the maintenance of critical societal and or economic activities'[4]. The service must also be dependent on network and information systems for its provision. If such systems were affected by an incident, this would have 'significant disruptive effects' on the provision of such a service.

1 Directive 2016/1148 Concerning Measures for a high common level of security of network and information systems across the Union

2 https://www.ncsc.gov.uk/

3 http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit

4 NIS Directive 2016/1148, Article 5

OESs must take appropriate measures to manage the risks posed to their network and information systems. In the event of an incident, they are required to notify their Member State's Computer Security Incident Response Team (CSIRT) or the relevant Competent Authority without undue delay.

ANTHONY WOOLICH, PARTNER

The extent of the disruption to a service and its cross-border impact is determined by reference to factors stipulated in the NIS Directive. Such factors include the duration of the disruption, the number of users relying on the service, the size of the area affected by the incident and the market share of the service provider.

There is no definitive list of what an OES is in the NIS Directive. Member States are required to determine which operators provide essential services by 9 November 2018. The definition in the NIS Directive is broad and OESs will include businesses in fields such as energy, transport, banking and health. As Member States are afforded some discretion in identifying OESs, it is possible that the same international operator may be classified as an OES in one Member State but not in another, although the recitals of the NIS Directive indicate that Member States may work together to establish a consistent approach.

The NIS Directive points out that the security aspects of water transport and banking are already regulated by other legislation and that the reporting requirements of that other legislation will apply as long as the reporting obligations are equivalent to those set out in the NIS Directive.

What must OESs do?

OESs must take appropriate measures to manage the risks posed to their network and information systems. In the event of an incident, they are required to notify their Member State's Computer Security Incident Response Team (CSIRT) or the relevant competent authority without undue delay. The notification should include sufficient information to enable the competent authority to determine the extent of the incident's cross-border impact.

What are Digital Service Providers?

Digital Service Providers (DSPs) are legal persons providing an 'information society service', for example providers of online search engines, marketplaces or cloud computing. Micro and small enterprises, in the sense of EU Recommendation 2003/361[5], are excluded from the scope of the definition.

What must DSPs do?

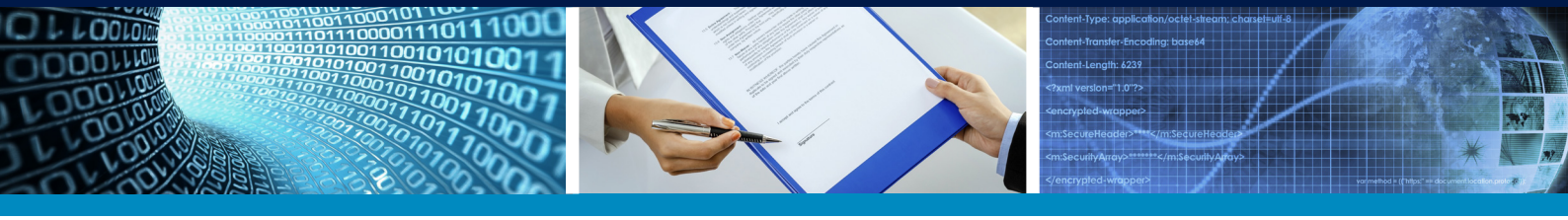
Under the NIS Directive, DSPs are required to manage the risks posed to the security of their systems. Risk-management measures should, with reference to the state of the art, be appropriate to the level of risk and should minimise the impact of security-infringing incidents on the service provided.

DSPs are also required to notify the competent authority or the CSIRT of an incident having a "substantial" impact on the provision of an information society service they offer within the Union, if they have access to the information needed to assess the impact of the incident against the factors referred to in the NIS Directive. As with OESs, the NIS Directive sets out factors determining an incident's impact on the provision of a service and whether it will qualify as substantial.

What if OESs and DSPs rely on each other?

In numerous cases OESs may rely on a service provided by a DSP, such as cloud storage, to provide their essential service effectively. If this digital service is subsequently interrupted by an incident, this could have a substantial impact on the continued provision of

5 EU Recommendation 2003/361 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361
Small Businesses are defined in EU Recommendation 2003/361 as those with less than 50 members of staff and either a turnover or balance sheet total of less than or equal to €10m.
Micro Businesses are defined in EU Recommendation 2003/361 as those with less than 10 members of staff and either a turnover or balance sheet total of less than or equal to €2m.



the essential service. In the event of such a disruption, unless otherwise contractually provided for, the OES has an obligation to notify the relevant authority or the CSIRT of the incident.

Obligations on Member States

Member States must ensure that OESs and DSPs comply with their notification obligations. Member States cannot impose more onerous obligations on DPSs and OESs than those included in the NIS Directive, except for reasons of national security or law and order.

The NIS Directive also requires Member States to develop and adopt a national strategy on cyber security to ensure secure network and information systems across essential services. To achieve this, the NIS Directive introduces minimum capabilities to which Member States must conform. The objectives of this national strategy must be defined and a governance framework set up to achieve these objectives, to identify the extent of the Member State's preparedness, and the efficacy of its response and recovery.

Each Member State must designate a national competent authority to monitor the national application of the NIS Directive and ensure that it is implemented effectively. In addition, the NIS Directive requires a Member State to create a CSIRT responsible for monitoring incidents, providing early warnings in respect of potential threats, liaising with the private sector and assisting other national CSIRTs in resolving incidents. In certain circumstances, such as where the incident concerns two or more Member States, CSIRTs are required to share information and details about such incidents with the affected Member States. This requirement may raise concerns as to the security of the data shared with CSIRTs.

Member States must ensure that OESs and DSPs comply with their notification obligations. Member States cannot impose more onerous obligations on DPSs and OESs than those included in the NIS Directive, except for reasons of national security or law and order.

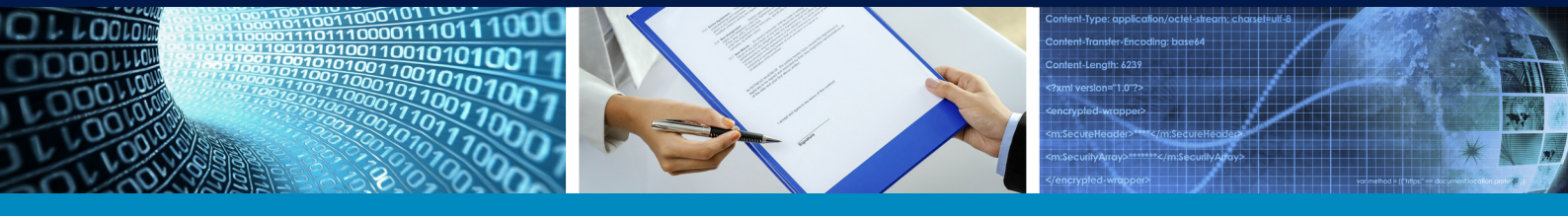
FELICITY BURLING, ASSOCIATE

The position in the UK

In the UK the National Cyber Security Centre (NCSC) is the UK's advisory authority on cyber security. The NCSC provides guidance on cyber security and coordinates responses to cyber threat in both the public and private sectors. Law enforcement agencies, including the National Cyber Crime Unit for the most serious cyber crime threats, are responsible for investigating and prosecuting for cyber crime.

The NIS Directive must be implemented into national law in all EU Member States by 9 May 2018. It is not yet clear whether the UK will be required to implement the NIS Directive, although it is likely that there will be a requirement for it to do so because Brexit negotiations are unlikely to be concluded before May 2018.

However, the UK certainly takes cyber security seriously and businesses should make sure that their security systems are appropriate and up to date, particularly if they operate critical infrastructure in the energy, IT, telecommunications, transport, health, water, food or finance sectors.



For more information, please contact the authors of this briefing:

Anthony Woolich
Partner, London
T: +44 (0)20 7264 8033
E: anthony.woolich@hfw.com

Felicity Burling
Associate, London
T: +44 (0)20 7264 8057
E: felicity.burling@hfw.com

HFW has over 450 lawyers working in offices across Australia, Asia, the Middle East, Europe and South America. For further information about EU, Competition and Regulatory issues in other jurisdictions, please contact:

Daniel Martin
Partner, London
T: +44 (0)20 7264 8136
E: daniel.martin@hfw.com

Robert Follie
Partner, Paris
T: +33 1 44 94 40 50
E: robert.follie@hfw.com

Pierre Frühling
Partner, Brussels
T: +32 (0) 2643 3406
E: pierre.fruhling@hfw.com

Michael Buisset
Partner, Geneva
T: +41 (0)22 322 4801
E: michael.buisset@hfw.com

Jasel Chauhan
Partner, Piraeus
T: +30 210 429 3978
E: jasel.chauhan@hfw.com

Ian Chung
Partner, Dubai
T: +971 4 423 0534
E: ian.chung@hfw.com

Brian Gordon
Partner, Singapore
T: +65 6411 5333
E: brian.gordon@hfw.com

Guy Hardaker
Partner, Hong Kong
T: +852 3983 7644
E: guy.hardaker@hfw.com

Julian Davies
Partner, Shanghai
T: +86 21 2080 1188
E: julian.davies@hfw.com

Aaron Jordan
Partner, Melbourne
T: +61 (0)3 8601 4535
E: aaron.jordan@hfw.com

Stephen Thompson
Partner, Sydney
T: +61 (0)2 9320 4646
E: stephen.thompson@hfw.com

Simon Adams
Partner, Perth
T: +61 (0) 8 9422 4715
E: simon.adams@hfw.com

Fernando Albino
Partner, São Paulo
T: +55 (11) 3179 2900
E: fernando.albino@hfw.com

Lawyers for international commerce hfw.com

São Paulo London Paris Brussels Geneva Piraeus Beirut Riyadh Kuwait Dubai
Singapore Hong Kong Shanghai Perth Melbourne Sydney