Dechert LLP

Tough New EU-Wide Cybersecurity Rules in Prospect: The Network and Information Security Directive

OnPoint: A Legal Update from Dechert's International Trade and EU Regulation, and Privacy and Cybersecurity Practices

May 2016

Tough new EU-wide Cybersecurity Rules in Prospect: The Network and Information Security Directive

Two-thirds of large UK companies have come under cyber attack in the past year, according to the UK Government, and a quarter have been attacked at least once a month. But only half have taken any recommended actions to address their vulnerabilities, only a third have formal cyber security policies and under 10% have an incident management plan. EU Governments have now decided to legislate against such complacency: the Network and Information Security Directive, agreed by the EU Ministers on 17 May 2016, will impose mandatory requirements on firms in key sectors to protect their systems from such attacks and to notify national authorities if they occur. Companies subject to these regulations should be proactive about developing plans for compliance.

Background

While many EU governments have well-established voluntary schemes and national advisory bodies to help companies identify and mitigate the risks (in the UK, the 'Cyber Essentials'[1] programme and the upcoming National Cyber Security Centre[2]), their patience with voluntary measures has been wearing increasingly thin in the face of the growing scale of the threat and the continuing failure of companies to take adequate steps to protect themselves and the data they hold.

Within the EU, most current regulation is based on national legislation. In the UK, the Financial Conduct Authority expects regulated firms to notify it of breaches and the Information Commissioners' Office encourages disclosure of breaches of personal data. At an EU level, cybersecurity requirements apply only to the telecommunications sector.

In 2013 the European Commission set out an EU Cybersecurity Strategy[3] alongside its Digital Single Market Initiative[4]. The Strategy aims to:

- Promote cyber resilience;
- Reduce cybercrime;
- Develop cyber-defence policies and capabilities; and
- Establish a coherent cyber policy for the EU.

To implement this strategy, the EU is introducing a range of new regulatory requirements that will have a significant impact on businesses, of which the Network and Information Security Directive (NISD) is the most recent. Formally adopted by the Council on 17 May, the NISD must be approved by the European Parliament (it has already agreed to the rules in principle) and will enter into force 21 months later, in national legislation.

The NISD aims to promote the adoption of good risk management practices in the public and private sectors, to prevent cyber attacks that could impact on national security and to provide for the most effective response when

[1] Cyber Essentials is a voluntary scheme through which companies can receive certification that they have taken basic precautions. Certification is now mandatory for companies bidding for higher-risk government contracts and this requirement is likely soon to be extended to all government contractors. See: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

[2] The National Cyber Security Centre, due to open in London in October 2016, will bring together cyber expertise 'to transform how the UK tackles cyber security issues.' One of its first tasks will be to work with the Bank of England to produce advice for the financial sector. See: https://www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together

[3] https://ec.europa.eu/digital-single-market/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[4] https://ec.europa.eu/digital-single-market/en/digital-single-market

they occur. Its provisions are similar to those of the US Cyber Security Framework but it will establish mandatory rather than voluntary requirements. There are no current EU plans to mirror the US capacity to impose sanctions on foreign individuals and groups that use cyberattacks to threaten security or economic interests (the US capability has yet to be exercised).

The NISD will impose three different sets of obligations: on governments, on operators of essential services and on digital service providers.

Governments

All EU governments will be obliged to adopt a Network and Information Security strategy, to designate a national point of contact and competent authority/ies, to set up Computer Security Incident Response Teams (CSIRTs) and to co-operate with each other and with the European Union Agency for Network and Information Security (ENISA).

Operators of essential services

These organisations will be identified by national governments from among entities that are active on a stable basis on their territory, on the basis of a common set of EU criteria, primarily that they provide a service which depends on network and information systems and which is essential for the maintenance of critical societal and/or economic activities. These will include businesses in the following sectors:

- **Digital infrastructure**: internet exchange points, top-level domain name registries, and domain name system service providers (but not e-commerce platforms);
- **Energy**: electricity/gas suppliers, distribution system operators, transmission system operators, storage system operators, LNG operators, and operators of oil and natural gas production, refining and treatment facilities;
- **Transport**: air and maritime carriers, traffic management control operators, airports, railways, road traffic management control and intelligent transport system operators;
- **Banking**: credit institutions, in accordance with the Capital Requirements Regulation;
- **Financial market infrastructure**: stock exchanges and central counterparties;
- **Healthcare providers**: including hospitals and private clinics; and
- **Drinking water**: supply and distribution operators.

Telecommunications companies are already regulated under the Framework Directive for electronic communications (2002/21/EC) and are therefore excluded from the NISD.

Organisations identified as ‘operators of essential services’ will be required (regardless of whether they perform the maintenance of their networks and information systems themselves or outsource the work) to:

- Take appropriate and proportionate risk management measures to prevent and minimise the impact of incidents that affect the security of their networks and information systems;

- Comply with a reporting scheme, to be established by the Member State in question, under which they must notify without undue delay incidents[5] having a significant impact on the continuity of the essential services they provide; and

- If so required by the competent national authority, to provide information needed to assess the security of their systems and evidence of the effective implementation of security policies (such as the results of a security audit). The competent authority may issue binding instructions to the entity to remedy its operations.

Digital Service Providers

Any entity providing one of the following services within any EU Member State will be subject to the NISD under the jurisdiction of the Member State where it has its main establishment (entities with under 50 employees are exempt; if an entity is established outside the EU, it must designate a representative established in a Member State):

- Online marketplaces: services allowing consumers and/or traders to conclude online sales and service contracts (but not online services which compare products or services and redirect the user to the preferred trader);

- Online search engines: services which allow the user to perform searches of all websites or all websites in a particular language on the basis of a query (but not search functions that are limited to the content of a specific website); and

- Cloud computing services: services that enable access to a scalable and elastic pool of shareable computer resources. This means cloud computing services which can respond to an increase or decrease in demand for resources or processing power from multiple users accessing the service in different geographical locations, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment.

These organisations will be required (regardless of whether they perform the maintenance of their networks and information systems themselves or outsource the work) to:

- Take appropriate and proportionate measures to manage risks, taking into consideration: the security of systems and facilities; incident management; business continuity management; monitoring, auditing and testing; and compliance with international standards;

- Take measures to ensure the continuity of their services by preventing and minimising the impact of incidents;

- Notify the competent authority of any incident that has a substantial impact on the provision of a digital service. The NISD establishes parameters to be taken into account when assessing the impact of any incident including the number of users affected, the duration, the geographical spread, the extent of the disruption, and the impact on economic and societal activities; and

[5] "Incidents" are those events that have an actual adverse effect on the security of networks and information systems. The Directive establishes criteria to be taken into account when assessing the impact of any incident, including the number of users affected, the duration of an incident and its geographical spread. Member States may be granted some discretion to develop national, sector-specific guidelines on what constitutes a reportable incident, enabling differences between states and sectors to be taken into account, although EU-level discussion would aim to avoid the development of widely-divergent approaches.

- If so required by a competent authority, to provide information needed to assess the security of their networks and information systems and to remedy any failure to fulfil the relevant requirements.

As the degree of risk is generally lower than for operators of essential services, the NISD does not oblige competent authorities to supervise digital service providers, who will be subject only to reactive, ex-post supervisory activities i.e. the competent authorities will only take action when they have evidence of non-compliance. A digital service provider, unlike an operator of essential services, is under no obligation to provide such evidence.

Notifications

If an operator of essential services or a digital service provider gives notice of an incident:

- The notice should include information to enable the competent authority to determine any cross-border impact of the incident and to inform other affected Member States;

- After consulting the entity making a notification, the competent authority may inform the public if this is judged necessary either to prevent an incident or to deal with an on-going incident (or, in the case of notifications by digital service providers only, where such a disclosure is otherwise in the public interest). The notifying party will be consulted before a disclosure to the public is made, and its commercial interests and the confidentiality of information it has provided will, in principle, be preserved. Notification will not expose the notifying party to increased liability;

- They should also consider the potential need to report the same incidents under the new General Data Protection Regulation (if the incident concerns a breach of personal data) and/or to financial services regulating bodies (for incidents compromising the integrity of client data or impacting the continuity of services).

Entities outside the scope of the NISD may, if they experience significant incidents, give notice on a voluntary basis.

The NISD will require Member States to lay down and enforce 'effective, proportionate and dissuasive' penalties. These, and which agency will be responsible for enforcing them, remain to be defined by each Member State. Additionally, there will be a risk of legal action against companies who breach these requirements by shareholders, customers and others whose data is compromised as a result.

What do firms need to do and how can Dechert help?

Although most of these changes to the law are still some way off, businesses should be proactive in preparing for their implementation. In particular, businesses that may be defined as 'operators of essential services' or 'digital services providers' should be aware of the compliance obligations to be imposed on them, assess the risks they face and ensure that appropriate measures are in place to meet the new requirements.

Dechert has extensive experience advising clients on all aspects of compliance with EU and national regulatory standards and notification requirements; our team includes former senior Government regulators with first-hand experience of developing and implementing regulation in this and related areas. We can advise on how best to prepare for the introduction of these new regulations including determining which obligations may apply, developing proportionate policies and plans, testing response processes (we can assist with bringing in relevant

technical specialists), drafting compliance policies and contracts, and conducting investigations if concerns are discovered. Our legal reports are covered by privilege and therefore not subject to disclosure.

This update was written by Richard Tauwhare.

For more information on these issues, please contact:

Miriam Gonzalez
Partner
London: +44 20 7184 7892
miriam.gonzalez@dechert.com

Caroline Black
Partner
London: +44 20 7184 7543
caroline.black@dechert.com

Andrew Hood
Senior Director
London: +44 20 7184 7315
andrew.hood@dechert.com

Renzo Marchini
Special Counsel
London: +44 20 7184 7563
renzo.marchini@dechert.com

Richard Tauwhare
Senior Director
London: +44 20 7184 7350
richard.tauwhare@dechert.com

For further information,
visit our website at dechert.com

Dechert
LLP