UK Implements EU Cybersecurity Rules

Date : June 14, 2018

The UK recently adopted the EU Cybersecurity Directive into UK law, called the Network and Information Systems Regulations 2018 (the NIS regime), which are now in force and can be found here: https://www.legislation.gov.uk/uksi/2018/506/made. We have written previously about this matter here http://www.corderycompliance.com/eu-cyber-security-rules-adopted/ and here http://www.corderycompliance.com/uk-to-implement-eu-cybersecurity-directive/.

What's this all about?

In 2016 the EU introduced new rules to ensure that:

- "Operators of essential services" (OESs) and "relevant digital services providers" (RDSPs) in the EU have appropriate and proportionate cyber security measures in place and report cyber security incidents to a regulator; and,
- EU Member States improve their national cyber security capabilities and co-operation between them on cyber security issues.

This article focuses solely on the aspects of the NIS regime affecting OESs and RDSPs.

Is my organisation affected by this?

OESs are those which are essential for the maintenance of critical societal and/or economic activities – the NIS regime designates when an organisation is considered to be an OES and also sets out detailed quantitative and qualitative threshold criteria that determine whether an essential service falls within the regime. OESs (falling under the NIS regime) include those operating in the following sectors and sub-sectors:

- Energy – electricity, oil and gas;
- Transport – air, water, rail and road;
- Healthcare – including hospitals, private clinics and online settings;
- Drinking water supply and distribution; and,
- Digital infrastructure – domain name registries and service providers and internet exchange points.

A regulator (a so-called "designated competent authority") also has discretionary power to designate an organisation as an OES where a cyber incident affecting that organisation would likely have a significant disruptive effect on the provision of essential services. It should also be noted that the UK has not included in the NIS regime organisations operating in the banking and financial market infrastructures sectors (which are included in the EU Cybersecurity Directive) as these sectors are already otherwise regulated in the cyber security domain in the UK.

RDSPs that fall under the scope of the NIS regime are:

- Online marketplaces;
- Online search engines; and,
- Cloud computing services.

An organisation will be considered to be an RDSP if it has its head office or "nominated representative" in the UK (and is not a micro or small enterprise).

An OES that meets the quantitative and qualitative threshold criteria referred to above must notify the relevant "designated competent authority" by **10 August 2018 or within 3 months of satisfying the OES criteria**.

An RDSP must notify itself to and register with the UK data protection regulator, the Information Commissioner's Office (ICO) by **1 November 2018**.

Micro and small digital companies are generally exempt from security requirements and incident notification.

What are the requirements?

OESs and RDSPs are required to:

- Have in place relevant cyber security measures – these are set out in very broad terms and they differ for OESs and RDSPs as follows:

- An OES: *"must take appropriate and proportionate technical and organizational measures to manage risks posed to the security of the network and information systems on which their essential service relies"* and these measures *"must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed"*; "*must take appropriate and proportionate measures to prevent and minmise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services"*; and, *"must have regard to any relevant guidance issued by the relevant competent authority when carrying out their duties [as set out immediately above]"*. Although the UK National Cyber Security Centre is not an NIS regime "designated competent authority" it has issued sector neutral guidance (which can be found here: https://www.ncsc.gov.uk/guidance/nis-guidance-collection) to assist OESs comply with the NIS regime which sets out four high-level outcomes (managing security risk, defending systems against cyber attack, detecting cyber security events, and minimising the impact of cyber security incidents) and fourteen core security principles (covering aspects such as governance, risk management, system and network resilience, security monitoring, and response and recovery planning);
- An RDSP: *"must identify and take appropriate and proportionate measures to mange the risks posed to the security of network and information systems on which it relies to provide [in the EU online marketplace, online search engine or cloud computing services]*; these measures *"must (having regard to the state of the art) ensure a level of security of network and information systems appropriate to the risk posed", "prevent and minmise the impact of incidents affecting their network and information systems with a view to ensuring the continuity of those services"*, and take into account *"the security of systems and facilities, incident handling, business continuity management, monitoring auditing and testing, and compliance with international standards"*; and,

- OESs must report any incident that *"has a significant impact on the continuity of the essential service which that OES provides ("a network and information systems ("NIS") incident")"* and RDSPs must report *"any incident having a substantial impact on the provision of any of the [applicable] digital services […] that it provides".* The "*incidents*" that will have to be reported are broadly defined as "*any event having an actual adverse effect on the security of network and information systems*." Incidents must be reported to a "relevant competent authority" "without undue delay" and no later than 72 hours after they are aware that the incident has occurred. The NIS regime sets out what has to be reported, which is broadly similar for OESs and RDSPs (operator name, essential service provided, number of users affected by the incident, geographical scope, time, duration, name and impact of incident etc.) but with a few important differences. A "designated competent authority" may inform the public about an incident if public awareness is necessary to handle etc. the incident (again the criteria differ slightly for OESs and RDSPs);

Who is my regulator?

There is no one central regulator in the UK for the purposes of the NIS regime – instead a sectoral approach has been adopted and so an array of "designated competent authorities" are involved who have authority and responsibility for regulatory decisions under the NIS regime. This set-up is based on the relevant UK government departments responsible for: energy, transport, healthcare and environment (for drinking water supply and distribution); Ofcom applies for digital infrastructure; and, the ICO applies for RDSPs.

What are the sanctions for non-compliance?

The regulators have a number of powers including the ability to impose sanctions for non-compliance as follows:

- Up to UK £1 million for any contravention that doesn't cause an *"NIS incident"* (i.e. for OESs);
- Up to UK £3.4 million for a "material contravention" which has caused or could cause an incident resulting in a reduction of service provision by the OES or RDSP for a significant period of time;
- Up to UK £8.5 million for a "material contravention" which has caused or could cause an incident resulting in a disruption of service provision by the OES or RDSP for a significant period of time; and,
- Up to UK £17 million for a "material contravention" which could cause or has caused an incident resulting in an immediate threat to life or significant adverse impact on the UK economy.

A "material contravention" includes failure to take steps or any adequate steps within stipulated time periods of a number of issues including notifying an incident.

The regulator can also undertake inspections in order to assess whether or not an OES or an RDSP has fulfilled its security or incident reporting obligations.

Is there any overlap with the General Data Protection Regulation (GDPR)?

GDPR is now fully up and running and requires all organisations processing personal data to keep personal data secure and report data security breaches to a regulator (the ICO in the UK). It is likely that organisations falling under the NIS regime will also be data controllers under GDPR (and the UK Data Protection Act 2018). In addition to reporting incidents under the NIS regime, incidents that affect or compromise personal data may therefore have to be reported by OESs and RDPSs under GDPR – there is a risk of double jeopardy here (although the UK government says that it is will try and avoid this where possible). Expert counsel is likely to be needed in coordinating these reports.

What can I do to prepare?

Businesses would do well to consider undertaking the following actions.

- Determine if they are either an OES or an RDSP;
- If they are an OES or an RDSP, evaluate the cyber security measures that they have in place to ensure that they comply with the NIS regime security obligations, including if they are an OES the UK four high-level outcomes and fourteen principles;
- Set up (or update) their incident plans and procedures (and tie plans with GDPR data security breach reporting) and regularly fire-drill these procedures;
- Alert the Board to the NIS regime and plan resources to address it – this should include hardware, software and training;
- Undertake training and develop internal cyber security advocacy – make sure this is not simply off-the-shelf training but that it is tailored to the risks that may be faced;
- Re-evaluate existing public relations strategy to deal with an incident or set up a new one; and,
- Reassess existing cyber insurance or take out a new policy.

In addition, although the NIS regime does not apply directly to OES and RDSP supply chains, OESs and RDSPs should ensure that their supply chains put in place appropriate measures to manage the risk that their services might be disrupted through their supply chains.

Cordery regularly reports on cyber security and related issues. Details can be found here: http://www.corderycompliance.com/category/cyber-security/. If you'd like help with the NIS regime then please call Cordery. We also write and make films about data protection issues (including data security breaches) that can be found here: http://www.corderycompliance.com/category/data-protection-privacy/. We also have a GDPR Navigator subscription service, the details of which can be found here: http://www.corderycompliance.com/solutions/cordery-gdpr-navigator/.

For more information please contact André Bywater or Jonathan Armstrong who are commercial lawyers with Cordery in London where their focus is on compliance issues.

André Bywater

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com

Jonathan Armstrong

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com