The NIS Regulations: the need-to-know points for UK providers of essential infrastructure and digital services

Fiona Maclean and Olga Phillips, Associates with Latham & Watkins LLP, explore the UK Network and Information Security Regulations and how implicated organisations can best adapt to ensure that the new obligations are fulfilled

Although the NIS Regulations have been somewhat overshadowed by the General Data Protection Regulation ("GDPR"), organisations should not underestimate the importance of this new network and information security law.

The Network and Information Security Directive ("NISD") and the UK implementing legislation, the Network and Information Security Regulations (the "NIS Regulations"), came into force on 10 May 2018.

The NISD's objective is to raise levels of the overall security and resilience of network and information systems across the European Union. Since the NISD is an EU directive as opposed to being an EU regulation, unlike the GDPR, the NISD had to be transposed into local law by each EU member state.

The NIS Regulations, as well as the other EU implementing laws, have been somewhat overshadowed by the GDPR. However, organisations should not underestimate the importance of this new law which imposes penalties of up to £17,000,000 for breaches of its terms. This article explores the practical and legal implications for providers of essential infrastructure and digital services in the UK.

The NIS Regulations

The NIS Regulations aim to establish a common framework for network and information systems security. Network and information systems are systems that process any data for the purpose of "operation, use protection and maintenance" which, in theory, could cause significant damage to the UK's economy, society and individuals' welfare if disrupted. In response to the increasing risk landscape, the NIS Regulations aim to reduce cyber threats, as well as physical and environmental threats, to these systems.

The NIS Regulations apply to "operators of essential services" ("OES") and "relevant digital service providers" ("RDSPs").

What is an OES?

An OES is an organisation that operates services that are critical to the economy and wider society. Schedule 2 of the NIS Regulations lists the kinds of services considered essential in the UK — including electricity, oil, gas, air transport, water transport, rail transport, road transport, healthcare, drinking water and distribution and digital infrastructure.

Schedule 2 also sets forth thresholds that can be used to determine whether or not an entity is an OES within the framework of the NIS Regulations. The threshold criteria vary per essential service: for example, in the healthcare subsector, specific organisations are listed in the NIS Regulations (section 8, Schedule 2) whilst for services such as drinking water, the criteria depend on the number of individuals the organisation supplies (section 5, Schedule 2).

What is an RDSP?

The NIS Regulations apply to RDSPs that provide their services "for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".

To fall within the NIS Regulations' scope, RDSPs must:

- provide either an online marketplace, an online search engine or a cloud computing service, in the United Kingdom;
- have a main establishment or nominated representative in the UK; and
- not fall within the small and micro-sized enterprises exemption.

The last criterion exempts businesses that have fewer than 50 employees and an annual turnover of less than €10 million. This exemption is not described within the NIS Regulation itself but is derived from the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

Among group companies seeking to benefit from the exemption, the test includes looking at the overall group structure and assessing, among other factors, the degree of power exercised by the parent company / other group members over the relevant entity. Therefore RDSPs with a relatively small establishment in the UK may still find themselves subject to the NIS Regulations if the staff and turnover of their wider group gets taken into account.

Are financial service providers off the hook?

Notably, banking and financial services are not considered to be an OES under the NIS Regulations although they are described as such in NISD. In its Consultation Paper on Security of Network and Information Systems, the UK Government concluded that the financial services industry did not need to be in scope of the NIS Regulations on the basis that financial services laws currently exist that include provisions "at least equivalent" to those identified in NISD (as per the permitted exemption set forth in Article 1.7 of NISD).

Firms and financial market infrastructure providers within this sector must continue to adhere to requirements and standards as set by the Bank of England and/or the Financial Conduct Authority ("FCA").

The FCA's and the Prudential Regulation Authority's ("PRA's") 2018/19 Business Plans focus respectively on strengthening "resilience to cyberattacks" and assessing the sector's ability to "respond to major disruption" demonstrating that systems security remains a prominent focus for financial services.

What obligations do OES and RDSPs have under the NIS Regulations?

Registration

All persons falling within the definition of an OES as at 10 May 2018 had until 10 August 2018 to register with their competent authority, under Regulation 8(2). A list of the relevant competent authorities is set out at Schedule 1 of the NIS Regulations. Separately, any person falling within the definition of a RDSP as at 10th May 2018 has until 1 November 2018 to register with the Information Commissioner's Office ("ICO") (Regulation 14).

In addition, any new organisations have three months from the date they satisfy the relevant definition to register with the applicable authority. Both OES and RDSPs should ensure timely notification in accordance with the NIS Regulations.

Security measures

The NIS Regulations require OES and RDSPs to take "appropriate and proportionate" technical and organisational measures to manage security risks to their network and information systems (Regulations 10 and 12).

The NIS Regulation is reasonably prescriptive as to the measures required by RDSPs in this regard. Referring out to the terms of the Commission's Implementing Regulation 2018/151 ("Security Regulation"), the NIS Regulations list a set of elements for RDSPs to incorporate into their security measures, including:

- access controls to network and information systems;
- the establishment and use of contingency plans to ensure the continuity of the service;
- disaster recovery capabilities that are regularly tested; and
- the availability of adequate documentation to enable the competent authority to verify compliance with Regulation 2018/151.

"For OES… NIS Regulations provide very little guidance on the nature of the security measures required. The National Cyber Security Centre …acknowledged that the principles were outcome-based and stated that it does not intend to produce an "all-encompassing cyber-security to do list". Additional guidance is expected from other regulators, including the ICO"

For OES, on the other hand, the NIS Regulations provide very little guidance on the nature of the security measures required. The National Cyber Security Centre ("NCSC"), the UK's computer security incident response team ("CSIRT") under the new regulatory framework, has issued 14 principles on network security to help guide OES; however, these principles have been widely criticised as being "too vague", see https://www.ncsc.gov.uk/guidance/introduction-nis-NISD.

The NCSC itself acknowledged that the principles were outcome-based and stated that it does not intend to produce an "all-encompassing cyber-security to do list". Additional guidance is expected from other regulators, including the ICO, but it is anticipated that this guidance will be similar in approach.

Countless organisations will have implemented adequate security measures under the GDPR and will already be accustomed to dealing with the GDPR's accountability principle of maintaining appropriate documentation. Accordingly, many organisations may have little more to do by way of security. Nonetheless,

(Continued on page 4)

(Continued from page 3)

organisations should appreciate that the GDPR is concerned with personal data whilst the application of the NIS Regulations is broader, as the NIS Regulations relate to system security and service continuity as a whole.

All organisations should therefore ensure their security measures are broad enough to cover both regimes and maintain documentation to demonstrate this analysis. For organisations falling within the remit of the NIS Regulations that did little in the way of GDPR compliance, additional work will be required to ensure current security measures are enhanced to meet these requirements.

Incident reporting obligations

Like the GDPR, the NIS Regulations introduce onerous incident reporting obligations on organisations. An OES must provide notification of any incident that has a "significant impact" on the continuity of the essential service, taking into account factors such as the number of users affected, the duration of the incident and the geographical area affected by the incident.

Meanwhile, an RDSP must provide notification of any incident having a "substantial impact" on the provision of any of the digital services that it provides. (Notably the NIS Regulations does not explain the distinction between "significant" and "substantial" and one may wonder whether this is an intentional distinction or a drafting error).

The NIS Regulations helpfully describe certain factors that OES and RDSPs should take into account when assessing their reporting obligations, which, for both, include the number of users affected, the geography of the incident and duration of the incident. RDSPs must also take account of the extent of disruption caused and the extent of impact on economic and societal activities.

Mirroring the GDPR, both the OES and RDSP must notify their competent authority without undue delay and in any event no later than 72 hours after becoming aware that an incident has occurred.

What should OES and RDSPs be doing now?

There are a number of positive steps that OES and RDSPs can take to prepare the compliance environment for the new obligations. These steps relate chiefly to updating contractual terms and considering the enhancement of security due diligence.

Contractual terms

Existing contracts should be adjusted to take account of incident reporting obligations, to cover the extension of the obligations to subcontractors, and to deal with the apportionment of liability and appropriate indemnities in the event of a breach.

Notification obligations

Customers may wish to put contractual obligations in place to ensure a coherent approach in respect of incident reporting. This is particularly important if the customer has reporting obligations that are independent of the NIS Regulations; for example, if RDSPs contract with OES, or in agreements between banks and RDSPs. In the event of an outage, both the RDSP and the bank, for example, are likely to have incident reporting obligations which, if fulfilled by one party, could put the other party under pressure to report without having time to mobilise an effective incident response committee and develop a strategy.

"All organisations should therefore ensure their security measures are broad enough to cover both regimes and maintain documentation to demonstrate this analysis. For organisations falling within the remit of the NIS Regulations that did little in the way of GDPR compliance, additional work will be required to ensure current security measures are enhanced to meet these requirements"

Contracting and subcontracting

Notably, the NIS Regulations are unlikely to require the same level of repapering as the GDPR. The non-prescriptive nature of the NIS Regulations and its related security requirements is, while peppered with uncertainty for organisations, a blessing in this regard.

For those organisations reluctant to re-open contractual negotiations, ensuring an open dialogue with service providers combined with a comprehensive governance structure and robust organisational security measures is one way to mitigate these risks. An open dialogue is also relevant to coordinating voluntary disclosures to the NCSC and ensuring information sharing with the NCSC is managed strategically.

Unlike the GDPR, the NIS Regulations do not expressly address subcontracting. In practice, both OES and RDSPs that use subcontractors must satisfy themselves that their subcontractors are able to fulfil the security requirements under the NIS Regulations; the OES/RDSP is ultimately responsible for its subcontractors' actions. OES/RDSPs should also ensure that audit provisions in subcontracting agreements are wide enough to allow a competent authority to conduct inspections, as required by the NIS Regulations (Regulation 16(1), 16(2)).

OES/RDSPs should consider whether to impose specific obligations on service providers to notify the OES/ RDSP of any incidents that may trigger notification in order that the OES/RDSP can satisfy its incident reporting requirements under the NIS Regulations.

In practice, many organisations will be aware of any "significant/ substantial impact on the continuity of the services" even without a formal notification provision and/ or may already have terms in the contract which are triggered by outages of any nature, e.g. incident reporting obligations, business continuity provisions and security governance forums. Therefore, unlike the GDPR, a standard form appendix may not be an apt way of meeting NIS Regulations requirements and a more tailored approach may be more appropriate.

Liability

Critically, liability for failing to notify the competent authority of a breach remains the sole liability of the relevant OES/ RDSP. Therefore, where service providers are used, the OES/ RDSP may seek to include robust indemnities for any fines incurred as a result of a failure by the service provider. Conversely, service providers to OES/ RDSP will be wary of accepting liabilities for a regulation which, but for their relationship with the OES/ RDSP, would not apply to that service provider. As with any liability discussion, commercial considerations and negotiating leverage will be key.

Security due diligence

OES/RDSPs should consider whether to enhance security due diligence of their service providers as a result of the NIS Regulations.

Many organisations that strengthened their due diligence processes prior to the implementation of the GDPR may have sufficient measures in place to ensure they can meet security requirements under both regimes. However, others may need to ensure they build additional steps into the security review process to ensure they can satisfy themselves that the third parties they rely on are able to meet their obligations under the NIS Regulations. RDSPs should also be prepared to answer similar questions from OES.

Internal policies and procedures

Organisations should review current incident response plans to reflect the requirements of the NIS Regulations. For many who went through this process less than a year ago for the GDPR, this will be a case of extending existing plans and processes to cover non-personal data and rolling out further staff- training regarding the expanded scope of reporting obligations.

One issue for OES/RDSPs to consider is whether reporting an incident under the GDPR, if the NIS Regulations are not directly triggered, could lead an organisation to inadvertently highlight its non-compliance with the security elements of the NIS Regulations. Although the Government has expressly stated that organisations should not be fined twice, it has not precluded the possibility of fining organisations under different regimes in relation to the same event, to the extent the fine relates to different aspects of the wrongdoing and has different impacts. OES and RDSPs should therefore ensure robust policies and procedures are in place to mobilise a strategic incident response committee in the event such a situation arises.

What can OES and RDSPs expect next?

The NIS Regulations reflect an increasing focus on improving the security of the systems and the networks that underpin our economy. OES and RDSPs must assess now whether they are caught by the NIS Regulations and must act quickly to ensure they are compliant.

As regulatory oversight becomes more significant and more intrusive, and with fines of up to £17 million, organisations should not underestimate the potential implications of the NIS Regulations.

Fiona Maclean
Olga Phillips
Latham & Watkins LLP
fiona.maclean@lw.com
olga.phillips@lw.com