New cyber rules apply from today: what should you do to comply?

10 May 2018

UK implementation of NIS Directive

The Network and Information System Regulations 2018 (the 'Regulations') were laid before Parliament on 20th April and apply in the UK from today. They implement the NIS Directive and impose obligations on Operators of Essential Services ('OES') and Relevant Digital Service Providers (RDSPs).

In this briefing we focus on what this means for OES: looking at some of the steps they can take now to comply, before setting out the obligations and enforcement methods they face.

Purpose of the new law

The National Cyber Security Centre (NCSC) has said '[t]he magnitude, frequency and impact of network and information system security incidents is increasing' and events such as the 2017 WannaCry ransomware attack demonstrate the impact such incidents can have. The Regulations are therefore intended to improve the security of these systems across the UK and increase co-operation through the EU. Security in this context includes cyber security, as well as other threats affecting IT, such as power failures, hardware failures and environmental hazards.

The Regulations impose security and breach notification obligations on OES (and RDSPs, who are outside the scope of this note) and appoint sector specific regulators (known as designated competent authorities) to enforce these.

Operators in the energy, transport, health, drinking water and digital infrastructure sectors who meet certain conditions and thresholds are within scope. In addition, competent authorities can designate that operators who do not meet the required thresholds are OES in certain circumstances.

What steps should an OES take now to comply?

- Check if you are in-scope and notify if you are

  The first thing to do is check if you fall within the sector and threshold criteria set out in the Regulations. If you do, you have three months (until 10 August) to notify your competent authority of that fact. We are currently helping potential OES determine whether they are within scope, and have produced a guide to assist clients with this process.

- Prepare representations if you do not meet thresholds but worry you may be designated

  If you do not meet the thresholds, but are concerned that the nature of your services are such that you may be designated as an OES by the competent authority, consider whether to start preparing any written representations now. Before designating an OES, competent authorities can request information or invite representations from the prospective OES, and it may be beneficial to prepare for this.

- Ensure you have sufficient security measures and breach notification procedures in place

  Your GDPR preparations should assist with this process, although it is important to appreciate the differences between the two regimes. For example, the focus of the two regimes is different (one on personal data, the other on system security and service continuity) as are some of the details around the security and breach notification obligations. You must therefore ensure that your security measures and internal processes and procedures around breach notification are wide enough to cover both regimes, and work together if both are triggered.

- Don't forget your supply chain

  Unlike the GDPR, the NIS regime does not expressly cover sub-contracting, but in practice it is likely OES may want to ensure that their suppliers have sufficient security protections in place, and notify them of any incidents to enable them to satisfy their breach notification requirements. OES should also check that the audit provisions in their supply arrangements are wide enough to allow an OES competent authority to obtain the information and access they may request in the event of an inspection.

Key points to note for OES

Who is in scope?

- Operators in the energy, transport, health, drinking water and digital infrastructure sectors who meet certain conditions and thresholds are automatically deemed to be designated as an OES. They must notify their competent authority of that fact before 10th August 2018 or, if they fall within scope once the Regulations are already in operation, three months after they fall within scope.

- The competent authorities must keep a list of all OES, which will be reviewed on 9 May 2020 and at regular intervals (at least biannually) following that.

- Competent authorities also have the power to add operators of essential services that do not meet the thresholds to their list or delete organisations from it (revoking their deemed designation). This largely depends (subject to various criteria and factors) on whether an incident affecting the provision of that essential service by that organisation is likely (or not) to have a significant disruptive effect on the provision of the essential service. An OES designation may also be revoked if the conditions set out in the Regulations are no longer met, or if another Member State requests revocation and the competent authority agrees with such request.

- Competent authorities must consult with relevant authorities in another Member State before adding an organisation as an OES if that organisation already provides an essential service in that other Member State.

Security and breach obligations

- OES must take appropriate and proportionate technical and organisational measures to manage the risks posed to their network and information systems and to prevent and minimise the impact of any incidents. This includes having 'regard' to any relevant guidance issued and the state of the art. The NCSC produced general guidance this January to help organisations comply with their security obligations, and specific competent authorities are also releasing guidance (for example OFCOM released guidance for the digital infrastructure sector on 8 May). The NCSC guidance is based around the 14 key security principles that were set out in the Government's NIS consultation and its response (and for more detail, see our articles on the consultation and response).

- OES must also notify their competent authority (without undue delay, and within 72

hours) about any incident which has a significant impact on the continuity of the essential service they provide (an 'NIS incident'). Again OES must have regard to any relevant guidance. Competent authorities must share this information with the national Computer Security Incident Response Team (or 'CSIRT', which in the UK is the NCSC) and either the regulator or CSIRT may (following consultation with that OES) inform the public about the NIS incident if necessary.

Enforcement and Penalties

- A regulator may serve an information notice on an organisation, requiring it to provide information, both to help it assess whether that organisation should be an OES (in which case it may take the form of a general request for a certain category of persons/organisations) and to help it assess the security of that OES.

- Regulators also have the power to:

    - inspect/audit, at the OES's cost, compliance with the security and breach notification obligations (either themselves, through an appointed person or by directing an OES to appoint an approved person). The audit right is wide, requiring the OES to co-operate and provide access to premises, documentation (which can also be copied and removed) and people. The competent authority also has the freedom to appoint auditors on such terms and in such a manner as it considers appropriate;

    - serve an enforcement notice for breach of duties (for example around security, incident notification or directions to appoint an auditor). This may contain any steps which must be taken to rectify an alleged failure, and how and when an OES can make representations about the content of the notice; and

    - fine OES who have received an enforcement notice and have failed to: (i) take the required steps to rectify their failure within the specified time period; or (ii) satisfy the competent authority with their representations. Fines must be appropriate and proportionate and accord with the limits set out in the Regulations (which maintain the £17 million upper limit discussed in the Government's consultation response but also contain new thresholds – see box below).

Fine (not to exceed…)	Criteria
£1,000,000	Any contravention which could not cause a NIS incident
£3,400,000	Material contravention which has/could cause incident resulting in reduction of service for a significant period
£8,500,000	Material contravention which has/could cause incident resulting in disruption of service for a significant period
£17,000,000	Material contravention which has/could cause incident resulting in immediate threat to life or significant adverse impact on UK economy

- OES can challenge a designation decision or penalty decision by requesting (in writing and within 30 days of receipt of the decision) an independent review.

- Any enforcement action taken must be reasonable and proportionate, having regard to a number of factors, including whether the contravention is also liable to enforcement under another enactment. The Government already confirmed in its consultation process relating to the Regulations that 'double jeopardy' (for example being fined under both the NIS and GDPR regimes for the same

incident) could not be eliminated completely without undermining either the NIS or other regime. However, it promised to include wording in the Regulations to encourage competent authorities to work with other regulators to determine the best approach to take.

Fees

OES may have to pay a competent authority (in its capacity as an enforcement authority) a fee to recover the reasonable costs incurred in carrying out a NIS function in relation to that OES.

Comment

Cyber threats and cyber regulation are both on the increase making now an interesting time for those advising on cyber risk. It is a threat which is unlikely to diminish, with the NCA's recent report 'The Cyber Threat to UK Business 2017-18' citing data breaches (and the impact of the GDPR), cryptojacking, supply chain compromises, increased use of worms, the internet of things and cloud security as key future threats. However, the guidance and advice available to tackle the threat is also increasing, and with many cyber criminals still exploiting long-standing and well-known vulnerabilities, understanding the risk, and getting the basics right, is now more important than ever.

This article was written by Rob Sumroy (Partner) and Natalie Donovan (PSL) from Slaughter and May's cyber advisory team. For more information contact Rob, Natalie or your usual Slaughter and May contact

Our cyber advisory team provides hands-on support to your internal stakeholders in the event of an attack, guiding you through this critical time, from your immediate response to designing a longer-term investigation, communication and response strategy. We can also help your business plan for and manage its cyber risk, working closely with you to develop tailored cyber risk management frameworks and training and response plans and helping you to mitigate cyber risk generally in your business.

Rob Sumroy
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Natalie Donovan
T +44 (0)20 7090 4058
E natalie.donovan@slaughterandmay.com