UK updates plans for the NIS Directive

January 2018

This week the Government took a further step toward implementing the NIS Directive, publishing the response to its summer consultation on UK implementation.

The EU's Security of Network and Information Systems (NIS) Directive is designed to improve the security and resilience of Europe's essential services, and imposes new security and incident notification obligations on operators of essential services and certain digital service providers. For more detail on the NIS Directive and the original consultation see our article: Regulating Cyber: the UK's plans for the NIS Directive.

While the consultation response states that there was broad support for the UK's implementation plans, it also details changes to some key areas. These include:

- **Clarifying which organisations are covered by the new regime** - this includes clarifying the thresholds required to identify 'Operators of Essential Services' and providing additional guidance on the definitions of 'Digital Service Providers'. While some respondents called on the Government to widen the scope of sectors covered by the NIS Directive, this will remain unchanged. The water, energy, digital infrastructure, health and transport sectors are therefore in scope, while banks are still excluded (despite being listed in the NIS Directive). The Government plans to conduct a post-implementation review three years after the legislation comes into effect, and any decision to extend the scope of the legislation would be considered at that time.

- **Providing more detail on the regulatory function** - the Government plans to maintain the multiple regulator (or 'Competent Authority') approach suggested in its initial consultation, with each sector being assigned a designated Competent Authority. The response provides more detail on the role of the Competent Authority and discusses that powers may be delegated to agencies. It also acknowledges a need for clarification on how Competent Authorities will interact with each other and across other regimes such as the GDPR. Further guidance will be provided (before May, when both the GDPR and NIS Directive will apply) to assist Competent Authorities to carry out their functions.

- **Confirming the role of the National Cyber Security Centre (NCSC) -** this is limited to providing guidance and incident response capability regarding cyber security (although the scope of the Directive is wider than cyber). It would not be appropriate for the NCSC to act as a regulator.

- **Reviewing the security principles** – the Government does not intend to fundamentally change its approach, but has slightly amended the wording of some of the security principles attached to the consultation. It is committed to an outcome-based approach to implementation (which allows organisations to make judgments based on their own risk management approach). Organisations are also free to decide how best to ensure appropriate measures are flowed down their supply chain (although supply chain security is included in NCSC guidance).

- **Simplifying the incident response regime -** clearer guidance and actual thresholds will help determine what constitutes a reportable incident (which may differ by sector). The incident reporting structure has also changed to distinguish 'incident response' (a support function where the Government can provide assistance) from 'incident reporting' (which is more of a regulatory notification process). The Government originally proposed a 72 hour incident notification timescale, to keep in-line with the GDPR notification requirements. This has been tweaked, so that it now tracks the GDPR wording "without undue delay and, where feasible, no later than 72 hours after having become aware of an [incident]."

- **Setting out the expectations on organisations within the first year -** the Government acknowledges that it will take a number of years to improve the security of the network and information systems of the UK's essential services. Competent Authorities will initially work collaboratively with industry to develop a detailed picture of the current levels of security, and it is expected the NCSC's Cyber Assessment Framework (which is due to be published this Spring) will form the basis of these assessments. They will also consider how long an organisation has had to implement the requirements of the regime when deciding whether to take regulatory action. However, the Government balances this collaborative message with confirmation that (even in the first year) Competent Authorities will have the power to issue penalties where significant compliance issues exist and no active effort is being taken to remedy them.

- **Simplifying the penalty regime -** this was originally linked to the GDPR fines, with two bands of fines and the inclusion of caps based on global turnover. Following significant feedback, the revised approach includes only one cap of £17 million (removing reference to global turnover). This is designed to still link to the GDPR (tracking the higher band of fines in the GDPR), although a breach of the security obligations under the NIS regime could result in a higher fine than under the GDPR (which only applies the lower €10m or 2% of global turnover threshold to such breaches). The £17 million maximum limit would only be reserved for the most severe cases.

The consultation report sets out some important changes to the proposals which should help organisations understand more clearly whether the new regime will apply to them, and how it will work in practice. It also addresses (while failing to provide total comfort on) one of the main concerns which arose from the initial plans – 'double jeopardy'. In particular, organisations were concerned they may face penalties under both the NIS and GDPR regimes which could involve potentially huge fines. Where different regimes apply, Competent Authorities must have regard to this, and will be encouraged to work with other regulators to determine what approach to take. Any penalty issued must also be proportionate and appropriate. However, the Government does recognise that there may be reasons for organisations to be penalised under both regimes (for example, where they relate to different aspects of the same wrongdoing). Consequently 'double jeopardy' (whether in relation to the GDPR or other regulatory regimes) cannot be completely removed.

This article was written by Duncan Blaikie and Natalie Donovan of Slaughter and May's Cyber Team.

In our cyber advisory unit we have experts from across the firm helping clients understand and mitigate cyber risks, and prepare for and respond to cyber-attacks.

For further information, please contact your usual Slaughter and May contact, or any of the following:

Duncan Blaikie
T +44 (0)20 7090 4275
E duncan.blaikie@slaughterandmay.com

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

Date January 2018