Press release: New fines for essential service operators with poor cyber security

- Fines could be as much as £17 million or 4 per cent of global turnover
- NIS Directive will help make UK most secure place to live and do business online

Organisations who fail to implement effective cyber security measures could be fined as much as £17 million or 4 per cent of global turnover, as part of plans to make Britain's essential networks and infrastructure safe, secure and resilient against the risk of future cyber attacks.

The plans are being considered as part of a consultation launched today by the Department for Digital, Culture, Media and Sport to decide how to implement the Network and Information Systems (NIS) Directive from May 2018.

Fines would be a last resort, and they will not apply to operators that have assessed the risks adequately, taken appropriate security measures, and engaged with competent authorities but still suffered an attack.

The NIS Directive relates to loss of service rather than loss of data, which falls under the General Data Protection Regulations (GDPR).

It will help make sure UK operators in electricity, transport, water, energy, transport, health and digital infrastructure are prepared to deal with the increasing numbers of cyber threats. It will also cover other threats affecting IT such as power failures, hardware failures and environmental hazards.

Minister for Digital Matt Hancock said:

> We want the UK to be the safest place in the world to live and be online, with our essential services and infrastructure prepared for the increasing risk of cyber attack and more resilient against other threats such as power failures and environmental hazards.
>
> The NIS Directive is an important part of this work and I encourage all public and private organisations in those sectors to take part in this consultation so together we can achieve this aim.

The NIS Directive, once implemented, will form an important part of the Government's five-year £1.9 billion National Cyber Security Strategy. It will compel essential service operators to make sure they are taking the necessary action to protect their IT systems.

The Government is proposing a number of security measures in line with

existing cyber security standards.

Operators will be required to develop a strategy and policies to understand and manage their risk; to implement security measures to prevent attacks or system failures, including measures to detect attacks, develop security monitoring, and to raise staff awareness and training; to report incidents as soon as they happen; and to have systems in place to ensure that they can recover quickly after any event, with the capability to respond and restore systems.

Any operator which takes cyber security seriously should already have such measures in place.

The Government is fully committed to defending against cyber threats and a five-year National Cyber Security Strategy (NCSS) was announced in November 2016, supported by £1.9 billion of transformational investment. The strategy includes opening the National Cyber Security Centre and offering free online advice as well as training schemes to help businesses protect themselves.

NCSC CEO Ciaran Martin said:

> We welcome this consultation and agree that many organisations need to do more to increase their cyber security.
>
> The NCSC is committed to making the UK the safest place in the world to live and do business online, but we can’t do this alone.
>
> Everyone has a part to play and that’s why since our launch we have been offering organisations expert advice on our website and the Government’s Cyber Essentials Scheme.

The consultation proposes similar penalties for flaws in network and information systems as those coming for data protection with the General Data Protection Regulation, due to be in force by May 2018. Failure to implement effective security could see penalties as large £17 million or 4 per cent of global turnover.

The Government will shortly hold workshops with operators so they can provide feedback on the proposals.

Notes to editors

For media enquiries please contact the DCMS News and Communications team on 020 7211 2210 or out of hours on 07699 751153.

- The consultation documents are available online.

- The Government has committed to NIS Directive and is consulting on a number of issues:

- The essential services the directive needs to cover
- The penalties
- The competent authorities to regulate and audit specific sectors
- The security measures we propose to impose
- Timelines for incident reporting;

- How this affects Digital Service Providers

- This initiative is part of the Government’s £1.9 billion investment to significantly transform the UK’s cyber security. The 2016-2021 National Cyber Security Strategy sets out how the UK Government will deliver a UK that is secure and resilient to cyber threats; prosperous and confident in the digital world. The National Cyber Security Programme managed by the Cabinet Office coordinates the work undertaken to implement the UK’s National Cyber Security Strategy.