Press release: Government acts to protect essential services from cyber attack

- Organisations risk fines of up to £17 million if they do not have effective cyber security measures
- Sector-specific regulators will be appointed so essential services are protected
- National Cyber Security Centre today publishes new guidance for industry

Bosses of Britain's most critical industries are being warned to boost cyber security or face hefty fines for leaving themselves vulnerable to attack following our consultation.

Energy, transport, water and health firms could be fined up to £17million if they fail to have the most robust safeguards in place against cyber attack.

New regulators will be able to assess critical industries to make sure plans are as robust as possible.

A simple, straightforward reporting system will be set up to make it easy to report cyber breaches and IT failures so they can be quickly identified and acted upon.

This will ensure 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 outages, hardware failures and environmental hazards. Under the new measures recent cyber breaches such as WannaCry and high profile systems failures would be covered by the Network and Information Systems (NIS) Directive.

These incidents would have to be reported to the regulator who would assess whether appropriate security measures were in place. The regulator will have the power to issue legally-binding instructions to improve security, and – if appropriate – impose financial penalties.

Margot James, Minister for Digital and the Creative Industries, said:

> Today we are setting out new and robust cyber security measures to help ensure the UK is the safest place in the world to live and be online.
>
> We want our essential services and infrastructure to be primed and ready to tackle cyber attacks and be resilient against major disruption to services.

> I encourage all public and private operators in these essential sectors to take action now and consult NCSC's advice on how they can improve their cyber security.

The National Cyber Security Centre (NCSC), the UK's centre of cyber excellence established in 2017, has today published detailed guidance on the security measures to help organisations comply. These are based around 14 key principles set out in our consultation and government response, and are aligned with existing cyber security standards.

National Cyber Security Centre CEO Ciaran Martin said:

> Our new guidance will give clear advice on what organisations need to do to implement essential cyber security measures.
>
> Network and information systems give critical support to everyday activities, so it is absolutely vital that they are as secure as possible.

The new measures follow the consultation held last year by the Department for Digital, Culture, Media and Sport seeking views from industry on how to implement the NIS Directive from 10 May 2018.

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

Following the consultation, incident reporting arrangements have been simplified, with operators reporting to their Competent Authority. Penalties will be fixed at a maximum of £17 million and the new legislation will be made clearer for companies to know whether they have to comply with the NIS Directive.

The NIS Directive is an important part of the Government's five-year £1.9 billion National Cyber Security Strategy to protect the nation from cyber threats and make the UK the safest place to live and work online. It will ensure essential service operators are taking the necessary action to protect their IT systems.

Notes to editors