News story: Tough new rules to protect UK's critical infrastructure come into force

New measures to protect the nation's critical infrastructure and digital services from cyber attacks and computer network failure come into force today.

Bosses of firms in health, water, energy, transport and digital infrastructure will now be expected to have robust safeguards in place against cyber threats and report breaches and network outages to regulators within 72 hours or they face fines of up to £17 million.

The new law announced by Digital Minister Margot James will help reduce the number of damaging cyber attacks affecting the UK.

The National Cyber Security Centre, set up by the government in October 2016 as part of GCHQ, has already responded to more than 950 significant incidents, including WannaCry.

It will also give new regulators powers to assess critical industries and make sure plans are in place to prevent attacks.

The regulator will have the power to issue legally-binding instructions to improve security, and – if necessary – impose significant fines.

The legislation will also cover other threats affecting IT such as hardware failures and environmental hazards.

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

> It's vital that we put in place tough new measures to strengthen the UK's cyber security and make sure we are the safest place in the world to live and be online.
>
> Organisations must act now to make sure that they are primed and ready to stop potential cyber attacks and be resilient against major disruption to the services we all rely on.

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.

Incidents must be reported directly to the appropriate regulator. Where an incident has a cyber security aspect, organisations should contact the NCSC for support and advice. The NCSC will also act as the Single Point of Contact between the UK and EU Member States.

As the UK’s technical authority on cyber security, the NCSC is supporting competent authorities and has developed a set of 14 cyber security principles, as well as supporting guidance, to improve the cyber security of operators of essential services.

Ciaran Martin, Chief Executive of the NCSC, said:

> These new measures will help to strengthen the security of the UK’s infrastructure.
>
> By acting on the National Cyber Security Centre’s expert technical advice and reporting incidents, organisations can protect themselves against those who would do us harm.
>
> The UK government is committed to making the UK the safest place to live and do business online, but we can’t do this alone. Every citizen, business and organisation must play their part.

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.