# New laws proposed to strengthen the UK's resilience from cyber attack

- More firms providing essential digital services should follow strict cyber security duties with large fines for non-compliance

- Other legislative proposals include improved incident reporting and driving up standards in the cyber security profession

New laws are needed to drive up security standards in outsourced IT services used by almost all UK businesses, the government says.

Other proposals being published today include making improvements in the way organisations report cyber security incidents and reforming legislation so that it is more flexible and can react to the speed of technological change.

The UK Cyber Security Council, which regulates the cyber security profession, also needs powers to raise the bar and create a set of agreed qualifications and certifications so those working in cyber security can prove they are properly equipped to protect businesses online.

The plans follow recent high-profile cyber incidents such as the cyber attack on SolarWinds and on Microsoft Exchange Servers which showed vulnerabilities in the third-party products and services used by businesses can be exploited by cybercriminals and hostile states, affecting hundreds of thousands of organisations at the same time.

They also follow an increase in ransomware threats to organisations, including some in critical national infrastructure such as the Colonial Pipeline attack in the US.

Minister of State for Media, Data, and Digital Infrastructure, Julia Lopez, said:

> Cyber attacks are often made possible because criminals and hostile states cynically exploit vulnerabilities in businesses' digital supply chains and outsourced IT services that could be fixed or patched.
>
> The plans we are announcing today will help protect essential services and our wider economy from cyber threats
>
> Every UK organisation must take their cyber resilience seriously as we strive to grow, innovate and protect people online. It is not an optional extra.

To make the UK more secure and help prevent these types of attacks the government is aiming, through new legislation, to take a stronger approach to getting at-risk businesses to improve their cyber resilience as part of its new £2.6 billion National Cyber Strategy.

Updating the NIS regulations

Network and Information Systems (NIS) Regulations came into force in 2018 to improve the cyber security of companies which provide essential services such as water, energy, transport, healthcare and digital infrastructure. Organisations which fail to put in place effective cyber security measures can be fined as much as £17 million.

The government wants to update the NIS Regulations and widen the list of companies in scope to include Managed Service Providers (MSPs) which provide specialised online and digital services. MSPs include security services, workplace services and IT outsourcing. These firms are crucial to boosting the growth of the country's £150.6 billion digital sector and have privileged access to their clients' networks and systems.

The NIS regulations require essential service providers to undertake risk assessments and put in place reasonable and proportionate security measures to protect their network. They have to report significant incidents and have plans to ensure they quickly recover from them.

While the regulations apply to some digital services such as online marketplaces, online search engines and cloud computing, there has been an increase in the use and dependence on digital services for providing corporate needs such as information storage, data processing and running software.

Research by the Department for Digital, Culture, Media and Sport shows only 12 per cent of organisations review the cyber security risks coming from their immediate suppliers and only one in twenty firms (5 per cent) address the vulnerabilities in their wider supply chain.

The government is today launching a consultation on amending the NIS regulations which includes proposals to:

- Expand the scope of the NIS Regulations' to include managed services. These are typically provided by companies which manage IT services on behalf of other organisations.

- Require large companies to provide better cyber incident reporting to regulators such as Ofcom, Ofgem and the ICO, including a requirement to notify regulators of all cyber security attacks they suffer, not just those which impact their services.

- Give the government the ability to future-proof the NIS regulations by updating them and if necessary bring into scope more organisations in

the future which provide critical support to essential services.

- Transfer all relevant costs incurred by regulators for enforcing the NIS regulations from the taxpayer to the organisations covered by the legislation to create a more flexible finance system and reduce the taxpayers' burden.

- Update the regulatory regime so the most critical digital service providers in the economy have to demonstrate proactively they are following NIS Regulations to the ICO, and take a more light-touch approach with the remaining digital providers.

NCSC Technical Director Dr Ian Levy, said:

> I welcome these proposed updates to the NIS regulations, which will help to enhance the UK's overall cyber security resilience.
>
> These measures will ensure that cyber security risks are properly managed by organisations and those on whom they rely.

Empowering the cyber security profession

Cyber security is a core part of the UK's booming tech sector which already has hundreds of successful cyber startups and more than a hundred tech 'unicorns' – companies worth more than £1 billion. As more people are drawn into cyber careers it can be difficult for businesses to know which skills to look for and whether a job candidate has those skills and the necessary qualifications or experience.

In March the government established and funded the UK Cyber Security Council, a new independent body to lead the cyber workforce and put it on a par with established professions such as engineering.

Today's proposals would give the council the ability to define and recognise cyber job titles and link them to existing qualifications and certifications. People would have to meet competency standards set by the council before they could utilise a specific job title across the range of specialisms in cyber security.

This would make it easier for employers to identify the specific cyber skills they need in their organisations and create clearer information on career pathways for young people as well as existing practitioners, without providing unnecessary barriers to entry and progression.

The proposals include the creation of a Register of Practitioners, similar to what exists in the medical and legal professions, setting out the practitioners who are recognised as ethical, suitably-qualified or senior.

Simon Hepburn, CEO, UK Cyber Security Council, said:

> The UK Cyber Security Council is delighted that these proposals recognise our cyber workforce lead role that will help to define and recognise cyber job roles and map them to existing certifications and qualifications.
>
> We look forward to being involved in and contributing to this important government consultation and would encourage all key stakeholders to participate too.

ENDS

Notes to Editors:

The consultations can be found here:

These consultations are part of the government's wider work on cyber resilience which is helping organisations across the economy adopt stronger cyber security measures. The consultation on the NIS Regulations follows a recent call for views which saw government proposals to boost the cyber security of UK's digital supply chains.

The work is part of the UK Government's ambition to maintain the UK's position as a leading democratic and responsible Cyber Power, outlined through the 2022 National Cyber Strategy, which was released on 15 December 2022.

The government is also publishing the 2022 Cyber Security Incentives and Regulation Review, which sets out how the government can strengthen cyber resilience, revealing UK organisations currently do not have enough robust measures to successfully defend against the rapidly increasing risk of cyber attacks.