# Businesses urged to boost cyber standards as new data reveals nearly a third of firms suffering cyber attacks hit every week

- New report today shows cyber attacks are becoming more frequent with organisations reporting more breaches over the last 12 months

- Data shows two in five businesses use a managed IT provider but only 13 per cent review the security risks posed by their immediate suppliers

Businesses and charities are being urged to strengthen their cyber security practices now as new figures show the frequency of cyber attacks is increasing.

Almost one in three businesses (31 per cent) and a quarter (26 per cent) of charities suffering attacks said they now experience breaches or attacks at least once a week.

Although the Cyber Security Breaches Survey 2022 report from the Department for Digital, Culture, Media and Sport (DCMS) revealed the frequency of cyber attacks is rising, the number of businesses which experienced an attack or breach remained the same as 2021 levels. Almost a third of charities (30 per cent) and two in five businesses (39 per cent) reported cyber security breaches or attacks in the last 12 months.

The National Cyber Security Centre (NCSC) has issued a note declaring it is not aware of any current specific cyber threats to UK organisations in relation to events around Ukraine, but is encouraging organisations to follow simple steps in its guidance to reduce the risk of falling victim to an attack.

Small businesses should adopt the Cyber Essentials scheme to protect against the most common cyber threats such as phishing attacks and use the Small Business Guide to improve cyber security practices. Larger organisations should use the Board Toolkit to get company executives to act on cyber resilience and charities should follow the Small Charity Guide to boost cyber security operations.

Cyber Minister Julia Lopez said:

> It is vital that every organisation take cyber security seriously as more and more business is done online and we live in a time of increasing cyber risk.

> No matter how big or small your organisation is, you need to take steps to improve digital resilience now and follow the free government advice to help keep us all safe online.

Following a wave of high profile attacks over the past year including on Kaseya, Colonial Pipeline and Microsoft Exchange, there has been increased attention on the cyber security of supply chains and digital services.

Four out of five senior managers (82 per cent) in UK businesses now see cyber security as a 'very high' or 'fairly high' priority, up from 77 per cent in 2021. This is a significant increase and the highest figure seen in any year of the cyber security breaches survey.

The report also found four in ten businesses (40 per cent) and almost a third of charities (32 per cent) were using at least one managed service provider but only 13 per cent of businesses reviewed the risks posed by immediate suppliers.

The government is aiming to strengthen critical businesses' cyber resilience by updating the Network and Information Systems (NIS) Regulations which set out cyber security rules for essential services such as water, energy, transport, healthcare and digital infrastructure.

This will make sure the legislation remains effective and keeps pace with technology. It includes proposals to expand the NIS Regulations to include managed service providers which essential and digital services depend on to operate, to minimise the risk of attacks.

The government is committed to protecting the UK from cyber threats, which is at the centre of its £2.6 billion National Cyber Strategy, by investing in cyber skills, expanding the country's offensive and defensive cyber capabilities, and prioritising cyber security in the workplace, boardrooms and digital supply chains.

ENDS

Notes to editors:

- The Cyber Security Breaches Survey is an Official Statistic and has been produced to the standards set out in the Code of Practice for Statistics.
- The Cyber Security Breaches Survey 2022 was carried out for DCMS by Ipsos MORI with the fieldwork conducted between October 2021 and January 2022.
- It is part of the government's National Cyber Strategy.