Press release: Almost half of UK firms hit by cyber breach or attack in the past year

- Firms holding personal data more likely to be attacked
- Most common attacks were fraudulent emails, followed by viruses and malware

The Cyber Security Breaches Survey 2017 reveals nearly seven in ten large businesses identified a breach or attack, with the average cost to large businesses of all breaches over the period being £20,000 and in some cases reaching millions. The survey also shows businesses holding electronic personal data on customers were much more likely to suffer cyber breaches than those that do not (51 per cent compared to 37 per cent).

The most common breaches or attacks were via fraudulent emails – for example coaxing staff into revealing passwords or financial information, or opening dangerous attachments – followed by viruses and malware, such as people impersonating the organisation online and ransomware.

Businesses also identified these common breaches as their single most disruptive breach, and the vast majority of them could have been prevented using the Government-backed, industry supported Cyber Essentials scheme, a source of expert guidance showing how to protect against these threats.

These new statistics show businesses across the UK are being targeted by cyber criminals every day and the scale and size of the threat is growing, which risks damaging profits and customer confidence.

The Government has committed to investing £1.9 billion to protect the nation from cyber attacks to help make the UK the safest place to live and do business online.

Business also has a role to play to protect customer data. The government offers free advice, online training and Cyber Essentials and Cyber Aware schemes.

The survey also revealed:

Of the businesses which identified a breach or attack, almost a quarter had a temporary loss of files, a fifth had software or systems corrupted, one in ten lost access to third party systems they rely on, and one in ten had their website taken down or slowed.

Firms are increasingly concerned about data protection, with the need to protect customer data cited as the top reason for investing by half of all firms who spend money on cyber security measures.

Following a number of high profile cyber attacks, businesses are taking the

threat seriously, with three quarters of all firms saying cyber security is a high priority for senior managers and directors; nine in ten businesses regularly update their software and malware protection; and two thirds of businesses invest money in cyber security measures.

Small businesses can also be hit particularly hard by attacks, with nearly one in five taking a day or more to recover from their most disruptive breach.

Areas where industry could do more to protect itself include around guidance on acceptably strong passwords (only seven in ten firms currently do this), formal policies on managing cyber security risk (only one third of firms), cyber security training (only one in five firms), and planning for an attack with a cyber security incident management plan (only one in ten firms).

All businesses which hold personal data will have to make sure they are compliant with the new General Data Protection Regulation (GDPR) legislation from May 2018. This will strengthen the right to data protection, which is a fundamental right, and allow individuals to have trust when they give their personal data.

The Cyber Breaches Survey is part of the Government's five-year National Cyber Security Strategy to transform this country's cyber security and to protect the UK online. As part of the strategy, the Government recently opened the new National Cyber Security Centre (NCSC), a part of GCHQ.

One of the key objectives of the NCSC is to increase the UK's cyberspace resilience by working with and providing expert advice tailored to organisations and businesses in every sector of the UK economy and society.

Ciaran Martin, CEO of the National Cyber Security Centre, said:

> UK businesses must treat cyber security as a top priority if they want to take advantage of the opportunities offered by the UK's vibrant digital economy.
>
> The majority of successful cyber attacks are not that sophisticated but can cause serious commercial damage. By getting the basic defences right, businesses of every size can protect their reputation, finances and operating capabilities.
>
> Cyber Essentials, technical advice on CiSP and regularly updated guidance on the NCSC website offers companies, big and small, simple steps that can significantly reduce the risk of a successful attack.

ENDS

Notes to editors:

1. Read the Cyber Security Breaches Survey 2017

2. The Cyber Security Breaches Survey is an Official Statistic and has been produced to the standards set out in the Code of Practice for Official Statistics.

3. The survey was carried out by Ipsos MORI in partnership with the Institute for Criminal Justice Studies at the University of Portsmouth.

4. The survey fieldwork has been endorsed by the Association of British Insurers (ABI), the Confederation of British Industry (CBI), the Federation of Small Businesses (FSB), ICAEW and techUK.

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

6. The Cyber Security Breaches Survey comes on the back of recent Government action to boost cyber security, including:
    - Strengthening the Cyber Essentials scheme, which protects organisations against the most common online threats. A number large firms, such as BT, Airbus, Vodafone, Astra Zeneca and Barclays, are also encouraging their suppliers to adopt the scheme.
    - New measures to support the UK's £22 billion cyber security industry, including boosting the cyber ecosystem by helping academics commercialise their research and funding an early stage accelerator programme.
    - Funding Academic Centres of Excellence to specialise in developing the latest cyber security techniques and contribute to the UK's increased knowledge and capability in this field.
    - Working to develop cyber innovation centres in London and Cheltenham to support entrepreneurs and innovators to develop new cyber security products and businesses.
    - Developing the cyber security skills pipeline so the UK has the people it needs now and in the future, including a cyber security apprenticeships scheme, a cyber schools programme and a cyber retraining programme to help fast-track professionals into the industry.
    - The popular CyberFirst programme is inspiring, encouraging and developing a cyber-savvy cohort of students to help protect the UK's digital society.
    - The Government is encouraging all firms to act: the 10 Steps to Cyber Security provides advice to large businesses, and the Cyber Essentials scheme is available to all UK firms. The Cyber Aware scheme (formerly Cyber Streetwise) aims to drive behaviour change

amongst small businesses and individuals, so that they adopt simple secure online behaviours to help protect themselves from cyber criminals.

7. Ipsos MORI surveyed 1,523 UK businesses (including 171 large businesses employing 250 or more staff) by telephone from 24 October 2016 to 11 January 2017.
    - Sole traders and public sector organisations were outside the scope of the survey, so were excluded. In addition, businesses with no IT capacity or online presence were deemed ineligible, which meant that a small number of specific sectors (agriculture, forestry, fishing, mining and quarrying) were excluded.
    - The data is weighted to be representative of all UK businesses (who were in scope).
    - A total of 30 in-depth interviews were undertaken in January and February 2017 to follow up businesses that participated in the survey.