CYBER SECURITY BREACHES SURVEY 2017 | GENERAL BUSINESS FINDINGS

The Cyber Security Breaches Survey measures how well UK businesses approach cyber security, and the level, nature, and impact of cyber attacks on businesses.

Just under half (46%) of all businesses identified at least one breach or attack in the last year. The most common types of breaches related to staff receiving fraudulent emails (72% of those who identified a breach or attack), followed by viruses and malware (33%), people impersonating the organisation online (27%) and ransomware (17%).

Breaches were often linked to human factors, highlighting the importance of staff awareness and vigilance. However, few businesses currently provide staff with cyber security training (20%) or have formal policies in this area (33%). Technical controls are also important, with nine in ten businesses regularly updating their software and malware protections, configuring firewalls or securely backing up their data, but only around two-thirds (69%) having guidance on acceptably strong passwords.

- The main report detailing all the survey findings is available at: **www.gov.uk/government/statistics/cyber-security-breaches-survey-2017**
- Further guidance on how businesses can protect themselves can be found on the National Cyber Security Centre website and GOV.UK website: **www.ncsc.gov.uk/guidance** and **www.gov.uk/government/collections/cyber-security-guidance-for-business**
- Information on Cyber Essentials can be found at: **www.cyberaware.gov.uk/cyberessentials/**

Technical note: Bases for graphics: 1,523 UK businesses (excluding agriculture, forestry and fishing businesses, and mining and quarrying businesses); 597 who say online services are not at all core to their business; 781 who identified a breach or attack in the last 12 months; 930 who spend money on cyber security. Fieldwork dates: 24 October 2016 to 11 January 2017. The data is weighted to be representative of UK businesses by size and sector.

Department for Culture Media & Sport

Ipsos MORI Social Research Institute

University of Portsmouth

● GENERAL BUSINESS FINDINGS ●

EXPERIENCE OF BREACHES

46% of UK businesses overall identified cyber security breaches or attacks in the last 12 months

45% among micro/small businesses

66% among medium/large businesses

41% among businesses who say online services are not at all core to their business

AMONG THE 46% WHO IDENTIFIED A BREACH OR ATTACK

23% Had a temporary loss of files

20% Had software or systems corrupted

10% Had a permanent loss or change of files or personal data

9% Lost access to third-party systems they rely on

9% Had their website slowed or taken down

6% Had money, assets or intellectual property stolen

PRIORITISING CYBER SECURITY

74% of UK businesses where directors or senior management say cyber security is a high priority

67% of UK businesses overall spend money on cyber security

Among the 67%, the top (unprompted) reasons for spending in this area were: