CYBER SECURITY BREACHES SURVEY 2018

MICRO/SMALL BUSINESS FINDINGS

The Cyber Security Breaches Survey is an Official Statistic, measuring how organisations in the UK approach cyber security and the impact of breaches.

- The directors or senior management in three-quarters (74%) of micro/small businesses say that cyber security is a high priority.
- Two in five micro/small businesses (42%) identified at least one breach or attack in the last 12 months, which is no lower than in the 2017 survey.
- In almost one-fifth (17%) of cases, it took these businesses a day or more to recover from the breach.
- Seven in ten micro/small businesses (70%) think that the staff dealing with cyber security have the capacity to manage it effectively, compared to eight in ten medium/large businesses (81%).
- However, micro/small businesses are less likely than medium/large businesses to:
  - have sought any information, advice or guidance about cyber security (58%, vs. 79% of medium/large businesses)
  - have formal cyber security policies (26% vs. 62%)
  - have any cyber security training (19% vs. 47%).
- For the full survey report, plus previous reports of the Cyber Security Breaches Survey, visit www.gov.uk/government/collections/cyber-security-breaches-survey.
- For further cyber security guidance for your business or charity, visit the National Cyber Security Centre website: www.ncsc.gov.uk/guidance. This includes the Cyber Security Small Business Guide drafted especially for micro/small businesses: www.ncsc.gov.uk/smallbusiness.

Technical note

Bases for text and graphics: 1,004 micro/small UK businesses with 1 to 49 staff (excluding agriculture, forestry and fishing businesses); 515 medium/large businesses with 50 or more staff for comparison; 422 small/medium businesses that identified a breach or attack in the last 12 months; 254 that have none of the governance or risk management arrangements listed in the survey (board members with cyber security responsibilities, outsourced cyber security providers, formal cyber security policies, business continuity plans or staff assigned to information security or governance).

Fieldwork dates: 9 October 2017 to 14 December 2017.

Data are weighted by size and sector to be representative of UK businesses. Where findings do not add to 100%, this is due to the exclusion of "don't know" responses and rounding.

Department for Digital, Culture, Media & Sport

Ipsos MORI Social Research Institute

University of Portsmouth

MICRO/SMALL BUSINESS FINDINGS

EXPERIENCE OF BREACHES

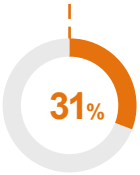
42% of micro/small businesses identified cyber security breaches or attacks in the last 12 months.

£894 was the average (mean) cost of all breaches identified in the last 12 months.

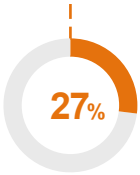
17% took a day or more to recover from their most disruptive breach.

AMONG THE 42% THAT IDENTIFIED BREACHES OR ATTACKS IN THE LAST 12 MONTHS:

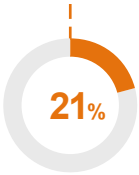
36% needed new measures to prevent or protect against future breaches.



31% used additional staff time to deal with breaches.



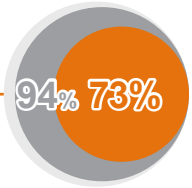
27% said that breaches stopped staff carrying out day-to-day work.

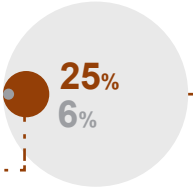


21% said that breaches incurred further recovery or repair costs.

TAKING PREVENTATIVE ACTION

Micro/small businesses with any cyber security governance or risk management measures in place (vs. medium/large businesses)

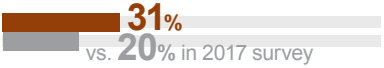




Micro/small businesses with no cyber security governance or risk management measures in place (vs. medium/large businesses)

AMONG THE 25% WITH NO RISK MANAGEMENT MEASURES IN PLACE, TOP (UNPROMPTED) REASONS GIVEN IN THE 2018 SURVEY ARE:

not considering cyber security a priority.



thinking their business is too small/insignificant.

55% of micro/small businesses have carried out any health checks, risk assessments or audits to identify cyber security risks.

9% of micro/small businesses have cyber security insurance, with a further 12% having considered getting this.

12% of micro/small businesses have a formal cyber security incident management process in place.