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

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.

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

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)

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

said that breaches incurred further recovery or repair costs.

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

used additional staff time to deal with breaches.

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

55% of micro/small businesses have cyber security insurance, with a further 12% having considered getting this.

Among the 42% that identified breaches or attacks in the last 12 months:

used additional staff time to deal with breaches.

needed new measures to prevent or protect against future breaches.

said that breaches incurred further recovery or repair costs.

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

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

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.

Among the 42% that identified breaches or attacks in the last 12 months:

said that breaches incurred further recovery or repair costs.

used additional staff time to deal with breaches.

needed new measures to prevent or protect against future breaches.

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

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.

Among the 42% that identified breaches or attacks in the last 12 months:

used additional staff time to deal with breaches.

needed new measures to prevent or protect against future breaches.

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

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.

Among the 42% that identified breaches or attacks in the last 12 months:

used additional staff time to deal with breaches.

needed new measures to prevent or protect against future breaches.

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

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.