CYBER SECURITY BREACHES SURVEY 2019

MICRO AND SMALL BUSINESS FINDINGS

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

In this year's survey, 31% of micro and small businesses identified breaches or attacks. This is lower than in 2018 (when it was 42%). Nonetheless, cyber attacks continue to cause problems for smaller businesses. Among this 31%:

- 19% lost files or network access
- 10% had their website slowed or taken down
- 9% had software or systems corrupted or damaged.

More micro and small businesses say cyber security is a high priority now (78%, vs. 74% in 2018). But this is still lower than for medium (92%) and large firms (95%). While attitudes have changed, micro and small firms could still do more to protect themselves:

- More now have cyber security policies (32%, vs. 26% in 2018). But this is lower than medium (71%) and large firms (74%). Among those without policies or other forms of risk management, reasons include thinking they are too small (35%), not prioritising cyber security (21%) and not seeing it as a risk (19%).
- 77% believe the staff dealing with their cyber security have the necessary skills and knowledge. However, only 26% sent staff on cyber security training or conferences this year (vs. 19% in 2018).
- While most (88%) have heard of the General Data Protection Regulation (GDPR), relatively few are aware of the implications. These include potential fines and the need to report personal data breaches to the Information Commissioner's Office (ICO).

- For the full results, visit www.gov.uk/government/collections/cyber-security-breaches-survey.
- For further cyber security guidance for your business, visit the National Cyber Security Centre website: www.ncsc.gov.uk. This includes the Cyber Security Small Business Guide drafted especially for micro/small businesses: www.ncsc.gov.uk/collection/small-business-guide.

Technical note

Ipsos MORI carried out the telephone survey from 10 October to 20 December 2018.

Bases for text and graphics: 1,078 micro/small firms with 1 to 49 staff (excluding agriculture, forestry and fishing businesses); 347 that identified breaches or attacks in the last 12 months; 99 that lost data or assets after breaches; 238 without risk management or governance arrangements.

Data are weighted to represent UK businesses.

Department for Digital, Culture, Media & Sport

Ipsos MORI

UNIVERSITY OF PORTSMOUTH

EXPERIENCE OF BREACHES OR ATTACKS

Key: MICRO/SMALL BUSINESSES

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

15%
of micro/small businesses have a formal cyber incident management process

£3,650
is the average annual cost for those that lost data or assets after breaches

Among the 31% identifying breaches or attacks:

15%
took a day or more to recover from their most disruptive breach

63%
had their most disruptive breach reported by staff rather than by antivirus software

After their most disruptive breach:

- **19%** had extra staff training or communications
- **17%** installed new antivirus or anti-malware
- **17%** changed firewall or system configurations
- **29%** did nothing

IDENTIFYING RISKS

62%
of micro/small businesses have taken action to identify cyber risks in the last 12 months

For example among all micro/small businesses:

- **39%** have regular health checks
- **30%** conducted a cyber risk assessment
- **27%** conducted an internal audit
- **18%** conducted an external audit

GDPR AND CYBER SECURITY

88%
of micro/small businesses are aware of GDPR

58%
know they can be fined by the ICO for personal data breaches

45%
know they need to report personal data breaches to the ICO within 72 hours of discovery