CYBER SECURITY BREACHES SURVEY 2019

MEDIUM AND LARGE BUSINESS FINDINGS

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

This year's survey finds that 60% of medium firms and 61% of large firms have identified breaches or attacks. For large firms, this is lower than in 2018 (when it was 72%), but cyber attacks still cause problems for both medium and large businesses.

- Businesses of this size tend to pay particularly high costs when their defences are breached.
- Among those identifying breaches or attacks, 25% of medium firms and 20% of large firms have these at least once a week.

Directors in 92% of medium firms and 95% of large businesses say cyber security is a high priority. The majority of boards in these businesses are taking positive actions:

- 71% of medium firms and 74% of large firms have a cyber security policy.
- Most boards receive cyber security updates at least monthly, or after every breach (in 57% of medium firms and 58% of large firms).

The vast majority of medium (86%) and large firms (83%) believe the staff dealing with their cyber security have the necessary skills and knowledge.

The proportion offering relevant training is much lower, but has grown. This year, 54% of medium firms and 73% of large firms have sent staff on cyber security training or conferences (vs. 43% and 65% in 2018).

Many could also review their risk management approaches. Only 23% of medium firms and 40% of large firms have taken action towards all of the Government's 10 Steps to Cyber Security.

- 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.

Technical note

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

Bases for text and graphics: 281 medium firms with 50 to 249 staff and 207 large firms with 250 or more staff (all excluding agriculture, forestry and fishing businesses); 161 medium firms and 129 large firms that identified breaches or attacks in the last 12 months; 50 medium firms and 43 large firms that lost data or assets after breaches.

Data are weighted to represent UK businesses.

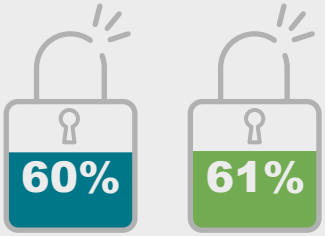
Department for Digital, Culture, Media & Sport

Ipsos MORI

UNIVERSITY OF PORTSMOUTH

EXPERIENCE OF BREACHES OR ATTACKS

Key: MEDIUM BUSINESSES
LARGE BUSINESSES

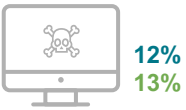


of medium/large businesses identified breaches or attacks in the last 12 months

£9,270
£22,700
is the average (mean) annual cost for medium/large businesses that lost data or assets after breaches

Among the 60%/61% identifying breaches or attacks:

23%
22%
lost files or network access



12%
13%
had software or systems corrupted or damaged

10%
12%
had their website slowed or taken down

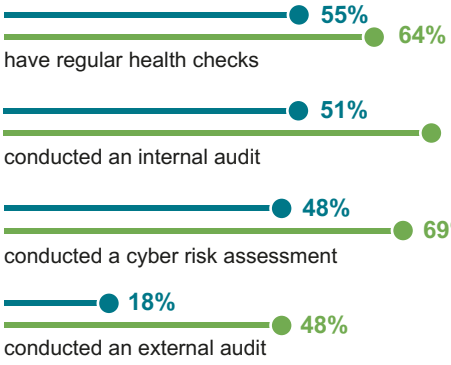
6
12
was the typical (median) number of breaches identified

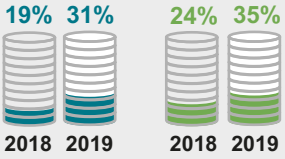
MANAGING CYBER RISKS

79%/93%
of medium/large businesses have taken action to identify cyber risks in the last 12 months

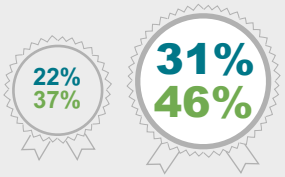
47%/59%
have board members with a cyber security brief

For example among all medium/large businesses:





have cyber insurance



have minimum cyber security standards for suppliers