CYBER SECURITY BREACHES SURVEY 2020

UK MICRO AND SMALL BUSINESS TRENDS

The Cyber Security Breaches Survey is an official statistic. Since 2016, it has measured how UK organisations approach cyber security, and the impact of breaches. This infographic shows the key findings for smaller businesses.

1.

Cyber attacks have become more frequent. Among the 46% of **micro** and **small** businesses identifying any breaches or attacks, more now experience them at least once a week (32%, vs. 22% in 2017).

2.

The nature of cyber attacks has evolved. Among those identifying breaches or attacks, 86% had phishing attacks (vs. 71% in 2017), 24% were impersonated and 18% had malware (including ransomware).

3.

Cyber security is increasingly important for smaller businesses. 79% of these businesses say that cyber security is a high priority for their management boards, up from 69% in 2016.

4.

Almost all smaller businesses report having technical controls. This includes having up-to-date malware protection (87%), network firewalls (82%), restricting IT admin rights (80%) and password policies (80%).

5.

Most smaller businesses are seeking information. 54% sought information in the last 12 months (vs. 43% in 2016). But just 16% have heard of the National Cyber Security Centre's Small Business Guide.

Technical note: Ipsos MORI carried out a telephone survey of 919 micro and small businesses with 1 to 49 staff (excluding sole traders, and agriculture, forestry and fishing businesses) from 9 October to 23 December 2019. This included 443 micro and small businesses that identified a breach or attack in the last 12 months. N.B. this year's survey omitted the denial-of-service attacks category that had been included previously – this has a negligible impact on the trend. Data are weighted to represent UK businesses by size and sector.

For the full results, visit www.gov.uk/government/statistics/cyber-security-breaches-survey-2020.

For further cyber security guidance for your business, visit the National Cyber Security Centre website (www.ncsc.gov.uk) to find:

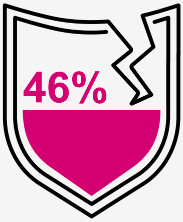
- the Small Business Guide drafted especially for smaller businesses (www.ncsc.gov.uk/smallbusiness)
- the government-endorsed Cyber Essentials scheme, which enables organisations to be certified independently for having met a good-practice standard in cyber security (www.cyberessentials.ncsc.gov.uk).

Department for
Digital, Culture,
Media & Sport

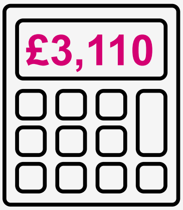
Ipsos MORI

UK MICRO AND SMALL BUSINESS TRENDS

EXPERIENCE OF BREACHES OR ATTACKS

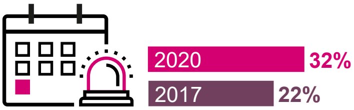


of micro and small businesses identified cyber security breaches or attacks in the last 12 months



is the average annual cost for micro and small businesses that lost data or assets after breaches

Among these 46%:

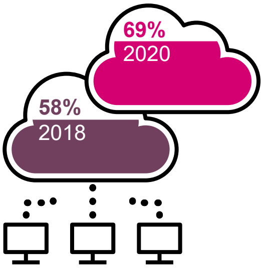


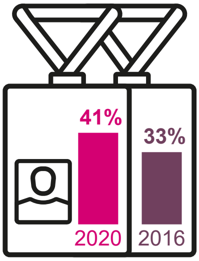
32%
were attacked at least once a week **(up from 2017)**

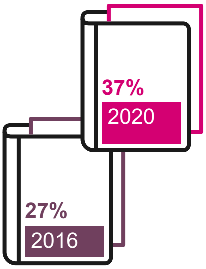
26%
needed new measures for future attacks

20%
lost staff time dealing with the breach

MANAGING RISKS







69%
have cloud backups
(up from 2018)

50%
have applied technical controls in all five Cyber Essentials areas

41%
have staff whose job role includes information security or governance
(up from 2016)

37%
have cyber security policies
(up from 2016)