CYBER SECURITY BREACHES SURVEY 2021

UK MEDIUM AND LARGE 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 and attacks. This infographic shows the key findings for medium and large firms.

1.

Despite COVID-19, cyber security remains a priority for management boards. **95%**/**93%** of **medium**/**large** firms say that cyber security is a high priority for their directors or senior managers.

2.

These firms experience a wide range of incidents. Among those identifying breaches or attacks, **85%**/**91%** had phishing attacks, **56%**/**63%** were impersonated and **14%**/**17%** had malware (including ransomware).

3.

Unprepared staff risk being caught unaware. A total of **38%**/**47%** train staff on cyber security and **42%**/**49%** have tested their staff response, for example with mock phishing exercises.

4.

COVID-19 has made cyber security harder. With resources stretched, fewer large firms report having up-to-date malware protection (**90%**, vs. **94%** in 2020) and monitoring of users (**72%**, vs. **84%** in 2020).

5.

These firms must adapt their cyber security to COVID-19. For example, **53%**/**66%** currently cover the use of personal devices for work in their cyber security policies.

Technical note: Ipsos MORI carried out a telephone survey of 210 medium businesses with 50 to 249 staff) and 203 large businesses with 250+ staff (excluding sole traders, and agriculture, forestry and fishing businesses) from 12 October 2020 to 22 January 2021. This included 139 medium and 135 large businesses that identified a breach or attack in the last 12 months. 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-2021.

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

This includes COVID-19 guidance covering:

- the **Board Toolkit**, which helps boards understand their obligations and discuss cyber security with the technical experts in their organisation
- cyber security under the COVID-19 pandemic, including guidance on **home working, video conferencing** and **moving your business online**

Department for Digital, Culture, Media & Sport

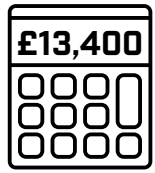
Ipsos MORI

Key MEDIUM BUSINESSES LARGE BUSINESSES

UK MEDIUM AND LARGE BUSINESS TRENDS

EXPERIENCE OF BREACHES OR ATTACKS

of **medium** | **large** businesses identified breaches or attacks in the last 12 months **(down from 2020)**



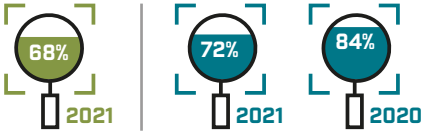
is the average annual cost for medium/large businesses that lost data or assets after breaches

AMONG THE 65% | 64% IN 2021:

30% | 21%
were attacked at least once a week

29% | 43%
needed new measures to stop future attacks

DEALING WITH COVID-19



monitor user activity **(down from 2020 for large businesses only)**

cover home working in a cyber security policy

have staff using personal devices for work

MANAGING RISKS

68% | 77%
use insecure smart devices in work settings

48% | 57%
have board members with a cyber security brief **(down from 2020 for large businesses only)**

42% | 48%
have done a cyber security vulnerability audit

37% | 52%
carry out penetration testing

32% | 36%
have reviewed cyber risks from immediate suppliers