

CYBER SECURITY BREACHES SURVEY 2020

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. This infographic shows the key findings for medium and large firms.



1. Cyber attacks have become more frequent. Among the **medium/large** firms that identified breaches or attacks in the last 12 months, **33%/26%** experience them at least once a week (vs. **17%/17%** in 2017).



2. These firms experience a wide range of attacks. Among those identifying breaches or attacks, **90%/93%** had phishing attacks, **62%/62%** were impersonated and **31%/29%** had malware (e.g. ransomware).



3. Board engagement is becoming more widespread. **72%/74%** update their board members on actions taken on cyber security at least quarterly, but just **48%/48%** do it at least monthly.*



4. Many medium and large firms formally assess their cyber risks. **79%/86%** have had internal or external audits that cover cyber security in the last 12 months.



5. Many are insuring themselves against the risks. **52%/53%** report being insured against cyber risks. **20%/21%** have a specific cyber insurance policy.

Technical note: Ipsos MORI carried out a telephone survey of 216 medium businesses with 50 to 249 staff and 213 large businesses with 250+ staff (excluding sole traders, and agriculture, forestry and fishing businesses) from 9 October to 23 December 2019. This included 149 medium and 156 large 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.

*This excludes businesses that say they update senior managers "each time there is a breach".

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). This includes the Board Toolkit, which helps management boards to understand their obligations and to discuss cyber security with the technical experts in their organisation (www.ncsc.gov.uk/collection/board-toolkit).



Department for
Digital, Culture,
Media & Sport



Ipsos MORI

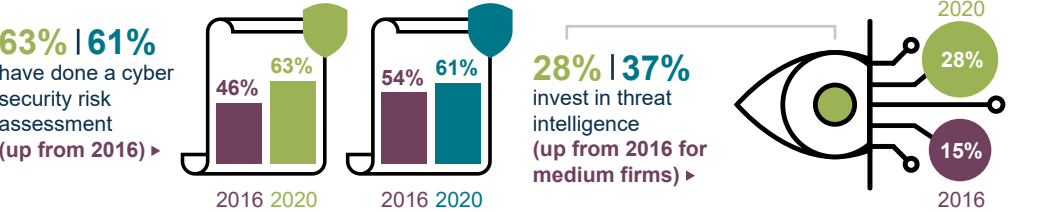
UK MEDIUM AND LARGE BUSINESS TRENDS

Key: **MEDIUM BUSINESSES** **LARGE BUSINESSES**

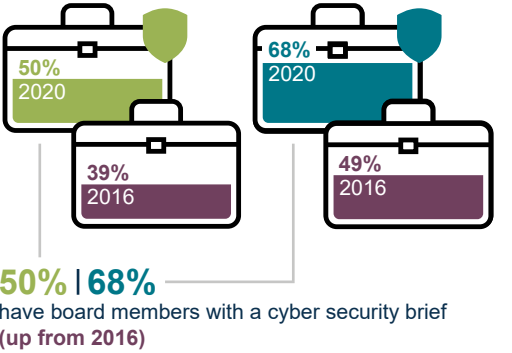
EXPERIENCE OF BREACHES OR ATTACKS



IDENTIFYING RISKS



BOARD INVOLVEMENT



SUPPLY CHAIN

