CYBER SECURITY BREACHES SURVEY 2020

UK 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 UK businesses.

1. **Cyber attacks have become more frequent.** Among the 46% of businesses that identified breaches or attacks in the last 12 months, 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. 72% in 2017), 26% were impersonated and 19% had malware (including ransomware).

3. **Cyber security is increasingly important for senior managers.** 80% of businesses say that cyber security is a high priority for their management boards, up from 69% in 2016.

4. **Many businesses formally assess their cyber risks.** 50% have had internal or external audits that cover cyber security in the last 12 months. 35% have done a cyber risk assessment, up from 23% in 2016.

5. **Some are insuring themselves against the risks.** 32% of businesses report being insured against cyber risks, either through a specific cyber insurance policy or as part of wider business insurance.

6. **There is room for improvement when it comes to suppliers.** Just 15% of businesses have reviewed cyber security risks posed by their suppliers and 9% have done this for their wider supply chain.

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).

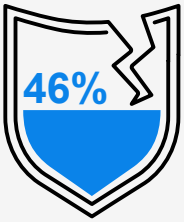
Technical note: Ipsos MORI carried out a telephone survey of 1,348 businesses (excluding sole traders, and agriculture, forestry and fishing businesses) from 9 October to 23 December 2019. This included 748 businesses that identified a breach or attack in the last 12 months. N.B. this year's survey omitted 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.

Department for Digital, Culture, Media & Sport

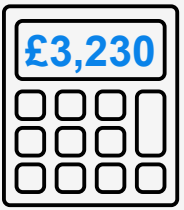
Ipsos MORI

UK BUSINESS TRENDS

EXPERIENCE OF BREACHES OR ATTACKS

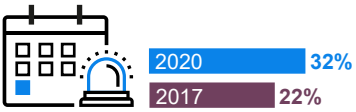


of businesses identified cyber security breaches or attacks in the last 12 months



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

Among these 46%:



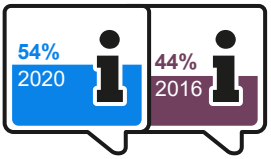
32%
were attacked at least once a week **(up from 2017)**

27%
needed new measures for future attacks

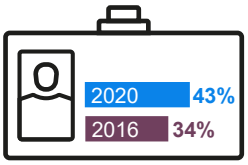
20%
lost staff time dealing with the breach

MANAGING RISKS

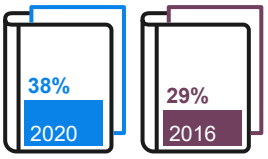
54%
have sought external information or guidance **(up from 2016)** ▸



43%
have staff whose job role includes information security or governance **(up from 2016)** ▸

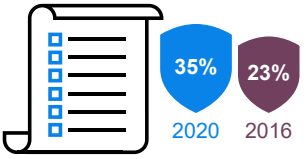


38%
have cyber security policies **(up from 2016)** ▸



IDENTIFYING RISKS

35%
have done a cyber security risk assessment **(up from 2016)** ▸



INCIDENT RESPONSE

44%
assign incident management roles to specific people

40%
formally log incidents

37%
have written guidance on who to notify of breaches