Cyber Security Breaches Survey: 2022

Micro & Small businesses

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

Cyber attack

A cyber-attack is a malicious and deliberate attempt by an individual or organisation to breach the information system of another individual or organisation. **38%** of UK micro and small businesses identified a cyber-attack in the last 12 months, with **82%** of these businesses reporting phishing attempts, and **25%** identifying a more sophisticated attack type such as a denial of service, malware or ransomware attack.

Incident response

The ability to detect and quickly respond to cyber breaches will help reduce the operational, financial and reputational damage. When experiencing a cyber breach, **84%** of UK businesses would inform their board, and **73%** would conduct an impact assessment. However, only **18%** of micro and small businesses have a written incident management plan, with qualitative findings suggesting an informal approach with reliance on internal expertise or external business partners such as IT providers.

Vulnerability management

Many cyber attackers exploit publicly disclosed vulnerabilities to gain access to systems and networks, and so regular updates are essential to guard against emerging vulnerabilities. **82%** of UK businesses have up-to-date anti malware protection, and **38%** have a policy for patch management. Additionally in the last 12 months; **34%** of UK businesses have used security monitoring tools, **17%** undertook a cyber vulnerability audit and **13%** used threat intelligence.

For the full results, visit:
Cyber Security Beaches Survey 2022

Technical note: Ipsos MORI carried out a telephone survey of 960 micro and small businesses (excluding sole traders, between 1 and 49 employees) from 12 October 2021 to 21 January 2022. This included 393 micro and small businesses that identified an attack in the last 12 months. Data are weighted to represent UK businesses by size and sector. We have omitted comparisons with the 2021 results, as there is not substantial year on year change.

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

This includes guidance covering:
- **home working**
- **video conferencing**
- **encouraging cyber security discussions**

Department for Digital, Culture, Media & Sport

Ipsos

Micro & Small businesses

Internal activity

22%
Have a formal cyber security strategy

In the last twelve months...

32%
Have done a cyber security risk assessment

16%
Have carried out staff or awareness training

7%
Have assessed risks presented by their wider supply chain

External engagement

48%
of businesses have sought external information on cyber security

43%
Have some form of cyber insurance. **5%** Have a standalone cyber policy

39%
Use an outsourced cyber security provider

6%
of businesses has a Cyber Essentials certification

Threat landscape

Identified a cyber attack in the last twelve months

Of these…

34%
Had an impact on the business

31%
Were attacked at least once a week

20%
Resulted in a negative outcome

Board engagement

81%
State their board sees cyber security as a high priority

49%
of boards discuss cyber security at least quarterly

33%
Have a board member with responsibility for cyber security