Cyber Security Breaches Survey: 2022

Medium & Large 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. **61%** of UK medium and large businesses identified a cyber-attack in the last 12 months, with **94%** of these businesses reporting phishing attempts, and **49%** 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, **93%** of UK medium and large businesses would inform their board, and **81%** would conduct an impact assessment. **52%** of medium and large businesses have a written incident management plan.

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. **91%** of UK medium and large businesses have up-to-date anti malware protection, and **52%** have a policy for patch management. Additionally in the last 12 months; **58%** of UK medium and large businesses have used security monitoring tools, **40%** undertook a cyber vulnerability audit and **31%** used threat intelligence.

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

Technical note: Ipsos MORI carried out a telephone survey of 283 medium and large businesses (50 or more employees) from 12 October 2021 to 21 January 2022. This included 180 medium or large 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

Medium & Large businesses

Internal activity

50%
Have a formal cyber security strategy

In the last twelve months...

56%
Have done a cyber security risk assessment

43%
Have carried out staff or awareness training

14%
Have assessed risks presented by their wider supply chain

External engagement

67%
of businesses have sought external information on cyber security

61%
Have some form of cyber insurance. **22%** Have a standalone cyber policy

57%
Use an outsourced cyber security provider

23%
of businesses has a Cyber Essentials certification

Threat landscape

Identified a cyber attack in the last twelve months

Of these…

55%
Had an impact on the business

32%
Were attacked at least once a week

28%
Resulted in a negative outcome

Board engagement

92%
State their board sees cyber security as a high priority

70%
of boards discuss cyber security at least quarterly

49%
Have a board member with responsibility for cyber security