Cyber Security Breaches Survey: 2022

Charities

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 charities.

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. **30%** of UK charities identified a cyber-attack in the last 12 months, with **87%** of these charities reporting phishing attempts, and **23%** 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 charities would inform their board, and **73%** would conduct an impact assessment. However, only **22%** of charities 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. **68%** of UK charities have up-to-date anti malware protection, and **23%** have a policy for patch management. Additionally in the last 12 months; **27%** of UK charities have used security monitoring tools, **14%** undertook a cyber vulnerability audit and **10%** used threat intelligence.

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

Technical note: Ipsos MORI carried out a telephone survey of 424 charities (excluding sole traders) from 12 October 2021 to 21 January 2022. This included 180 charities 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

Charities

Internal activity

19%
Have a formal cyber security strategy

In the last twelve months...

26%
Have done a cyber security risk assessment

19%
Have carried out staff or awareness training

5%
Have assessed risks presented by their wider supply chain

External engagement

31%
Use an outsourced cyber security provider

27%
Have some form of cyber insurance. **5%** Have a standalone cyber policy

14%
of businesses have sought external information on cyber security

6%
of businesses has a Cyber Essentials certification

Threat landscape

Identified a cyber attack in the last twelve months

Of these…

38%
Had an impact on the business

26%
Were attacked at least once a week

19%
Resulted in a negative outcome

Board engagement

72%
State their board sees cyber security as a high priority

42%
of boards discuss cyber security at least quarterly

26%
Have a board member with responsibility for cyber security