CYBER SECURITY BREACHES SURVEY 2019

CHARITY FINDINGS BY INCOME BAND

The Cyber Security Breaches Survey is an Official Statistic, measuring how UK organisations approach cyber security, and the impact of breaches.

Trustees and senior managers in 75% of UK charities see cyber security as a high priority, which is up from 53% in 2018. However, this is still lower in smaller charities with less annual income:

- 68% in low-income charities with under £100,000 (vs. 46% in 2018)
- 82% in middle-income charities with £100,000 to under £500,000 (vs. 76% in 2018)
- 94% in high-income charities with £500,000 or more (vs. 86% in 2018).

The General Data Protection Regulation (GDPR), introduced in May 2018, has played a major part in this change in attitudes. Awareness of GDPR among charities is very high (at 94%), but fewer understand some key implications. This is particularly true for low-income charities:

- 68% are aware they could be fined by the Information Commissioner's Office (ICO) for personal data breaches (vs. 79% of middle-income charities and 88% of high-income charities).
- 52% know they need to report personal data breaches to the ICO within 72 hours of discovery (vs. 67% and 80%).

There is still more that charities can do to protect themselves, their donors and their beneficiaries.

- Just 53% have undertaken 5 or more of the Government's 10 Steps to Cyber Security.
- In 25% of low-income charities, trustees are never updated on cyber security (vs. 10% of middle-income charities and 3% of high-income charities).

- For the full results, visit www.gov.uk/government/collections/cyber-security-breaches-survey.
- For further cyber security guidance for your charity, visit the National Cyber Security Centre website: www.ncsc.gov.uk. This includes the Cyber Security Small Charity Guide drafted especially for charities: www.ncsc.gov.uk/collection/charity.

Technical note

Ipsos MORI carried out the telephone survey from 10 October to 20 December 2018.

Bases for text and graphics: 514 charities; 56 that lost data or assets after breaches; 154 with an income under £100,000; 141 with £100,000 to under £500,000; 205 with £500,000 or more (income unknown for 14).

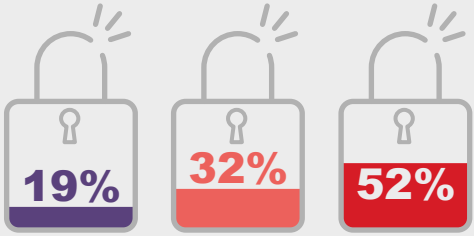
Data are weighted to represent UK registered charities.

Department for Digital, Culture, Media & Sport

Ipsos MORI

UNIVERSITY OF PORTSMOUTH

EXPERIENCE OF BREACHES OR ATTACKS



of charities in each income band identified breaches or attacks in the last 12 months

Key by charity income:

- UNDER £100K
- £100K TO UNDER £500K
- £500K OR MORE

£9,470
is the average annual cost for **all charities** that lost data or assets after breaches

15%
23%
46%

of charities in each income band had phishing emails

2%
6%
18%

had viruses or other malware, including ransomware

2%
5%
22%

had others impersonating them in emails or online

MANAGING CYBER RISKS

Via internal staff

43%
65%
82%

have staff members in information security or governance roles

27%
36%
35%

have a trustee with a cyber security brief

Via documentation or external expertise

28%
41%
73%

have cyber security policies

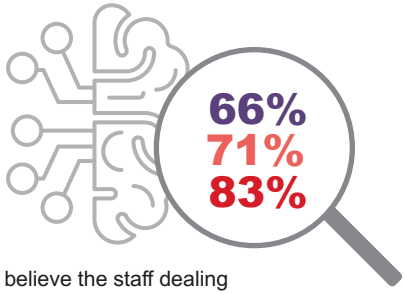
25%
37%
72%

have an external cyber security provider

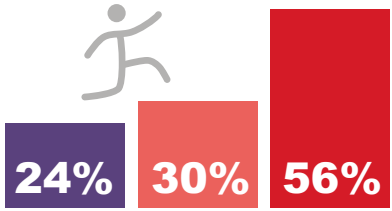
10%
23%
31%

have minimum cyber security standards for suppliers

SKILLS AND TRAINING



believe the staff dealing with their cyber security have the necessary skills and knowledge



have sent staff on cyber security training or conferences in the last 12 months