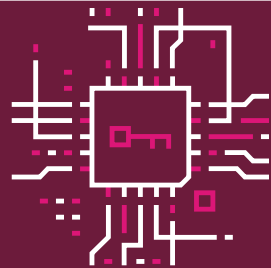


CYBER SECURITY BREACHES SURVEY 2018



CHARITY FINDINGS BY INCOME BAND

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

- The trustees and senior management in most charities agree that cyber security is a high priority for them. This is the case for:
 - almost nine in ten (86%) charities with £500,000+ in income
 - three-quarters (76%) of those with £100,000 to under £500,000
 - just under half (46%) with under £100,000.
- Just over half (54%) of the charities with incomes below £100,000 think the staff dealing with cyber security have the capacity to manage it effectively (compared to 66% of charities with incomes between £100,000 and £500,000, and 77% of charities with high incomes of £500,000 or more).
- Charities in the lower income band are also less likely than others to:
 - have any cyber security training (9%, vs. 26% of middle-income charities and 56% of high-income charities)
 - have formal cyber security policies (14%, vs. 37% and 63%)
 - have sought any information, advice or guidance about cyber security (33%, vs. 68% and 81%).
- For the full survey report, plus previous reports of the Cyber Security Breaches Survey, 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/charity.

Technical note

Overall bases for text and graphics: 207 UK registered charities with under £100,000; 138 with £100,000 to under £500,000; 210 with £500,000 or more.

Filtered bases: 46 with £100,000 to under £500,000 and 135 with £500,000 or more that identified a breach or attack in the last 12 months (too few respondents – under 30 – with under £100,000 that identified breaches to analyse); 83 with under £100,000 that have none of the governance or risk management arrangements listed in the survey (trustees with cyber security responsibilities, outsourced cyber security providers, formal cyber security policies, business continuity plans or staff assigned to information security or governance).

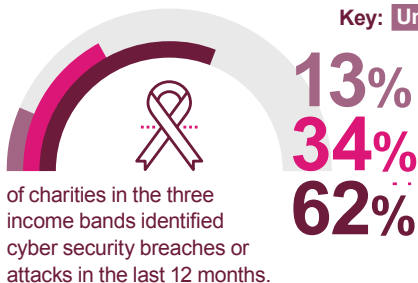
Fieldwork dates: 9 October 2017 to 14 December 2017.

Data are weighted by income and country to be representative of UK registered charities.



EXPERIENCE OF BREACHES

Key: **Under £100,000** | **£100,000 to under £500,000** | **£500,000 or more**

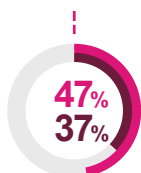


£309 | £1,460
was the average (mean) cost of all breaches identified in the last 12 months.

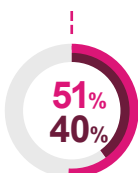


2 | 4 was the median number of breaches experienced in the last 12 months.

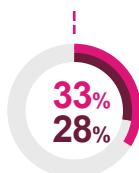
AMONG THE 34%/62% THAT IDENTIFIED BREACHES OR ATTACKS IN THE LAST 12 MONTHS:



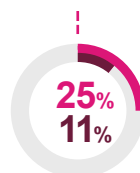
needed new measures to prevent or protect against future breaches.



used additional staff time to deal with breaches.



said that breaches stopped staff carrying out day to day work.



said that breaches incurred further recovery or repair costs.

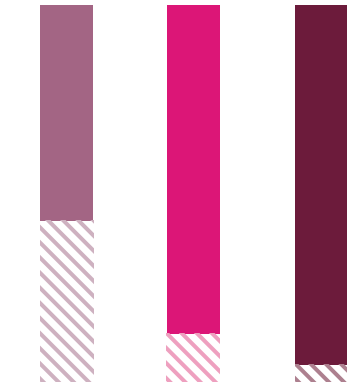
TAKING PREVENTATIVE ACTION

Key: **Under £100,000** | **£100,000 to under £500,000** | **£500,000 or more**

Charities in the three income bands with any cyber security governance or risk management measures in place

HAVE ANY MEASURES IN PLACE

57% 87% 95%



HAVE NO MEASURES IN PLACE



38%



68%



84%

of charities in the three income bands have carried out any health checks, risk assessments or audits to identify cyber security risks.



of charities in the three income bands have cyber security insurance.