CYBER SECURITY BREACHES SURVEY 2020

UK CHARITY TRENDS

The Cyber Security Breaches Survey is an official statistic. Since 2016, it has measured how UK organisations approach cyber security, and the impact of breaches. This infographic shows the key findings for charities, which were first included in the 2018 survey.

Cyber attacks have become more frequent. In 2018, 19% of charities identified any cyber security breaches or attacks over a 12-month period. In 2020, this has risen to 26%.

Cyber security is increasingly important for charities. 74% of charities say that cyber security is a high priority for their trustees and senior managers, up from 53% in 2018.

More charities are engaging their trustees and senior managers. 38% of charities update their board on actions taken on cyber security at least quarterly. 12% never update them, down from 38% in 2018.

Half of charities are seeking information. 51% sought information in the last 12 months, up from 36% in 2018. But just 16% have heard of the National Cyber Security Centre's Small Charity Guide.

Some are insuring themselves against the risks. 31% of charities report being insured against cyber risks, either through a specific cyber insurance policy or as part of wider business insurance.

There is room for improvement when it comes to suppliers and partners that charities work with. Just 13% of charities have reviewed cyber security risks posed by their suppliers.

For the full results, visit www.gov.uk/government/statistics/cyber-security-breaches-survey-2020.

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/charity).

Technical note: Ipsos MORI carried out a telephone survey of 337 UK registered charities from 9 October to 23 December 2019. This included 134 charities that identified a breach or attack in the last 12 months. N.B. this year's survey omitted the denial-of-service attacks category that had been included previously – this has a negligible impact on the trend. Data are weighted to represent UK registered charities by income band and country.

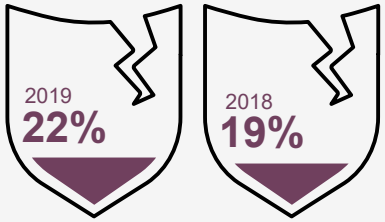
Department for Digital, Culture, Media & Sport

Ipsos MORI

UK CHARITY TRENDS

EXPERIENCE OF BREACHES OR ATTACKS

of charities identified cyber security breaches or attacks in the last 12 months **(up from 2018) ▸**



Among these 26%:

42%
needed new measures for future attacks

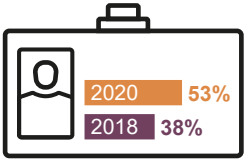
33%
lost staff time dealing with the breach

22%
had staff stopped from doing day-to-day work

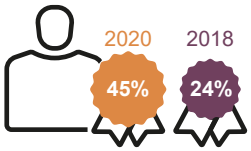
22%
were attacked at least once a week

MANAGING RISKS

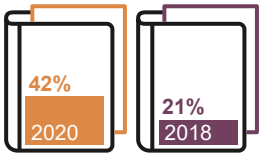
53%
have staff whose job role includes information security or governance **(up from 2018) ▸**



45%
have trustees with a cyber security brief **(up from 2018) ▸**

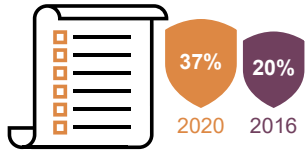


42%
have cyber security policies **(up from 2018) ▸**



IDENTIFYING RISKS

37%
have done a cyber security risk assessment **(up from 2018) ▸**



INCIDENT RESPONSE

50%
assign incident management roles to specific people

43%
have written guidance on who to notify of breaches

23%
have a communications plan