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

This fourth annual survey finds cyber security is increasingly a priority issue for organisations. 78% of businesses (vs. 74% in 2018) and 75% of charities (vs. 53% in 2018) now rate it as a high priority.

This year, 32% of businesses and 22% of charities have identified breaches or attacks. Among these organisations, the most common attacks are:

- phishing emails (80% of businesses and 81% of charities experiencing breaches or attacks)
- others impersonating their organisation online (28% and 20%)
- viruses or other malware, including ransomware (27% and 18%).

Businesses and charities are taking action on cyber security as a result of the General Data Protection Regulation (GDPR) introduced in May 2018. However, many could still take a more holistic approach around staff engagement and training.

- In 34% of businesses and 49% of charities, directors or trustees are only updated once a year or less on cyber security, if at all.
- A majority of businesses (77%) and charities (69%) believe the staff dealing with their cyber security have the right skills and knowledge. But staff have only had cyber security training in 27% of businesses and 29% of charities.

Many could also review their risk management approaches. Only 58% of businesses and 53% of charities have taken action towards 5 or more of the Government's 10 Steps to Cyber Security.

- For the full results, visit www.gov.uk/government/collections/cyber-security-breaches-survey.
- For further cyber security guidance for your business or charity, visit the National Cyber Security Centre website: www.ncsc.gov.uk.

Technical note

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

Bases for text and graphics: 1,566 businesses (excluding sole traders, and agriculture, forestry and fishing businesses) and 514 charities; 637/192 (businesses/charities) that identified breaches or attacks in the last 12 months; 192/56 that lost data or assets after breaches; 625/277 that made changes to cyber security because of GDPR; 742/266 that have cyber security policies.

Data are weighted to represent UK businesses and registered charities.
Among the 32%/22% identifying breaches or attacks:

- 32% of businesses/charities created new policies.
- 27% of businesses/charities had extra staff training or communications.
- 19% of businesses/charities had staff stopped from carrying out daily work.
- 48% identified at least one breach or attack a month.

Key:
- UK BUSINESSES
- UK CHARITIES

£4,180/£9,470 is the average annual cost for businesses/charities that lost data or assets after breaches.

GDPR AND CYBER SECURITY

- 30%/36% have made changes to cyber security because of GDPR.
- Among the 30%/36%:
  - Created new policies: 60%/60%.
  - Had extra staff training or communications: 15%/17%.
  - Changed firewall or system configurations: 11%/4%.
  - Created new contingency plans: 6%/10%.

Among these, 58%/56% created or reviewed in the last 6 months.

- Have cyber security policies in place: 27% in 2018, 33% in 2019, +6.
- Have done a cyber risk assessment in the last 12 months: 21% in 2018, 36% in 2019, +15.

EXPERIENCE OF BREACHES OR ATTACKS