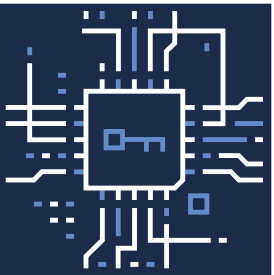
CYBER SECURITY BREACHES SURVEY 2018

UK BUSINESS AND CHARITY FINDINGS



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

For the third year running, the survey highlights the importance of cyber security, with over two in five businesses (43%) identifying breaches in the last 12 months. One in five charities (19%) – surveyed for the first time this year – identified a breach. Among these, the most common were:

- staff receiving fraudulent emails (75% of businesses and 74% of charities experiencing breaches)
- others impersonating the organisation online (28% and 27%)
- viruses and malware (24% and 24%).

Once more, staff awareness and vigilance are key issues. Seven in ten businesses (70%) and nearly six in ten charities (57%) think the staff dealing with cyber security are capable of doing so, but few have cyber security training (20% of businesses and 15% of charities) or have cyber security policies (27% and 21%).

Both businesses and charities consider technical controls important. This includes:

- updating software and malware protections (90% of businesses and 73% of charities do this)
- securely backing up data (90% and 70%)
- configuring firewalls (89% and 69%)
- providing guidance on passwords (67% and 47%).

- 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 business or charity, visit the National Cyber Security Centre website: www.ncsc.gov.uk/guidance.

Technical note

Bases for text and graphics: 1,519 UK businesses (excluding sole traders, and agriculture, forestry and fishing businesses) and 569 UK registered charities; 1,004 micro/small businesses with 1 to 49 staff; 515 medium/large businesses with 50 or more staff; 778 businesses and 218 charities that identified a breach or attack in the last 12 months; 849 businesses and 250 charities that spend money on cyber security.

Fieldwork dates: 9 October 2017 to 14 December 2017.

The business and charities data are weighted separately to be representative of their respective populations (by size and sector for businesses, and by income and country for charities).

Department for Digital, Culture, Media & Sport

Ipsos MORI Social Research Institute

University of Portsmouth

UK BUSINESS AND CHARITY FINDINGS

EXPERIENCE OF BREACHES

Key: **Businesses** Charities

43%
19%

of businesses and charities identified cyber security breaches or attacks in the last 12 months.

42% of micro/small businesses identified cyber security breaches or attacks in the last 12 months.

65% of medium/large businesses identified cyber security breaches or attacks in the last 12 months.

AMONG THE 43% OF BUSINESSES/19% OF CHARITIES THAT IDENTIFIED A BREACH OR ATTACK:

- **22%** / **25%** had a temporary loss of files.
- **15%** / **14%** had software or systems corrupted.
- **10%** / **14%** had their website slowed or taken down.
- **7%** / **4%** had money, assets or intellectual property stolen.
- **6%** / **3%** had a permanent loss of files or personal data.

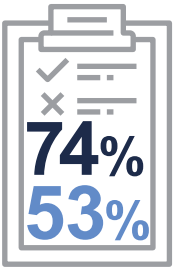
INVESTMENT AND PREVENTATIVE ACTION

Key: **Businesses** Charities

67%/32%

of businesses/charities spend money on cyber security. Among these, top (unprompted) reasons for spending are:

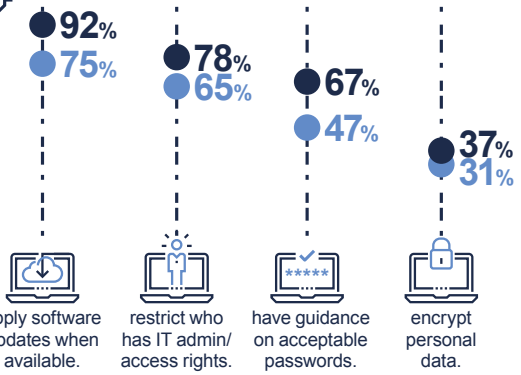
- to protect customer/beneficiary/donor data. **47%** / **62%**
- to prevent fraud/theft. **16%** / **19%**
- to protect cash or other assets. **15%** / **14%**
- to protect intellectual property. **12%** / **3%**



74%
53%

of businesses/charities say cyber security is a high priority for their directors, trustees or senior management.

Across all businesses/charities:



- **92%** / **75%** apply software updates when available.
- **78%** / **65%** restrict who has IT admin/access rights.
- **67%** / **47%** have guidance on acceptable passwords.
- **37%** / **31%** encrypt personal data.