Cyber Security
Longitudinal survey: Wave 2

Large businesses

The Cyber Security Longitudinal Survey (CSLS) is a three-year longitudinal study which follows the same organisations over time. It aims to better understand cyber security policies and processes within medium and large businesses and high income charities and to what extent these change and improve over this time. It will also quantify specific actions resulting in improved cyber incident outcomes.

Risk management

93% of large businesses took some kind of action to identify cyber security risks over the last 12 months. Using specific tools designed for security monitoring, such as Intrusion Detection Systems, was the most commonly reported action **(78%)**.

Supplier risk

Among large businesses that had carried out a risk assessment of their suppliers, the most common action was to request cyber security information on their own supply chains **(59%)**.

Cyber security training

In the last 12 months, **67%** of large businesses have carried out any cyber security training or awareness raising sessions for any staff or volunteers who are not directly involved in cyber security. This was significantly more than the previous year **(51%)**. More than half **(53%)** of the board have ever received any cyber security training.

For the full results, visit the Cyber Security Longitudinal Survey.

Technical note: Ipsos undertook a multimode (telephone and online) survey of 688 UK businesses (incl. 408 medium and 108 large businesses) and 373 UK registered charities. The main stage survey took place between 8 April and 29 June 2022. The data for businesses and charities have been weighted to be statistically representative of these two populations. A large business is defined as a business with 250 or more employees.

For further cyber security guidance for your charity, visit the National Cyber Security Centre website (www.ncsc.gov.uk).

This includes guidance covering:

- **Secure home working**
- **Secure video conferencing**
- **Encouraging cyber security discussions**

Department for Digital, Culture, Media & Sport

Ipsos

Large businesses

During the three research years, this survey aims to provide a trend analysis of how organisations are improving their cyber security defences and to understand key drivers for changing practices and policies. Below is the summary of findings from the second year of the survey. Significant differences from the baseline survey are indicated by an arrow.

Peer influence

Over the last 12 months, a quarter of large businesses have changed any of their cyber security policies or processes because of an organisation in their sector experiencing a cyber security incident.

20%
because an organisation in their sector experienced a cyber security incident

10%
because an organisation in their sector implemented similar measures

External influence

External IT or cyber security consultants were the most likely to have influenced the actions of organisations on cyber security in the last year. Influences asked about were:

45%
External IT or cyber security consultants

36% ▼
Insurers

20% ▼
Regulators for your sector

20% ▼
Whoever audits your accounts

Expand or improve

Over the last 12 months, more than nine in ten (92%) large businesses reported taking steps to expand or improve aspects of their cyber security. Steps taken:

67%
Improved network security

66%
Improved processes for user authentication and access control

59%
Improved malware defences

55%
Improved the way they monitor systems or network traffic

54%
Improved processes for updating and patching systems and software

45%
Improved processes for managing cyber security incidents

38%
Improved the way they monitor users

△▽ **Significant change from Wave One at 95% significance level**