Cyber Security
Longitudinal survey: Wave 1

Large sized 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

85% 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 **(74%)**.

Supplier risk

Among large businesses that had carried out a risk assessment of their suppliers, the most common action was to have set minimum cyber security standards in their supplier contracts **(69%)**.

Certifications

41% of large businesses adhere to at least one of Cyber Essentials, Cyber Essentials Plus or ISO27001. The most common is Cyber Essentials **(24%)**.

Board involvement

61% of large businesses agreed that their board integrates cyber risk considerations into wider business areas, while **10%** disagreed (17% neither, 12% don't know).

Cyber security training

In the last 12 months, **60%** of large businesses have carried out any cyber security training or awareness raising sessions for any staff who are not directly involved in cyber security. Almost half **(45%)** of the board have ever received any cyber security training.

Use of NCSC guidance

A third **(33%)** of large businesses have used NCSC information or guidance in the last year. Most used: The 10 Steps to Cyber Security, NCSC's Cyber Assessment Framework, and NCSC weekly threat reports.

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

Technical note: Ipsos MORI undertook a multimode (telephone and online) survey of 1,205 UK businesses (incl. 835 medium and 370 large businesses) and 536 UK registered charities. The pilot survey took place between 9 March and 6 April 2022, the main stage survey took place between 27 April and 15 July 2021. The data for businesses and charities have been weighted to be statistically representative of these two populations.

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

This includes guidance covering:

- **home working**
- **video conferencing**
- **encouraging cyber security discussions**

Department for
Digital, Culture,
Media & Sport

Ipsos MORI

Large sized businesses

During the three research years, this survey aims to provide a trend analysis of how organisations are improving their cybersecurity defences and to understand key drivers for changing practices and policies. Below is the summary of baseline findings.

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.

24% because an organisation in their sector experienced a cyber security incident

17% 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:

49% External IT or cyber security consultants

32% Insurers

26% Regulators for your sector

26% Whoever audits accounts

23% Customers

17% Any investors or shareholders

Expand or improve

Over the last 12 months, almost nine in ten (86%) large businesses reported taking steps to expand or improve aspects of their cyber security. Steps taken:

72% Improved network security

62% Improved malware defences

62% Improved the way they monitor users

57% Improved the way they monitor systems or network traffic

56% Improved processes for user authentication and access control

38% Improved processes for managing cyber security incidents

30% Improved processes for updating and patching systems and software