Cyber Security
Longitudinal survey: Wave Three

Medium businesses

The Cyber Security Longitudinal Survey (CSLS) is a multi-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.

Board engagement

Among medium businesses whose boards discuss cyber security, **60%** agreed that their board integrates cyber risk considerations into wider business areas. **47%** of medium businesses reported that board members had received cyber security training, significantly more than in Wave One **(33%)**.

Supplier risk

In the last 12 months, **24%** of medium businesses had carried out work to formally assess or manage the potential cyber security risks presented by their suppliers or partners. Setting minimum cyber security standards in supplier contracts was the most commonly reported action among medium businesses that had carried out a risk assessment of their suppliers **(55%)**.

Cyber Essentials adherence

35% of medium businesses adhered to a standard or accreditation related to cyber security, most commonly ISO 27001 **(18%)** and Cyber Essentials **(17%)**. Only **7%** adhered to the Cyber Essentials Plus standard.

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

Technical note: Ipsos undertook a multimode (telephone and online) survey of 542 businesses (incl. 302 medium and 223 large/very large businesses) and 310 charities between 27 March and 12 June 2023. The data for businesses and charities have been weighted to be statistically representative of these two populations. A medium business is defined as a business with 50-249 employees.

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

This includes the Cyber Security Board Toolkit and specific guidance for medium businesses.

Department for Science, Innovation, & Technology

Ipsos

Medium businesses

During the multiple 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 third year of the survey for medium businesses.

Peer influence

Over the last 12 months, more than one in ten medium businesses have changed any of their cyber security policies or processes because an organisation in their sector experienced a cyber security incident or implemented similar measures.

16%
Because an organisation in their sector experienced a cyber security incident

13%
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:

53% △
External IT or cyber security consultants

30% △
Their insurers

20%
Regulators for their sector

19% △
Whoever audits their accounts

Expand or improve

Over the last 12 months, 84% of medium businesses reported taking steps to expand or improve aspects of their cyber security. This was significantly more than in Wave One (70%). Steps taken:

68% △
Improved network security

63% △
Improved processes for user authentication and access control

63% △
Improved malware defences

54% △
Improved processes for updating and patching systems and software

48% △
Improved processes for managing cyber security incidents

47%
Improved the way they monitor systems or network traffic

30%
Improved the way they monitor users

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

Cyber Security
Longitudinal survey: Wave Three

Large businesses

The Cyber Security Longitudinal Survey (CSLS) is a multi-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.

Board engagement

Among large businesses whose boards discuss cyber security, **65%** agreed that their board integrates cyber risk considerations into wider business areas. **61%** of large businesses reported that board members had received cyber security training. This was significantly more than in Wave One **(45%)**.

Supplier risk

In the last 12 months, **39%** of large businesses had carried out work to formally assess or manage the potential cyber security risks presented by their suppliers or partners. Setting minimum cyber security standards in supplier contracts was the most commonly reported action among large businesses that had carried out a risk assessment of their suppliers **(66%)**.

Cyber Essentials adherence

Nearly half of large businesses **(47%)** adhered to a standard or accreditation related to cyber security, most commonly ISO 27001 **(23%)** and Cyber Essentials **(22%)**. **15%** adhered to the Cyber Essentials Plus standard.

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

Technical note: Ipsos undertook a multimode (telephone and online) survey of 542 businesses (incl. 302 medium and 223 large/very large businesses) and 310 charities between 27 March and 12 June 2023. 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+ employees.

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

This includes the Cyber Security Board Toolkit and specific guidance for large businesses.

Department for Science, Innovation, & Technology

Ipsos

Large businesses

During the multiple 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 third year of the survey for large businesses.

Peer influence

Over the last 12 months, more than one in five large businesses have changed any of their cyber security policies or processes because an organisation in their sector experienced a cyber security incident or implemented similar measures.

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

15%
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:

55%
External IT or cyber security consultants

43% △
Their insurers

27%
Whoever audits their accounts

26%
Their customers

Expand or improve

Over the last 12 months, 93% of large businesses reported taking steps to expand or improve aspects of their cyber security. This was significantly more than in Wave One (88%). Steps taken:

80% △
Improved network security

73% △
Improved malware defences

72%
Improved processes for user authentication and access control

61%
Improved the way they monitor systems or network traffic

60%
Improved processes for managing cyber security incidents

59%
Improved processes for updating and patching systems and software

51%
Improved the way they monitor users

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

Cyber Security
Longitudinal survey: Wave Three

Charities

The Cyber Security Longitudinal Survey (CSLS) is a multi-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.

Board engagement

Among high income charities whose boards discuss cyber security, **55%** agreed that their board integrates cyber risk considerations into wider business areas. **38%** of high income charities reported that board members had received cyber security training, significantly more than in Wave One **(28%)**.

Supplier risk

In the last 12 months, **26%** of high income charities had carried out work to formally assess or manage the potential cyber security risks presented by their suppliers or partners. Setting minimum cyber security standards in supplier contracts was the most commonly reported action among high income charities that had carried out a risk assessment of their suppliers **(63%)**.

Cyber Essentials adherence

36% of high income charities adhered to a standard or accreditation related to cyber security, most commonly Cyber Essentials **(23%)**. Only **7%** adhered to the ISO 27001 standard and **8%** to the Cyber Essentials Plus standard.

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

Technical note: Ipsos undertook a multimode (telephone and online) survey of 542 businesses (incl. 302 medium and 223 large/very large businesses) and 310 charities between 27 March and 12 June 2023. The data for businesses and charities have been weighted to be statistically representative of these two populations. A high income charity is defined as a charity with a turnover of at least £1 million.

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

This includes the Cyber Security Board Toolkit.

Department for Science, Innovation, & Technology

Ipsos

Charities

During the multiple 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 third year of the survey for charities.

Peer influence

Over the last 12 months, more than one in five high income charities have changed any of their cyber security policies or processes because an organisation in their sector experienced a cyber security incident or implemented similar measures.

19%
Because an organisation in their sector experienced a cyber security incident

13%
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:

70%
Whoever audits their accounts

68%
Regulators for their sector

52% ▼
Their insurers

37%
External IT or cyber security consultants

Expand or improve

Over the last 12 months, 87% of high income charities reported taking steps to expand or improve aspects of their cyber security. Steps taken:

70% ▲
Improved processes for user authentication and access control

68%
Improved network security

62% ▲
Improved malware defences

48%
Improved processes for managing cyber security incidents

45%
Improved processes for updating and patching systems and software

44%
Improved the way they monitor systems or network traffic

31%
Improved the way they monitor their users

▲▼ **Significant change from Wave One at 95% significance level**