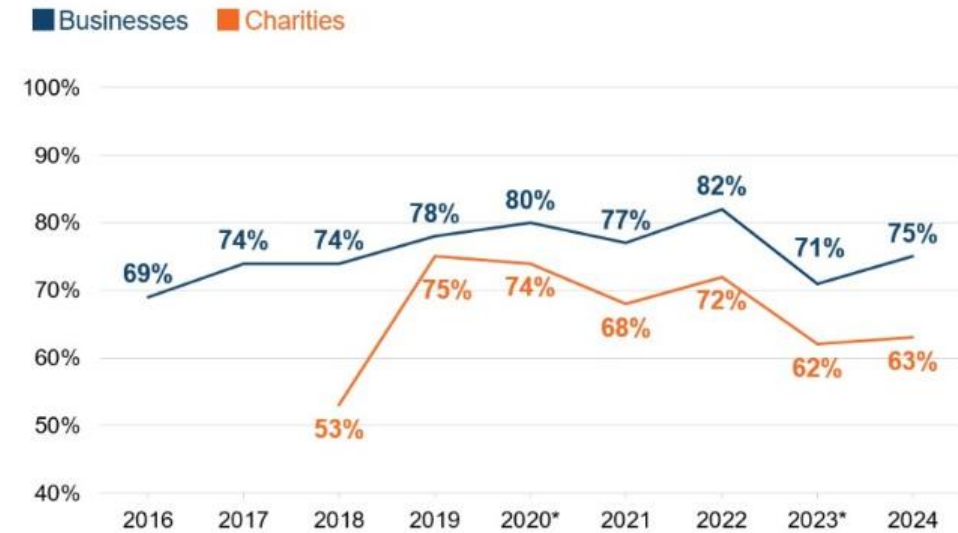


D1

Percentage of organisations over time where cyber security is seen as a high priority for directors, trustees, and other senior managers (1000+ UK businesses & 300+ charities per year).

C5

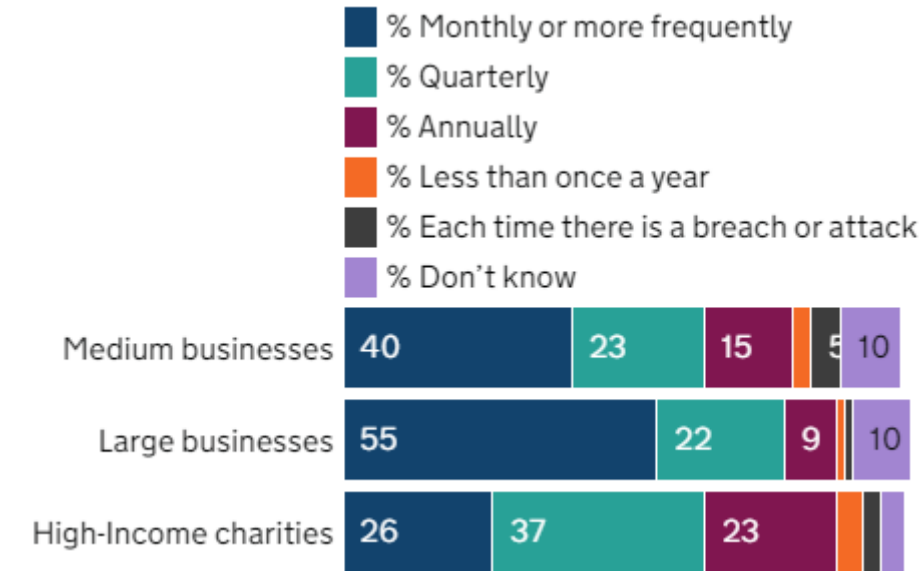


A3

The chart shows how the prioritisation score has changed over time. For businesses, the apparent drop in prioritisation of cyber security in 2023 (71% saying it was a high priority) is somewhat reversed with 75% now rating it as a high priority, more in line with previous years of the survey.

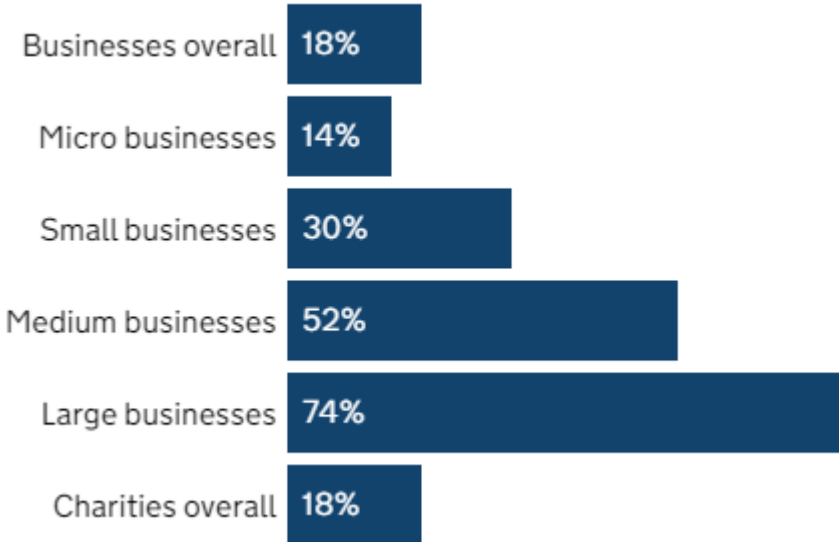
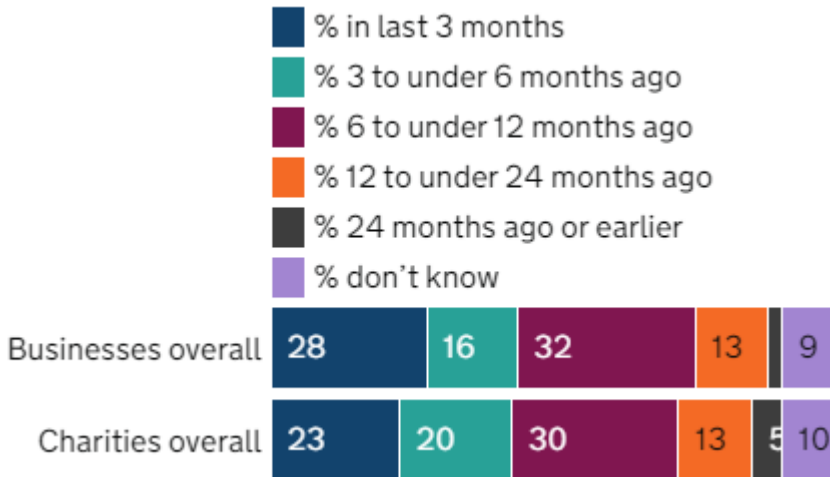
D2 How often directors, trustees or other senior managers are given an update on any actions taken around cyber security. (264 medium businesses; 170 large businesses; 335 high-income charities).

C1



A7

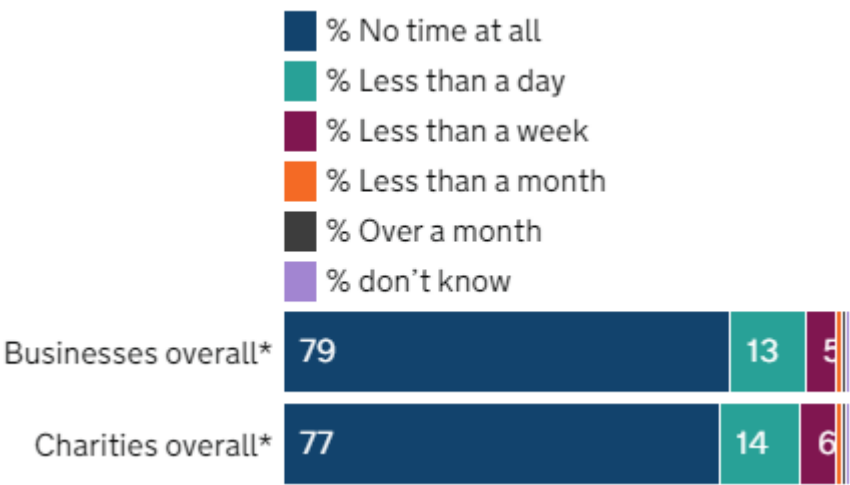
The results break down how often senior managers get updates on the state of cyber security and any actions being taken. It shows that updates tend to be more frequent in businesses than in charities, continuing a trend from previous years.

D3 Percentage of organisations that have had training or awareness raising sessions on cyber security in the last 12 months. (2,000 UK businesses; 1,058 micro businesses; 504 small businesses; 264 medium businesses; 170 large businesses; 1,004 charities).	C4  <table><tr><td>Businesses overall</td><td>18%</td></tr><tr><td>Micro businesses</td><td>14%</td></tr><tr><td>Small businesses</td><td>30%</td></tr><tr><td>Medium businesses</td><td>52%</td></tr><tr><td>Large businesses</td><td>74%</td></tr><tr><td>Charities overall</td><td>18%</td></tr></table>	Businesses overall	18%	Micro businesses	14%	Small businesses	30%	Medium businesses	52%	Large businesses	74%	Charities overall	18%	A2 Results show that in the last 12 months, around a fifth of businesses (18%) and charities (18%) have provided some form of staff training. Half of all medium businesses (52%), four-fifths of large businesses (74%) which is a decline vs 2023 of 77%) and half (52%) of high-income charities provided this training.									
Businesses overall	18%																						
Micro businesses	14%																						
Small businesses	30%																						
Medium businesses	52%																						
Large businesses	74%																						
Charities overall	18%																						
D4 When organisations last created, updated, or reviewed their cyber security policies or documentation. (658 businesses with cyber security policies; 329 charities)	C8  <table><tr><td></td><td>% in last 3 months</td><td>% 3 to under 6 months ago</td><td>% 6 to under 12 months ago</td><td>% 12 to under 24 months ago</td><td>% 24 months ago or earlier</td><td>% don't know</td></tr><tr><td>Businesses overall</td><td>28</td><td>16</td><td>32</td><td>13</td><td>5</td><td>9</td></tr><tr><td>Charities overall</td><td>23</td><td>20</td><td>30</td><td>13</td><td>5</td><td>10</td></tr></table>		% in last 3 months	% 3 to under 6 months ago	% 6 to under 12 months ago	% 12 to under 24 months ago	% 24 months ago or earlier	% don't know	Businesses overall	28	16	32	13	5	9	Charities overall	23	20	30	13	5	10	A1 Of the 33% of businesses and 32% of charities that have cyber security policies in place, over four in ten (44%) of those businesses and a similar proportion (43%) of those charities reviewed these policies within the last six months. For businesses, the figure is similar to the last three years, however, is still significantly lower than 2020 when 52% said they had reviewed policies or documentation in the past six months.
	% in last 3 months	% 3 to under 6 months ago	% 6 to under 12 months ago	% 12 to under 24 months ago	% 24 months ago or earlier	% don't know																	
Businesses overall	28	16	32	13	5	9																	
Charities overall	23	20	30	13	5	10																	

D5

How long it took to get operations back to normal after their most disruptive breach or attack was identified. (1,028 UK businesses; 428 charities; Unlabelled bars are less than 5%).

C2



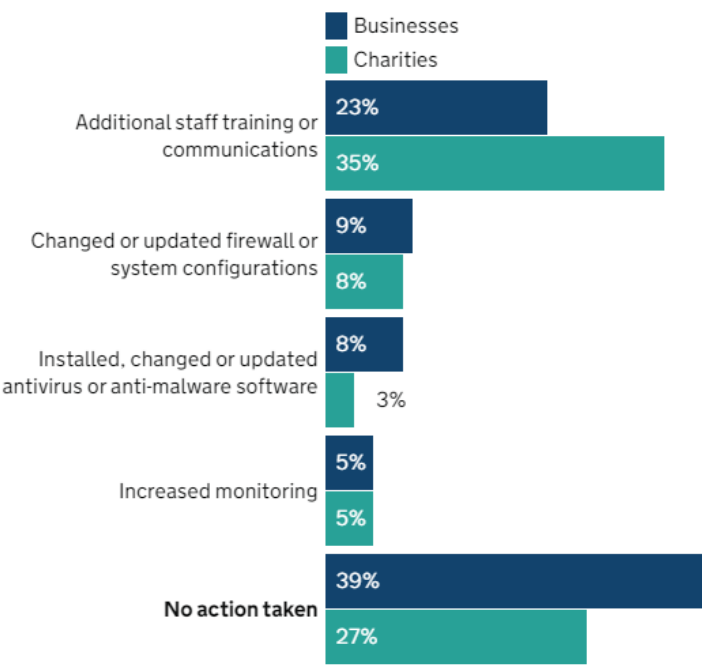
A4

When considering their most disruptive breach or attack, the vast majority of businesses (92%) and charities (91%) report being able to restore their operations within 24 hours.

D6

Percentage of organisations that have done any of the following since their most disruptive breach or attack of the last 12 months. Top unprompted responses of 5% or more. 1,028 businesses that recalled their most disruptive breach or attack in the last 12 months; 429 charities.

C7



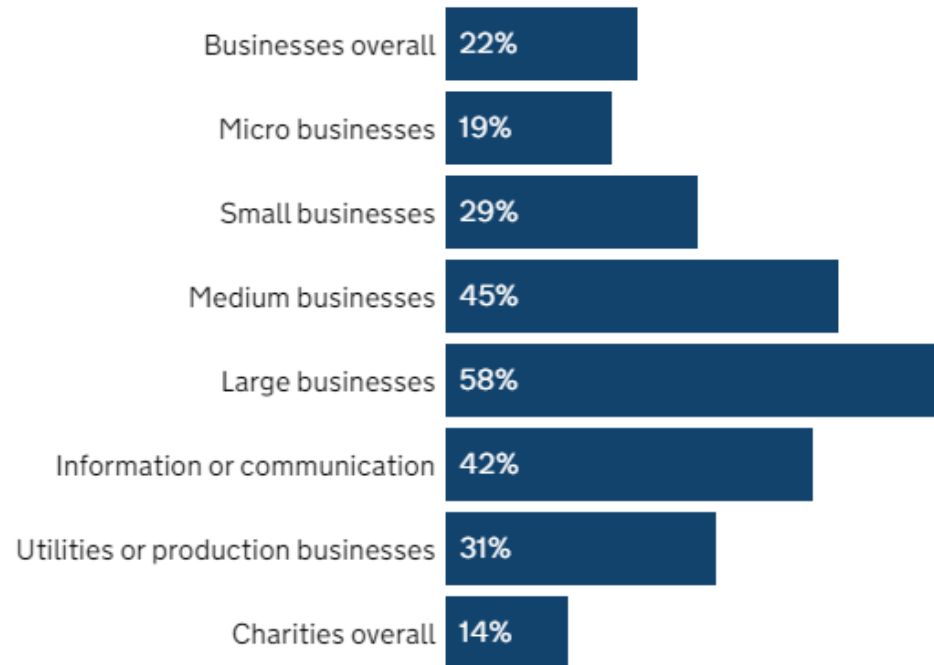
A5

Among those that have identified any breaches or attacks, 59% of businesses and 70% of charities report taking any action to prevent further breaches. As the chart shows, the most common specific action taken are a mixture of additional staff training or communications and implementing new technical controls.

D7

Percentage of organisations that have experienced any cybercrime (excluding cyber-facilitated fraud) in the last 12 months. (2,000 UK businesses; 1,060 micro businesses; 506 small businesses; 264 medium businesses; 170 large businesses; 124 Information or communication; 156 utilities or production businesses; 1,004 charities).

C3



A8

As the chart shows, across all organisations (i.e. not just those identifying breaches or attacks), medium and large businesses are significantly more likely to experience a cybercrime than smaller ones. Similarly, high-income charities (37% of those with an income of £500,000 or more, vs. 14% of all charities) are also significantly more likely to have experienced a cybercrime.

D8

Percentage of businesses that had specific breaches or attacks leading to cyber-facilitated fraud, among the businesses experiencing any cyber-facilitated fraud. (73 businesses that incurred fraud as a direct result of cybercrime in the last 12 months).

C6



A6

Among the 3% of businesses that fell victim to cyber-facilitated fraud, Figure 6.3 shows the cybercrimes that led to the fraud. For example, 43% say that they were a victim of fraud which resulted from a phishing attack. The most common enablers of cyber-facilitated fraud, in terms of the types of cybercrime, are therefore phishing, and hacking of online bank accounts.

DCA Round Answers for Marking

D1	C5	A3
D2	C1	A7
D3	C4	A2
D4	C8	A1
D5	C2	A4
D6	C7	A5
D7	C3	A8
D8	C6	A6

Source

<https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024>