Department for Digital, Culture, Media & Sport

Ipsos MORI
Social Research Institute

UNIVERSITY OF PORTSMOUTH

Cyber Security Breaches Survey 2019

The Cyber Security Breaches Survey is a quantitative and qualitative survey of UK businesses and charities. For this latest release, the quantitative survey was carried out in winter 2018 and the qualitative element in early 2019. It helps these organisations to understand the nature and significance of the cyber security threats they face, and what others are doing to stay secure. It also supports the Government to shape future policy in this area.

Responsible statistician:

Rishi Vaidya
020 7211 2320

Statistical enquiries:

evidence@culture.gov.uk
@DCMSinsight

General enquiries:

enquiries@culture.gov.uk
0207 211 6200

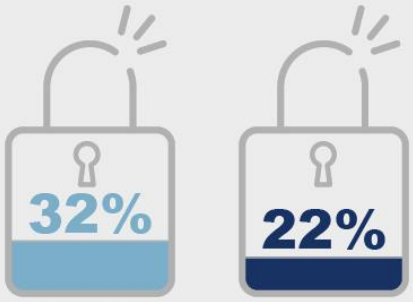
Media enquiries:

020 7211 2210

Contents

EXPERIENCE OF BREACHES OR ATTACKS

Key: UK BUSINESSES / UK CHARITIES



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

£4,180/£9,470

is the average annual cost for businesses/charities that lost data or assets after breaches

Among the 32%/22% identifying breaches or attacks:

32% / 29%

needed new measures to prevent future attacks

27% / 32%

took up staff time dealing with breaches or attacks

19% / 21%

had staff stopped from carrying out daily work

48% / 39%

identified at least one breach or attack a month

GDPR AND CYBER SECURITY

30%/36%

have made changes to cyber security because of GDPR

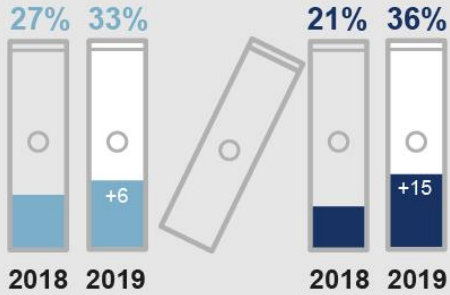
Among the 30%/36%:

60% / 60%
created new policies

15% / 17%
had extra staff training or communications

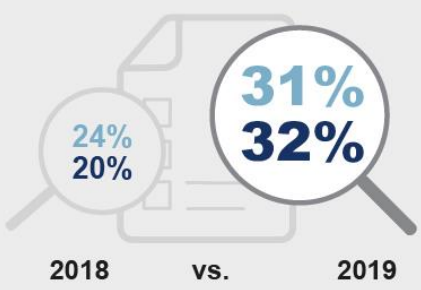
11% / 4%
changed firewall or system configurations

6% / 10%
created new contingency plans



have cyber security policies in place

Among these, 58%/56% created or reviewed in the last 6 months



have done a cyber risk assessment in the last 12 months

Summary

Cyber attacks are a persistent threat to businesses and charities. While fewer businesses have identified breaches or attacks than before, the ones that have identified them are typically experiencing more of them. These are consistent trends since the 2017 survey.[1]

Around a third (32%) of businesses and two in ten charities (22%) report having cyber security breaches or attacks in the last 12 months. As in previous years, this is much higher specifically among medium businesses (60%), large businesses (61%) and high-income charities (52%).[2]

Among this 32 per cent of businesses and 22 per cent of charities facing breaches or attacks, the most common types are:

- phishing attacks (identified by 80% of these businesses and 81% of these charities)
- others impersonating an organisation in emails or online (28% of these businesses and 20% of these charities)
- viruses, spyware or malware, including ransomware attacks (27% of these businesses and 18% of these charities).

For businesses, the proportion identifying breaches or attacks (32%) is lower than in 2018 (when it was 43%) and 2017 (46%). The charities result is similar to 2018. At the same time, among the 32 per cent of businesses that did identify any breaches or attacks, the typical (median) number they recall facing has gone up, from 2 attacks in 2017 to 6 in 2019.

The fall in the number of businesses identifying any breaches or attacks is consistent with a similar trend found among the general public in the Crime Survey for England and Wales (CSEW).[3] It has found that, between September 2017 and September 2018, the number of computer misuse incidents among individuals fell from c.1.5 million to c.1 million.

One plausible explanation for fewer businesses identifying breaches is if they are generally becoming more cyber secure. The survey shows that businesses have increased their planning and defences against cyber attacks since 2018. This may have resulted in fewer attacks overcoming their systems, and fewer businesses recording any cases.

Another possibility is a change in attacker behaviour, with more attacks being focused on a narrower (though still numerous) range of businesses. Although the survey does not directly measure attacker behaviour, this may help to explain the observed fall in the number of businesses identifying breaches, alongside the rise in the typical number of breaches among those that do identify them.

Alternatively, the trend may, in part, be explained by a change in the way business responded to the survey question, following the introduction of the General Data Protection Regulation (GDPR) in May 2018. GDPR might have changed what businesses consider to be a breach, or led to some businesses becoming less willing to admit to having cyber security breaches.

---

[1] For business results, comparisons are made where feasible to the 2018, 2017 and 2016 surveys (for which quantitative survey fieldwork was undertaken in late 2017, late 2016 and late 2015 respectively). Charities were surveyed for the first time in the 2018 survey.

[2] For businesses, analysis by size splits the population into micro businesses (1 to 9 employees), small businesses (10 to 49 employees), medium businesses (50 to 249 employees) and large businesses (250 employees or more). For charities, we look at annual income bands, with high income being £500,000 or more.

[3] See https://www.ons.gov.uk/releases/crimeinenglandandwalesyearendingseptember2018.

The findings also suggest that, where businesses have lost data or assets through cyber security breaches, the financial costs from such incidents have consistently risen since 2017.

Among the 32 per cent of businesses recording breaches or attacks, this resulted in a negative outcome, such as a loss of data or assets, in 30 per cent of cases. Among the charities recording breaches or attacks, this happened 21 per cent of the time.

In businesses that had these kinds of negative outcomes, the average (mean) cost to the business was £4,180 in 2019. This is higher than in 2018 (£3,160) and 2017 (£2,450). It indicates a broad trend of rising costs in cases where cyber attacks are able to penetrate an organisation's defences.[4]

Once again, the average costs faced by larger businesses in these cases tend to be much higher (£9,270 for medium firms and £22,700 for large firms in 2019). And for charities facing such negative outcomes from breaches, the average cost was £9,470 in 2019.

The quantitative survey highlights that the costs of cyber security breaches can be substantial. However, our qualitative findings suggest that, outside the survey, the indirect costs, long-term costs and intangible costs of breaches – things like lost productivity or reputational damage – tend to be overlooked. This means that, when organisations reflect on their approaches to cyber security, they may be undervaluing the true cost and impact of cyber security breaches.

In 2019, more businesses and charities than before have taken positive steps to improve their cyber security. This is in part linked to the introduction of GDPR.

Around three-quarters of businesses (78%) and charities (75%) say that cyber security is a high priority for their organisation's senior management. These proportions are higher than in 2018 (when it was 74% of businesses and 53% of charities). For businesses, there is a longer-term upwards trend going back to 2016 (when it was 69%).

Alongside this change in attitudes since 2018, there have also been various shifts in behaviour and action taken in this latest survey:

- More businesses (57%, vs. 51% in 2018) and charities (43%, vs. 27% in 2018) update their senior management on actions taken around cyber security at least once a quarter.
- Written cyber security policies are more common both among businesses (33%, vs. 27% in 2018) and charities (36%, vs. 21% in 2018).
- Both businesses (27%, vs. 20% in 2018) and charities (29%, vs. 15% in 2018) are more likely to have had staff attend any kind of cyber security training in the last 12 months.
- Over half of all businesses (56%, vs. 51% in 2018) and two-fifths of charities (41%, vs. 29% in 2018) say they have implemented controls in all the five technical areas listed under the Government's Cyber Essentials scheme.[5]
- More charities have taken actions to identify cyber risks, such as health checks, audits or risk assessments (60%, vs. 46% in 2018), bringing them in line with businesses (62%).
- More medium businesses (31%, vs. 19% in 2018) and large businesses (35%, vs. 24% in 2018) have cyber insurance, though the proportion of all businesses (11%) and charities (6%) that have this remains relatively low.

[4] These previous years' cost estimates have been adjusted for inflation up to 2019.

[5] This includes: applying software updates when available, up-to-date malware protection, firewalls with appropriate configurations, restricting IT admin and access rights to specific users, and security controls on company-owned devices. See https://www.cyberessentials.ncsc.gov.uk/.

GDPR has played a large part in these changes. Three in ten businesses (30%) and over a third of charities (36%) say they have made changes to their cyber security policies or processes as a result of GDPR. Our qualitative findings suggest that GDPR has encouraged and compelled some organisations over the past 12 months to engage formally with cyber security for the first time, and others to strengthen their existing policies and processes.

However, the qualitative findings also highlight that GDPR has had some unintended consequences. It has led some organisations to frame cyber security largely in terms of avoiding personal data breaches. These organisations were less focused on other kinds of breaches or attacks, and typically had a narrower set of technical controls in place. That is to say, GDPR appears to have had, on balance, a positive impact on cyber security to date, but to make progress beyond this, organisations may need to think more holistically about the issue.

There is still more that organisations can do to protect themselves from cyber risks. This includes taking important actions that are still relatively uncommon, around board-level involvement in cyber security, monitoring suppliers and planning incident response.

In some areas, the increasing prioritisation of cyber security has not always been matched by increased engagement and action.

- Just over a third of businesses (35%) and three in ten charities (30%) have a board member or trustee with specific responsibility for cyber security. For businesses, this is higher than in 2018 (when it was 30%), but the proportion remains low overall. Moreover, the qualitative findings suggest that embedding knowledge and understanding of cyber security within management boards is a strong driver of behaviour change.
- Around one in five businesses (18%) and one in seven charities (14%) require their suppliers to adhere to any cyber security standards. In the qualitative interviews, some had simply not considered suppliers as a potential source of cyber risk before, while some others simply did not consider their suppliers' cyber security to be their responsibility.
- Very few organisations (16% of businesses and 11% of charities) have formal cyber security incident management processes in place. For businesses, this is somewhat higher than in 2018 (when it was 13%), although again the proportion is still low overall. This continues to be the area in the Government's 10 Steps to Cyber Security guidance[6] where organisations are least likely to have taken action.

Organisations are open to receiving guidance or checklists for these areas, and for other aspects of cyber security. However, they expect such guidance to be pushed out to them.

Six in ten businesses (59%) and just under five in ten charities (47%, up from 36% in 2018) have sought external information or guidance on cyber security in the last 12 months.

However, only seven per cent of businesses and nine per cent of charities have sought information or guidance from the Government or public-sector bodies (such as the National Cyber Security Centre). The vast majority of these businesses (75%) say this information has been useful (the charity sample is too small to report on this). But the qualitative evidence suggests that organisations do not recognise a need to seek this information out for themselves.

Our qualitative interviews suggest that, as a result, organisations may benefit from better signposting to guidance, such as at the end of news stories about cyber attacks. We also found that there are key influencer groups that organisations often expect to receive guidance from, such as their external cyber security providers, trade associations and regulators. As such,

[6] See https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.

there may be a role for these groups in pushing out Government guidance in the future, capitalising on the higher engagement in cyber security brought about by GDPR.

Chapter 1: Introduction

1.1 Code of practice for Official Statistics

The Cyber Security Breaches Survey is an Official Statistic and has been produced to the standards set out in the Code of Practice for Official Statistics.

1.2 Background

Publication date: 3 April 2019

Geographic coverage: United Kingdom

The Department for Digital, Culture, Media and Sport (DCMS) commissioned the Cyber Security Breaches Survey of UK businesses and charities as part of the National Cyber Security Programme. The findings help these organisations to understand the nature and significance of the cyber security threats they face, and what others are doing to stay secure. It also supports the Government to shape future policy in this area, in line with the National Cyber Security Strategy 2016–2021.[7]

The latest survey was carried out by Ipsos MORI, in partnership with the Institute for Criminal Justice Studies at the University of Portsmouth. It covers:

- awareness and attitudes towards cyber security
- approaches to cyber security, including estimates of spending by organisations
- the nature and impact (including estimated costs) of cyber security breaches
- differences by size, sector and geographic location.

This 2019 publication follows previous surveys in this series, published in 2016 (with quantitative survey fieldwork in late 2015), 2017 (with quantitative fieldwork in late 2016)[8] and 2018 (with quantitative survey fieldwork in late 2017).

1.3 Methodology

As in previous years, there were two strands to the Cyber Security Breaches Survey:

- A random probability telephone survey of 1,566 UK businesses and 514 UK registered charities was undertaken from 10 October 2018 to 20 December 2018. The data have been weighted to be statistically representative of these two populations.
- A total of 52 in-depth interviews were undertaken in January and February 2019 to follow up with businesses and charities that had participated in the survey and gain further qualitative insights.

Sole traders and public-sector organisations were outside the scope of the survey. In addition, businesses with no IT capacity or online presence were deemed ineligible, which led to a small number of specific sectors (agriculture, forestry and fishing) being excluded. These exclusions are consistent with previous years, and the survey is considered comparable across years.[9]

---

[7] See https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

[8] See https://www.gov.uk/government/collections/cyber-security-breaches-survey for previous surveys.

[9] In previous years of the survey, the mining and quarrying sector was also excluded from the business sample. As of April 2018, this sector is estimated to account for under 0.1 per cent of all UK businesses, so the addition of this sector has not meaningfully impacted on the comparability of findings across years.

More technical details and a copy of the questionnaire are available in the separately published Technical Annex, available on the gov.uk website at: https://www.gov.uk/government/collections/cyber-security-breaches-survey.

1.4 Interpretation of findings

How to interpret the quantitative data

The survey results are subject to margins of error, which vary with the size of the sample and the percentage figure concerned. For all percentage[10] results, subgroup differences by size, sector and region, as well as changes since the previous surveys, have been highlighted only where statistically significant (at the 95% level of confidence).[11] In charts, arrows (⬆⬇) are used to highlight significant changes since 2018 (where comparison is feasible). There is a further guide to statistical reliability at the end of this release.

Subgroup definitions and conventions

For businesses, analysis by size splits the population into micro businesses (1 to 9 employees), small businesses (10 to 49 employees), medium businesses (50 to 249 employees) and large businesses (250 employees or more). Where there are also differences by business turnover, this is commented on separately.

For charities, analysis by size is primarily considered in terms of annual income band. In the main, the income banding primarily splits charities into low-income (under £100,000), middle-income (£100,000 to under £500,000) and high-income (£500,000 or more) groups. At the same time, where the data suggest more granular differences are present (e.g. for the smallest charities with incomes of under £10,000, or the largest ones with incomes of £5 million and over) these more granular subgroups are used.

Due to the relatively small sample sizes for certain business sectors, these have been grouped with other similar sectors for more robust analysis. Business sector groupings referred to across this report, and their respective SIC 2007 sectors, are:

- administration or real estate (L and N)
- construction (F)
- education (P)
- health, social care or social work (Q)
- entertainment, service or membership organisations (R and S)
- finance or insurance (K)
- food or hospitality (I)
- information or communications (J)
- utilities or production (including manufacturing) (B, C, D and E)
- professional, scientific or technical (M)
- retail or wholesale (including vehicle sales and repairs) (G)
- transport or storage (H).

Where figures in charts do not add to 100%, or to an associated net score, this is due to rounding of percentages or because the questions allow more than one response.

---

[10] Where subgroup mean scores are compared, the large variation in the data often means that these differences are not statistically significant – this is made clear throughout. However, looking at the pattern of mean scores across subgroups, and the direction of travel since the 2016 and 2017 surveys, can still generate valuable insights in these instances.

[11] Subgroup differences highlighted are either those that emerge consistently across multiple questions or evidence a particular hypothesis (i.e. not every single statistically significant finding has been commented on).

How to interpret the qualitative data

The qualitative survey findings offer more nuanced insights and case studies into how and why businesses and charities hold attitudes or adopt behaviours with regards to cyber security. The findings reported here represent common themes emerging across multiple interviews. Where examples or insights from one organisation, or a small number of organisations are pulled out, this is to illustrate findings that emerged more broadly across interviews. However, as with any qualitative findings, these examples are not intended to be statistically representative.

1.5 Acknowledgements

Ipsos MORI and DCMS would like to thank all the businesses, charities and individuals who agreed to participate in the survey and those that provided an input into the survey's development. We would also like to thank the organisations who endorsed the fieldwork and encouraged businesses to participate, including the Association of British Insurers (ABI), the Charity Commission for England and Wales, the Charity Commission for Northern Ireland, the Confederation of British Industry (CBI), the Federation of Small Businesses (FSB), ICAEW and techUK.

Chapter 2: Profiling UK businesses and charities

This chapter briefly sets out businesses' and charities' exposure to cyber security risks, as well as their use of cloud computing. These risks can come about via their reliance on digital services and e-commerce, and use of personal devices in the workplace (also known as bringing your own device, or BYOD). It provides the context for the different attitudes and approaches to cyber security evidenced in later chapters.

2.1 Online exposure

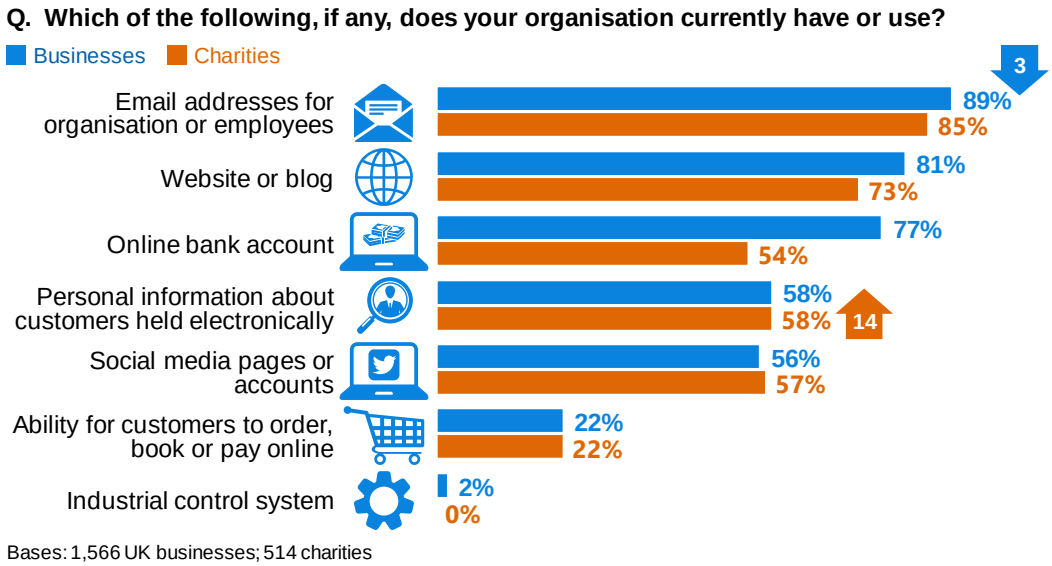
The quantitative survey once again illustrates that nearly all UK businesses and charities depend on some form of digital communication and services (98% of businesses and 95% of charities mention at least one of those listed in Figure 2.1). This is the case for the vast majority of smaller organisations (the result is 98% for micro businesses and 90% for charities with an income under £10,000), as well as larger ones.

As in 2018, charities are less likely overall than businesses to adopt online banking (54% vs. 77%). Nevertheless, over two-thirds of middle-income (68%) and high-income charities (77%) do have an online bank account.

The business findings in Figure 2.1 are very similar to previous years.

The proportion of charities noting that they hold personal data has increased by fourteen percentage points since 2018. This is probably due to an increase in *awareness* of what constitutes personal data, and charities knowing what personal data they hold, rather than an actual change in the volume of personal data being handled. This raised awareness might be expected after the introduction of the General Data Protection Regulation (GDPR) since the previous survey. Supporting this, the increase is greatest among low-income charities with less than £100,000 (up from 36% in 2018 to 54% in 2019), who also show the greatest increase in awareness of GDPR (see Chapter 3).

Figure 2.1: Organisations' reliance on online services



Bases: 1,566 UK businesses; 514 charities

In line with the differences found in 2018, businesses holding personal data are again most likely to be in the following sectors:

- finance or insurance (88% hold personal data, vs. 58% of all businesses)
- health and social care (80%)

- education (76%)
- administration or real estate (72%)
- professional, scientific or technical (68%).

Medium businesses (78%) and large businesses (79%) are also more likely than average to hold personal data. The same is true for middle-income charities (70% of those with £100,000 to under £500,000, vs. 58% of all charities) and high-income charities (84% of those with incomes of £500,000 or more).

2.2 Use of personal devices

Over four in ten businesses (44%) and six in ten charities (61%) say that staff in their organisation regularly use a personal device such as a non-work laptop for business purposes. This is known as bringing your own device (BYOD).

Among businesses, BYOD is consistent across size bands. Among charities, it is typically higher among low-income charities (63%) than middle-income or high-income ones (53% in each case).

2.3 Cloud computing

The use of externally-hosted web services, known as cloud computing, continues to be widespread across all types of organisations. Six in ten businesses and half of all charities use cloud computing, as shown in Figure 2.2. This is most prevalent among medium businesses, which is also consistent with the 2018 results.

Figure 2.2: Use of externally-hosted web services (cloud computing)

Bases: 1,566 UK businesses; 757 micro firms; 321 small firms; 281 medium firms; 207 large firms; 514 charities

Similar to the 2018 survey, the business sectors most likely to use cloud computing include:

- information or communications (75%, vs. 60% overall)
- education (74%)
- professional, scientific or technical (71%).

It is least prevalent among the retail or wholesale (64%), food or hospitality (50%) and construction (50%) sectors.

Chapter 3: Awareness and attitudes

This chapter looks at how much of a priority cyber security is to businesses and charities. It also covers where these organisations find information, advice or guidance about cyber security.

Cyber security is a broader issue than just the protection of personal data, although this is an important aspect of it. A major development since the previous survey was the introduction of the General Data Protection Regulation (GDPR) in May 2018, via the UK Data Protection Act 2018. This chapter also covers survey results on awareness of GDPR and its implications.

There is a relatively greater focus in this chapter on the qualitative findings, alongside the quantitative survey findings, compared to the rest of the report. This reflects that the qualitative interviews specifically covered: the actions businesses take when cyber security is a high priority, cyber security information and guidance, news coverage, and the impact of GDPR on attitudes and behaviours.

3.1 Perceived importance of cyber security

Around three-quarters of businesses (78%) and charities (75%) say that cyber security is a high priority for their organisation's senior management. Four in ten businesses (40%) and around a third of charities (35%) say it is a *very* high priority, as Figure 3.1 shows.

For both businesses and charities, the proportion who say cyber security is a high priority and, in particular, a very high priority, has increased since 2018.

Figure 3.1: Whether senior managers consider cyber security a high priority

Bases: 1,566 UK businesses; 514 charities

Larger businesses are more likely than the average to say that cyber security is a high priority (92% of medium and 95% of large businesses, vs. 78% overall). There is also a strong difference by size of charity, with more than nine in ten high-income charities saying cyber security is a high priority (94% of those with £500,000 or more, vs. 75% of all charities).

Senior managers are also more likely to consider cyber security a high priority in certain business sectors, such as:

- finance or insurance (97%, vs. 78% overall)
- education (93%)
- information or communications (88%).

In contrast, in the food and hospitality sector, senior managers are less likely than average to say cyber security is a high priority (62%).

From a regional perspective, businesses in London are more likely to see cyber security as a very high priority than others (51%, vs. 40% overall). Meanwhile, businesses based in the North of England are less likely to perceive it as either a very high or fairly high priority (71%).

There is a correlation between prioritisation and other measures in the survey, around the actions businesses take, and what they have seen or heard on the topic. The businesses for whom cyber security is a high priority are more likely than average to:

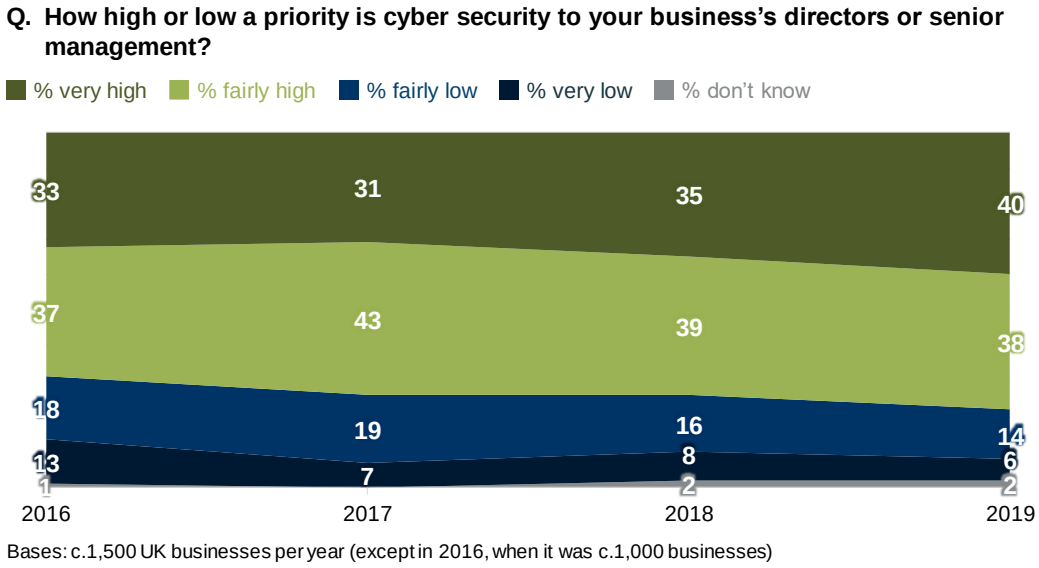
- have sought external information and guidance on the topic (67%, vs. 59% overall)
- have made changes to their cyber security measures after GDPR (35%, vs. 30% of all businesses)
- update their senior managers on cyber security issues at least once a quarter (65%, vs. 57% of all businesses).

Businesses who have heard of the Government's Cyber Aware campaign are also more likely to consider cyber security as high priority than those who are unaware of it (86% vs. 75%). It is important to remember that these findings cannot definitively show the direction of this relationship (i.e. whether exposure to Cyber Aware changes attitudes and, hence, prioritisation).

Longer-term trend in prioritisation

The extent to which organisations consider cyber security a priority has increased over time. Compared to last year, more businesses see it as a very high priority (40%, vs. 35% in 2018) and since 2016, there has been a nine percentage-point increase in businesses considering it a very or fairly high priority. This trend is shown in Figure 3.2.

Figure 3.2: Change over time in businesses considering cyber security as a high priority



Bases: c.1,500 UK businesses per year (except in 2016, when it was c.1,000 businesses)

For charities, this has also increased since last year (when charities were first included in the survey). In 2018, 53 per cent of charities said cyber security was a high priority (vs. 75% in 2019).

What does high prioritisation mean in practice?

The qualitative interviews show that, in practice, organisations that considered cyber security a high priority still had a range of different approaches to the issue.

Differences in how organisations framed and understood cyber security was a recurring theme. Some organisations, influenced by GDPR, were more focused on data protection, documentation and policies. Some focused more on financial fraud and protecting their bank accounts. Various organisations had not previously considered other potential implications of cyber breaches, such as the loss of business continuity and reputational damage.

In one case, we spoke to a general manager who was in charge of cyber security at a childcare centre. Their main focus was on data protection and compliance with GDPR, and they did not consider managing supplier risks as part of their role. Their finance department was in charge of supplier contracts, and the general manager played no part in this, suggesting a relatively disconnected approach to cyber security.

Those that did think more holistically about the issue were also typically taking a wider range of actions, such as implementing more technical rules and controls, and managing the risks associated with suppliers' cyber security.

"There has been a change in mindset. Whereas information security was something that sat in a little team and they used to come along at the end of a project and say, 'no, no, no', now it's fundamental to the start of any design decisions that we make."

High-income charity

Did organisations recognise they could do more?

When asked what more they could be doing to prioritise cyber security, responses in the qualitative interviews typically fell into two main categories.

Some smaller organisations felt that they could be doing more, but were unclear on what steps to take, and wanted guidance on further improvements they could make.

Others felt that they were already taking a reasonable approach with the fixed resources and budget they had. Low and middle-income charities in particular saw cost as an obstacle. Some organisations also mentioned the need to balance user controls with the flexibility to allow employees to carry out their day-to-day tasks, so they did not feel more control was necessary.

"We could spend between 0% and 100% of the company's turnover on cyber security. If we spent 100%, we would be out of business, and if we spent 0% we would probably be hacked all the time. Where we are at the moment is probably about right."

Large business

"We're always hanging on by our finger tips in financial terms, and I think that really prevents us investing in the time it takes to address cyber security in a strong way."

Middle-income charity

3.2 What drives engagement with cyber security?

The qualitative interviews highlighted several factors that drive engagement with cyber security, many of which are consistent with previous years' findings. Common themes included the perceived sensitivity of the data held, experience of breaches, perceptions that attacks were becoming more sophisticated, major changes in digital infrastructure, and compliance:

- Organisations that held sensitive personal data, such as customers' financial, tax or medical records, noted this as a main motivation for investing in cyber security. These organisations often discussed the potential for loss of trust and reputational damage if they had a breach, and how this could prevent them from operating. This appeared to be more of a concern in business-to-business relationships than in business-to-consumer relationships – some organisations that supplied other businesses raised the possibility of being blacklisted in the marketplace if they were not considered to be secure.

- Experiencing a breach with a negative outcome, such as a loss of data or assets, was a strong driver of behaviour change. One manufacturer we spoke to had lost their intellectual property after a ransomware attack, and subsequently reviewed their infrastructure, changed their firewall configurations and moved all their warehouses to a single secure network. Linked to this, some organisations said they had changed their approaches after hearing about breaches among organisations in the same sector.
- There was a sense across interviews that cyber attacks were becoming increasingly sophisticated and could no longer be tackled through common sense advice and guidance alone. For example, some organisations talked about phishing emails becoming more believable, and therefore harder to detect, than in previous years.

  "I think it will become more of a priority. Thinking of the phishing emails, they are going to get harder to spot. They are getting better at doing them. They are getting more and more sophisticated."

  High-income charity

- There were several common operational changes that led organisations to review their cyber security approaches. These included adopting new digital modes of service delivery, moving to online banking, migrating data to new servers or to the cloud, or allowing more flexible remote working among employees or suppliers.
- GDPR had compelled many organisations to review their approach to cyber security. We explore this further at the end of this chapter. Alongside this, a sector-specific driver for finance and insurance businesses seemed to be the emphasis that the Financial Conduct Authority placed on cyber security.

  "Cyber security is one in a long list of costs of doing business, so no-one's going to get excited about it unless you have regulatory focus."

  Large business

3.3 Involvement of senior management

How often is senior management updated on cyber security?

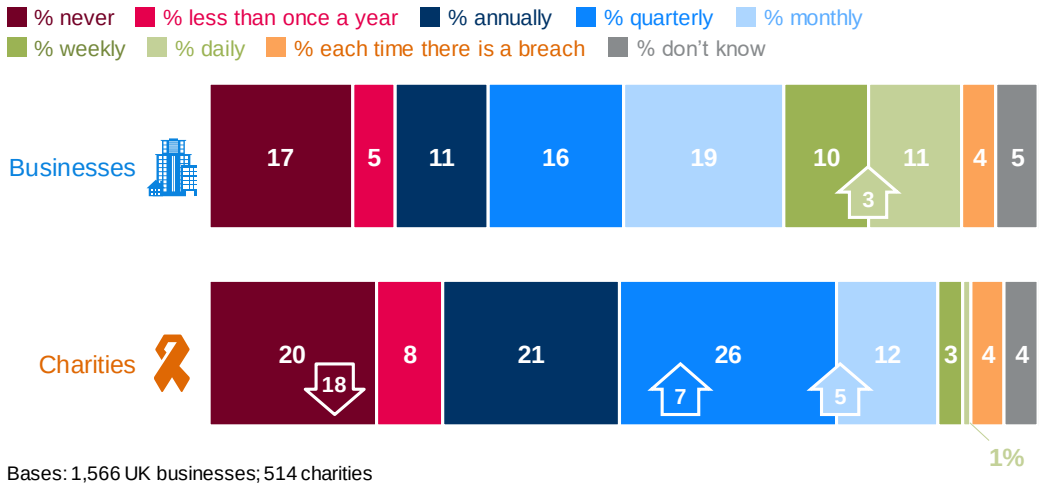
As shown in Figure 3.3 below, almost six in ten businesses (57%) update their senior management on cyber security issues at least every quarter (vs. 51% in 2018).[12] For charities, this is lower (43%), but has also markedly changed from a year ago (when it was 27%).

Looking at the longer-term trend, the proportion of businesses saying they never update senior managers has fallen consistently across each of the four years of the survey (from 26% in 2016 to 17% in 2019). The proportion of charities specifically saying they never update senior managers or trustees on this topic has also fallen considerably since last year (from 38% to 20%).

[12]This aggregated result excludes those who say they update senior managers each time there is a breach.

Figure 3.3: Updates given to senior management on cyber security

Q. Approximately how often, if at all, are your organisation's directors, trustees or senior management given an update on any actions taken around cyber security?



Bases: 1,566 UK businesses; 514 charities

Medium and large businesses more likely to give senior managers monthly updates on cyber security than others (32% and 35% respectively, vs. 19% overall). The proportion of medium and large businesses that never update senior managers is negligible (4% and 2% respectively). Similarly, only three per cent of senior managers or trustees in high-income charities are never updated.

Senior managers in the construction (25%) and food and hospitality (31%) sectors are more likely than in the average firm (17%) to never be updated.

The importance of board-level engagement

As previously noted, the quantitative survey finds a strong positive relationship between prioritisation of cyber security and updates to the board.

In the qualitative interviews with large businesses and high-income charities, the individuals that were in charge of cyber security day-to-day often suggested that more engagement from board-level staff would help improve cyber security in their organisation. This was, they felt, because board members set the organisational culture, which affected how seriously any policies and processes were taken. They also approved investment decisions around cyber security.

One cyber security professional in a high-income charity said, that having more cyber security knowledge across their board would make it harder for them to ignore advice from the IT team. They felt this would lead to quicker decisions, for example around training for wider staff or investment in products to protect their infrastructure.

Examples of board involvement from the interviews included: making cyber security a regular item on board meeting agendas, giving more formal updates, and having more frequent informal discussions with board members.

3.4 Sources of information

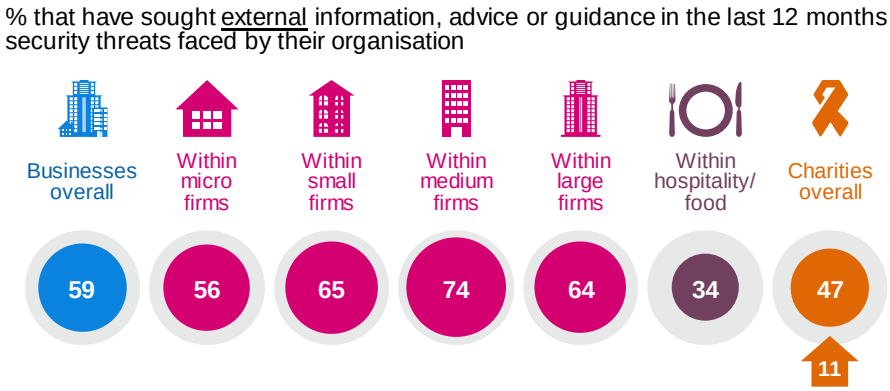
Overall proportion seeking cyber security information or guidance

Around three-in five businesses (59%) have actively sought information or guidance on cyber security from outside their organisation in the past year. Fewer charities (47%) have done so. As in previous years, medium businesses are most likely to seek external information or guidance, while micro businesses are the least likely to do so – shown in Figure 3.4.

Business results remain in line with last year, while more charities are seeking external information and guidance than before (47% in 2019, vs. 36% in 2018).

Charities are still much more likely than businesses to seek information and guidance from *within* their organisation (14% vs. 4%), from senior managers or other colleagues.

Figure 3.4: Whether organisations have sought information, advice or guidance



Bases: 1,566 UK businesses; 757 micro firms; 321 small firms; 281 medium firms; 207 large firms; 119 food or hospitality firms; 514 charities

Around two-fifths of businesses (38%) and charities (43%) have not knowingly sought *any* information or guidance, either from within their organisation or externally, in the past 12 months.

Where do organisations get information and guidance?

The most common sources of information and guidance, raised unprompted in the survey, are:

- external cyber security consultants, IT consultants or managed service providers (mentioned by 33% of businesses and 21% of charities)
- general online searching (13% of businesses and 8% of charities)
- trade associations (6% of businesses and 6% of charities).

The use of trade associations is higher than average among finance or insurance firms (14%) and information or communications firms (13%).

In total, seven per cent of businesses and nine per cent of charities have consulted Government or other public-sector sources. This includes:

- one per cent of businesses mentioning the National Cyber Security Centre (NCSC), including the NCSC website specifically
- three per cent of businesses and three per cent of charities mentioning the GOV.UK website (without explicitly mentioning the NCSC website)
- two per cent of charities mentioning their respective charity regulator (the Charity Commissions in England and Wales, and in Northern Ireland, and the Office of the Scottish Charity Regulator)
- nine per cent of health, social care or social work businesses mentioning the NHS.

Large businesses and those in the finance or insurance sector are more likely than average to have sought information from the Government or public sector (15% and 14% respectively).

Businesses' use of Government or other public-sector sources of information and guidance has risen gradually over time, from two per cent in 2016 to seven per cent in 2019. The share of businesses and charities seeking information from trade associations (both 6%) has also risen since 2018 (up from 3% and 2% respectively).

Qualitative evidence on how organisations receive information and guidance

In the qualitative interviews, IT and cyber security professionals tended to have a much wider range of information sources than those in non-technical roles (who were still responsible for cyber security in their organisation).

The information sources mentioned by those in technical roles included various Government, public sector or institutional sources, both in the UK and the US, such as:

- the NCSC website
- the Cyber Security Information Sharing Partnership (CiSP) run by the NCSC
- the US Government's National Institute of Standards and Technology (NIST)
- the SANS Institute (also in the US)
- security product vendor websites such as Microsoft, various online magazines such as the Register, and technical online forums such as Stack Overflow.

These technical individuals also often mentioned searching for bespoke solutions to queries on peer networks and on social media websites such as LinkedIn.

In contrast, for those in non-technical roles, the typical range of information sources was narrower and very different:

- Where organisations had external cyber security providers, IT providers or consultants, these were often their first port of call for information and guidance. This highlights the strong influence that external cyber security providers have on their clients.
- Some had searched on Google for information, guidance and training around GDPR and data protection – but not specifically on cyber security. Linked to this, some of these individuals mentioned arriving at the Information Commissioner's Office (ICO) website when looking for guidance on GDPR.
- In line with previous years' findings, organisations in sectors where there was a strong regulatory presence or trade association also said they would expect guidance from these organisations. Examples included the Charity Commission and Ofsted (or equivalent regulators in the devolved countries).
- Also in line with previous years, informal networks were commonly mentioned in smaller organisations, including friends and family that had IT backgrounds. Some of these smaller organisations also mentioned asking their business bank for guidance.

These individuals had generally not proactively searched for information and guidance on cyber security specifically (as opposed to data protection or GDPR). Some said that they would search on Google if they came up against specific problems or issues related to cyber security, but were not inclined to search for broader guidance. There was typically a low awareness of the NCSC among this group.

"I wouldn't say that I am the most informed person. It's not information I go out and seek, unless I am aware of a specific threat then absolutely we do the research."

Large business

Some said they did not expect Government to provide information and guidance on cyber security, so had not searched for it. Overall, there was a sense that information and guidance needed to be actively pushed out to these organisations, and that organisations without technical IT or cyber security staff needed better signposting to Government sources.

The impact of awareness campaigns and news stories on cyber security

In the quantitative survey, around three in ten businesses (32%) and charities (30%) say that they are not sure how to act on the advice they have seen or heard around cyber security. This is higher among food and hospitality businesses (43%) and construction businesses (42%).

These results are similar to last year, when this question was first asked. They highlight that for a sizeable minority of organisations, there is still a lack of clarity on what they should ideally be doing on this topic.

The qualitative interviews covered the impact of news stories about cyber security. Organisations often remembered seeing or hearing mainstream media news stories about cyber attacks on other organisations. There was often a focus on attacks on very large organisations, with examples (raised spontaneously in interviews) including the NHS, TalkTalk and British Airways. There was also a focus on the large financial cost, through fines or money lost.

Organisations generally felt that these stories had a positive impact. That is to say, they were considered effective in raising awareness of cyber security, and in helping to keep the topic fresh in people's minds. For example, in one large housing association we spoke to, the board of directors asked the head of IT to routinely brief them on cyber attacks in the news, and to reassure them that they had managed the risks.

However, there was a limit to the impact of these stories. At most, some organisations with cyber security or IT professionals had used them to see if they were exposed to the same vulnerabilities that were in the news story. However, other organisations said the types of organisations in these stories were too different from them to be relevant. Some also said they did not see a clear course of action they should take after reading these stories, as the stories did not signpost to further information or guidance.

"I don't think news stories [on cyber attacks] have any impact on a day-to-day basis because not every company is being hacked and is subject to cyber attacks all the time. It's like general crime, you don't think about it. It's not you, is it."

Medium business

Awareness of Government initiatives and communications

Once again, the quantitative survey finds that, among the six per cent of businesses that have sought out Government or public-sector information, the vast majority (75%) find this information useful. There are too few charities to analyse at this question.

It is still the case, however, that most businesses and charities are not aware of Government communications campaigns or initiatives in this area. This survey explores:

- the national Cyber Aware communications campaign, which offers tips and advice to protect individuals and businesses against cybercrime[13]
- the Government's 10 Steps to Cyber Security guidance, which aims to summarise what organisations should do to protect themselves[14]
- the Government's Cyber Essentials scheme, which enables organisations to be certified independently for having met a good-practice standard in cyber security.[15]

These results are shown in Figure 5.3. As can be seen here, awareness of these initiatives is far greater among large businesses, where around four in ten or more have heard of each one.

---

[13] See https://www.cyberaware.gov.uk/.

[14] See https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.

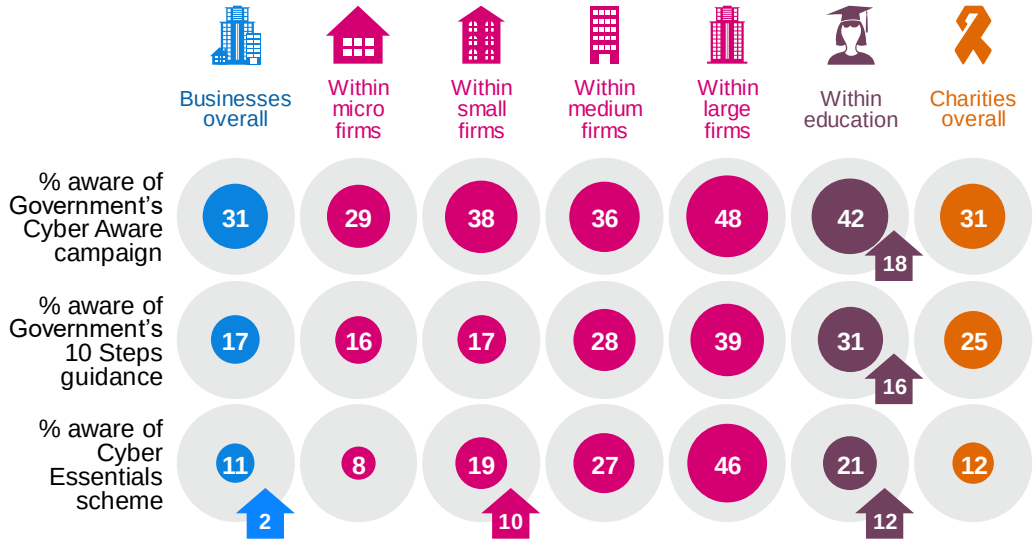
[15] See https://www.cyberessentials.ncsc.gov.uk/.

There is an especially wide gap between the largest and smallest businesses when it comes to Cyber Essentials, with just eight per cent of micro businesses having heard of this scheme.

There is a similar heightened awareness among high-income charities, where 45 per cent have heard of Cyber Aware, 40 per cent have heard of the 10 Steps guidance and 30 per cent have heard of Cyber Essentials.

Education firms tend to have greater awareness of all of these Government initiatives than firms in other sectors, as shown in Figure 3.5. Information and communications firms also tend to be more aware of the 10 Steps guidance (26%, vs. 17% overall) and Cyber Essentials (26%, vs. 11% overall).

Figure 3.5: Awareness of Government cyber security initiatives and accreditations



Bases: 1,566 UK businesses; 757 micro firms; 321 small firms; 281 medium firms; 207 large firms; 95 education firms; 514 charities

Among businesses, the longer-term trend shows rising awareness of all three initiatives across the four years of the survey. Awareness of Cyber Aware has increased by 10 percentage points since 2017 (when this question was first asked). Awareness of the 10 Steps guidance and Cyber Essentials have each risen by five percentage points since 2016.

What do organisations think of Government guidance?

In the qualitative interviews, there was a sense that the volume of Government guidance on cyber security had grown considerably over the past few years. However, this must be taken alongside the quantitative findings that many organisations are still not aware of such guidance. We specifically targeted those that had used Government guidance to take part in interviews.

Reflecting findings from previous years, Government sources were considered as highly trustworthy. For example, one business had used the NCSC website to verify things they had read elsewhere.

Those that had used the NCSC website, predominantly the individuals in IT or cyber professional roles, had considerable positive feedback. Some highlighted how the website had kept up with the latest developments and trends. This included, for example, moving beyond general password guidance towards two-factor authentication guidance, or covering emerging issues in blog posts.

There was a general consensus that the NCSC website was very well laid out, and that the guidance available on the website was often written with non-technical users in mind. On the

other hand, some cyber security or IT professionals felt that the level of information on the website was not technical enough. Some also felt the guidance they had seen was too generic, and that it was important to tailor guidance as much as possible to be relevant to their sector.

"[Government guidance] has allowed a very complex area to be boiled down in a way that non-technical, non-cyber people can get a handle on, and by doing that, they have enabled senior management and boards to engage in this area."

Medium business

Another common theme was that it was helpful to have guidance laid out in a variety of formats. Some were keen to see more case studies on the NCSC website that helped to show how to implement guidance in real-life business situations, while others mentioned having more succinct summary guidance, more top five or top ten lists, and more video guidance.

3.5 The General Data Protection Regulation

Overall awareness of GDPR

The majority of businesses (88%) have heard of GDPR, which came into force in May 2018 (a few months before the fieldwork for the 2019 survey). Awareness is even higher among charities (94%). As expected, this is substantively higher than in the 2018 survey, which was pre-GDPR implementation – at that time, 38 per cent of businesses and 44 per cent of charities were aware of the then-upcoming law.[16]

The organisations least likely to be aware of GDPR include businesses in the construction (79% aware) and food and hospitality sectors (78%), as well as firms based in the Yorkshire and Humberside region (77%). However, unlike most other measures in this survey, awareness of the existence of GDPR is broadly consistent across all business sizes and charity income groups.

Awareness of GDPR's implications for cyber security

While awareness of the GDPR law is near-unanimous, awareness of its implications for cyber security is much lower, and varies more with organisation size. These questions have been asked for the first time in this year's survey.

- Six in ten businesses (58%) and seven in ten charities (69%) are aware that organisations can incur fines for cyber security breaches involving personal data. Medium businesses (78%), large businesses (84%) and high-income charities (88%) tend to be more aware of this than average. Food and hospitality businesses are among the least aware (45%).
- Around half of all businesses (46%) and charities (54%) are aware that organisations need to report personal data breaches to the ICO within 72 hours of discovering them. Again, awareness is higher than average among medium (66%) and large businesses (77%) as well as high-income charities (80%). It is lower than average among construction firms (36% aware).

Impact of GDPR on cyber security

Three in ten businesses (30%) and over a third of charities (36%) say they have made changes to their cyber security policies or processes as a result of GDPR. Again, this is much greater among medium businesses (51%) and large businesses (62%), and among high-income charities (74%).

[16] Fieldwork for the 2018 survey took place in winter 2017.

We ask those that have made specific changes about what they have done. The most frequently mentioned changes (unprompted) are creating new policies or procedure (60% of the businesses and charities that have made changes), additional staff training and communications (15% of these businesses and 17% of these charities), updating firewall or systems configurations (11% and 4%), and new contingency plans (6% and 10%).

Qualitative findings on the broader attitudinal and behavioural impact of GDPR

The quantitative survey findings show that GDPR has, in many cases, led to changes in cyber security. In the qualitative interviews, we further explored its impact on attitudes and behaviours.

The general consensus was that GDPR has had a positive impact. For some organisations, it had played a large part in introducing them to the concept of cyber security. For those that already had cyber security policies and processes in places, it acted as a helpful incentive to check their existing approaches. Across interviews, examples of this impact included:

- greater engagement among board members, with data security becoming a regular discussion point at board meetings or the board getting more regular updates
- reviews and more consistent enforcement of data security policies and processes, for instance around the encryption of personal data
- the introduction of staff training around GDPR compliance, which often included a cyber security element
- reviews of IT infrastructure, including servers, laptops and website security
- improved awareness of the types of data held across the whole organisation.

“GDPR certainly sharpened things up … People became more aware of things we were doing that perhaps we shouldn't have been doing, or information we were holding we shouldn't have been.”

Large business

In some instances, however, the particular focus on data protection meant that cyber security was not being considered holistically. While this was not the case for all organisations, some appeared to use the terms data protection and cyber security interchangeably. These organisations were typically the ones that had done little on cyber security prior to GDPR, but had now introduced new policies and processes. They still tended to have fewer technical cyber security controls in place.

Will the impact of GDPR be sustained?

In the qualitative interviews, organisations typically felt that GDPR would have a lasting impact on their approaches to cyber security. Some organisations were continuing to make changes to their policies and processes at the time of fieldwork, meaning that GDPR was still a topic of conversation among staff. Even the organisations that felt they had already done enough around GDPR said that there was still an ongoing commitment to review policies and processes annually to make sure they continue to be fit for purpose.

"GDPR has been kicked into pretty long grass now, because we feel we are where we are. We are happy that we have progressed as we did. We've implemented the changes we needed to make. We are aware that we need to keep looking at things.”

Medium business

Chapter 4: Approaches to cyber security

This chapter looks at how much businesses and charities are investing in cyber security and what factors drive this level of investment. It then examines how organisations approach the subject of cyber security with their staff, and the policies and procedures they have in place to identify and reduce cyber security risks.

4.1 Investment in cyber security

Levels of investment

Seven in ten businesses have some level of spending on cyber security, which is a similar proportion to those who invested in cyber security in the last two years.[17]

Charities are again much less likely than businesses to spend anything on cyber security, with only four in ten doing so. However, the proportion of charities spending nothing has greatly decreased since 2018 (from 68% to 59%), reflecting their greater engagement with the topic, as seen throughout Chapter 3.

Larger businesses tend to spend more, as illustrated in Table 4.1. Spending for charities also follows a similar pattern, with high-income charities (with £500,000 or more) spending a median amount of £2,100, and the very largest charities (with £5 million or more) spending a median amount of £12,100.

Table 4.1: Average investment in cyber security in last financial year[18]

	All businesses	Micro/ small businesses[19]	Medium businesses	Large businesses	All charities
Mean spend	£5,100	£3,490	£25,100	£277,000	£1,500
Median spend	£200	£200	£5,000	£42,600	£0
% spending £0	33%	33%	18%	16%	59%
Base	1,272	933	204	135	424

There is typically a very high variance in the spending estimates collected in the quantitative survey. This may, to a small extent, indicate a certain amount of noise in the survey data, with some organisations underestimating or overestimating their spending. It more predominantly reflects that many organisations spend very little on cyber security while others spend millions of pounds in this area. For this reason, we do not expect to find – and have not found – statistically significant differences in mean spending figures across years.[20] In addition, looking

[17] Respondents were asked to include spending on any activities or projects to prevent or identify cyber security breaches or attacks, including software, hardware, staff salaries, outsourcing and training-related expenses, but excluding any spending undertaken to repair or recover from breaches or attacks.

[18] The estimates in this table are presented to three significant figures, or to the nearest whole number (if under 100). The mean and median scores exclude “don’t know” and “refused” responses. They merge together the answers from respondents who gave a numeric value as well as those who gave only a banded value (because they did not know the exact answer). For the latter, we have imputed numeric values from the given banded values. We lay out this approach in detail in the Technical Annex.

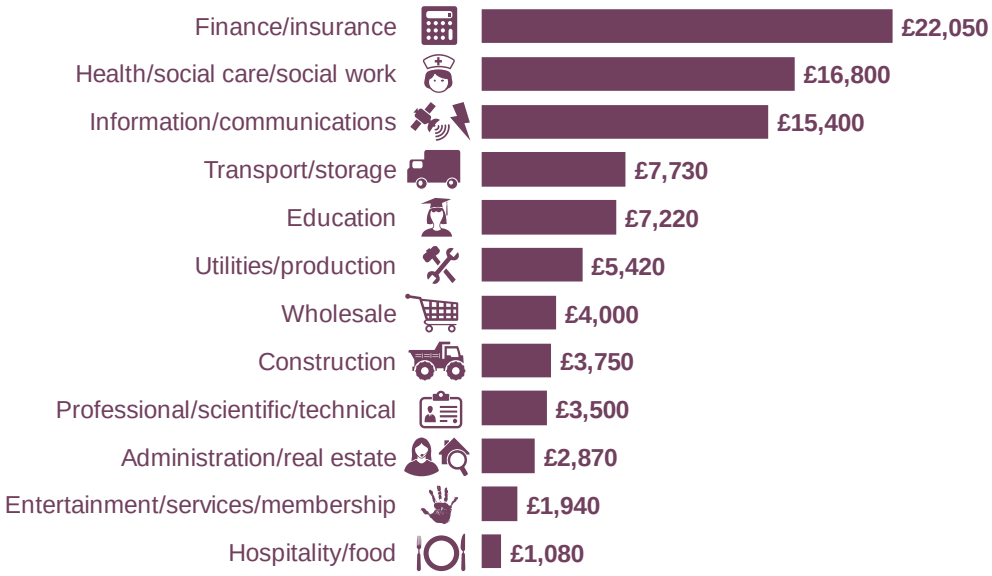
[19] Statistical significance testing of spending estimates against previous years takes into

[20] Statistical significance testing of spending estimates against previous years takes into account inflation of 2.2% since the 2018 survey, 5.1% since the 2017 survey and 6.6% since the 2016 survey, based on Office for National

at the general trend in spending estimates (means and medians) across the four years of the survey, there is no pattern to suggest that organisations have increased or decreased their spending in this area.

As shown in Figure 4.1, spending across businesses tends to be higher in sectors that consider cyber security as more of a priority, notably among finance or insurance, health, social work and social care, and information or communications firms – this is consistent with previous years.

Figure 4.1: Average (mean) investment in cyber security in last financial year, by business sector grouping



Bases: 138 administration or real estate firms; 113 construction firms; 79 education firms; 73 entertainment, service or membership organisations firms; 95 finance or insurance firms; 104 food or hospitality firms; 55 health, social care or social work firms; 82 information, communications or utility firms; 144 professional, scientific or technical firms; 181 retail or wholesale firms; 96 transport or storage firms; 112 utilities or production firms

Drivers of investment

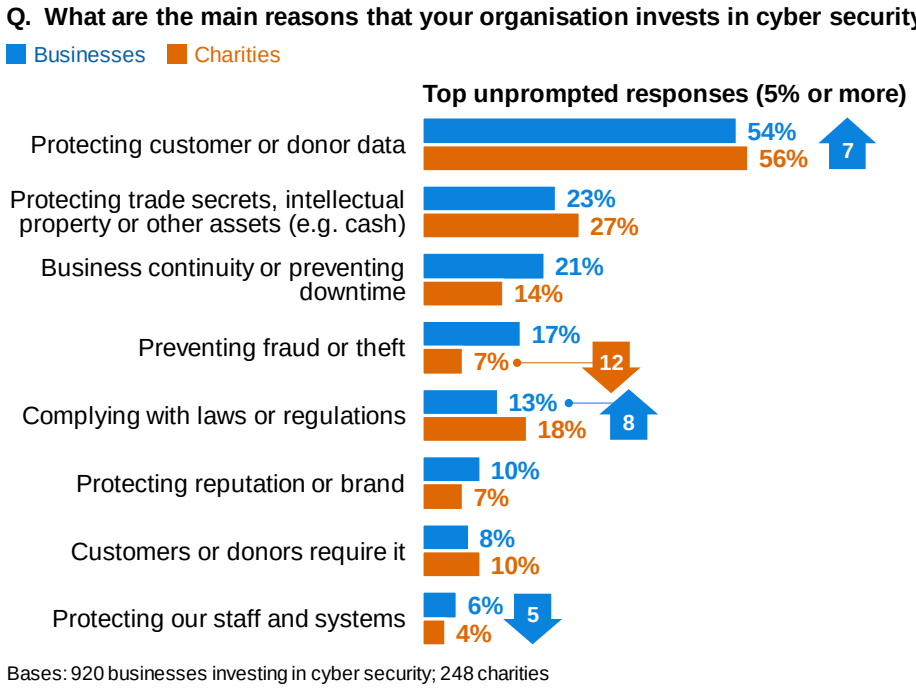
Among the organisations that do invest in cyber security, the main (unprompted) reason they give for doing so is to protect customer or donor data, as Figure 4.2 shows. The next most common concern is around protecting trade secrets, intellectual property or cash, followed by other reasons such as business continuity, fraud prevention and compliance.

There have been various shifts in these figures compared to the 2018 survey. For businesses, the increase in the proportion stating protection of customer data and compliance may be linked to the introduction of GDPR in May 2018.

The ranking of these answers has not changed amongst charities. However, the proportion mentioning fraud or theft has gone down. This may also suggest a realignment of priorities to focus on personal data as a result of GDPR. In qualitative interviews, as noted in Chapter 3, we found some evidence of this realignment, with some organisations framing cyber security narrowly in terms of data protection. However, the proportion that give GDPR as a specific reason only accounts for one per cent of the businesses and one per cent of the charities that invest in cyber security.

Statistics (ONS) data. This has been taken from the ONS website, at: https://www.ons.gov.uk/economy/inflationandpriceindices.

Figure 4.2: Main reasons for investing in cyber security, among organisations that invest



Bases: 920 businesses investing in cyber security; 248 charities

Among businesses, the key reasons for investing vary by size and sector:

- Large businesses are more likely than others to cite reputation (24%, vs. 10% overall), compliance (23%, vs. 13% overall), protecting trade secrets or intellectual property (21%, vs. 11% overall)[21] and customers requiring it (16%, vs. 8% overall).
- Information or communications businesses are more likely to mention business continuity (33%, vs. 17% overall) and protecting trade secrets or intellectual property (21%, vs. 11% overall)[21].
- Education businesses are more likely to say customers require it (21%, vs. 8% overall).

Investment in cyber insurance and claims made

A total of 11 per cent of businesses and six per cent of charities say that they have a specific cyber security insurance policy. This is higher among medium businesses (31%) and large businesses (35%), as well as the very largest charities (45% of those with incomes of £5 million or more). By sector, it is higher among finance or insurance businesses (23%) and health, social care or social work businesses (21%).

While the overall percentages have not significantly changed year-on-year, they have risen for medium businesses (up from 19% in 2018) and large businesses (up from 24% in 2018), suggesting that the cyber insurance market has experienced growth in the last 12 months.

A further 15 per cent of businesses and 10 per cent of charities have previously considered but ruled out having cyber insurance.

Of those who have cyber insurance, a very small proportion have made an insurance claim (3% of businesses and 12% of charities).

[21] This mention of trade secrets or intellectual property excludes those specifically saying cash, so is different from Figure 4.2.

Reasons for not taking up cyber insurance

Among those who do not have cyber insurance, the main reasons they give for this are:

- already being covered by an external cyber security provider (23% of businesses and 26% of charities)
- lack of awareness of cyber insurance (23% of businesses and 15% of charities)
- considering themselves to have too low a risk, which is a more common response among charities (29%) than businesses (22%).

Charities are somewhat more likely than businesses to say they are aware of cyber insurance but have not weighed it up yet (7% vs. 3%, among those that do not have insurance).

Qualitative views on cyber insurance

In the qualitative interviews, we spoke to various organisations that had cyber insurance policies. Some had only adopted these policies within the last year.

There was a sense among these organisations that the cyber insurance market had become more developed, with policies appearing to be more accessible than before, and with some organisations saying that insurance premiums had decreased.

Across interviews, we found several motivations for purchasing cyber insurance, beyond just the level of liability being covered:

- Various organisations were frank that, in the case of a breach, they might not get a substantive payment from an insurance claim. However, their main drivers for taking up insurance were often the extras that went alongside any payment, such as having access to a breach management team or a forensics team to analyse the breach. They felt that these extras would help them manage the reputational damage from a breach, which was their greatest concern.

  "We have to pay the first £25,000 … but for me, the most important thing is that it gives me access to a breach management team, including solicitors and PR."

  Large business

- Some organisations that supplied other businesses were using cyber insurance as a proxy form of accreditation. Having insurance was something they could advertise to their business clients to demonstrate they had undertaken due diligence.

  "Increasingly, you're beginning to see it on supplier questionnaires: do you have cyber insurance? A bit like a number of the cyber security badges … they are useful in demonstrating to other people that you take this seriously."

  Large business

- In some organisations, the individuals responsible for cyber security did not have a clear understanding of what the insurance covered. They had agreed to take it on for peace of mind, on the advice of their insurance broker. In these cases, the insurance broker was a particularly powerful influencer.

  "It's a bit of peace of mind … It reduces the risk a little bit because you get some compensation, but at the end of the day, I don't ever want to claim on that."

  Small business

We also explored views on how the presence of cyber insurance might affect behaviour and attitudes to risk management. Organisations noted that they considered cyber insurance as complementary, rather than as a substitute for other forms of cyber risk management.

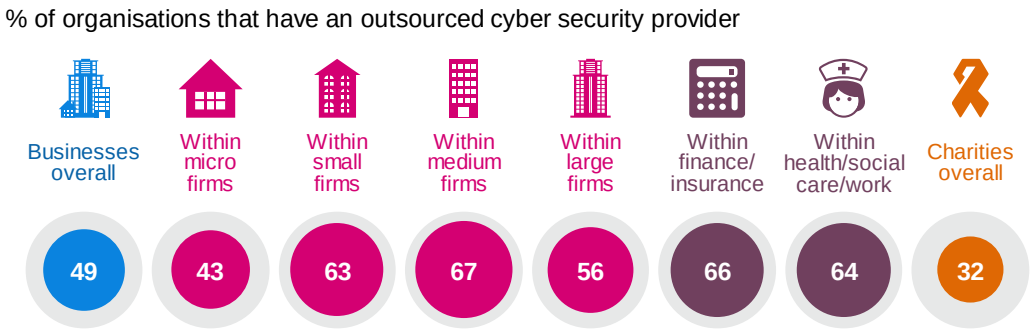
One rationale for this was that some organisations did not expect insurance claims to necessarily cover the direct financial loss of breaches. Instead, they had purchased insurance policies for the previously mentioned reasons. Another rationale was the fact that wider staff would not typically know that an organisation had cyber insurance, so there would not be a direct link between their actions and the presence of insurance.

4.2 Outsourcing cyber security

Around half of all businesses (49%) and three in ten charities (32%) have an external cyber security provider. There is an indication that this has risen among charities since 2018, although the change is not statistically significant.

As Figure 4.3 shows, outsourcing is more common among small and medium businesses than others – a similar pattern to previous years – and among firms in the finance or insurance, and health, social care or social work sectors. The pattern is different for charities, where outsourcing is more typical among high-income charities with incomes of £500,000 or more (72%).

Figure 4.3: Use of external cyber security providers



Bases: 1,566 UK businesses; 757 micro firms; 321 small firms; 281 medium firms; 207 large firms; 117 finance or insurance firms; 79 health and social care firms; 514 charities

A further five per cent of businesses and six per cent of charities say they do not currently outsource any aspects of cyber security but intend to do so.

Qualitative insights on outsourcing decisions

In the qualitative interviews with organisations that outsourced aspects of their cyber security, we found that the extent of what was outsourced, rather than done in-house, was unique to each organisation. Some said they outsourced everything, while others only sought outside help for specific functions such as firewall installation. Typically, organisations outsourced any areas they felt they did not have the skills, time or resources to cover themselves. Some organisations also saw outsourcing as a cost-effective way of bringing in additional expertise to supplement the skills within their organisation. These mirror the findings from an earlier DCMS study (published in December 2018) on the UK cyber security skills labour market.[22]

There were, however, a small number of recurring themes around what organisations preferred to keep in-house:

- anything that provided access to the organisation's finances

[22] See https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market.

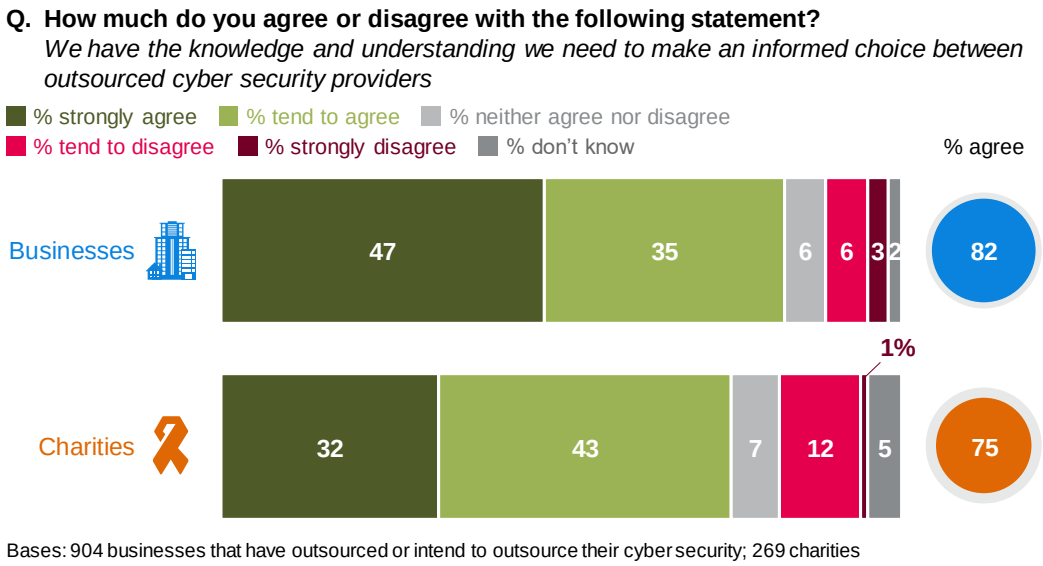
- infrastructure changes that might significantly affect day-to-day performance, which some organisations felt were better managed by internal IT teams.

The types of organisations we spoke to were outsourcing to professional service providers or consultants. As such, their outsourcing decisions were service-led rather than product-led. This meant that they did not have any specific knowledge about the actual products and tools that their external providers were using. This was not something that organisations felt they needed to evaluate – they felt it was the external provider's responsibility to choose the best tools for the job – and, moreover, some did not feel capable of evaluating specific cyber security products.

Choosing a provider

Among the businesses and charities that outsource cyber security or intend to do so, four in five businesses (82%) and three-quarters of charities (75%) agree that they have sufficient knowledge and understanding to make an informed choice between outsourced cyber security providers. Relatively few disagree (9% of businesses and 13% of charities), and there are no particular size bands or sectors that stand out as being more likely to disagree. This is shown in Figure 4.4.

Figure 4.4: Whether organisations fell they can make an informed choice between outsourced cyber security providers



Bases: 904 businesses that have outsourced or intend to outsource their cyber security; 269 charities

Impact of outsourcing cyber security

Analysis of the quantitative data shows a positive relationship between outsourcing cyber security and treating it as a high priority, even when controlling for size. When looking just at micro businesses that outsource, 47 per cent consider cyber security to be a very high priority (vs. 31% of micro businesses that do not outsource).

The qualitative findings also support this view. Some organisations saw having a contract with an external cyber security provider both as a way of signalling that they were taking cyber security seriously, and as a way of improving their overall cyber resilience. It showed their willingness to invest in the area and brought in expertise beyond that in the organisation. This contrasts with the alternative hypothesis that organisations were deprioritising cyber security by outsourcing it – the qualitative evidence here suggests that this is not how organisations felt.

External providers were also an important source of information and guidance for organisations, so were also able to spread best practice. For example, one high-income charity working in

social care had their external provider carry out training with staff around phishing emails. The charity felt this had led to improved staff awareness and behaviour.

At the same time, there was little evidence of ongoing monitoring or checks being carried out on external providers. These relationships were instead often built on trust – another finding that reflects previous DCMS research on the cyber security skills labour market. Some organisations did not feel capable of monitoring their performance and felt they would not know what questions to ask. Unless something had gone visibly wrong, like a visible cyber security breach, there were no clear metrics for organisations to use to assess whether their provider was doing a good job or not.

"We do rely heavily on our outsourced provider. That's their speciality … I'm confident they know what they are doing, and that we have the right policies and procedures in place."

Medium business

"I suppose the danger of [the external provider] having done it for so long is that we are complacent, because it is all done by them and we don't have to think about it."

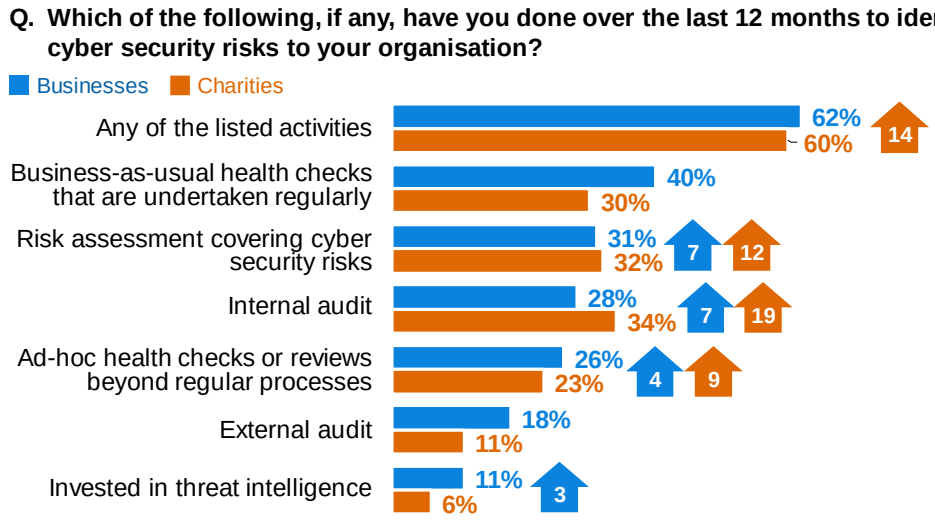
Small business

4.3 Risk management

Actions taken to identify risks

Around six in ten businesses (62%) and charities (60%) have taken actions in the last 12 months to help identify cyber security risks to their organisation. As Figure 4.5 indicates, businesses and charities are more likely to take one or more of these actions than they were in 2018. The longer-term trend for businesses shows a more substantive increase since the 2016 survey, when 51 per cent of businesses were doing any of these things (vs. 62% in 2019).

Figure 4.5: Ways in which organisations have identified cyber security risks in the last 12 months



Bases: 1,566 UK businesses; 757 micro firms; 321 small firms; 281 medium firms; 207 large firms; 514 charities

The changes over time are largely driven by changing behaviour among micro businesses (59% take any of these actions, vs. 42% in 2016) and low-income charities (52% take any action, vs. 38% in 2018), which are catching up with larger organisations. This is likely to be one of the impacts of GDPR on small organisations that had previously not documented their risks.

Medium businesses (79%) and large businesses (93%), as well as high-income charities (86%) are still more likely than others to have taken any of these actions. Finance or insurance firms

(82%), education firms (76%) and professional, scientific or technical firms (73%) are also more likely than average (62%) to have taken any of these actions.

All organisations are more likely to be undertaking more than one of these actions than in previous years. For businesses, 42 per cent have done two or more of these things in the last 12 months (vs. 34% in the 2018 survey, and 30% in 2016). For charities, 40 per cent have done two or more of these things (vs. 24% in the 2018 survey).

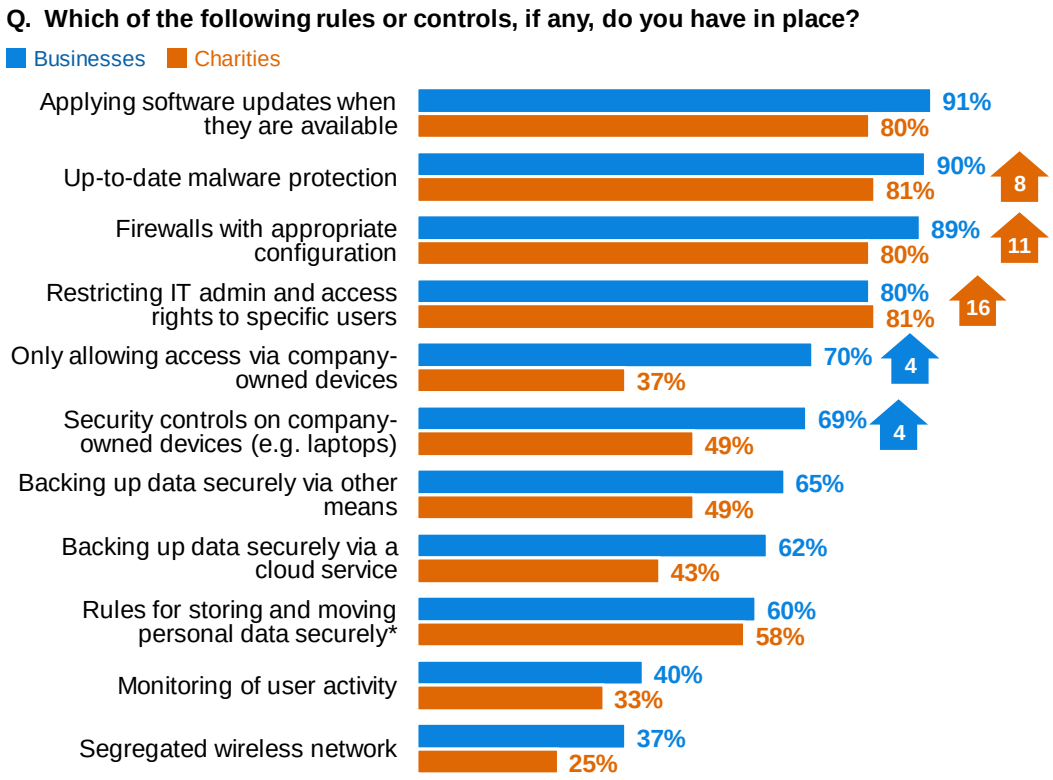
Actions taken to prevent or minimise risks

The overwhelming majority of organisations have certain cyber security rules or controls in place (Figure 4.6). The vast majority of both businesses and charities say they apply software updates when available, have up-to-date malware protection, have configured firewalls, and restrict admin rights to specific users. Charities are more likely to have several of these basic technical controls in place than they were last year (indicated by the arrows in Figure 4.6), which may be another impact of the introduction of GDPR.

Businesses have also seen an increase in the proportions placing security controls on company devices and restricting access to company-owned devices.

In several areas, charities are still behind businesses on average. This includes having security controls on devices, restricting BYOD, backing up data, and monitoring user activity.

Figure 4.6: Rules or controls that organisations have implemented



Bases: 1,566 UK businesses, 514 charities
*This was a new answer option for 2019.

Businesses in the food and hospitality sector, who are less likely to say that cyber security is a high priority, are also among the least likely to have each of these rules or controls in place. For example, fewer say they apply software updates when available (78%, vs. 91% overall) or have up-to-date malware protection (75%, vs. 90% overall). And just a third (35%, vs. 60% overall) have specific rules on storing and moving personal data.

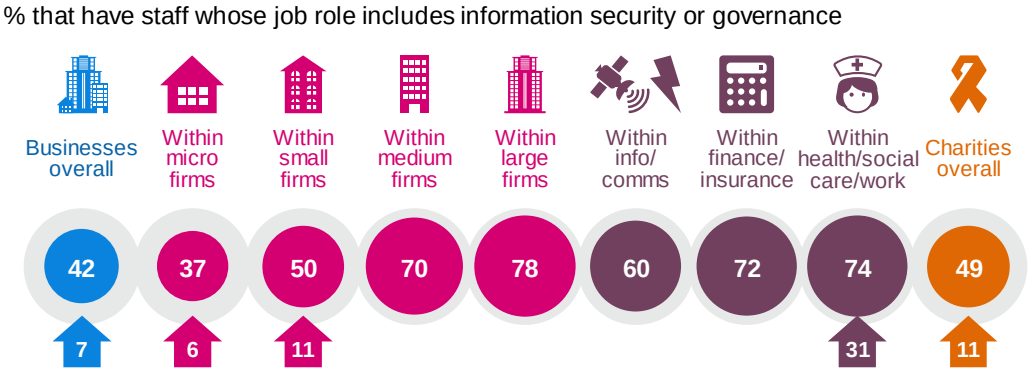
4.4 Staff approaches

Who is responsible for cyber security?

Around four in ten businesses (42%) and half of all charities (49%) have staff whose job role includes information security or governance. These have both increased since last year, as Figure 4.7 shows. This increase may again be linked to GDPR – this law requires organisations that regularly process personal data on a large scale to appoint a Data Protection Officer within their organisation, whose role would cover parts of information security and governance.

Medium and large firms are again more likely than the average business to have specialist staff dealing with cyber security, as are specific sectors such as health, social care or social work, finance or insurance, and information or communications. High-income charities are also much more likely to have someone in this role (82%, vs.49% overall).

Figure 4.7: Whether businesses have specialist staff dealing with cyber security



Bases: 1,566 UK businesses; 757 micro firms; 321 small firms; 281 medium firms; 207 large firms; 102 information and communication firms; 117 finance and insurance firms; 79 health and social care firms; 514 charities

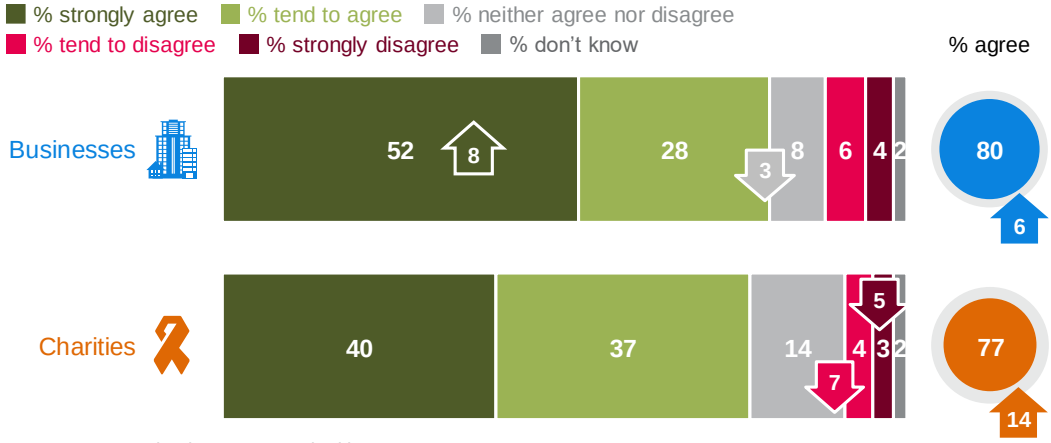
Perceived skills shortages and skills gaps

Skills shortages occur when organisations cannot recruit the individuals with the necessary skills to carry out the jobs required. As Figure 4.8 illustrates, the vast majority of businesses (80%) and charities (77%) feel that they have enough people within their organisation dealing with cyber security to be able to effectively manage the risks. And, for both businesses and charities, the proportion agreeing has risen since this question was first asked in 2018.

Businesses in the food and hospitality sector are among the least likely to agree (70%, vs. 80% overall). Businesses in the East of England are more likely to disagree they have enough people (15% disagree, vs. 9% of all businesses).

Figure 4.8: Perceptions of cyber skills shortages

Q. How much do you agree or disagree with the following statement?
We have enough people dealing with cyber security in our organisation to effectively manage the risks



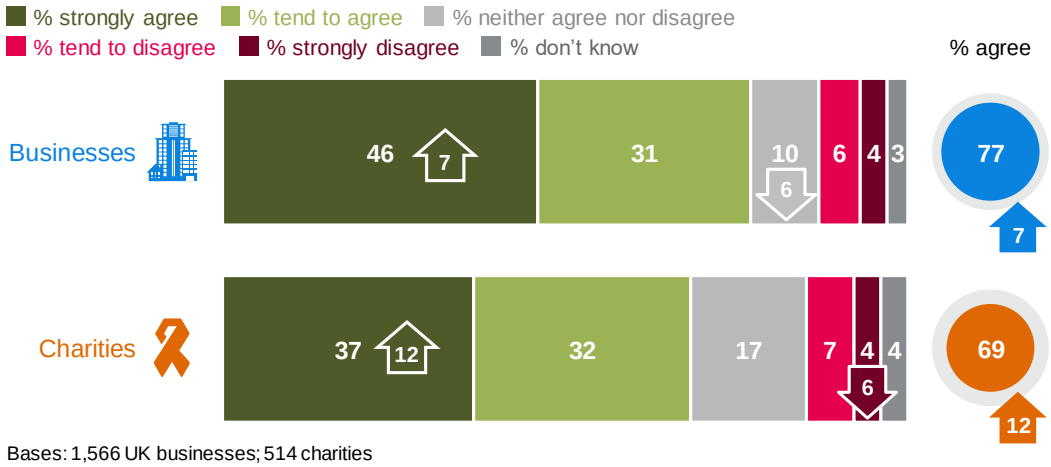
Bases: 1,566 UK businesses; 514 charities

Skills gaps refer to situations when current employees within an organisation do not have the right skills to carry out their job as required. The vast majority of organisations do not feel they have a skills gap in cyber security, and this belief has also gone up since the 2018 survey, as Figure 4.9 illustrates.

However, this differs by size. Micro businesses are less likely to agree than large ones (74% vs. 83%) and low-income charities are less likely to agree than high-income ones (66% vs. 83%). As with the skills shortages question, businesses in the food and hospitality sector are less likely than average to agree (62%, vs. 77% overall).

Figure 4.9: Perceptions of cyber skills gaps

Q. How much do you agree or disagree with the following statement?
The people dealing with cyber security in our organisation have the right cyber security skills and knowledge to do this job effectively



Bases: 1,566 UK businesses; 514 charities

It is important to put the findings on skills shortages and skills gaps in context. The previously mentioned DCMS research in 2018 on the UK cyber security skills labour market highlighted the large number of staff working informally – lacking basic technical skills – in cyber security roles. This was particularly common in micro and small businesses and in low-income charities.[23] The

[23] See https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market.

next section of this report highlights that while the proportion of organisations training staff in cyber security is increasing, it is still relatively low. Many organisations may assume they have the necessary skills, without fully understanding the technical requirements of the role.

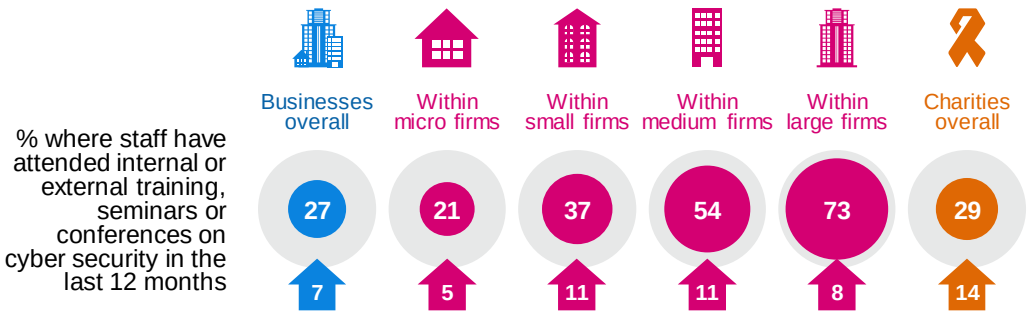
Staff training

Just under three in ten businesses (27%) and charities (29%) report that staff have attended internal or external training, including seminars or conferences on cyber security in the previous 12 months.

As Figure 4.10 shows, this is still more common among larger firms. Staff from high-income charities are also more likely than average to have attended relevant training (56%, vs. 29% overall). Although overall figures remain low, there have been increases across the board compared to 2018.

There are also a large number of sectors that stand out as being more likely to train their staff. These include finance or insurance (56%, vs. 27% overall), information or communications (45%), health, social care and social work (45%), education (42%), and professional, scientific or technical firms (37%).

Figure 4.10: Organisations where staff have had cyber security training in the last 12 months



Bases: 1,566 UK businesses; 757 micro firms; 321 small firms; 281 medium firms; 207 large firms; 514 charities

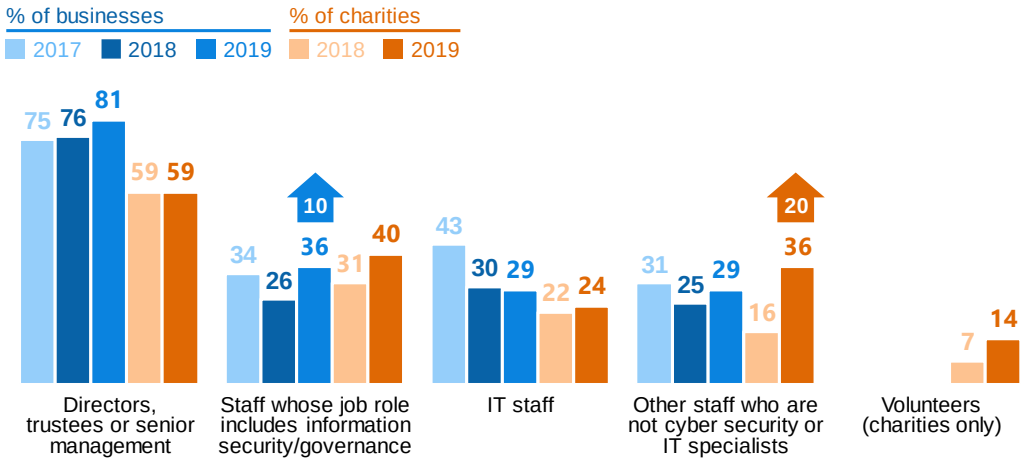
Figure 4.11 shows which staff have attended cyber security training, within the organisations that have arranged it. As in previous years, directors, trustees or senior managers are the ones most likely to go to such training.

In businesses, the increase in the proportion of information security or governance staff attending represents a return to the 2017 result (34% in 2017 and 36% in 2019). The proportion of IT staff attending such training fell from 43% in 2017 to 30% in 2018, and this drop has been maintained in 2019. For this chart, we have shown all the trend data from previous years, to highlight that the trend for information security or governance staff is inconsistent across years.

The substantive increase in non-specialist staff in charities attending cyber security training may, in particular, be related to GDPR. The qualitative interviews highlight that charities are typically sending general managers on GDPR-related training, and charities may be conflating this with specific cyber security training when responding to the survey.

Figure 4.11: Which individuals receive cyber security training where it is offered

Q. Who in your organisation attended any of the training, seminars or conferences over the last 12 months?



Bases: 621 businesses that offer cyber security training; 217 charities
Arrows only show significant changes from the 2018 survey.

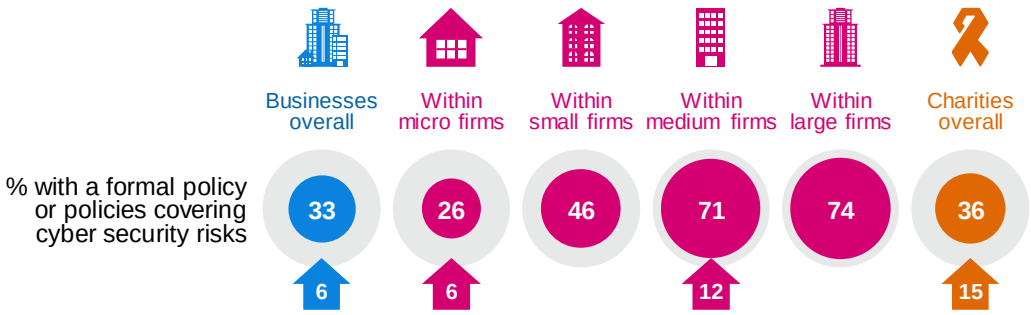
4.5 Governance and planning

Formal cyber security policies

Around a third of businesses (33%) and charities (36%) have a formal policy or policies covering cyber security risks, which has increased for both groups since 2018. For businesses, this is a return to the 2017 score.

Importantly, as Figure 4.12 shows, it is still much rarer for micro and small businesses to have such policies than it is for larger businesses.

Figure 4.12: Whether organisations have formal policies covering cyber security risks



Bases: 1,566 UK businesses; 757 micro firms; 321 small firms; 281 medium firms; 207 large firms; 514 charities

The following sectors are all more likely than average to have cyber security policies in place:

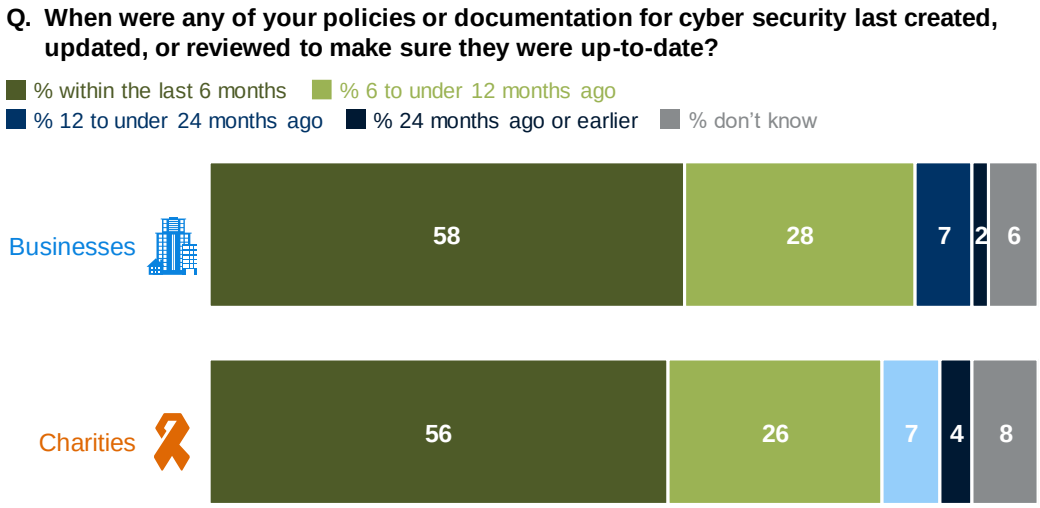
- finance or insurance (66%, vs. 33% of all businesses)
- health, social care or social work (60%)
- education (57%)
- information or communications (50%).

When were policies last reviewed?

For the first time this year, we ask when those who have cyber security policies last created, updated or reviewed them. Around six in ten organisations reviewed their policies within the last six months (Figure 4.13), and this is consistent across business size bands. This may be uniquely high this year, as this six-month timeframe would have overlapped with the introduction

of GDPR in May 2018 for many organisations. Very few (9% of businesses and 11% of charities) say they last reviewed them more than a year ago.

Figure 4.13: When organisations last reviewed their cyber security policies



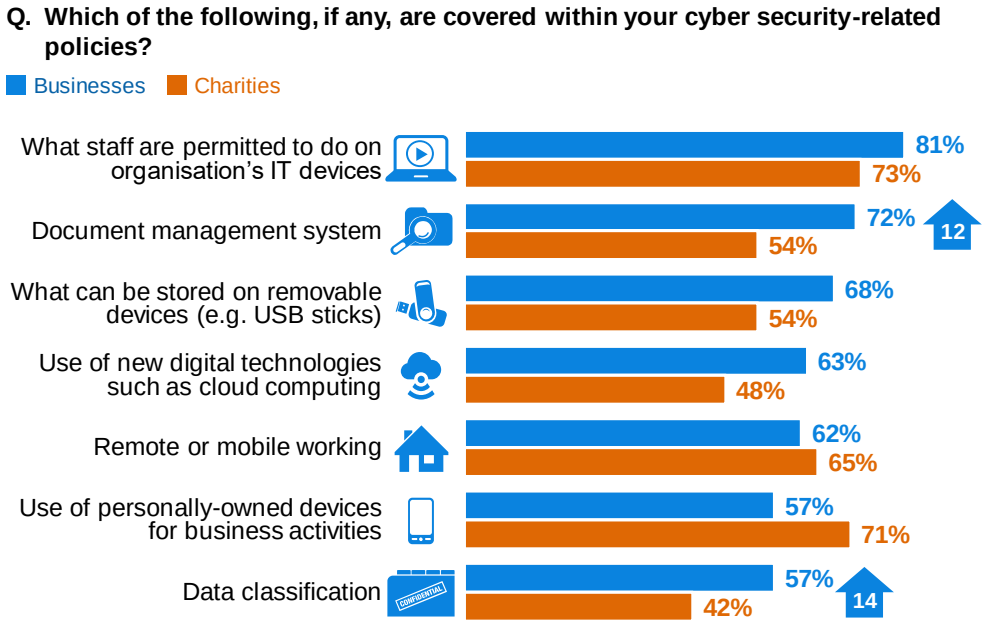
Bases: 742 businesses with cyber security policies; 266 charities

What is covered in cyber security policies?

The most common attributes of cyber security policies, among the organisations that have them, are displayed in Figure 4.14. Businesses' cyber security policies typically cover several of the topics shown here, but use of personal devices, or BYOD, and data classification still tend to be less commonly covered than other topics.

Charities are less likely to have many of these topics featured in their cyber security policies, including document management, removable devices, new digital technologies and data classification. The use of personally-owned devices for business activities is, by contrast, a more common feature in charities' cyber security policies than in businesses' policies. This may be because charities, particularly low-income charities, are more likely than businesses to use personal devices, such as mobiles or laptops, for work purposes.

Figure 4.14: Most common features of cyber security policies



Bases: 742 businesses with cyber security policies; 266 charities

The increases in the proportion of businesses mentioning document management and data classification may reflect that these two topics are particularly linked to GDPR, and how the use of personal data is controlled – although the same rise is not seen among charities.

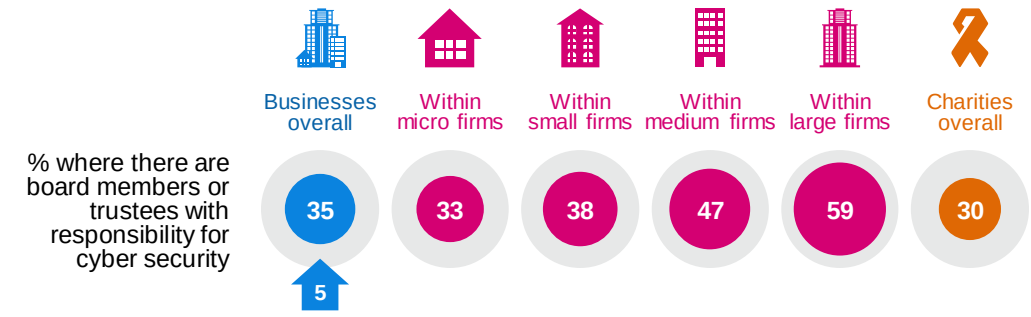
Looking over all four years of the survey, the proportion of businesses writing about new digital technologies such as cloud computing in their policies has also increased year-on-year (from 52% in 2016 to 63% in 2019).

Board responsibilities

The proportion of businesses with a board member dedicated to cyber security has increased since 2018, to over a third (35%) this year. Three in ten charities (30%) also have a trustee with responsibility for cyber security.

The larger the business, the more likely it is to have this role at board level, as Figure 4.15 shows.

Figure 4.15: Whether organisations have board members or trustees with responsibility for cyber security



Bases: 1,566 UK businesses; 757 micro firms; 321 small firms; 281 medium firms; 207 large firms; 514 charities

Finance or insurance firms (56%), information or communications firms (53%) and education businesses (50%) are also more likely than the average firm (35%) to have board members with

a cyber security brief. Conversely, those in the food and hospitality sector are among the least likely to have this (14%).

Reasons for not having governance procedures in place

In total, 23 per cent of businesses and 27 per cent of charities have none of the governance measures mentioned in the quantitative survey (and discussed across this chapter). This includes: board members or trustees with cyber security responsibilities, cyber security policies, an external cyber security provider, staff members covering information security or governance, or a business continuity plan.

The most common reason that these businesses and charities give (unprompted) for this is that they consider themselves too small or insignificant to warrant such measures (for 35% of businesses and 46% of charities without these measures). The second most common reason for businesses is that cyber security is not considered enough of a priority (for 21%, vs. 16% of charities). This is followed by not considering cyber attacks to be a significant risk (for 19% of these businesses, vs. 26% of charities).

It is worth noting that the ranking of these reasons has tended to shift around across years, although the top reasons given tend to be consistent. In the 2018 survey, the top reason for both businesses and charities was that cyber security was not considered enough of a priority, followed by being too small, or not feeling at risk. In 2017, the top three reasons given by businesses, and their ranking, were the same as they are in 2019.

4.6 Dealing with third-party suppliers or contractors

Fewer than one in five businesses (18%), and around one in seven charities (14%), require their suppliers to have, or adhere to, any cyber security standard or good practice guides. The figure for businesses is a significant increase of six percentage points from the 2018 survey (when it was 12%).

In line with last year, medium businesses (31%) and large businesses (46%) are more likely than others to have this requirement, as are high-income charities (31%). Among medium businesses in particular, minimum supplier standards are more common than in the 2018 survey (when 22% of medium businesses had these).

Minimum supplier standards are more common among finance or insurance businesses (47%, vs. 18% overall), information or communications firms (33%), and health, social care or social work firms (30%).

What standards do organisations demand from suppliers?

As Figure 4.16 shows, when organisations do set standards for their suppliers, the most common requirements are to adhere to recognised international standards, such as the Payment Card Industry Data Security Standard (PCI DSS) or ISO 27001. For businesses, the proportion requiring PCI DSS from their suppliers has fallen thirteen percentage points since the 2018 survey, meaning that ISO 27001 is now their most commonly requested minimum standard.

Figure 4.16: Most commonly required cyber security standards for suppliers

Bases: 401 businesses with supplier standards; 130 charities

The challenges of supplier risk management

The qualitative interviews reveal that some organisations had simply not considered their suppliers as a potential source of cyber risk before. This seemed to be a more common finding among charities. There was a sense among some organisations that, because it had never been a problem before, they did not need to look into it.

There were also attitudinal barriers, as well as awareness barriers, when it came to addressing supplier risks. One medium-sized insurance business said they had not thought about the issue until they suffered a breach emanating from one of their suppliers. Their supplier's email account was hacked and they (the insurance business) were sent new bank details alongside a fraudulent supplier invoice, which they paid. However, since the breach, they had not implemented any new risk management processes, because they felt that the breach was not their responsibility.

Further challenges included a lack of capability or resource among organisations – particularly smaller organisations. Some said they did not know what questions they should be asking suppliers or felt they lacked the authority to question larger businesses in their supply chain. Others noted that, beyond their initial due diligence when drawing up supplier contracts, they did not have the resources to regularly follow up with suppliers. This lack of resources was also frequently raised when discussing checks on the wider supply chain. Therefore, some supplier relationships were largely based on trust, particularly if they were a long-term supplier, a large company, or perceived to be a reputable brand.

"We just trust them. They've been in business for a long time. They run huge events. They are world renowned and respected. We have faith based on that."

Micro business

"Once you move on to the suppliers of your suppliers, you are getting into a 'how long is a piece of string' question. You could keep pulling … unless you're going to do an end-to-end audit of the entire supply chain, which we do not have the resources to do."

Large business

To help them with these challenges, some organisations raised the possibility of receiving guidance or checklists laying out the kinds of things they should be thinking about when taking on suppliers, or the kinds of questions they should be asking around cyber security.

"You don't know what to ask. I would just trust that my suppliers wouldn't breach anything. So, it would help to get some guidance."

Micro business

A general view was that, despite the existence of Cyber Essentials, there was not necessarily an accepted minimum standard of cyber security across sectors. For example, we found that one micro business, who were themselves a supplier to several law firms, had faced challenges when being asked to adhere to varying cyber security and data protection standards for each of their business customers. This had become a significant cost to their business, because each customer insisted on their own standards and processes being followed.

How are organisations evaluating suppliers?

In the qualitative interviews, we also spoke to organisations that had carried out various forms of due diligence when procuring suppliers. This included things like service level agreements, audits, demanding certain credentials like Cyber Essentials, or asking cyber security-related questions in interviews. Some had more thorough checks in place for suppliers that had direct access to the organisation's data, or said they would naturally pay extra attention to suppliers if they were handling sensitive data.

"If they're providing us with connectivity, we need to know as much as we can about how they're securing that, whereas if someone provides us with a flat-panel television, the security issues with that are non-existent."

Large business

There was again a sense that GDPR had strongly influenced the due diligence process. As a result, in some organisations, the supplier checks focused on GDPR-compliance and personal data, rather than cyber security more generally.

As previously mentioned, we found fewer instances of organisations continuing to monitor their suppliers' post-procurement. This links back to the attitudinal barriers – organisations did not necessarily see this kind of monitoring as their responsibility – and time and resource barriers discussed in the previous section.

4.7 Implementing Government initiatives

Cyber Essentials

The Government's Cyber Essentials scheme enables organisations to be independently certified for having met a good-practice standard in cyber security. Specifically, it requires them to enact basic technical controls across five areas: boundary firewalls and internet gateways, secure configurations, user access controls, malware protection, and patch management (applying software updates).[24]

Regardless of whether they are aware of Cyber Essentials or not, over half of all businesses (56%) and two-fifths of charities (41%) say they have implemented technical controls in all five of these areas.[25] This is higher than in 2018 (when it was 51% for businesses and 29% for charities).

---

[24] See https://www.cyberessentials.ncsc.gov.uk/.

[25] We have derived these figures from five separate questions in the survey. They represent the percentage of businesses and charities that say they have all the following rules or controls: firewalls with appropriate configurations, security controls on company-owned devices, restricting IT admin and access rights to specific users, up-to-date malware protection, and applying software updates when they are available.

As in previous years, most organisations, particularly smaller ones, do not currently realise that they can receive Cyber Essentials certification for the measures they already have in place. As seen in Chapter 3, it is still only a small proportion (11% of businesses and 12% of charities) that are aware of the scheme.

Only six per cent of businesses, and five per cent of charities, recognise that they have fully achieved the Cyber Essentials (or Cyber Essentials Plus) standard. For businesses, this is nonetheless higher than in 2016 (when it was 2%). Among large businesses, this is at 27 per cent (vs. 11% in 2016).

10 Steps to Cyber Security

The Government's 10 Steps to Cyber Security guidance[26] sets out a comprehensive risk management regime that both businesses and charities can follow to improve their cyber security standards. These steps have been mapped to specific questions in the survey (in Table 4.2), and these are covered individually across this report. This is not a perfect mapping, but gives an indication of whether organisations have taken action in relevant areas.

Table 4.2 below brings these findings together, and for businesses shows a situation similar to the findings from the 2016, 2017 and 2018 surveys, with the exception of the user education and awareness score, which has increased by seven percentage points since 2018.

In line with last year, while most organisations have certain technical controls such as secure configuration, firewalls and malware protection, they are less likely to have formal cyber security policies – particularly ones covering home working or what can be stored on removable devices.

Table 4.2: Proportion of organisations undertaking action in each of the 10 Steps areas

	Step description – *and how derived from the survey*	Businesses	Charities
1	Information risk management regime – *formal cyber security policies and the board are kept updated on actions taken*	32%	34%
2	Secure configuration – *organisation applies software updates when they are available*	91%	80%
3	Network security – *firewalls with appropriate configurations*	89%	80% (vs. 69% in 2018)
4	Managing user privileges – *restricting IT admin and access rights to specific users*	80%	81% (vs. 65% in 2018)
5	User education and awareness – *staff training, or formal policy covers what staff are permitted to do on the organisation's IT devices*	37% (vs. 30% in 2018)	38% (vs. 21% in 2018
6	Incident management – *formal incident management plan*	16%	11%
7	Malware protection – *up-to-date malware protection*	90%	81% (vs. 73% in 2018)
8	Monitoring – *monitoring of user activity or regular health checks to identify cyber risks*	57%	47%

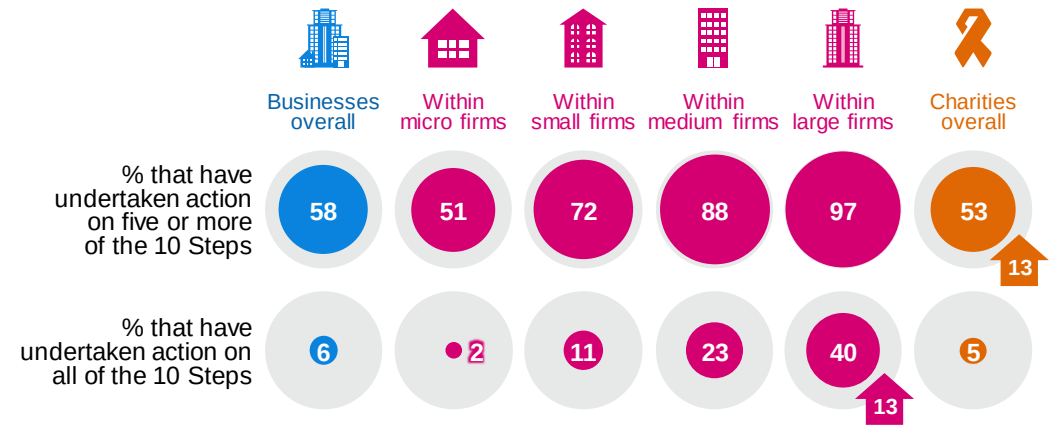
[26] See https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.

	Step description – *and how derived from the survey*	Businesses	Charities
9	Removable media controls – *policy covers what can be stored on removable devices*	22%	19%
10	Home and mobile working – *policy covers remote or mobile working*	20%	23% (vs. 12% in 2018)

Despite only 17% of businesses and 25% of charities report having heard of the 10 Steps to cyber security guidance, the vast majority of businesses (97%) and charities (92%) have implemented at least one of the 10 Steps to cyber security. In addition, over half have implemented five or more of the 10 Steps (58% of businesses and 53% of charities). This is in line with last year for businesses, but the proportion of charities who have implemented at least five of the 10 Steps has increased from 40% in 2018 to 53% in 2019. As Table 4.2 illustrates, the proportion of charities implementing the 10 Steps has increased across several measures, including firewalls, managing user privileges, user education and awareness, malware protection and home and mobile working.

Very few businesses and charities have undertaken all 10 Steps (6% and 5% respectively), as was the case in previous years. Large businesses are the most likely to have implemented all 10 Steps (40%, vs. 6% overall). This is also higher than in 2018, as Figure 4.17 shows.

Figure 4.17: Progress in undertaking action on the 10 Steps by size of business



Bases: 1,566 UK businesses; 757 micro firms; 321 small firms; 281 medium firms; 207 large firms; 514 charities

Chapter 5: Incidence and impact of breaches or attacks

This chapter provides measures of the nature, level and impact of cyber attacks and other cyber security breaches on businesses and charities over the past year. We also provide estimates of the financial cost of these breaches or attacks.

Across these findings, the survey aims to account for all the types of breaches or attacks that organisations might face. This includes accidental breaches, as well as ones perpetrated intentionally. It also includes recorded cyber attacks that did not necessarily get past an organisation's defences (but attempted to do so). We do, nevertheless, isolate and discuss the cases that had a material outcome, such as a loss of money, assets or other data.

It is important to remember that the survey can only measure the breaches or attacks that organisations have themselves identified. There are likely to be hidden attacks, and others that go unidentified, so the findings reported here may underestimate the full extent of the problem.

The findings in this chapter are not comparable with those from the 2016 survey, due to significant changes in the types of breaches or attacks being recorded from 2017 onwards.

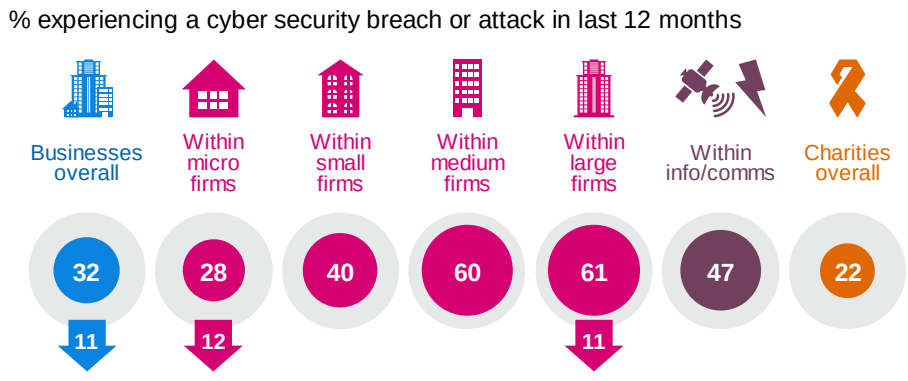
5.1 Experience of breaches or attacks

Around a third (32%) of businesses and two in ten charities (22%) reported having any kind of cyber security breach or attack in the last 12 months.

As Figure 5.1 illustrates, larger businesses are still more likely to identify breaches or attacks than smaller ones. This has been a consistent pattern in each year of the survey. Charities follow the same pattern, with 52 per cent of high-income charities recording a breach or attack – and this rises to 65 per cent among the biggest charities (with £5 million or more in income).

The information and communications sector has also been consistently more likely to identify breaches or attacks in each year of the survey. At the other end of the scale, the fewest breaches or attacks are recorded in the construction (23%, vs, 32% overall) and food or hospitality sectors (16%). This does not simply mean these two sectors are less at risk. Instead, it may also reflect that businesses in sectors more engaged with cyber security, such as those in the information and communications sector, have a heightened awareness, or carry out more monitoring, so are more likely to identify attacks.

Figure 5.1: Proportion of organisations that have identified breaches or attacks in the last 12 months



Bases: 1,566 UK businesses; 757 micro firms; 321 small firms; 281 medium firms; 207 large firms; 102 information or communications firms; 514 charities

Once again, businesses that hold personal data are more likely than average to have experienced breaches or attacks (39%, vs. 32% overall), highlighting the importance of protecting this information.

With that said, as in previous years, breaches and attacks still affect organisations that may consider themselves to have a lower risk profile. Among the businesses that say cyber security is a low priority for senior management, one in five (22%) have nonetheless experienced a breach or attack in the past year.

Changes over time

For businesses, the proportion identifying breaches or attacks (32%) is lower than in 2018 (when it was 43%) and 2017 (46%). The drop is across a range of different types of breaches and attacks (across all the categories listed in the following section). It is also across different sectors and size bands – while Figure 5.1 highlights statistically significant decreases among micro and large businesses, the percentage has also fallen for small and medium businesses (but this fall is not observed to be statistically significant).

The fall in the number of businesses identifying any breaches or attacks is consistent with a similar trend found among the general public in the Crime Survey for England and Wales (CSEW).[27] This is a representative survey by the Office for National Statistics (ONS). It has found that between September 2017 and September 2018, the number of computer misuse incident fell from c.1.5 million to c.1 million. This was driven, according to ONS data, by a significant reduction in computer viruses (down by 45% over the same period).[28]

We do not currently know the specific reasons for this change. There are a number of possible reasons for it. However, they do not necessarily align with each other:

- It may signify that businesses have increased their defences against breaches and attacks, so are recording fewer cases. This potential explanation ties in with the findings in Chapter 4, which showed that more businesses in 2019 have implemented rules or controls, governance processes and cyber security training. Further analysis of the data is inconclusive for this hypothesis. It shows that the drop in breaches or attacks from 2018 to 2019 has happened both among businesses that have formal cyber security rules, controls and processes, and among those that do not. However, it does indicate that the drop is slightly more pronounced among those that have rules, controls and processes.
- It could suggest a change in attacker behaviour, although the survey cannot directly evidence this. For example, those carrying out cyber attacks could be focusing on a narrower (though still numerous) set of businesses. This fits with another broad trend in the survey showing that, among the 32 per cent of businesses that *did* identify any breaches or attacks, the typical (median) number they recall facing has gone up, from 2 attacks in 2017 to 6 in 2019. Alternatively, attacks may simply have become harder to detect, so while fewer businesses are *identifying* them, more may be going undetected.
- It may be that GDPR has taken the focus away from breaches or attacks that are not related to personal data. This ties in with the qualitative finding that some businesses and charities, particularly smaller ones, were framing cyber security solely in terms of GDPR and data protection. However, the wider picture, from both quantitative and qualitative

[27] See https://www.ons.gov.uk/releases/crimeinenglandandwalesyearendingseptember2018.

[28] This is covered in the ONS September 2018 statistical release: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2018#computer-misuse-offences-show-a-decrease-in-computer-viruses.

evidence, is that GDPR has been a driver of improvements to cyber security. Therefore, this is also not a definitive explanation.

- It is also possible that a change like GDPR has led to some businesses answering this question in a different way from previous years. Anecdotal feedback from the survey suggests that businesses may have, in light of GDPR, become less willing to admit to cyber security breaches during an interview. If true, this would mean that the true drop in breaches or attacks observed this year is perhaps not as substantive as the estimates from the quantitative survey suggest.

It should be noted that the change from 2017 to 2018 alone was not statistically significant, and the change from 2018 to 2019 may not indicate a longer-term trend. Data from subsequent years will help to validate this trend.

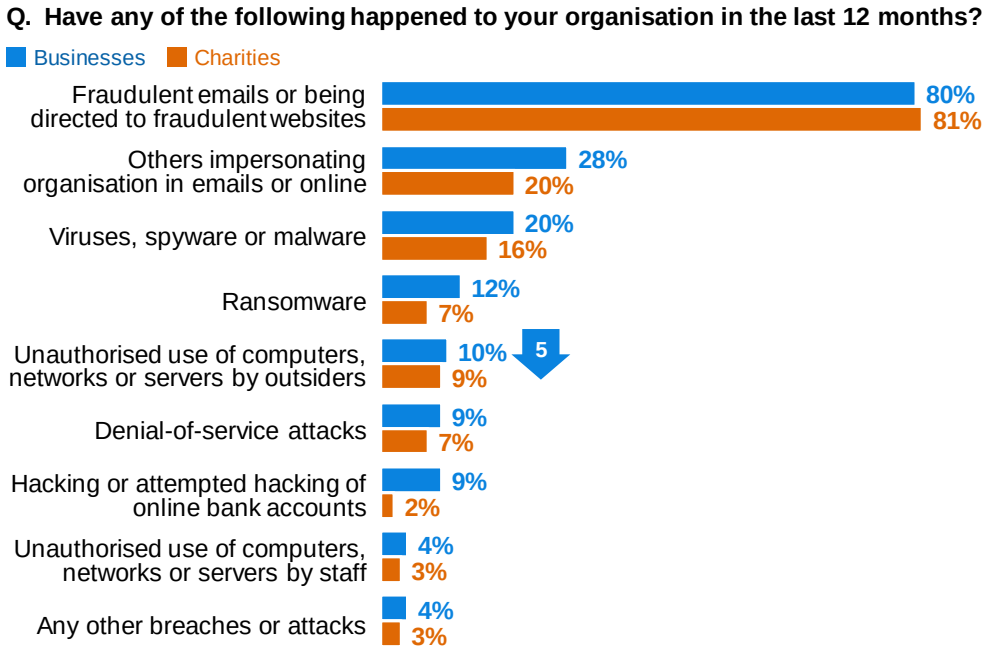
Types of breaches or attacks experienced

As in previous years, by far the most common type of cyber attacks are phishing attacks – through fraudulent emails, or being directed to fraudulent websites. Beyond this, as Figure 5.2 shows, both businesses and charities face a similar range of breaches or attacks.

Protection against these kinds of breaches or attacks requires both technical controls *and* good staff awareness. This includes non-specialist staff, who are typically the ones directly targeted in phishing attacks. As in previous years, breaches or attacks that rely solely on technical factors beyond the reach of non-specialist staff, such as denial-of-service attacks (which attempt to take down an organisation's website) are relatively less common.

Since this question was first asked in 2017, the proportion identifying viruses, spyware or malware has consistently fallen (from 33% of those identifying any breaches or attacks in 2017, to 24% in 2018, and 16% this year). This suggests that this type of activity is becoming relatively less common or less visible, overtaken by other types of breaches or attacks. Figure 5.2 also shows that the incidence of outsider hacking activity has also fallen since 2018, and this marks a return to the 2017 level.

Figure 5.2: Types of breaches or attacks suffered (among the organisations that have identified breaches or attacks)



Bases: 637 businesses that identified a breach or attack in the last 12 months; 192 charities

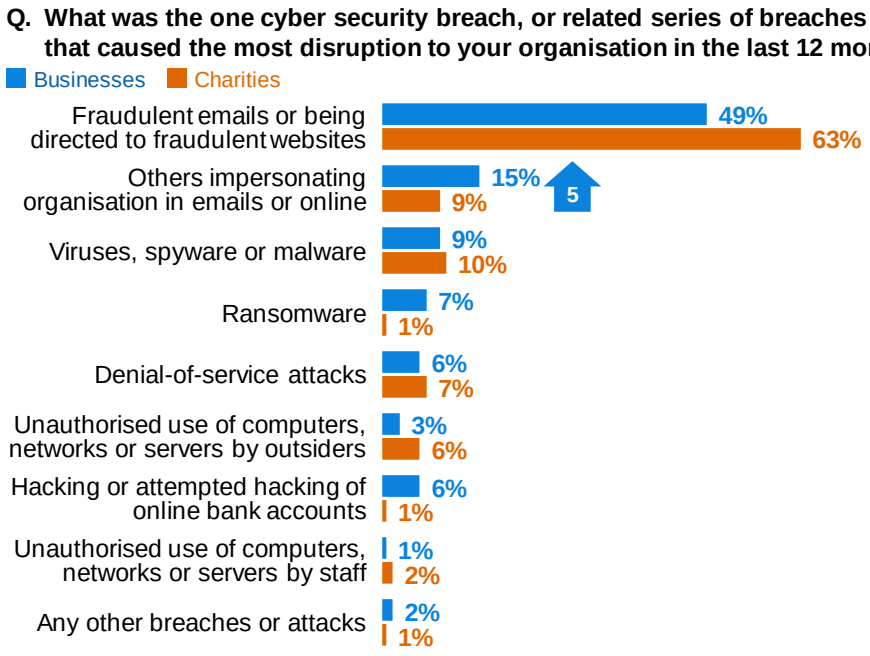
This broad pattern is similar across size bands and sectors. However, denial-of-service attacks are more prevalent in information and communications firms (14% of such firms have experienced them in the past year, vs. 3% of all firms) and the education sector (8%). Large firms are also more likely than average to experience denial-of-service attacks (11%), as well as impersonation of their organisation online (41%, vs. 9% of all firms) and viruses, spyware or malware (18%, vs. 7% of all firms).[29]

Most disruptive breaches or attacks

Among those organisations that have experienced breaches in the past 12 months, phishing attacks are also typically the single most disruptive cyber attacks that organisations face.

The full breakdown of breaches considered to be the most disruptive is shown in Figure 5.3. This is largely in line with the 2018 findings, although the proportion of businesses viewing impersonation as their most disruptive type of breach (among those experiencing breaches) has increased.

Figure 5.3: The single most disruptive breach or attack suffered (among the organisations that have identified breaches or attacks)



Bases: 637 businesses that identified a breach or attack in the last 12 months; 192 charities

Extent of breaches or attacks experienced

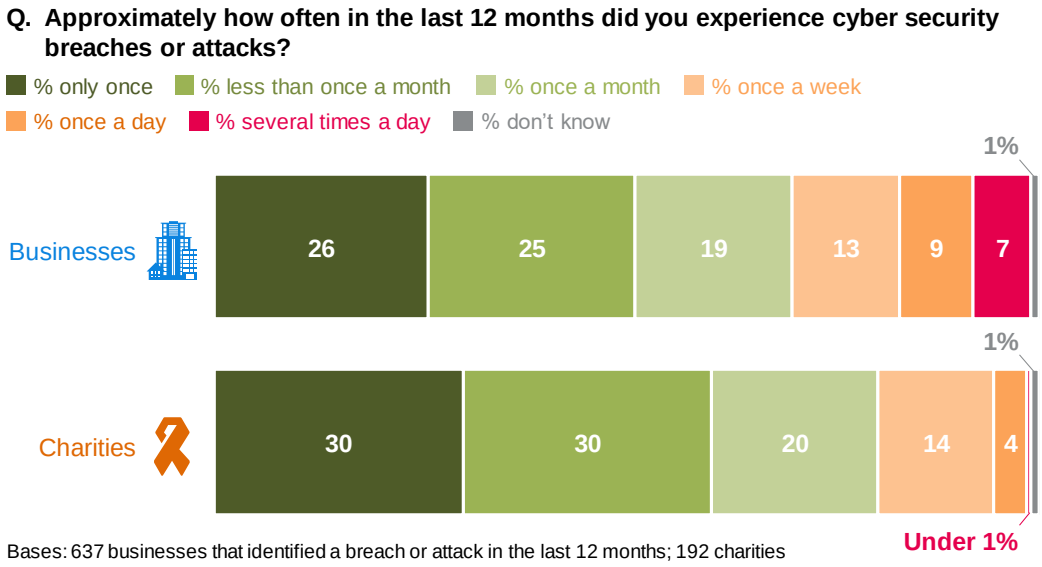
It is rare for either businesses or charities to experience breaches or attacks more than once a month, as Figure 5.4 shows. Businesses are more likely than charities to be recording breaches more than once a day (16% vs. 5%).

The trend over time is that fewer businesses are experiencing breaches or attacks as a one-off event. In 2017, 37 per cent of the businesses identifying breaches had only identified one in the previous 12 months, which fell to 30 per cent in 2018, and 26% in this latest survey. Conversely, more businesses in 2019 say they experience these issues at least once a week (29%, vs. 22%

[29] These percentages are based on all firms, rather than just on firms that have identified breaches or attacks, so are different from those in Figure 5.2.

in 2017). There is a similar pattern over time for charities (first surveyed in 2018), although the changes across a single year are not statistically significant in this case.

Figure 5.4: Frequency of breaches or attacks experienced in the last 12 months



Bases: 637 businesses that identified a breach or attack in the last 12 months; 192 charities

Table 5.1 shows the overall number of breaches or attacks recorded. In line with previous years, the mean number[30] is substantially higher than the median number. What this indicates is that the typical business or charity is likely to only experience a handful of breaches in the space of a year, but that a minority experience hundreds of breaches or attacks in this timeframe – particularly, but not exclusively, larger organisations.

Table 5.1: Average number of breaches or attacks among those that identified any cases in last 12 months[31]

	All businesses	Micro/small businesses[32]	Medium businesses	Large businesses	All charities
Mean number	7,350	7,690	330	7,710	131
Median number	6	6	6	12	4
Base	597	337	147	113	187

Given the extremely high variance in responses on this measure, we tend not to find statistically significant changes over time. The mean estimate for businesses this year (7,350) is

[30] Figures in all the tables in this chapter are presented to three significant figures, or to the nearest whole number (if under 100). It should be noted that the mean results here are driven up by a very small number of respondents across all size bands reporting an extremely high number of breaches in the past year (in the thousands). The median figures are therefore also shown to give a better sense of what a business is typically likely to face.

[31] All mean and median scores presented across this chapter merge together the answers from respondents who gave a numeric value as well as those who gave only a banded value (because they did not know the exact answer). For the latter, we have imputed numeric values from the given banded values. We lay out this approach in detail in the Technical Annex.

[32] Across this chapter, micro and small firms have been merged to make the analysis more statistically robust.

considerably higher than in 2018 (886) and 2017 (998). Nevertheless, these figures are not statistically significantly different from each other.[33]

However, it is worth noting that the median number of breaches or attacks, among businesses that have experienced them, has consistently risen (from 2 in 2017 and 4 in 2018, to 6 in 2019). This is indicative evidence, alongside the rising frequency of breaches or attacks (Figure 5.4), that cyber security is becoming a more prevalent issue over time for some organisations.

As previously mentioned, this trend should be considered alongside the fall in the number of businesses overall identifying any breaches or attacks. Taken together, these findings may also indicate a change in attacker behaviour or targeting. Attackers may be targeting fewer businesses, but may be attacking these ones more frequently or substantively. However, this is not something that this survey measures directly.

5.2 How are businesses affected?

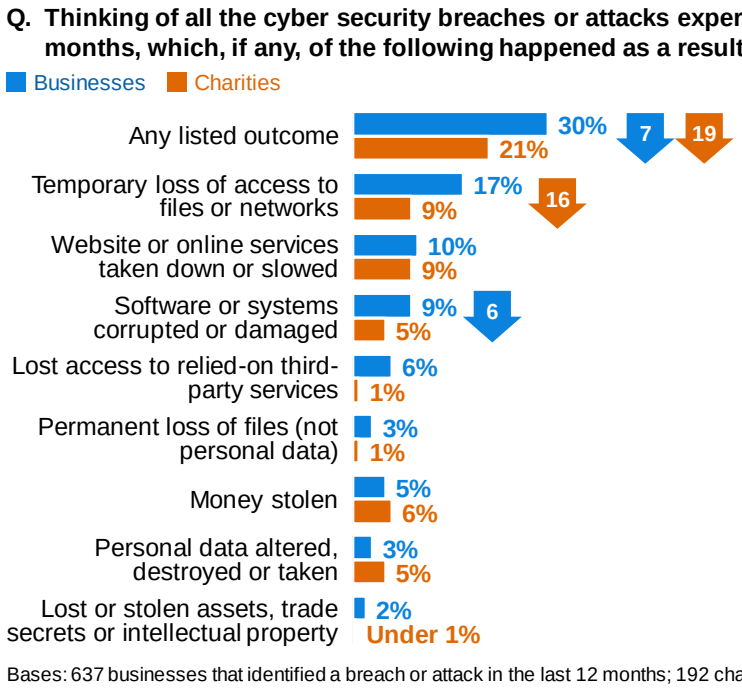
Outcomes of breaches or attacks

Not all breaches or attacks lead to a negative consequence, in terms of a loss of money or data. This attests to the preventative measures that many organisations have in place. Nonetheless, as Figure 5.5 illustrates, three in ten businesses (30%, among those that experience any breaches or attacks) and two in ten charities (21%) do have such outcomes from the breaches or attacks they face. Temporary loss of access to files or networks, software or systems damage, and website disruption are the most commonly reported outcomes.

Certain types of breaches or attacks are more likely to result in these kinds of negative outcomes. Broadly, businesses that face less common types of cyber security breaches, including viruses or ransomware, denial-of-service attacks, hacking attempts or other unauthorised use of their computers or networks, are much more likely than average to experience a negative outcome as a result (58%, vs. 30% overall). This means that while these kinds of breaches are rarer, the damage they can inflict on organisations is much more significant. They still, therefore, represent a significant threat for all organisations to consider, alongside more common and still-burdensome threats like phishing emails.

[33] The very large margin of error for the 2019 estimate is, in part. due to outlier results among two micro business respondents, both in the information or communications sector. Both businesses recorded 1,000,000 breaches or attacks over 12 months – the maximum possible value in the survey. For any answer over 99,999, the survey script prompted interviewers to double-check the figure with the respondent before moving onto the next question.

Figure 5.5: Outcome of breaches among organisations that identified any breaches or attacks in the last 12 months



Bases: 637 businesses that identified a breach or attack in the last 12 months; 192 charities

Compared to 2018, fewer of the businesses and charities incurring breaches or attacks have had this kind of material outcome as a result. For businesses, this is part of a longer trend, going back to 2017 (when 41% had a material outcome, vs. 37% in 2018 and 30% in 2019). Alongside the other changes over time reported in this chapter, this potentially indicates that organisations have become more resilient to breaches or attacks – they record fewer of them, and the ones they do experience are less likely to cause damage. Alternatively, it may indicate that a smaller number of organisations are being subjected to more sophisticated attacks, for example due a change in the behaviour of attackers.

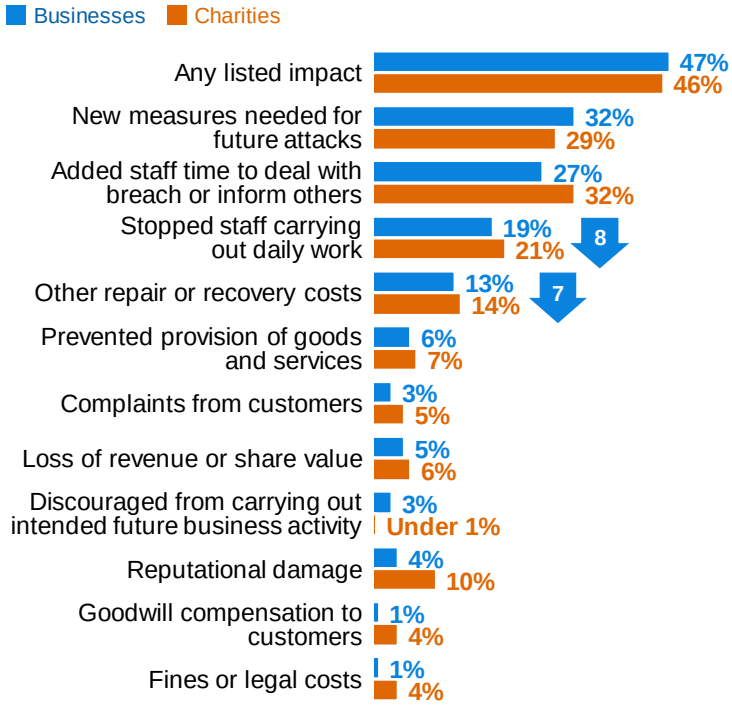
Nature of the impact

Even breaches that do not result in negative financial consequences or data loss can still have an impact on organisations. Just under half of the businesses (47%) and the charities (46%) that have had breaches or attacks report being impacted in one of the ways noted in Figure 5.6.

Most commonly, breaches or attacks lead to organisations having to take up new measures to prevent or protect against future cases, staff time being taken up to deal with the breach, or preventing day-to-day work. The time impact is most substantial for large businesses – 53 per cent need extra staff time to deal with breaches (vs. 27% of all businesses facing breaches or attacks) and 35 per cent report lost productivity among staff, from being unable to carry out their work (vs. 19% overall).

Figure 5.6: Impacts of breaches among organisations that identified any breaches or attacks in the last 12 months

Q. Have the breaches or attacks experienced in the last 12 months impacted your organisation in any of the following ways, or not?



Bases: 637 businesses that identified a breach or attack in the last 12 months; 192 charities

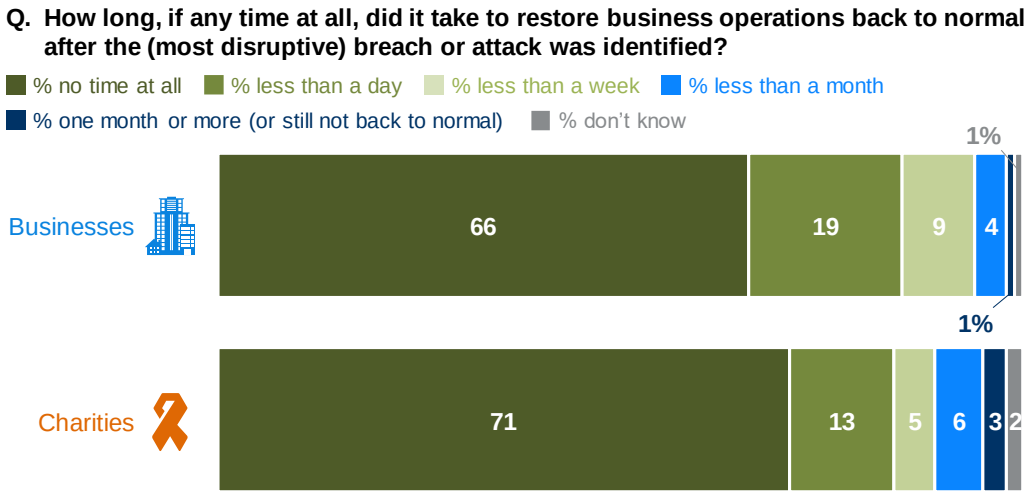
This measure has also changed over time. Fewer of the businesses experiencing breaches or attacks report an impact compared to previous years (47%, vs. 53% in 2018 and 57% in 2017). There is also a similar downwards trend for charities (59% in 2018 to 46% in 2019), although this is indicative, rather than statistically significant. Once again, these trends may indicate that organisations are coping better than before when dealing with cyber security breaches or attacks.

Time taken to recover from breaches

Focusing on the single most disruptive attack faced by organisations in the past year, around two-thirds of businesses and seven in ten charities say it took no time at all to recover, shown in Figure 5.7. For businesses, this immediate recovery is more common than in 2017 (66%, vs. 57% in 2017), when this question was first asked. This may also reflect that fewer attacks end in a negative outcome, so do not necessarily need time to recover from.

The situation is very different, however, for businesses that experience breaches or attacks with a material outcome (as discussed in the previous section). In these cases, 40 per cent of these businesses take a day or more to recover, or say they have not yet recovered at all (vs. 15% overall, including breaches or attacks without outcomes).

Figure 5.7: Time taken to recover from the most disruptive breach or attack of the last 12 months[34]



Bases: 616 businesses that recalled their most disruptive breach or attack in the last 12 months; 185 charities

As shown in Table 5.2, businesses and charities spend a similar amount of staff time dealing with breaches. In a similar pattern to the previous two years (since this question was first asked), medium-sized firms take the most time overall to deal with breaches or attacks.

When looking at breaches with a material outcome (such as loss of files, money or other assets), the average number of days is higher across the board, as might be expected.

[34] There were 637 businesses and 192 charities in the sample that had at least one breach or attack in the last 12 months. However, only 616 and 185 of these respectively are able to say which breach or attack was the most disruptive.

Table 5.2: Average time spent dealing with the most disruptive breach or attack of last 12 months

	All businesses	Micro/small businesses	Medium businesses	Large businesses	All charities
	Across organisations identifying any breaches or attacks				
Mean days	1.3	1.3	2.2	1.6	1.3
Median days	0.5	0.5	0.5	0.5	0.5
Base	610	340	154	116	182
	Only across organisations identifying breaches with an outcome				
Mean days	3.0	2.9	5.0	3.1	4.5
Median days	0.5	0.5	0.5	3.8	0.5
Base	202	103	54	45	62

5.3 Financial cost of breaches or attacks

Overall cost of breaches or attacks

Table 5.3 shows the estimated costs businesses incurred from all breaches over the past 12 months. When considering the cost, organisations are asked to bear in mind all the potential impacts mentioned in Figure 5.6.

As in previous years, the median cost is typically £0 across businesses and charities (with the exception of large businesses). This implies that, typically, organisations incur no specific financial cost from breaches or attacks. It reflects the fact that most breaches or attacks do not have any material outcome (a loss of assets or data), so do not always need a response. When filtering down only to breaches with such a material outcome, median costs are much higher, particularly for large businesses.

Due to the high variance in cost estimates and the relatively small sample sizes for organisations experiencing breaches or attacks, it is unusual to find statistically significant differences in mean costs between years. Nonetheless, it is worth noting that the recorded mean cost (adjusted for inflation) of breaches *with outcomes* has risen consistently since 2017 for businesses. The mean cost was £2,450 in 2017, up to £3,160 in 2018, and £4,180 in 2019.[35]

[35] These differences have not been found to be statistically significant at the 95% level of confidence after factoring in inflation. However, it is worth noting that the difference between the 2017 mean cost of breaches with outcomes and the 2019 cost estimate is statistically significant *at the 90% level of confidence*, even when factoring in inflation. Inflation is assumed to be 2.2% since the 2018 survey and 5.1% since the 2017 survey, based on ONS data (see https://www.ons.gov.uk/economy/inflationandpriceindices).

Table 5.3: Average cost of all breaches or attacks identified in the last 12 months

	All businesses	Micro/small businesses	Medium businesses	Large businesses	All charities
	Across organisations identifying any breaches or attacks				
Mean cost	£1,410	£1,210	£3,770	£9,130	£2,150
Median cost	£0	£0	£0	£98	£0
Base	600	335	150	115	184
	Only across organisations identifying breaches with an outcome				
Mean cost	£4,180	£3,650	£9,270	£22,700	£9,470
Median cost	£500	£500	£727	£9,980	£600
Base	192	99	50	43	56

Costs associated with the most disruptive breaches

Tables 5.4 to 5.7 show cost estimates for the single most disruptive breach that organisations have identified in the last 12 months. Again, these are presented for all breaches, as well as those with an actual outcome, such as a loss of assets or data.

Mirroring the 2018 findings, direct cost and recovery cost estimates tend to be higher for medium and large businesses, whereas long-term cost estimates (for costs to date and expected future costs) tend to be a bigger consideration for large businesses specifically.

Direct costs include the cost of: staff being prevented from carrying out their work; lost, damaged or stolen outputs, data, or assets; and lost revenue if customers could not access online services.

Table 5.4: Average direct cost of the most disruptive breach or attack from the last 12 months

	All businesses	Micro/small businesses	Medium businesses	Large businesses	All charities
	Across organisations identifying any breaches or attacks				
Mean cost	£1,020	£910	£2,080	£7,090	£916
Median cost	£0	£0	£0	£0	£0
Base	592	335	146	111	176
	Only across organisations identifying breaches with an outcome				
Mean cost	£3,150	£2,830	£5,710	£17,500	£4,100
Median cost	£200	£200	£312	£2,570	£254
Base	190	100	49	41	57

Recovery costs include: additional staff time needed to deal with the breach or to inform customers or stakeholders; costs to repair equipment or infrastructure; and any other associated repair costs.

Table 5.5: Average recovery cost of the most disruptive breach or attack from the last 12 months

	All businesses	Micro/small businesses	Medium businesses	Large businesses	All charities
	Across organisations identifying any breaches or attacks				
Mean cost	£472	£411	£1,480	£1,540	£766
Median cost	£0	£0	£0	£0	£0
Base	588	330	146	112	178
	Only across organisations identifying breaches with an outcome				
Mean cost	£1,550	£1,380	£4,020	£3,810	£3,830
Median cost	£0	£0	£141	£1,970	£38
Base	185	95	49	41	59

As defined in the survey, the long-term cost of breaches includes: the loss of share value; loss of investors or funding; long-term loss of customers; costs from handling customer complaints; and any compensation, fines or legal costs.

Outside of large businesses, the typical long-term cost estimates, even for breaches with material outcomes, are £0. This does not necessarily imply that smaller businesses incur no long-term costs from breaches. It may instead suggest that only large businesses are really considering the wider potential costs of breaches. Other, smaller organisations may be underestimating the full impact, in terms of costs such as lost business or reputational damage.

Table 5.6: Average estimated long-term cost of the most disruptive breach or attack from the last 12 months

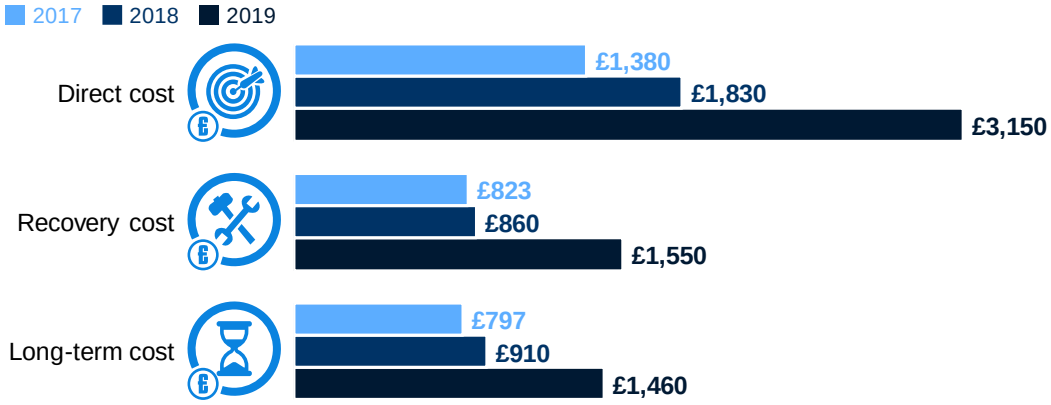
	All businesses	Micro/small businesses	Medium businesses	Large businesses	All charities
	Across organisations identifying any breaches or attacks				
Mean cost	£466	£369	£867	£7,990	£51
Median cost	£0	£0	£0	£0	£0
Base	580	328	144	108	173
	Only across organisations identifying breaches with an outcome				
Mean cost	£1,460	£1,220	£740	£22,900	£280
Median cost	£0	£0	£0	£2,810	£0
Base	177	93	47	37	56

How have the costs associated with the most disruptive breaches changed over time?

Similar to the mean cost of *all* breaches with a material outcome (such as loss of assets or data), the mean cost estimates for the single most disruptive breaches with an outcome have also increased consistently over time – when looking across the direct, recovery and long-term costs. The cost estimates for businesses going back to 2017 (and adjusted for inflation) are shown in Figure 5.8. The increase from £1,380 in direct costs for the average business in 2017 to £3,150 in 2019 is statistically significant.

Earlier in this chapter, we noted that organisations are less likely to have cyber security breaches or attacks that result in a material outcome, compared to previous years. However, those that do have such breaches are often paying a higher price for them than they used to.

Figure 5.8: Changes over time in average (mean) costs for the most disruptive breaches with outcomes



Bases: 150+ businesses per year that recalled their most disruptive breach or attack in the last 12 month
Mean £ amounts adjusted for inflation up to 2019.

How well do organisations understand their costs?

In the qualitative interviews, we spoke to a range of organisations that had suffered financially costly cyber security breaches in the past year. These included a mix of malware and ransomware attacks, phishing emails, emails and servers being hacked, fraud committed internally by staff members and company laptops being stolen. The estimated costs of these breaches ranged from around £300 to around £100,000.

The quantitative survey asks organisations to consider a wide range of possible costs, including indirect costs and long-term costs that might result from breaches. This approach, set out clearly during the interview, aims to generate a comprehensive economic cost estimate. However, the qualitative interviews show that this kind of in-depth reflection on the costs is unusual in real-life situations – organisations often overlook certain types of costs of breaches, and so may undervalue their true impact.

This was especially a concern among some of the individuals we spoke to from larger organisations. They believed that their management boards lacked an understanding of the full economic impact. For breaches that had an obvious direct cost, such as stolen money, they felt it was challenging for senior managers to conceptualise costs beyond this.

Often, organisations did not have any kind of cost monitoring in place for cyber security breaches. This was because understanding the overall economic cost of the breach was not a priority for them, compared to taking immediate actions to deal with the breach, and subsequent actions to prevent the same kind of breach happening again.

Three types of costs that tended to be overlooked included:

- indirect costs, such as loss of productivity if staff could not carry out their work
- ongoing or longer-term costs, such as the recurring cost of new measures put in place after a breach
- relatively intangible costs, such as reputational damage.

As an example, one high-income charity had suffered a breach after an employee email account was hacked. The email account sent a fake supplier invoice worth around £10,000 to their finance department, which a team leader mistakenly approved. When considering the cost

of this breach, the initial cost considered was the stolen £10,000. They considered the recovery cost, but felt this was negligible, as securing the hacked email account was relatively straightforward. However, they did not initially consider the ongoing cost. As a result of the breach, all new supplier invoices now have to be approved by senior finance staff – an ongoing time cost that senior managers had not considered.

This qualitative insight suggests that the cost estimates from the quantitative survey each year may underestimate the true impact of cyber security breaches, because organisations find it very challenging to consider indirect or ongoing costs. However, the quantitative survey is still far more comprehensive in its approach than just asking about the tangible, direct costs of breaches.

Chapter 6: Dealing with breaches or attacks

This chapter explores how well businesses and charities deal with breaches or attacks, including identification, response, reporting and adaptation to prevent future cases.

In the survey, questions on this topic were generally framed in terms of the most disruptive breach or attack an organisation had faced in the last 12 months. Therefore, almost all findings in this chapter are among the subgroup of business and charities that have identified breaches or attacks (32% of all businesses and 22% of all charities). We have not undertaken business sector, region or charity income band subgroup analysis on these questions, due to the relatively small sample size of organisations that have experienced breaches.

6.1 Identifying and understanding breaches or attacks

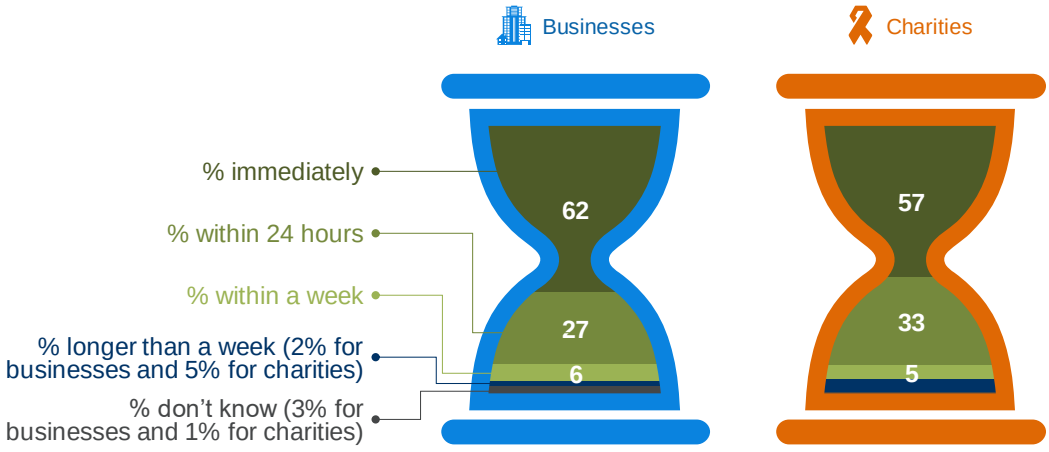
When and how were breaches or attacks identified?

The vast majority of businesses (89%) and charities (90%) report identifying their most disruptive breach or attack within 24 hours, if not immediately, as Figure 6.1 shows.

These figures are in line with previous surveys. They are also consistent across business sizes.

Figure 6.1: Time taken to identify the most disruptive breach or attack of the last 12 months

Q. How long was it, if any time at all, between this breach or attack occurring and it being identified as a breach?



Bases: 616 businesses that recalled their most disruptive breach or attack in the last 12 months; 185 charities

As in previous years, the most disruptive breach or attack was most commonly spotted by individuals rather than being picked up by cyber security software. For over six in ten businesses (63%) and seven in ten charities (70%), the most disruptive breaches were reported directly by staff, contractors or volunteers. Among businesses, nine per cent also identified the case when an individual noticed unusual email or file activity.

Only one in ten businesses and charities (10% in each case) identified their most disruptive breach or attack through antivirus and antimalware software. This illustrates the importance of staff vigilance, as well as technical controls, in identifying breaches promptly.

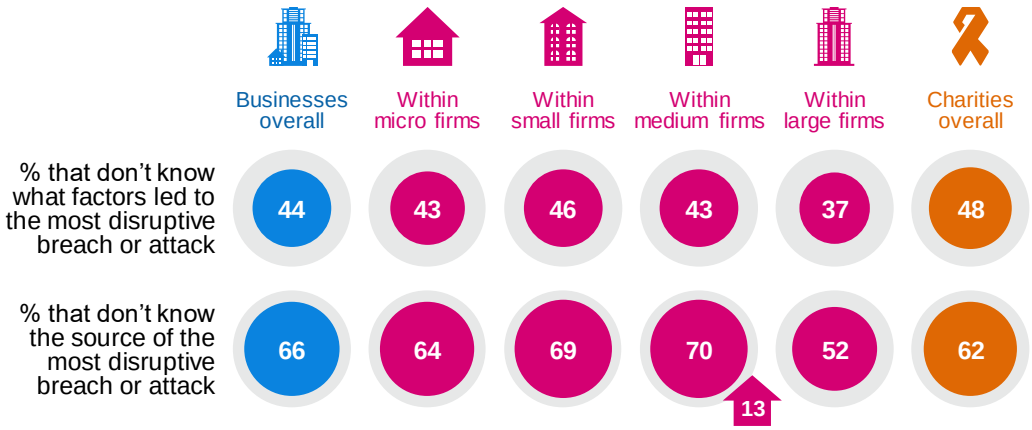
How well do businesses understand the breaches or attacks they face?

Just under half of the businesses (44%) and charities (48%) identifying breaches or attacks do not know what factors led to their most disruptive case.

The source of the breach continues to be a much greater unknown for both businesses (66% do not know) and charities (62%).

Broadly, these findings are similar to previous years, although the proportion of medium businesses saying they do not know the source of their most disruptive breach or attack has increased (to 70%, from 57% in 2018 and 52% in 2017). There has also been an indicative increase this year in the proportion of large businesses and charities saying they do not know the factors that led to this breach or attack, but these changes are not statistically significant.

Figure 6.2: Organisations' understanding of the factors and sources behind their most disruptive breaches or attacks of the last 12 months



Bases: 616 businesses that recalled their most disruptive breach or attack in the last 12 months; 210 micro firms; 130 small firms; 155 medium firms; 121 large firms; 185 charities

When thinking of the factors that led to the breach or attack, businesses and charities are again more likely to report (unprompted) that these were external attacks not specifically targeted at any particular organisation (12% and 15% respectively), than an attack specifically targeted against them (7% and 4% respectively). This highlights that many cyber attacks are indiscriminate.

The most common source of disruptive breaches or attacks is considered (unprompted) to be fraudulent emails or websites (for 18% of businesses and 25% of charities). The next most commonly mentioned is organised crime (by 5% of businesses and 5% of charities). For businesses, this is a return to the 2017 level, with this response having fallen in 2018 (to 1%).

Accidental vs. intentional breaches

Around three in four businesses (75%) and charities (76%) identifying breaches or attacks think that their most disruptive case was intentional. For businesses, this is in line with last year's findings, but still higher than in the 2017 survey (when it was 66%).

As in previous years, smaller organisations are just as likely as larger organisations to say the attack was intentional.

6.2 Incident response

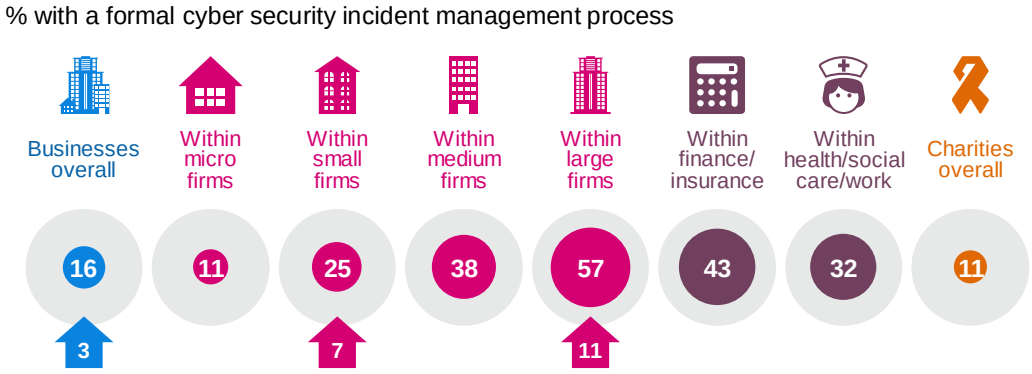
Incident response plans

Very few organisations (16% of businesses and 11% of charities) have formal cyber security incident management processes in place. For businesses, this has increased since last year, and over the longer term (up six percentage points since 2016). This question is asked of all businesses and charities, not only those that identify breaches or attacks.

As Figure 6.3 shows, larger firms are much more likely to have a formal plan in place. There is a similar difference among charities, with high-income charities more likely to have such a plan (37% among those with £500,000 or more). This is even higher among the very largest charities with £5 million or more (51%).

Having an incident management plan is also more prevalent in the sectors where firms are typically more engaged with cyber security. This includes finance and insurance and health, social care and social work firms.

Figure 6.3: Whether organisations have incident management processes



Bases: 1,566 UK businesses; 757 micro firms; 321 small firms; 281 medium firms; 207 large firms; 117 finance or insurance firms; 79 health, social care or social work firms; 514 charities

Reporting breaches or attacks

Among those who identified breaches or attacks, the vast majority of businesses (94%) reported their most disruptive one to their senior management. However, a much lower proportion of charities did so, which is a decrease from 2018 (45% this year, vs. 68% in 2018).

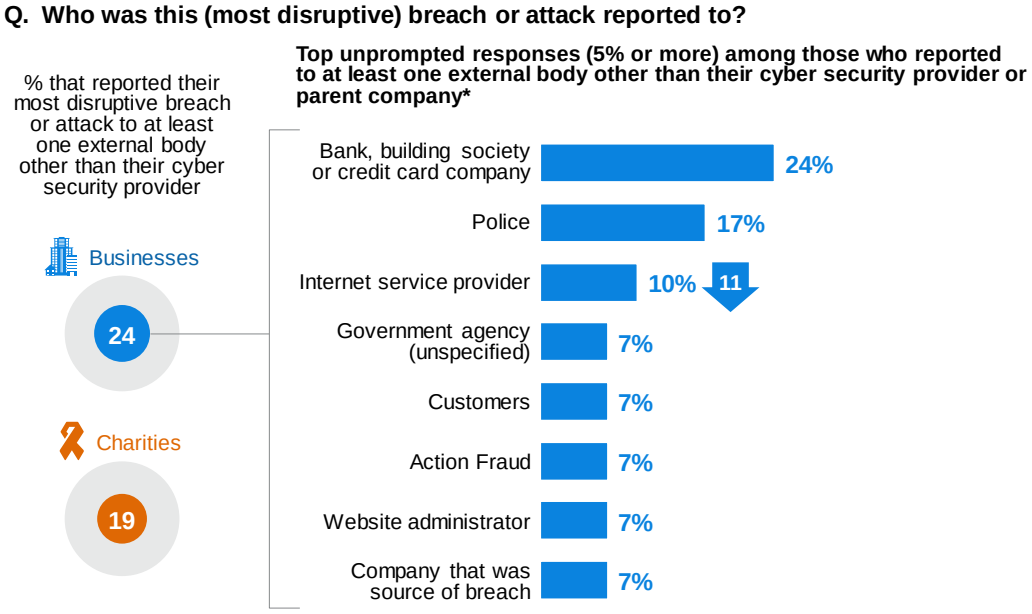
The reasons behind this shift among charities are unclear, given that charities are updating their senior managers and trustees more frequently on cyber security than before (as outlined in Chapter 3). It may reflect the fact that this year, far fewer breaches had material outcomes (such as a loss of money or data), so charities are potentially being more selective about what they update senior managers or trustees with.

On the other hand, it may indicate that charities have become more specifically focused on personal data breaches, due to the introduction of GDPR, so less focused on wider cyber security breaches. The latter explanation has emerged from our qualitative research – data protection was often the primary issue for charities in our interviews – but there are too few charities that have identified breaches or attacks in the quantitative survey sample to analyse this further.

External reporting remains rarer. In total, four in ten businesses (42%) and a quarter of charities (26%) identifying breaches or attacks reported their most disruptive one to someone outside their organisation. However, this includes a substantive number of businesses and charities who *only* reported breaches to their external cyber security providers or to their parent companies, rather than more widely. When excluding those responses, the proportions drop to 23 per cent for businesses, and 19 per cent for charities.

As Figure 6.4 shows, the top (unprompted) organisations that businesses report to are banks, the police, and internet service providers. Reporting elsewhere is particularly uncommon. Once again, there are too few charities in the sample to analyse for this question.

Figure 6.4: Reporting of the most disruptive breach or attack of the last 12 months, excluding those that only reported to their outsourced cyber security provider



Bases: 616 businesses that recalled their most disruptive breach or attack in the last 12 months (*137 that reported the breach, excluding those who reported only to their outsourced cyber security provider); 185 charities

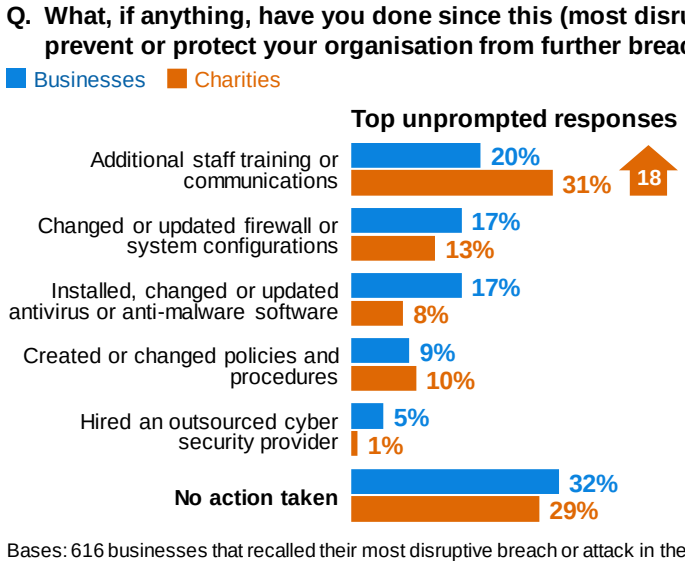
It is worth noting that, under GDPR, organisations are obliged to report breaches involving personal data to the ICO. However, only a very small proportion of the organisations incurring cyber security breaches or attacks (3% of these busineses and 5% of these charities) have suffered personal data being altered, lost or taken. Therefore, the organisations that do not report their breaches or attacks here are not necessarily required to do so, and would have to choose to do so.

Preventing future breaches or attacks

Among those who identified breaches or attacks, around seven in ten businesses (68%) and charities (71%) have taken, or are currently taking action to protect their organisation from further breaches. Around three in ten businesses (32%) and charities (29%) have taken no action since their most disruptive breach.

As Figure 6.5 shows, the most common action taken is additional staff training or communications. This figure has risen for charities since the 2018 survey (when it was 13%). The next most common responses include changes to internal systems such as installing, changing or updating firewalls or system configurations, antivirus or antimalware software, and creating or changing policies and procedures.

Figure 6.5: Most common actions following the most disruptive breach of the last 12 months



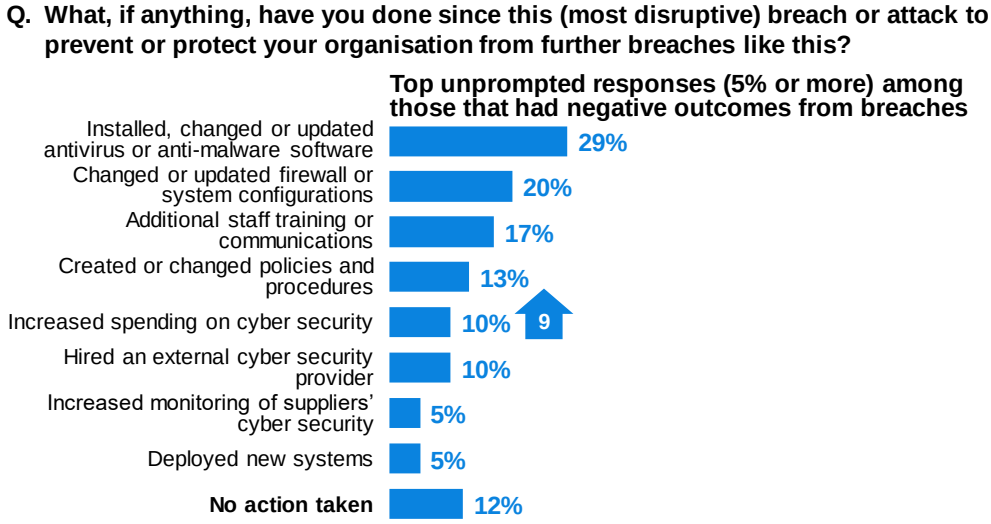
Bases: 616 businesses that recalled their most disruptive breach or attack in the last 12 months; 185 charities

Micro businesses are the least likely to have taken action to prevent further breaches or attacks (36% have taken no action, compared to 32% of businesses overall).

As may be expected, the picture in Figure 6.5 changes slightly when looking only at businesses whose most disruptive breach resulted in a material outcome (e.g. the loss of files, money or other assets). This is shown in Figure 6.6.

The most common responses are similar, but it is worth noting that the ranking of responses is different across both charts. In cases that resulted in a negative outcome, there is more weight placed on technical controls and on increased spending on cyber security, both of which rank substantively higher in Figure 6.6 than in Figure 6.5. Again, there are too few charities in the sample for analysis here.

Figure 6.6: Most common actions following the most disruptive breach of the last 12 months, where breaches had material outcomes



Base: 203 businesses that recalled their most disruptive breach or attack with an outcome in the last 12 months

Chapter 7: Conclusions

This survey series has illustrated the changing attitudes of organisations towards cyber security since its inception in 2016. The 2019 survey shows, in particular, how GDPR has accelerated the pace of change across organisations.

In 2019, both businesses and charities see cyber security as a higher priority than in previous years. The qualitative interviews indicate an enhanced level of understanding among organisations – they recognise that cyber attacks can no longer be prevented with common sense alone, and require action. The quantitative data suggest that, while fewer businesses overall are identifying breaches or attacks, the attacks that penetrate organisations' defences and cause the most disruption are also having more severe financial impacts than before.

Linked to this, we have seen a considerable rise in the number of organisations taking actions to assess and document the risks they face, implementing new rules and technical controls, and raising awareness through staff training. We have also seen cyber insurance become a more common part of the approach to cyber risk management, particularly among medium and large businesses (though it is still a minority of these groups taking it on).

These are long-term trends over all four years of the survey to date. Equally, it is clear from the 2019 survey – the first since GDPR was introduced – that the new data protection law has encouraged and compelled many organisations over the past 12 months to either engage formally with this issue for the first time, or in some cases to strengthen their existing policies and processes. This has helped to raise the floor in cyber security, with more micro businesses and more charities in particular taking action against the risks in 2019 than in 2018. It may help, among other factors, to explain the fall in the number of businesses, especially micro businesses, experiencing breaches or attacks since 2018.

The improvements in attitudes and behaviour measured in this survey mirror the findings from DCMS's FTSE 350 Cyber Governance Health Check 2018, which focuses on the 350 largest companies in the UK.[36] This serves to reinforce that progress has been made across the board, from the smallest organisations to the very largest ones.

However, GDPR may only take organisations up to a certain point. Beyond this, the findings show there is still room for a more holistic approach to cyber security.

While there has been considerable progress since 2018 across organisations of all sizes, only a minority of micro and small businesses, and of charities, have written cyber security policies or a formal incident management process, have arranged any form of cyber security training, or have senior staff with a specific responsibility for cyber security as part of their job role.

The sectoral differences seen in previous years also persist in the 2019 survey. Businesses in the food and hospitality, and construction sectors are again among the least likely to take action against cyber risks.

A key theme across the qualitative interviews was that different organisations frame the issue of cyber security in different ways. The qualitative findings show that while GDPR has played an important role in raising the floor, it may have, unintentionally, made some organisations think about cyber security almost exclusively in terms of data protection. And advances in the number of staff attending training on cyber security may be more to do with uptake of GDPR training, where the actual cyber security content could be relatively small.

[36] See https://www.gov.uk/government/publications/cyber-governance-health-check-2018.

After implementing GDPR, it may be important for organisations to consider cyber security more holistically. The organisations that had more sophisticated approaches to the issue in the qualitative interviews tended to be those that also considered the potential wider impacts of cyber attacks on business continuity, on reputations and on client-supplier relationships.

There are other major themes emerging from this year's results, around board-level engagement, skills development, access to information and guidance, and supply chain risks.

Once again, businesses and charities have taken positive steps in each of these areas, but there is still more that they can do:

- Our findings continue to highlight the importance of board-level engagement with cyber security. Board members and trustees are updated more frequently about cyber security in 2019 than in the previous years of the survey. More businesses in 2019 have board members with a cyber security brief, although this is still a minority among all but large businesses. Even among large businesses, four in ten (41%) do not have this. Instilling better knowledge and understanding of cyber security across board members can be the difference between cyber security being treated as a fairly high priority, or a very high priority. This is another area where this survey is consistent with DCMS's FTSE 350 Cyber Governance Health Check 2018.
- We also find that more businesses and charities have had staff attend training on cyber security since 2018. Over the same period, both businesses and charities have become less concerned about skills gaps and skills shortages hampering their ability to deal with cyber security. However, there is still a large difference between the relatively low proportions sending staff on training (27% of businesses and 29% of charities) and the much higher proportions that feel they have no skills needs. This could indicate that there is still an unacknowledged skills gap. This also reflects other recent DCMS research on cyber security skills, which showed that many organisations lack an understanding of the technical requirements of a cyber security role.[37]
- It is still relatively uncommon for organisations to systematically consider the cyber risks in their supply chain. Across all size bands, only a minority of organisations demand minimum cyber security standards from suppliers, although this has increased among medium businesses specifically. Moreover, the qualitative findings suggest that suppliers are often overlooked as a potential source of cyber risk, both due to a lack of awareness, as well as a lack of perceived responsibility for suppliers' own actions. Some organisations told us this was an area where they would benefit from more guidance or checklists.
- Finally, while more organisations have started to consider cyber security as a high priority over the years of the survey, there has not been an equivalent increase in the number seeking out information and guidance. This year saw an isolated increase among charities, but not businesses, seeking information. And overall awareness of the Government's Cyber Aware campaign has not increased. Moreover, it seems that organisations often expect this information to be pushed out to them, rather than to have to seek it out themselves. This potentially raises the prospect of greater signposting to Government information and guidance. We have found that there are various touchpoints, such as news stories about cyber attacks, and key influencers, such as external cyber security providers, trade associations and regulators, that might help to signpost and push information and guidance to organisations.

[37] See https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market.

Annex A: Further information

1. The Department for Digital, Culture, Media and Sport would like to thank the following people for their work in the development and carrying out of the survey and for their work compiling this report.

   - Kelly Finnerty, Ipsos MORI Social Research Institute
   - Sarah Fullick, Ipsos MORI Social Research Institute
   - Helen Motha, Ipsos MORI Social Research Institute
   - Jayesh Navin Shah, Ipsos MORI Social Research Institute
   - Professor Mark Button, Institute for Criminal Justice Studies, University of Portsmouth
   - Dr Victoria Wang, Institute for Criminal Justice Studies, University of Portsmouth

2. The Cyber Security Breaches Survey was first published in 2016 as a research report, and became an Official Statistic in 2017. The previous reports can be found at https://www.gov.uk/government/collections/cyber-security-breaches-survey. This includes the full report, infographics and the technical and methodological information for each year. The next version of the Cyber Security Breaches Survey is expected to be published in 2020.

3. The responsible DCMS statistician for this release is Rishi Vaidya. For enquiries on this release, please contact Rishi on 0207 211 2320 or evidence@culture.gov.uk.

4. For general enquiries contact:

   Department for Digital, Culture, Media and Sport
   100 Parliament Street
   London
   SW1A 2BQ

   Telephone: 020 7211 6000

5. DCMS statisticians can be followed on Twitter via @DCMSInsight.

6. The Cyber Security Breaches Survey is an Official Statistics publication and has been produced to the standards set out in the Code of Practice for Official Statistics. For more information, see https://www.statisticsauthority.gov.uk/code-of-practice/. Details of the pre-release access arrangements for this dataset have been published alongside this release.

Annex B: Guide to statistical reliability

The final data from the survey are based on weighted samples, rather than the entire population of UK businesses or charities. Percentage results are therefore subject to margins of error, which vary with the size of the sample and the percentage figure concerned.

For example, for a question where 50% of the 1,566 businesses sampled in the survey give a particular answer, the chances are 95 in 100 that this result would not vary more or less than 3.7 percentage points from the true figure – the figure that would have been obtained had the entire UK business population responded to the survey. The margins of error that are assumed to apply in this report are given in the following table.[38]

Margins of error (in percentage points) applicable to percentages at or near these levels

	10% or 90%	30% or 70%	50%
1,566 businesses	±1.8	±2.8	±3.1
757 micro firms	±2.3	±3.4	±3.8
321 small firms	±3.5	±5.4	±5.9
281 medium firms	±3.8	±5.7	±6.3
207 large firms	±4.4	±6.7	±7.3
514 charities	±4.0	±6.2	±6.7

There are also margins of error when looking at subgroup differences. A difference from the average must be of at least a certain size to be statistically significant. The following table is a guide to these margins of error.

Differences required (in percentage points) from overall result for significance at or near these percentage levels

	10% or 90%	30% or 70%	50%
757 micro firms	±1.3	±2.0	±2.2
321 small firms	±3.1	±4.7	±5.1
281 medium firms	±3.3	±5.1	±5.5
207 large firms	±4.0	±6.2	±6.7
154 low-income charities	±3.1	±4.8	±5.2
141 middle-income charities	±3.6	±5.5	±6.0
205 high-income charities	±3.1	±5.1	±5.6

[38] In calculating these margins of error, the design effect of the weighting has been taken into account. The overall *effective* base size was 1,019 for businesses (versus 931 in 2018) and 211 for charities.

Department for Digital, Culture, Media & Sport

4th Floor
100 Parliament Street
London
SW1A 2BQ