Department for Digital, Culture, Media & Sport

Ipsos MORI

Cyber Security Longitudinal Survey Wave 1

The Cyber Security Longitudinal Survey (CSLS) aims to better understand cyber security policies and processes within medium and large businesses and high-income charities by exploring the links over time between these policies and processes and the likelihood and impact of a cyber incident. This is the first research year, and therefore the main objective of this report is to establish a baseline of findings. The report also summarises additional insight from 30 follow-up qualitative interviews with survey respondents.

Responsible analyst:

Maddy Ell

Responsible statistician:

Robbie Gallucci

Statistical enquiries:

evidence@dcms.gov.uk

General enquiries:

enquiries@dcms.gov.uk

Media enquiries:

020 7211 2210

Contents

Executive summary

The Cyber Security Longitudinal Survey (CSLS) aims to better understand cyber security policies and processes within medium and large businesses and high-income charities, and to explore the links over time between these policies and processes and the likelihood and impact of a cyber incident. This is the first research year of a three-year study, and therefore the main objective of this report is to establish a baseline of findings as a precursor to further reports in subsequent research waves. This report also summarises additional insight from 30 follow-up qualitative interviews with survey respondents, that covered topics such as cyber security resilience, ransomware, record keeping, internal and external reporting, responsibility for cyber security and monitoring of supply chains. These are intertwined with reporting on quantitative findings.

Overall, this baseline study found that the cyber resilience profile of organisations varies between businesses and charities as well as by business size and sector. Businesses are more likely than charities to have formal, written cyber security policies and processes in place. Large businesses (250+ staff), and particularly very large businesses (500+ staff), demonstrate greater cyber maturity compared to medium businesses and charities. Additionally, businesses in the finance and insurance and information and communication sectors tend to be in the lead in terms of cyber maturity. However, overall, organisations' approach to cyber is likely to be more reactive than proactive, with many struggling to get senior level buy-in to improve their cyber defences. Below is a more detailed summary of key findings from each chapter of this report.

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 results, subgroup differences by size, sector and survey answers have been highlighted only where statistically significant[1] (at the 95% level of confidence).

Board involvement

This chapter investigates the level of awareness and engagement with cyber security among board members.

In most organisations, members of the board are unlikely to be involved in decisions or discussions around cyber security. Half of businesses (50%) and four in ten charities (40%) say they have one or more board members whose roles include oversight of cyber security risks. Additionally, only around one-third of businesses (37%) and charities (32%) have board-level discussions or updates on cyber security at least quarterly. On a related note, a relatively low proportion of businesses (35%) and charities (28%) say their board members have received any cyber security training.

However, among organisations where some form of board-level discussions about cyber security do happen, more than half of businesses (55%) and charities (60%) agree that their board integrates cyber risk considerations into wider business areas. This, together with findings from the qualitative interviews, suggests that the main problem is not in management taking ineffective action, but a lack of engagement from senior management in the first place.

[1] 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).

Sources of information

This chapter identifies key information sources used to inform organisations' approach to cyber security in the last year.

Around one-third (32%) of charities and one-quarter (23%) of businesses say they have used information or guidance from the National Cyber Security Centre (NCSC) to inform their approach to cyber security in the last year. Very large businesses with 500+ employees (37%), and businesses in the finance and insurance (51%) and information or communication (41%) sectors are the most likely to use NCSC guidance. In the qualitative research, participants mentioned that they had found the NCSC a useful source of information.

Regarding other sources of information or influences on cyber security policies and processes, feedback from external IT or cyber security consultants has influenced 47% of businesses and 55% of charities in the last twelve months.

Cyber security policies

This chapter sets the baseline of cyber security policies within our longitudinal sample. Monitoring any changes to these policies over time will help us better understand how organisations are evolving their cyber defences. It will also help explore the impact this may have on organisations' resilience to incidents.

When asked about various documentation in place to help manage cyber security risks, businesses and charities are both most likely to say that they have a Business Continuity Plan covering cyber security (69% and 73% respectively), while they are least likely to have documentation outlining how much cyber risk their organisation is willing to accept (26% and 31% respectively). Fewer than one in five organisations (17% of both businesses and charities) report having all five of the types of documentation[2] asked about in place – although the proportion of large businesses who have all five is higher (21%). During the qualitative interviews, respondents frequently suggested that they follow informal, 'common sense' processes when it comes to dealing with incidents rather than using formal, written policies or processes.

Having some form of cyber insurance cover is relatively common among both businesses and charities. Overall, charities are more likely than businesses to say they have some form of cyber insurance (66% vs. 53% respectively), and there is little difference by size of business (57% of large and 52% of medium businesses). Having cyber security cover as part of a broader insurance policy is more common than having a specific cyber insurance policy across both businesses and charities.

Around half of charities and businesses say they have carried out cyber security training or awareness raising sessions in the last twelve months for any staff (or volunteers) who are not directly involved in cyber security (55% and 48% respectively). This suggests that carrying out cyber security training is unlikely to be a universal practice, although staff training is more common among large businesses (250+ staff) (60%). During the qualitative interviews it was typical for organisations to say they had never assessed the cyber skills of their workforce and had limited understanding of what this would cover or its value for the organisation.

[2] The five types of documentation asked about in the survey are: A Business Continuity Plan that covers cyber security; A risk register that covers cyber security; Any documentation that outlines how much cyber risk the organisation is willing to accept; Any documentation that identifies the most critical assets that the organisation wants to protect; A written list of the organisation's IT estate and vulnerabilities.

Cyber security processes

This chapter provides insight on the uptake of cyber security certifications by organisations. It also sets the baseline for the cyber security processes that organisations have in place, the technical controls required to attain Cyber Essentials certification, and actions taken over the last twelve months to improve or expand various aspects of organisations' cyber security.

Most organisations do not have cyber security certifications. For example, just one in five (19% among both businesses and charities) say they are certified under the Cyber Essentials standard, which is the most frequently obtained certification.

Large businesses (250+ staff) are more likely to adhere to some form of cyber security certification (e.g., 19% of large businesses comply with ISO 27001 compared to 14% of medium businesses), and there are also clear sectoral differences in terms of the types of certifications businesses pursue. For example, businesses in the information or communications sector are more likely to have all three of the certifications asked about. Almost half (47%) of these have ISO 27001, 42% are Cyber Essentials certified, and 27% have Cyber Essentials Plus.

Reasons for obtaining certifications varied during the qualitative interviews, with drivers including contractual requirements, change in senior personnel and having a new IT supplier.

Organisations are taking action to improve their cyber defences and risk management, but this is still limited depending on the nature of the organisation and resources available. Businesses and charities are equally likely to have technical controls in all five of the areas required to attain Cyber Essentials certification[3] (57% for both), though this increases to 64% of large businesses. Despite having these processes in place, few organisations report including anything about cyber security in their most recent annual report, with 14% of businesses and 18% of charities saying this, and around three times as many businesses and charities (45% and 57% respectively) saying they did not.

Around four in five businesses (79%) and charities (84%) say they have taken at least one form of action to expand some aspect of their cyber security over the last twelve months. Regarding specific measures, more than half of organisations say they have expanded or improved their network security (62% of businesses and 66% of charities), processes for user authentication and access control (59% of businesses and 62% of charities), and their malware defences (55% each). Large businesses are more likely to report having made improvements in these areas over the last year than medium businesses. Hence, while organisations are taking action to be better prepared for and protected against incidents, most have gaps in their cyber hygiene and risk management processes.

Regarding cyber security processes in the supply chain, three in five organisations (60% of businesses and 64% of charities) say they did not carry out work in the last twelve months to formally assess or manage the potential cyber security risks presented by their suppliers.

There is a positive relationship between greater board involvement (i.e., more frequent board-level discussions or updates about cyber security) and having in place all five of the technical controls required to attain Cyber Essentials certification. There is also a positive relationship between board involvement and having processes in place to assess or manage cyber security risks presented by suppliers. For example, 68% of businesses with at least monthly board-level discussions and updates about cyber security have technical controls in place in all five of the areas required to attain Cyber Essentials, compared to 36% of businesses that never have board-level discussions and updates. This is similar for charities. In line with other findings, this suggests that buy-in from

[3] The five technical controls required to attain Cyber Essentials certification are: A policy to apply software security updates within 14 days; Up-to-date malware protection across all devices; Firewalls that cover the entire IT network, as well as individual devices; Restricting IT admin and access rights to specific users; Security controls on the organisation's own devices (e.g., laptops).

senior management is likely to have a positive impact on the kind of cyber defences in place. Additionally, businesses that experienced a cyber incident in the last twelve months are also more likely to have technical controls in place in all five of the areas required to attain Cyber Essentials (62% vs. 50% of businesses not reporting an incident).

Cyber incident management

This chapter captures the proportion of organisations that have written processes for cyber security incident management and what these may cover.

Businesses and charities are equally likely to have written processes for how to manage a cyber security incident (51% for each), although the likelihood of having these processes in place is higher among large businesses (250+ staff) (60%).

Additionally, having experience of a cyber security incident over the last twelve months is linked with a higher likelihood of having written processes in place. Just over half (54% of businesses and 55% of charities) of those experiencing an incident in the last twelve months say they have written processes for how to manage a cyber security incident, compared to 44% of both businesses and charities that have not experienced an incident in the last year. This link was implied during the qualitative interviews as well, with respondents often suggesting that experiencing an incident is among the main triggers for introducing formalised cyber security measures.

Among organisations with written processes in place, these are most likely to cover guidance for reporting incidents externally, for instance to regulators or insurers (77% of businesses and 86% of charities).

During the qualitative interviews, participants tended to refer to having informal processes in place, with an incident response plan among those, and the level of detail within these procedures and documents was varied.

Prevalence and impact of cyber incidents

This chapter looks at the different kinds of cyber incidents experienced by organisations and their impact and outcome.

Around half (50% of businesses and 47% of charities) say they experienced at least one cyber security incident – excluding phishing – in the last twelve months. This rises to 72% among businesses and 74% of charities when phishing is included.

Among organisations that reported cyber security incidents over the last twelve months, around four in five businesses and charities say that more than one incident happened during this time period (83% and 81% respectively), and this proportion is similar even when phishing incidents are excluded (79% of businesses and 83% of charities).

Around three in ten businesses (29%) and two in ten charities (19%) that experienced non-phishing incidents in the last year say they experienced an incident at least once a week.

Although most incidents have a short-term impact on operations, of those surveyed, around one in ten organisations (8% of businesses and 10% of charities) that experienced an incident in the last twelve months report that it took a day or longer to restore business operations back to normal. Conversely, nine in ten organisations (90% of businesses and 89% of charities) that experienced any incidents report that it took them less than a day to restore business operations back to normal.

Summary of findings

The summary table of key measures in Annex A shows some of the key baseline metrics, split by business size (50-249, 250-499 and 500+ employees). Further details on statistical reliability and margins of error can be found in Annex C.

Chapter 1 – Introduction

1.1 Background to the research

Publication date: 27 January 2022

Geographic coverage: United Kingdom

The Department for Digital, Culture, Media and Sport (DCMS) commissioned the Cyber Security Longitudinal Survey of medium and large UK businesses (50+ employees) and high-income charities (annual income of more than £1m) as part of the National Cyber Security Programme. The findings will evaluate long-term links between the cyber security policies and processes adopted by these organisations, and the likelihood and impact of a cyber incident. It also supports the Government to shape future policy in this area, in line with the National Cyber Strategy 2022, and will inform future government Cyber interventions and support future strategies with quality evidence.

There will be three annual waves of this study. Due to the longitudinal nature of the study, where the aim is to track trends over time, we will largely speak with the same organisations in each wave. This report is based on wave one (2021) data that will provide a baseline for future waves. The design of this research was influenced by a study DCMS previously commissioned to investigate the feasibility of creating a new longitudinal study of large organisations.

The core objectives of this study are to:

- Explore how and why UK organisations are changing their cyber security profile and how they implement, measure and improve their cyber defences
- Provide a more in-depth picture of larger organisations, covering topics that are lightly covered in the Cyber Security Breaches Survey (CSBS), such as corporate governance, supply chain risk management, internal and external reporting, cyber strategy, cyber insurance and ransomware
- In following waves, explore the effects of actions adopted by organisations to improve their Cyber Security on the likelihood and impact of a cyber incident

The results from this study complement findings from the Cyber Security Breaches Survey (CSBS), an annual study of UK businesses, charities and education institutions as part of the National Cyber Security Programme, as both studies explore UK Cyber Resilience and therefore help to inform and shape government activity in this area.

1.2 Difference from the Cyber Security Breaches Survey

This study differs from the CSBS in multiple important respects. Firstly, it uses a longitudinal approach, where the aim is to track changes in cyber resilience over time, whereas the CSBS uses a cross-sectional sample that provides a snapshot of cyber resilience. This three-year longitudinal study will collect data from the same unit (businesses or charities) on more than one occasion, to analyse the link between large and medium organisations' cyber security behaviours and the extent to which they influence the impact and likelihood of experiencing an incident over time. In comparison, results from CSBS track changes over time, and provides a static view of cyber resilience at a given time.

Secondly, this survey focuses only on medium and large businesses and high-income charities whereas the CSBS includes all businesses (micro, small, medium, and large), all charities and educational institutions. Additionally, different questions are used, so while there are some

similarities in the questions and topics covered by the two surveys, results are not comparable. Finally, as previously discussed, the two studies have different objectives.

The CSBS is an official government statistic, and representative of all UK businesses, charities and educational institutions. Therefore, for overall statistics on cyber security, results from CSBS should be used. Further detail on overlapping questions can be found in the Cyber Security Longitudinal Survey Technical Report.

Please visit the gov.uk website to see publications of the Cyber Security Breaches Survey .

1.3 Methodology

There are two strands to the Cyber Security Longitudinal Survey:

- Ipsos MORI undertook a random probability multimode[4] (telephone and online) survey of 1,205 businesses (1,051 telephone and 154 online) and 536 UK registered charities (454 telephone and 82 online) from 9 March to 7 July 2021[5]. The data for businesses and charities have been weighted to be statistically representative of these two populations.
- Subsequently, 30 in-depth interviews were conducted in July and August 2021, to gain further qualitative insights from some of the organisations that answered the survey.

This longitudinal study aims to track changes over time, so will follow the same organisations in all three annual waves. In wave one, 1,405 organisations (955 businesses; 450 charities) agreed to be recontacted in wave two, and the aim is to retain at least half of these in the panel in wave two (Spring 2022). In subsequent years there will be an additional cross-sectional sample to supplement the longitudinal sample.

The target population of this research is medium and large businesses and high-income charities. This is due to these organisations being more likely than their smaller counterparts to have specialist staff dealing with cyber security, and to have formal policies and processes covering cyber security risks. Additionally, according to the feasibility study conducted prior to this research, similar proportions of medium and large businesses experienced cyber security incidents within the last twelve months, and both report a higher rate than smaller organisations. Therefore, these organisations provide the most insight into how UK organisations are currently managing their Cyber Security.

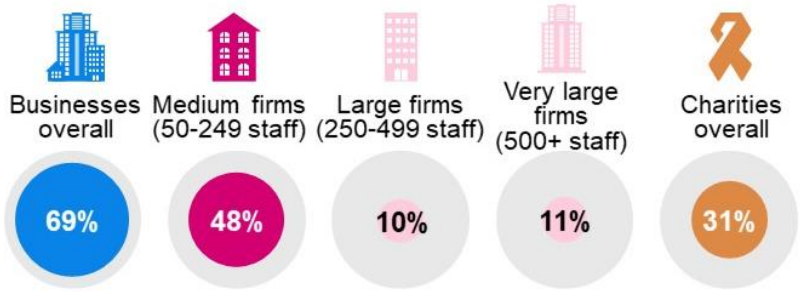
To draw the sample, random probability sampling was used to avoid selection bias. The business sample was proportionally stratified by region, and disproportionately stratified by size and sector. More technical details and a copy of the questionnaire are available in the separately published Technical Annex.

[4] The survey was set up predominantly as a telephone survey but using a multimode (telephone and online) approach aims to maximise response rates by allowing respondents the choice of whether to complete the survey by telephone or online (via a unique survey link emailed from the telephone script). Additionally, due to COVID-19 work from home guidance, it helps to overcome telephone recruitment challenges when many switchboard lines are not operational. The telephone survey aims to include businesses and charities with less of an online presence (compared to solely online surveys). Participants with a valid phone number were given the option to complete the survey over the phone or online.

[5] Including interviews from a pilot from 9 March to 6 April 2021, and main fieldwork from 27 April to 7 July 2021.

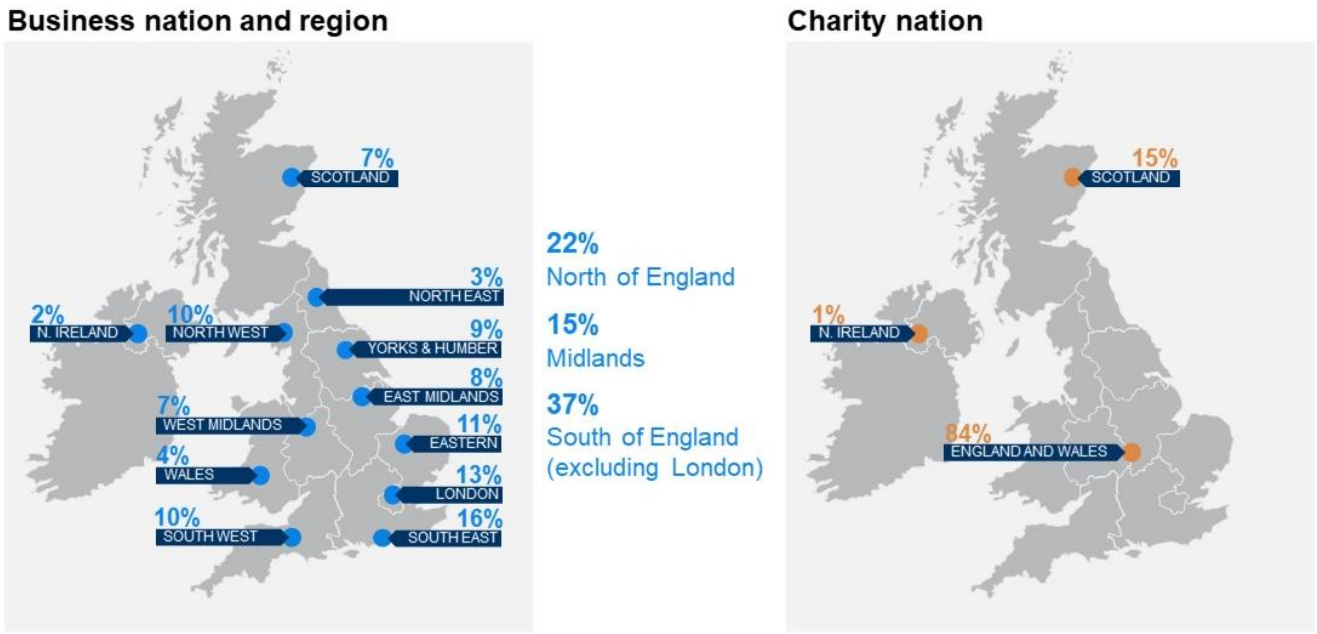
Profile of survey respondents

Figure 1.1: Businesses and charities overall and by business size (showing weighted %)



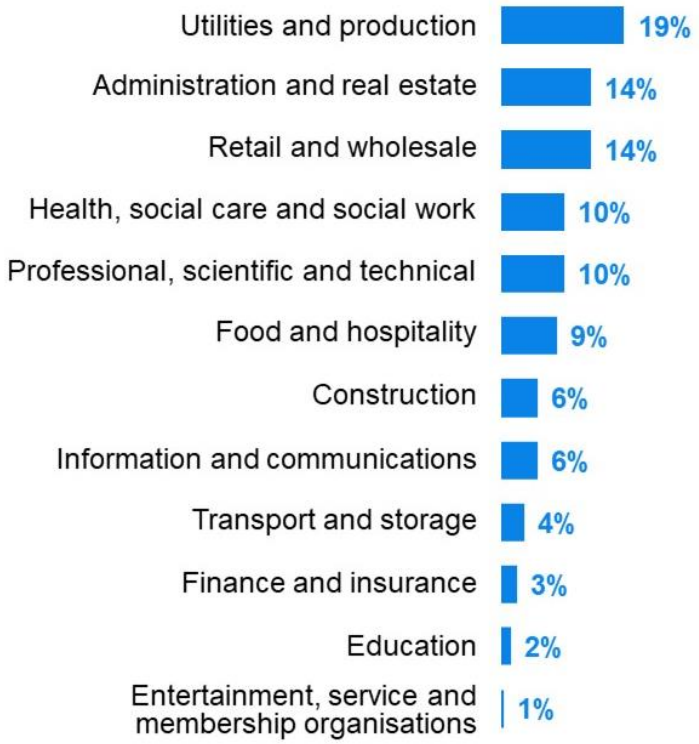
Base: All businesses (n=1,205); Medium firms (n=835); Large firms (n=173); Very large firms (n=197); All charities (n=536).

Figure 1.2: Businesses and charities by nation and region (showing weighted %)



Base: All businesses (n=1,205); All charities (n=536). Businesses in East Midlands (n=98); Eastern England (n=126); London (n=162); North East (n=35); North West (n-124); Northern Ireland (n=26); Scotland (n=81); South East (n=196); South West (n=124); Wales (n=46); West Midlands (n=86); Yorkshire and Humber (n=101); Charities in England and Wales (n=451); Northern Ireland (n=7); Scotland (n=78).

Figure 1.3: Businesses by sector (showing weighted %)



Base: All businesses (n=1,205); Administration and real estate (n=155); Construction (n=63); Education (n=36); Entertainment, service and membership organisations (n=10); Finance and insurance (n=50); Food and hospitality (n=116); Health, social care and social work (n=105); Information and communications (n=107); Professional, scientific and technical (n=92); Retail and wholesale(n=174); Transport and storage (n=64); Utilities and production (n=207)

Profile of qualitative respondents

Thirty follow-up interviews were carried out with a select number of organisations that completed the survey. They were asked to participate based on the following characteristics:

Table 1.1 Profile of qualitative respondents

Quota	Requirement	Achieved
Type	Businesses	18
	Charities	12
Business – size by staff	Medium (50-249)	7
	Large (250-499)	5
	Very large (500+)	6
Business – sector	Good mix across sectors	18
Business – region	Good mix across regions	18
Charity – region	Scotland	3
	England and Wales	9

Cyber roles and responsibilities

Both the survey and the follow-up qualitative interviews were targeted at the person with the most responsibility for cyber security in the organisation. However, in practice, many organisations don't have a specific person responsible for cyber security, so interview participants had a wide range of roles and responsibilities which often spread beyond cyber security or even IT. This was particularly the case among organisations that do not have their own IT department.

Large businesses (especially those in the very large category) are more likely to have employees with dedicated IT roles and larger IT teams than medium businesses or charities that often tend to fully outsource IT activities. Although there were some variances among large businesses in this by sector.

Among respondents with a more general, or sometimes non-IT specific role, awareness of cyber security issues tended to be lower. As a result, people at organisations with the most responsibility for cyber security are often stretched and as a result, cyber security tends to be low in their order of priorities. These participants frequently mentioned having full trust in their IT suppliers when it comes to processes and policies mitigating against any incidents, as well as in incident recovery. Not having dedicated cyber security or IT personnel in place was often explained by lack of resources both in terms of finances and skills.

"Being a small business, we outsource a lot of highly specialised things […] I'm the head of IT but, I'm the CSO as well so I have to wear many hats with it being quite a small business."

Business, Medium, Finance and insurance

Additionally, proportionality was also frequently mentioned, with those from medium businesses or charities suggesting that the cyber security risk faced by the organisation is low compared to a larger organisation or an organisation in the technology sector.

"I'm hoping that the size of our business means that we go below the radar."

Business, Medium, Construction

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 results, subgroup differences by size, sector and survey answers have been highlighted only where statistically significant[6] (at the 95% level of confidence).

There is a further guide to statistical reliability at the end of this report.

Subgroup definitions and conventions

For businesses, analysis by size splits the population into medium businesses (50-249 employees) and large businesses (250+ employees)[7]. Large businesses were compiled of large (250-499

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

[7] Some references to very large businesses (500+ employees) are included where data is of particular interest for this group. References to large businesses incorporate all businesses with 250+ employees unless stated.

employees) and very large businesses (500+ employees). All charities have a reported annual income of at least £1 million.

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 and real estate (L and N)
- Construction (F)
- Education (P)
- Health, social care and social work (Q)
- Entertainment, service and membership organisations (R and S)
- Finance and insurance (K)
- Food and hospitality (I)
- Information and communications (J)
- Utilities and production (including manufacturing) (B, C, D and E)
- Professional, scientific and technical (M)
- Retail and wholesale (including vehicle sales and repairs) (G)
- Transport and storage (H).

Where figures are marked with an asterisk (*) these refer to base sizes smaller than 50 and should be treated with caution.

1.5 Acknowledgements

Ipsos MORI and DCMS would like to thank all the organisations and individuals that participated in the survey. We would also like to thank the organisations that endorsed the fieldwork and encouraged businesses and charities to participate, including:

- The National Cyber Security Centre (NCSC)
- The Home Office
- The Scottish Government
- The Charity Commission
- The Confederation of British Industry (CBI)
- The Institute of Chartered Accountants in England and Wales (ICAEW)

Chapter 2 – Cyber profile of organisations

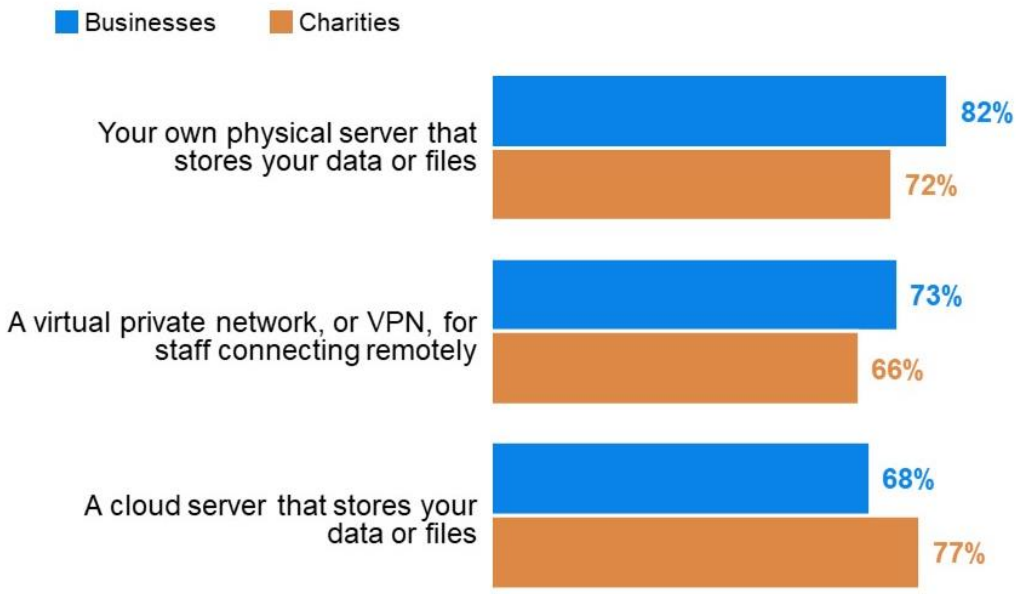
This chapter explores the cyber profile of organisations, if they use cloud computing, use of personal devices, and use of Artificial Intelligence (AI) and machine learning.

2.1 Cloud computing

Almost all organisations (97% of businesses, and 95% of charities) use at least one form of secure network to store or access their data and files. Charities (77%) are more likely than businesses (68%) to have a cloud server that stores their data or files. However, businesses (82%) are more likely than charities (72%) to have their own physical server that stores their data or files, and they are also more likely to have a virtual private network[8] (VPN) for staff when they connect remotely (73% of businesses; 66% of charities).

Figure 2.1: How organisations store or access their data and files

Does your organisation use or provide any of the following?



Base: All businesses (n=1,205); All charities (n=536). Don't know not shown.

2.2 Use of personal devices

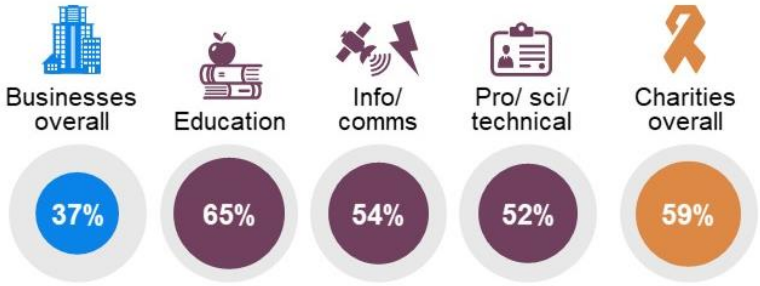
Charities (59%) are more likely than businesses (37%) to permit staff to access their organisation's network or files through personally owned devices such as a personal smartphone or home computer.

Businesses in the education (65%), information and communications (54%) and professional, scientific and technical (52%) sectors are more likely to permit their staff to use personally owned devices.

[8] Virtual Private Networks (VPNs) allow organisations to provide secure connectivity between devices in physically separate locations.

Figure 2.2: Use of personal devices to access organisation's network or files

Are staff permitted to access your organisation's network or files through personally owned devices?



Base: All businesses (n=1,205); Education sector (n=36); Information and communications sector (n=107); Professional, scientific or technical sector (n=92); Businesses in London (n=162); All charities (n=536). Don't know not shown.*

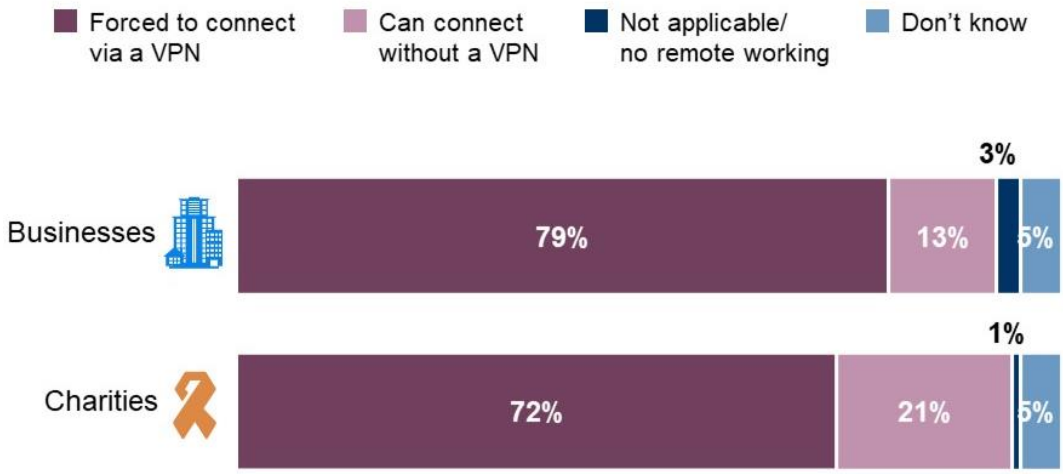
Of the organisations that use a VPN, businesses (79%) are more likely than charities (72%) to require their staff to connect via a VPN when connecting to the organisation's network or files outside of the workplace.

Businesses in the retail and wholesale (90%) and utilities and production (84%) sectors are the most likely to require their staff to connect via a VPN, while those in the health, social care and social work sector (58%) are the least likely to do this.

Businesses and charities that have technical controls in place in all five of the areas required to attain Cyber Essentials are more likely to require staff to connect via a VPN (84% and 76% respectively) than those without technical controls in place in all five of the areas required to attain Cyber Essentials (72% of businesses and 66% of charities).

Figure 2.3: Use of VPN

If staff connect to your network or files outside your own workplaces, are they forced to connect via a VPN, or can they access your network or files without a VPN?



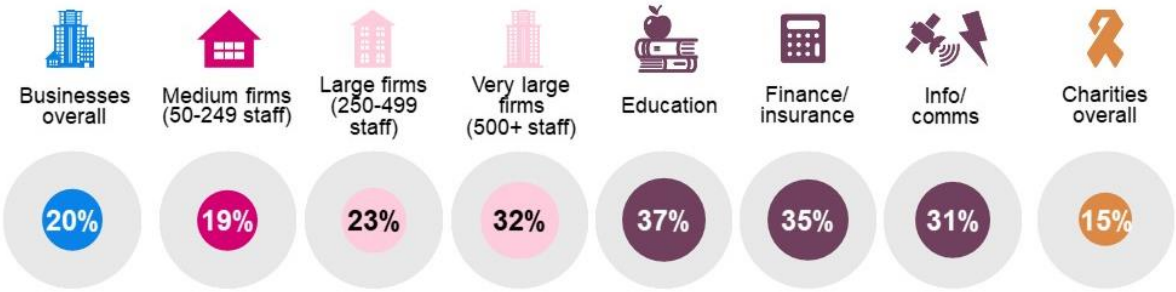
Base: All businesses (n=1,205); All charities (n=536).

2.3 Use of artificial intelligence (AI) and machine learning

AI is very important to cyber security because pattern recognition algorithms can be applied to network data flows to automate threat detection. Machine learning is a subset of AI that can be used to 'learn' any new patterns it identifies from recent incidents. Businesses (20%) are more likely than charities (15%) to use cyber security tools that use AI or machine learning. Almost one in three very large businesses with 500+ employees (32%) deploy AI or machine learning, compared to around one in five medium-sized businesses (19%). Businesses in the education (37%), finance and insurance (35%) and information and communications (31%) sectors are also more likely to deploy AI or machine learning.

Figure 2.4: Use of AI or machine learning

Does your organisation deploy any cyber security tools that use AI or machine learning? (% yes)



Base: All businesses (n=1,205); Medium firms with 50-249 employees (n=835); Large firms with 250-499 employees (n=173); Very large firms with 500+ employees (n=197); Finance and insurance sector (n=50); Education sector (n=36*); Information and communications sector (n=107); Businesses in London (n=162); All charities (n=536). Don't know not shown.*

2.4 Use of external IT providers

During the qualitative interviews, businesses and charities were asked whether they use external IT suppliers or cyber security consultants. Some organisations, particularly medium businesses and charities, choose to either completely outsource their IT to an external provider, so they have limited responsibility for it in-house, or they use outsourcing to complement their internal IT teams, for example, when out of hours, for advice or for specific services (e.g. penetration tests).

These relationships are often long-established and involve a high level of trust in these external partners. Additionally, organisations often consider their external IT providers to be an essential part of the organisation.

When asked about how IT suppliers were chosen, most have long-standing relationships with suppliers and limited recall on how the contract started. As a result, many are unlikely to regularly review contracts or shop around for other suppliers.

Outsourcing IT is a decision most often motivated by cost savings, with many respondents suggesting that due to the size of their organisation, having an in-house IT function or capability would be less cost-effective.

"It was a tactical decision to have that rather than having more IT manpower in the department. It was more cost effective to have a partner helping us."

Business, Large, Professional, scientific and technical

Chapter 3 – Board involvement

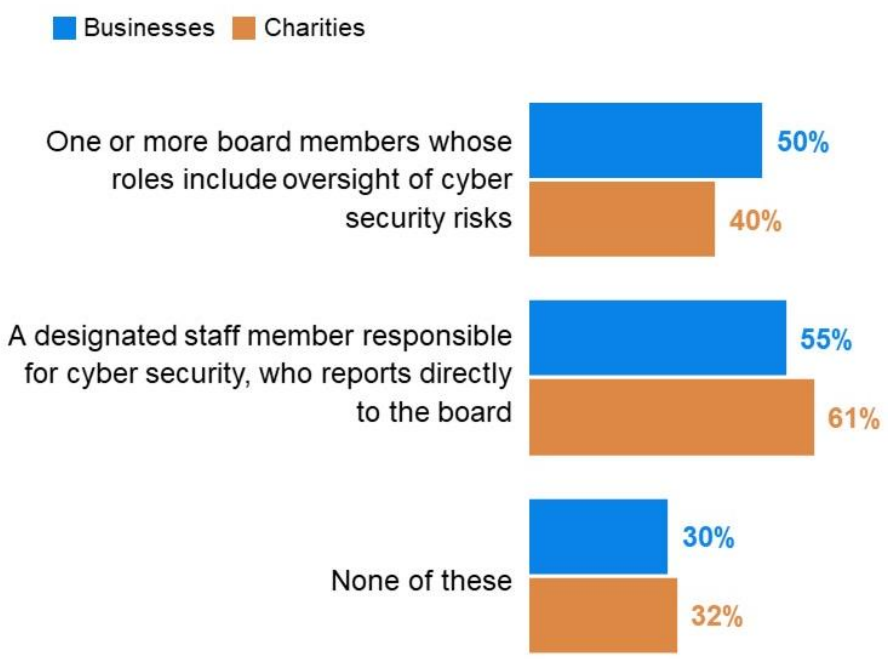
This section covers the roles and responsibilities of board members in relation to cyber security in larger organisations. It explores the ways in which board members engage with cyber security, and their frequency.

3.1 Roles and responsibilities

Businesses are more likely than charities to report having one or more board members with an oversight of cyber security risks (50% vs. 40% respectively). In comparison, a higher proportion of charities than businesses (61% vs. 55% respectively) say they have a designated staff member responsible for cyber security, who reports directly to the board. Around three in ten charities (32%) and businesses (30%) report having neither.

Figure 3.1: Cyber security roles and responsibilities within organisations

Does your organisation have any of the following?



Base: All businesses (n=1,205); All charities (n=536). Don't know not shown.

Large businesses (250+ staff) are more likely than medium businesses to report having board members with an oversight of cyber security risks (57% vs. 48% respectively) and a designated staff member who reports directly to the board about these issues (61% vs. 54% respectively). In turn, while three in ten medium businesses (31%) say they have neither, this applies to just 24% of large businesses.

Businesses in the finance and insurance and information and communication sectors are the most likely to have board members with an oversight of cyber security risks (76% and 66% respectively), and a designated staff member who reports directly to the board about these issues (75% and 69% respectively). Businesses in the food and hospitality sector are the least likely to have these, with two in five (41%) reporting having neither.

Across businesses and charities, during the qualitative interviews, respondents often mentioned a lack of understanding from board members around cyber security during the qualitative interviews. This was associated with a variety of interconnected factors, including the age of board members, lack of IT literacy or lack of board-level training opportunities on cyber security. As a result, respondents, who often personally identified as the 'designated staff member' reporting directly to the board about cyber security issues, frequently cited communication barriers and/or knowledge gaps when it comes to having conversations about cyber security with board members.

"Our CEO is diligent, interested [in cyber security], but not particularly IT literate. Our Board is interested, but absolutely IT illiterate."

Charity

In line with the quantitative findings, respondents from certain sectors, such as the food industry and retail, mentioned the issue of board members seeing cyber security as irrelevant for their sector. In comparison, respondents from sectors that tend to be more cyber-oriented, such as the information and communication sector, suggested that their board is likely to be invested in issues related to cyber security, due to historically seeing this as a highly relevant issue for the sector. However, particularly for medium businesses, board-level discussions about cyber security are likely to remain informal, regardless of the level of interest among board members.

"The chairman has a very keen interest, he worked in IT and cyber positions before. He occasionally reaches out and we have more informal discussions. I do have conversations with the chairman about how he wants things to be reported, what he sees as the issues, and [I] do the same with [the] CFO. For a business our size, it works well like that."

Business, Medium, Information and communications

Businesses that have technical controls in place in all five of the areas required to attain Cyber Essentials, and those with some form of cyber security certification, are more likely than businesses on average to have individuals with these roles and responsibilities within the organisation.

Additionally, businesses that have experienced a cyber incident in the last twelve months are more likely than those that have not to have board members with an oversight of cyber security risks (54% vs. 45% respectively) and a designated staff member who reports directly to the board about these issues (59% vs. 48% respectively).

An increase in interest from board members, and therefore appetite for cyber security certifications, was mentioned by some respondents during the qualitative interviews. These interviews also suggested that personal experience of cyber incidents or increased awareness due to a high-profile case in the news sometimes triggers increased interest from board members and prompts buy-in to cyber certifications. This suggests that board involvement and acquisition of cyber security certification tends to be reactive rather than proactive.

"They want everything in layman's terms, they don't want any technicalities at all. The best way would be me saying to them 'if you don't do this and something happens, this would be the likely scenario.' […] They want to see everything in black and white for cost justification. If you can make a decent case for it, generally it's going to go through."

Business, Large, Administration and real estate

"I think they are pretty good. If you look at the university hack which happened, it opened a lot of eyes to the impact it could have. All of the trustees are in industries that involve technology."

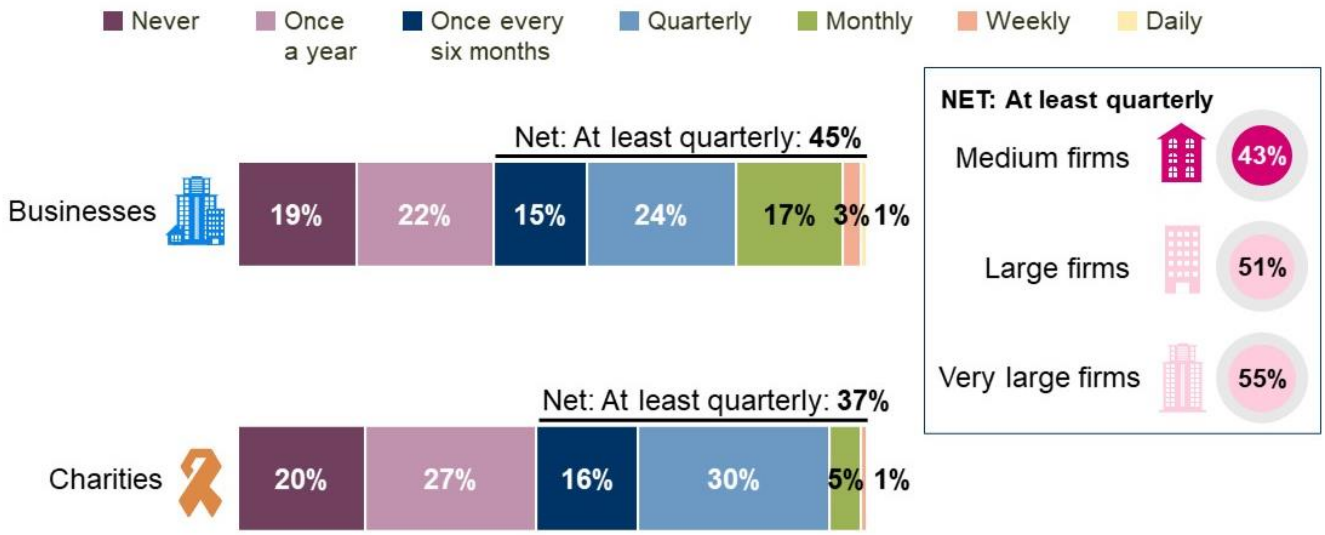
Charity

3.2 Awareness and training

When asked about roughly how often their board discussed or received updates on cyber security over the last twelve months, almost half (45%) of businesses say they did so at least quarterly (excluding don't know responses). Businesses are more likely to have more frequent board discussions or updates than charities, with 37% of charities reporting that their board had done so at least quarterly.

Figure 3.2: Frequency of board discussions or updates on cyber security

Over the last twelve months, roughly how often, if at all, has your board discussed or received updates on your organisation's cyber security?



Base: All businesses excluding don't know (n=974); All charities excluding don't know (n=473).

Looking across business sizes and sectors, very large businesses with 500+ employees (55%) and businesses in the finance and insurance (81%) and information and communications (74%) sectors are more likely to report having at least quarterly board discussions or updates about cyber security than businesses on average.

While this suggests that board members are likely to have a relatively high level of awareness of cyber security-related issues within organisations, one in five organisations (19% of businesses and 20% of charities) say the board had no such discussions or updates at all over the last twelve months. Non-engagement with cyber security issues, and IT more generally, was also frequently cited during the qualitative interviews, suggesting that even in organisations where discussions do happen, board members tend to have little to no interest or understanding of these issues.

A re-emerging theme during the qualitative interviews with respondents from medium-sized businesses was explaining the lack of interest among board members as often stemming from the culture of the organisation not evolving with growth and expansion. As a result, unless any incidents happen with a notable financial impact, cyber security is likely to be regarded as an issue outside of the board's remit and of lower priority than other risks.

“They [MD and General Manager] are happy to leave the paranoia to me and the IT Department. They are too busy running the rest of the business.”

Business, Medium, Utilities and production

“There just haven’t been any incidents apart from the one that happened a few weeks ago. Everyone was aware of it because everyone had to change their password. Everyone was briefed and that was an end to it.”

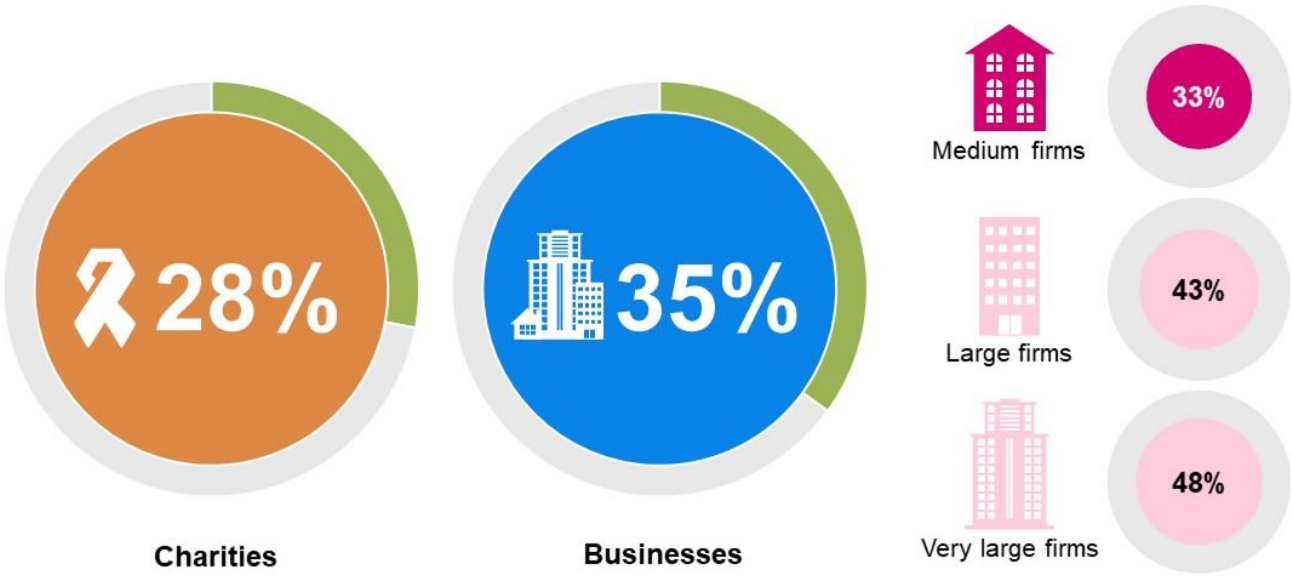
Business, Medium, Transport and storage

In addition to the relatively low levels of board engagement with cyber security, both businesses and charities are relatively unlikely to report that their board members have received any cyber security training.

There is a gap between the levels of board training and more general staff training on cyber security. The proportion of organisations reporting their board members had received any cyber security training is lower than the proportion offering cyber security training to their staff in the last twelve months, across both businesses (48% said they offered training to staff in the last twelve months vs. 35% saying board members had received training at any time) and charities (55% vs. 28% respectively).

Figure 3.3: Board-level cyber security training

Have any of the board received any cyber security training? (% yes)



Base: All charities (n=536), All businesses (n=1,205). Don't know responses not shown: 21% of businesses and 22% of charities

In terms of business size, around half of very large businesses with 500+ employees (48%) report their board members have received any cyber security training, compared to one in three medium businesses (33%). By sector, businesses in finance and insurance (64%) and information and communications (61%) are the most likely to say their board members have received any cyber security training, while those in the food and hospitality sector are the least likely (25%).

Businesses and charities where the board has received any cyber security training are also more likely to report more frequent board-level discussions or updates on cyber security. For example, 64% of businesses and 61% of charities where the board has received training on cyber security also say they have board-level discussions or updates on cyber security at least monthly. This is in comparison to just 21% of businesses and 24% of charities where the board has not received cyber security training. This suggests that there is a link between the level of board members' buy-in to cyber security issues and the levels of cyber training and discussions that take place among board members.

There is also a positive correlation between adhering to cyber security certifications or standards, and board members having received cyber security training. For example, more than half of businesses adhering to ISO 27001 (59%), the Cyber Essentials standard (57%) or the Cyber Essentials Plus standard (63%) say that their board has received cyber security training, compared to just 26% of those businesses who do not hold any of these certifications.

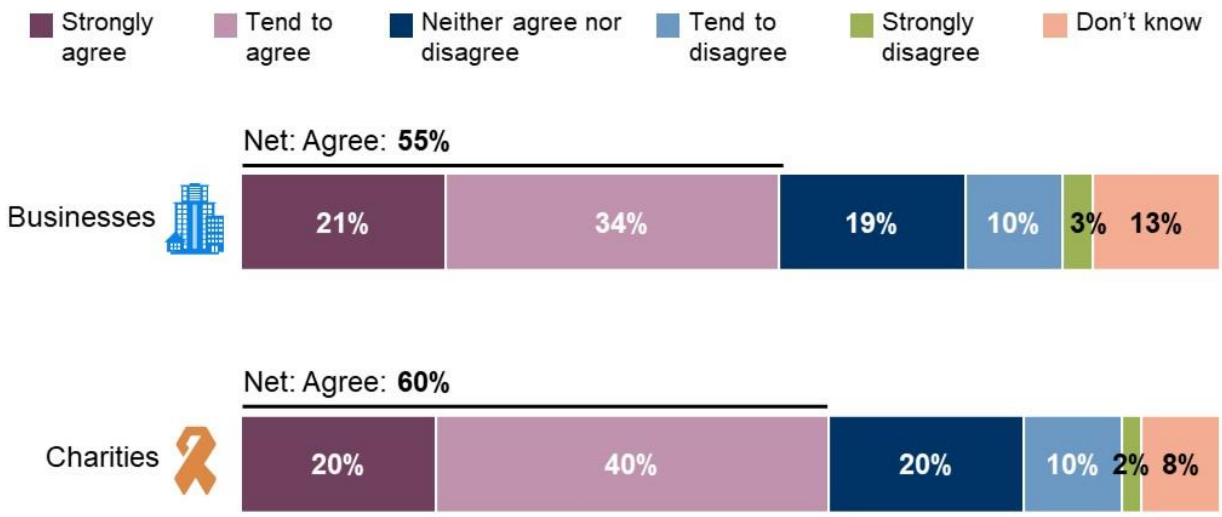
3.3 Attitudes to cyber risk

Businesses and charities reporting that their board has discussions or updates about cyber security were asked how they typically engage with any information on the cyber security risk the organisation faces. Around three in five such businesses (55%) and charities (60%) agree that their board integrates cyber risk considerations into wider business areas, while just over one in ten (13% of businesses and 11% of charities) disagree with this statement.

Looking specifically at businesses with boards discussing cyber security, large businesses (250+ staff) are more likely than medium businesses to agree with this statement (61% vs. 53% respectively). Additionally, businesses in the finance and insurance (70%) and information and communications (72%) sectors are the most likely to agree that their board integrates cyber risk considerations into wider business areas. In turn, those in the utilities and production (19%) and retail and wholesale (18%) sectors are the most likely to disagree.

Figure 3.4: Board engagement with cyber risk

How much would you agree or disagree with the following statement? The board integrates cyber risk considerations into wider business areas.



Base: All whose board discusses cyber security, businesses (n=1,037), charities (n=442)

As with previous findings, there is a positive relationship between having technical controls in place in all five of the areas required to attain Cyber Essentials, adhering to cyber security standards and more board engagement. For instance, three-quarters (73%) of businesses and an even higher proportion of charities (84%) that adhere to ISO 27001[9] agree that their board integrates cyber risk considerations into wider business areas.

Increased attention given to cyber security after an incident is experienced was a consistent theme during the qualitative interviews, with many respondents suggesting that the experience of an incident is often the only thing that incentivised or could incentivise board members to engage with cyber security more closely and integrate with wider business considerations.

Respondents also mentioned that cyber security, or more generally IT, tends to be seen more as a facilitator of the business than a strategic driver among senior leadership. Therefore, it is unlikely to be thought of in a strategic context.

"I think it [cyber security] is [included in our strategy], but it hasn't got a line item. If we have a new solution or improvement to be made, we make sure it is secure by default. We have privacy by design. It needs to be a given. It is not a strategy in itself, but [cyber security] is something we make sure by default that is what we want it to be."

Business, Large, Professional, scientific and technical

[9] An international standard on how to manage information security. An Information Security Management System (ISMS) is a set of policies, procedures, and roles designed to ensure cyber security risks are identified and managed.

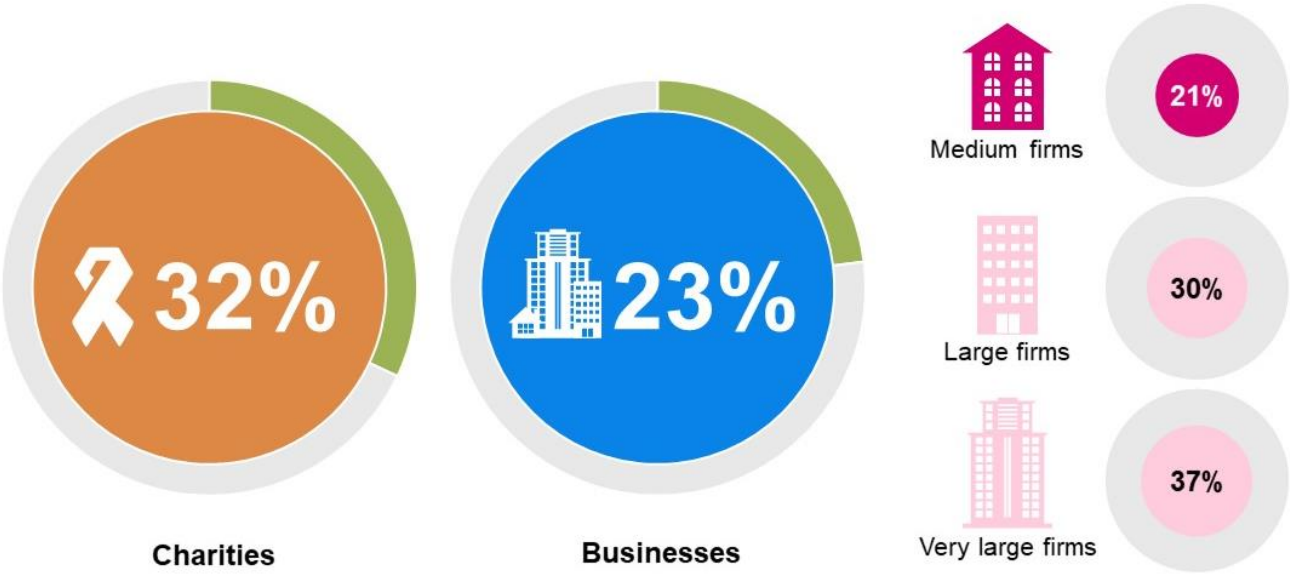
Chapter 4 – Sources of information

4.1 Use of NCSC guidance

Around one-third (32%) of charities and one-quarter (23%) of businesses have used information or guidance from the National Cyber Security Centre (NCSC) in the last twelve months. However, businesses are more likely than charities to say they do not know if they have used NCSC guidance (23% vs. 16%).

Figure 4.1: Use of NCSC guidance

In the last twelve months, has your organisation used any information or guidance from the National Cyber Security Centre (NCSC) to inform your approach to cyber security?



Base: All businesses (n=1,205); All charities (n=536). Don't know not shown.

Very large businesses (37%) are more likely than large businesses (30%), which are in turn more likely than medium businesses (21%), to have used NCSC information or guidance in the last year. Usage of NCSC guidance is also higher among finance and insurance (51%) and information and communications (41%) businesses.

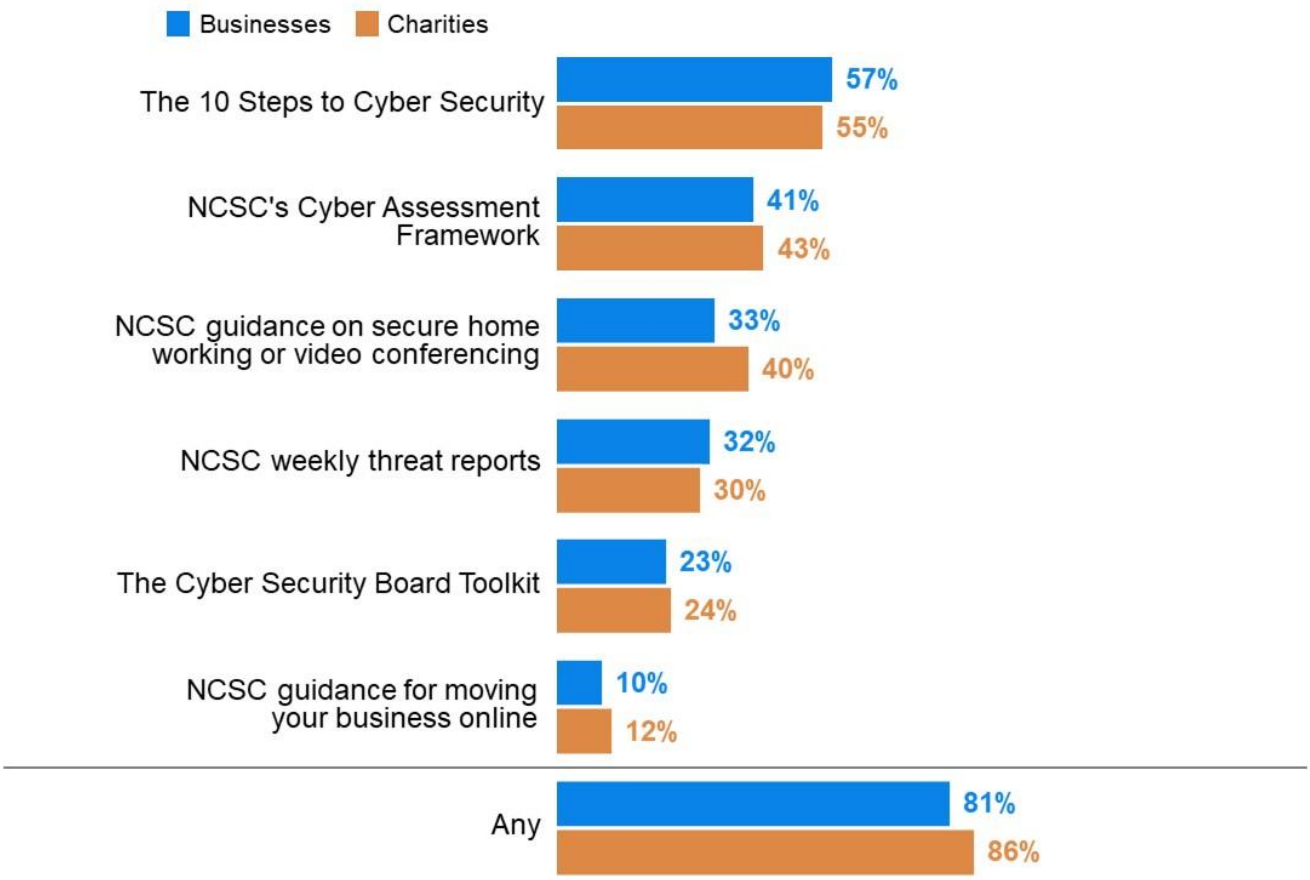
Around half of businesses certified to the Cyber Essentials (47%) or Cyber Essentials Plus (52%) standards used NCSC information in the last twelve months, a higher proportion than those certified under ISO 27001 (37%, which is still greater than the overall average). Prevalence is also higher among businesses whose boards discuss cyber security at least monthly (40%) and businesses that experienced a cyber incident in the last twelve months compared to those that did not (28% vs. 15% respectively).

Similar differences apply among charities. Just over half of charities certified to Cyber Essentials (51%) or Cyber Essentials Plus (55%) used NCSC information in the last year. Usage of NCSC guidance is also higher in charities whose boards discuss cyber security at least quarterly (40%), and those that experienced a cyber incident in the last twelve months compared to those that did not (38% vs 20%). As many as 45% of charities reporting non-phishing incidents in this time used NCSC guidance.

Among organisations that have made use of NCSC guidance, just over half have used 'The 10 Steps to Cyber Security' (57% of businesses and 55% of charities), followed by the NCSC's Cyber Assessment Framework (41% of businesses and 43% of charities).

Figure 4.2: Use of NCSC guidance (among organisations using NCSC guidance)

Which of the following, if any, have you used?



Base: All who used NCSC information or guidance in the last twelve months; Businesses (n=311); Charities (n=169). Don't know/ none of these not shown.

In the qualitative research, several participants mentioned that they had found the NCSC a useful source of information. Specific examples of this were sharing NCSC posters and guidance with staff to raise awareness of cyber security and implementing guidance on sharing passwords and regular alerts.

"I've got a whole folder of bookmarked pages from them [the NCSC website] that I find especially useful."

Business, Medium, Information and communications

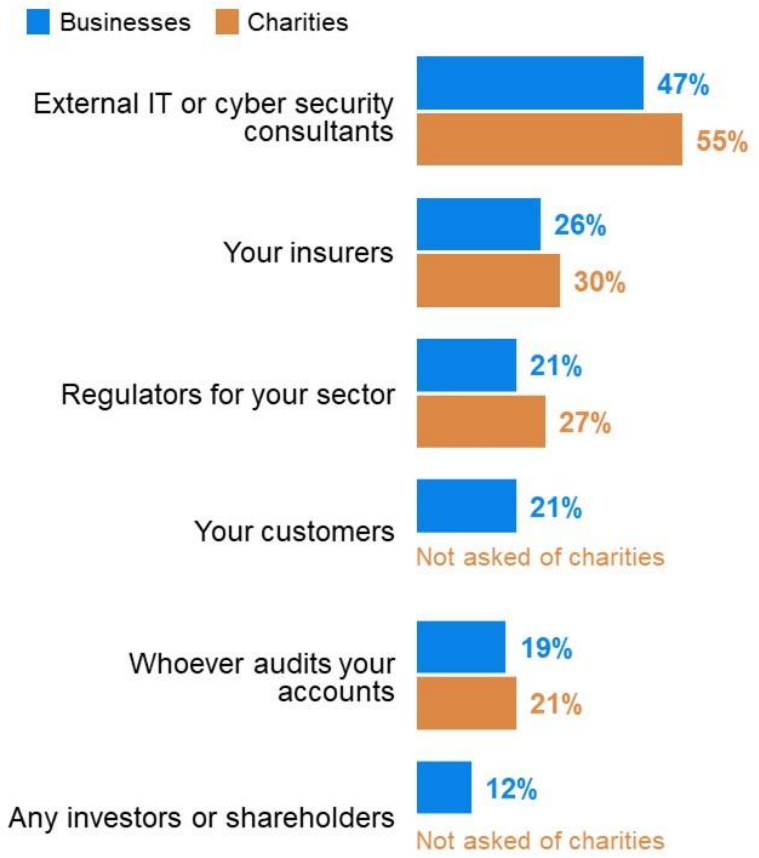
4.2 Other information sources/influencers

A crucial factor in strengthening UK cyber resilience is understanding how best to positively influence organisations to take action and improve their cyber defences. The survey highlights that, of the six groups asked about, the greatest external influence in the last twelve months has come from external cyber security consultants. Around half of businesses (47%) and charities (55%) say that feedback from external IT or cyber security consultants influenced their actions on cyber security.

Fewer organisations report being influenced by insurers (26% for businesses and 30% for charities), regulators (21% and 27% respectively), and auditors (19% and 21% respectively). Among businesses, 21% report being influenced by customers, and 12% by investors or shareholders in the last year. Charities are more likely than businesses to have been influenced by external consultants and regulators.

Figure 4.3: Influence of external sources on actions

Over the last twelve months, how much have your actions on cyber security been influenced by feedback from any of the following groups?



Base: All businesses (n=1,205); All charities (n=536). Showing Net: A great deal/fair amount only.

Very large businesses with 500+ employees are more likely than average to mention auditors (28%) and are also more likely than medium sized businesses to say they have been influenced by regulators (27% vs. 20%) and investors (19% vs. 11%). Large businesses with 250+ employees are more likely than medium sized businesses to have been influenced by insurers (32% vs. 25%).

Patterns of influence differ by sector:

- **External IT or cyber security consultants** are more likely to be mentioned by finance and insurance (64%) businesses
- Finance and insurance (67%), information and communications (37%) and health, social care and social work (33%) businesses are more likely than average to have been influenced by **regulators**
- **Customers** are more likely to have influenced businesses in the information and communications (45%) and transport and storage (28%) sectors
- **Investors or shareholders** are more likely to be sources of influence for finance and insurance (25%), information and communications (also 25%) and transport and storage (20%) businesses

In general, organisations with certifications, with boards that discuss cyber security at least monthly, and which experienced a cyber incident in the last twelve months, are more likely to say they are influenced by each of the stakeholders mentioned in the survey.

Charities (20%) are more likely than businesses (14%) overall to have reviewed or changed any of their cyber security policies or processes because of an organisation in their sector experiencing a cyber security incident. Charities are also more likely than businesses (14% vs. 10%) to have acted because of another organisation in their sector implementing similar measures.

Large businesses (250+ staff) are more likely than medium businesses to have reviewed or amended their policies because of an organisation in their sector experiencing a cyber incident (24% vs. 12% respectively) or implementing similar measures (17% vs. 9% respectively). The likelihood of both is also greater among organisations with boards that discuss cyber security at least monthly, that have cyber security certifications, and which have experienced a cyber incident in the last twelve months. Businesses in the information and communications sector (20%) are more likely than businesses on average to have reviewed or changed their cyber security policies or processes because of another organisation in their sector implementing similar measures.

The qualitative research found that some organisations fully depend on their IT consultants to keep them up to date with any actions required on cyber security. There is typically a high degree of trust in this relationship, though services could also be switched between contractors for a fresh perspective. For other organisations, suppliers have a more informative role, providing them with updates and alerts that they can then choose how to action.

“I do my best to keep in touch with the whole field. I subscribe to all the vulnerability stuff that comes through from the vendors we use. The Microsoft security centre blogs. A lot of it is keeping your ear to the ground internet-wise and you can pick up a lot of what is going on.”

Charity

Chapter 5 – Cyber security policies

This section discusses the cyber security policies organisations have in place, including documentation, cyber insurance policies and staff training.

5.1 Governance and planning

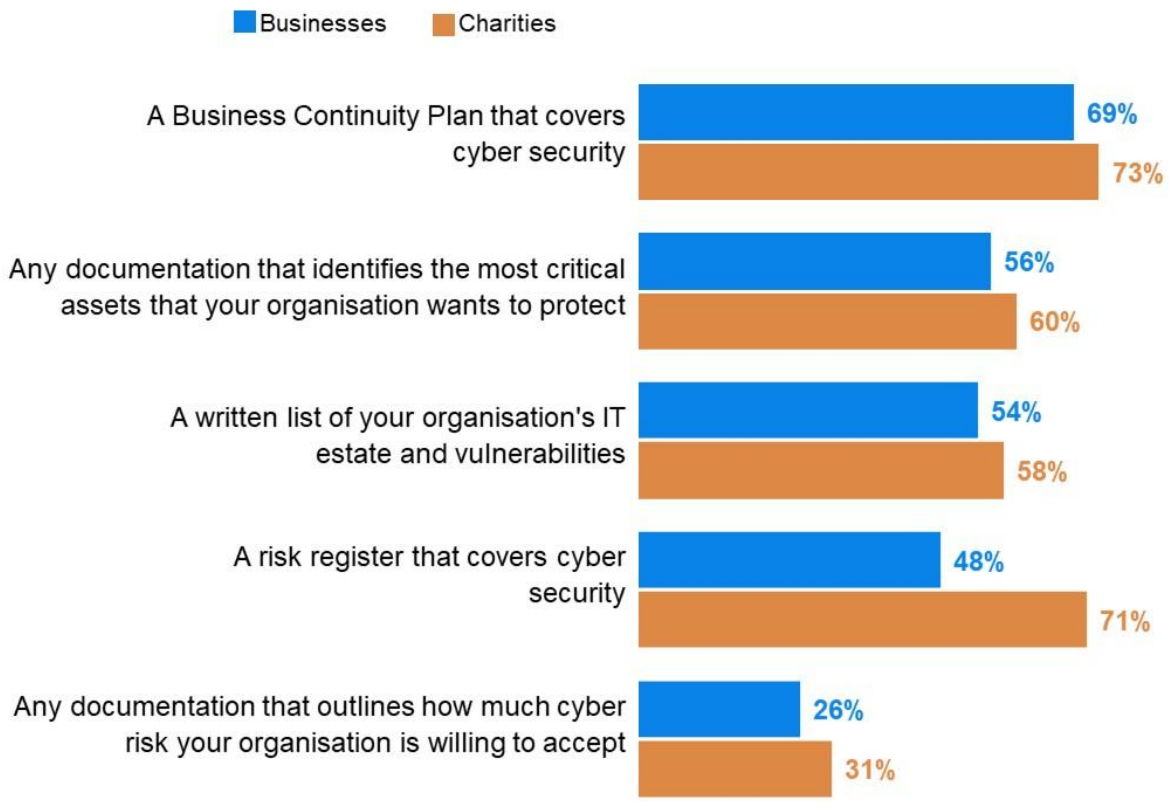
The survey asked about five types of documentation that organisations may have in place as part of an effective cyber security strategy. This included: a Business Continuity Plan covering cyber security, documentation identifying critical assets, documentation about the IT estate and vulnerabilities, a risk register covering cyber security, and documentation on the organisation's 'risk appetite' (i.e., the level of cyber risk the organisation is willing to accept).

Of the five different types of documentation tested that help organisations manage cyber security risks, having a Business Continuity Plan that covers cyber security is the most common across both businesses and charities (69% and 73% respectively). Of the types of documents tested, both businesses (26%) and charities (31%) are least likely to have documentation that outlines how much cyber risk the organisation is willing to accept.

More than half of organisations say they have documentation that identifies the most critical assets that the organisation wants to protect (56% of businesses and 60% of charities), and a written list of the organisation's IT estate and vulnerabilities (54% of businesses and 58% of charities). Having a risk register that covers cyber security in place is much more common among charities than businesses, with seven in ten (71%) charities saying they have this compared to just under half (48%) of businesses.

Figure 5.1: Documentation in place to manage cyber security risks

Does your organisation have any of the following documentation in place to help manage cyber security risks?



Base: All businesses (n=1,205); All charities (n=536). Don't know not shown.

Overall, fewer than one in five organisations say they have all five types of documentation in place to manage cyber security risk (17% both for businesses and charities). Businesses are more than twice as likely as charities to say they have none of these documents (18% vs. 8% respectively).

Large businesses (250+ staff) are more likely than medium businesses to report having all five documents (21% vs. 16% respectively), while medium businesses are more likely than large businesses to say they have none (19% vs. 12% respectively). Having all five types of documentation is most common among businesses in the information and communications (35%) and finance and insurance (34%) sectors. In contrast, businesses in the food and hospitality (28%) and retail and wholesale (25%) sectors are the most likely to say they have none of the documents in place.

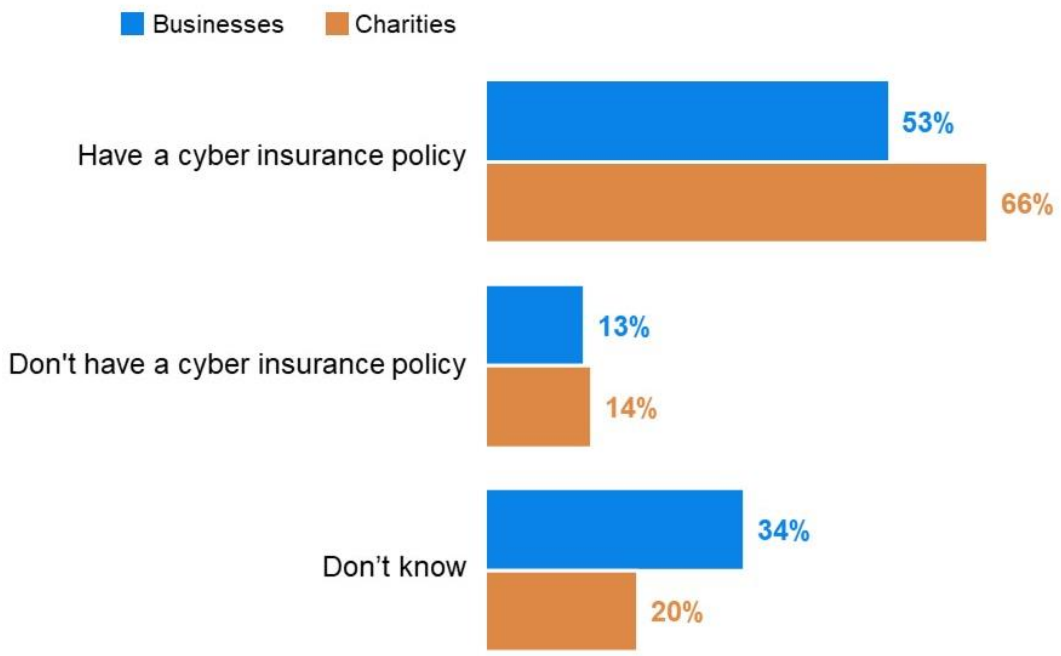
During the qualitative interviews these processes were further explored, particularly focusing on incident response plans which are discussed in more detail in section 6 of this report. Whether organisations had a written incident response plan varied from relying completely on external IT suppliers to having processes in place adhering to ISO standards. In line with the quantitative findings, respondents from large businesses were the most likely to report having sophisticated cyber security policies and processes in place, including robust, ISO 27001 compliant incident response plans. Respondents adhering to standards and certifications suggested that the periodic testing required by these helped to reinforce governance and planning more generally.

5.2 Cyber insurance policies

Having some form of cyber insurance cover is relatively common among organisations. Charities are more likely than businesses to report they have some form of cyber insurance (66% vs. 53% respectively). However, at least some of this difference is explained by more business respondents than charity respondents saying that they do not know their organisation’s cyber insurance status (34% vs. 20% respectively). Among businesses, 57% of both large (250-499 staff) and very large (500+ staff) businesses say they have some form of cyber insurance.

Figure 5.2: Organisations with cyber insurance

Which of the following best describes your situation?



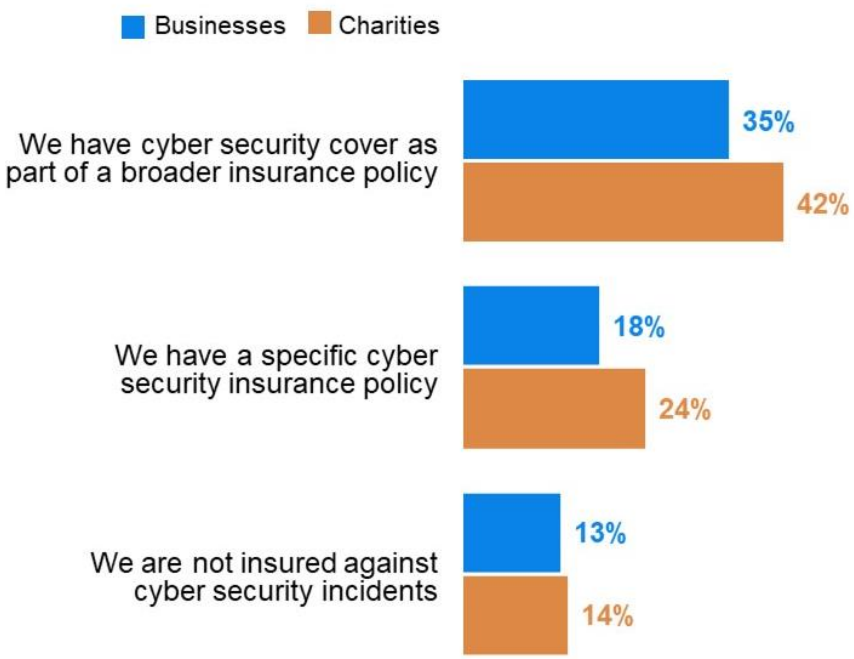
Base: All businesses (n=1,205); All charities (n=536).

Regarding the type of cover held, businesses and charities are both more likely to have cyber security cover as part of a broader insurance policy than having a specific cyber insurance policy. Having a specific cyber security insurance policy is more common among charities than businesses, with one-quarter of charities having this type of cover compared to fewer than one in five businesses (24% vs. 18% respectively).

While one-quarter of large businesses (250+ staff) (24%) report having a specific policy, only 17% of medium businesses say the same. One in three businesses in the finance and insurance sector (34%), and close to three in ten (28%) businesses in the information and communication sector, say they have a specific cyber insurance policy. This compares to 9% of businesses in the health and social care sector.

Figure 5.3: Type of cyber insurance policy organisations have

Which of the following best describes your situation?



Base: All businesses (n=1,205); All charities (n=536). Don't know not shown.

5.3 Staff training

When asked about whether they carried out any cyber security training or awareness raising sessions in the last twelve months specifically for any staff/staff or volunteers who are not directly involved in cyber security, charities are more likely than businesses to say they did (55% vs. 48%), although this varied by business size and sector. While just under half (45%) of medium businesses say they carried out such training, six in ten (60%) large businesses (250+ staff) say they did. However, looking at large businesses in more detail, businesses with 500+ staff were much more likely than those with 250-499 staff to say they had carried out cyber security training in the last year (70% vs. 51%).

Around eight in ten businesses in the finance and insurance (79%) and information and communications (78%) sectors say they had offered training to staff in the last twelve months, compared to around just one in three businesses in the food or hospitality (31%), construction (35%) or health, social care and social work (also 35%) sectors.

Respondents during the qualitative interviews were asked whether their organisation had conducted a cyber skills assessment of their workforce. Most respondents had limited understanding of what this might cover and some thought of it as interchangeable with offering training.

"Something else to do! Is there a standard one around?"

Business, Medium, Construction

Among those familiar with the concept, a common view among charity respondents was that conducting a cyber skills assessment of their workforce would have little to no value, citing either that staff members tend to only use email, or assuming high level of IT illiteracy among staff. Among businesses, those that did some form of skills assessment referred to sending out fake phishing emails and testing the likelihood of reporting these.

Chapter 6 – Cyber security processes

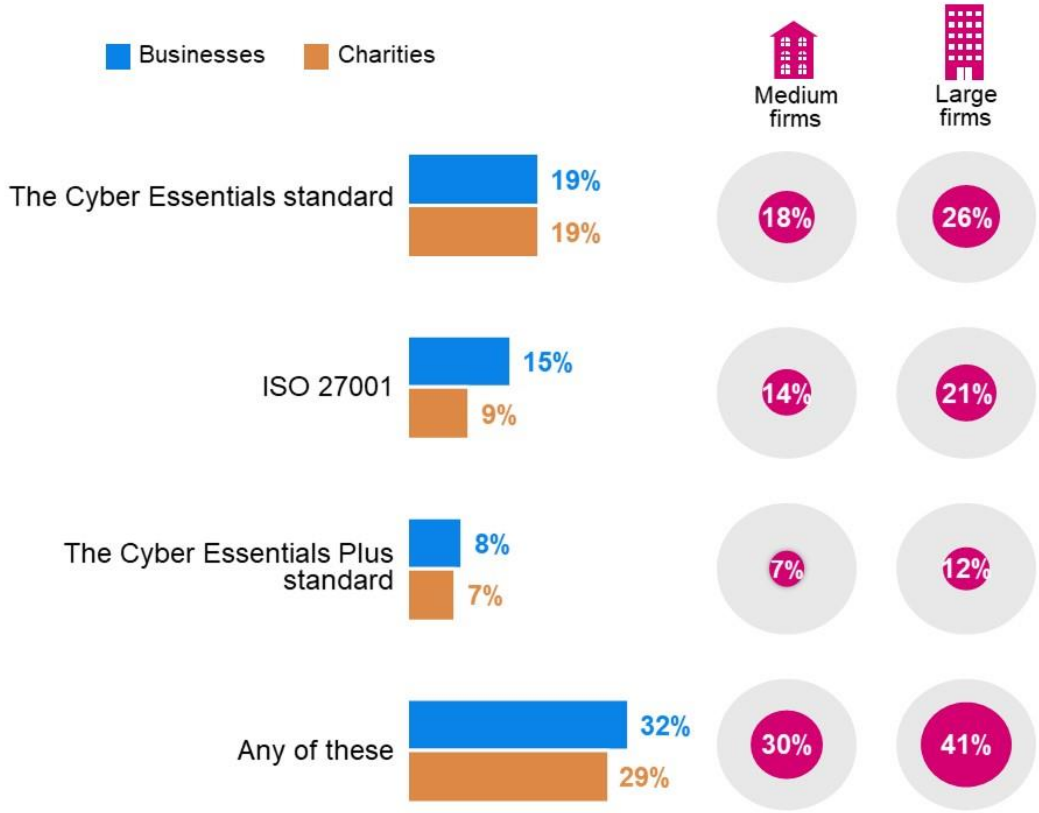
This section discusses the cyber security processes businesses and charities have in place, including any standards and certifications held, as well as the monitoring and evaluation of their policies where relevant and any improvements made over the last twelve months.

6.1 Standards and certifications

Around three in ten businesses (32%) and charities (29%) report having one or more of the three cyber security certifications asked about. The most common certification adhered to by businesses and charities (19% of both) is Cyber Essentials[10], followed by ISO 27001[11], which is more common among businesses (15%) than charities (9%). Cyber Essentials Plus[12] is less common, at eight per cent among businesses and seven per cent among charities. Around two-fifths (41% of businesses and 46% of charities) have none of the three certifications asked about, and a further quarter (26% of businesses and 25% of charities) say they do not know.

Figure 6.1: Standards or certifications adhered to by organisations

Which of the following standards or accreditations, if any, does your organisation adhere to?



Base: All businesses (n=1,205); All charities (n=536). Don't know not shown.

[10] Developed and operated by the National Cyber Security Centre (NCSC), Cyber Essentials is a foundation level certification designed to provide a statement of the basic controls an organisation should have in place to mitigate the risk from common cyber threats.

[11] An international standard on how to manage information security. An Information Security Management System (ISMS) is a set of policies, procedures, and roles designed to ensure cyber security risks are identified and managed.

[12] The protections that need to be put in place are the same as for Cyber Essentials, but for Cyber Essentials Plus a hands-on technical verification is carried out.

Large businesses and businesses with boards that discuss cyber security at least monthly are more likely than businesses on average to have each of the three certifications.

There are some clear differences by sector:

- Businesses in the information and communications sector are more likely than businesses on average to have each of the three certifications. Almost half (47%) have ISO 27001, 42% are certified with Cyber Essentials and 27% have Cyber Essentials Plus.
- Finance and insurance sector businesses are more likely than businesses on average to hold Cyber Essentials (32%) and Cyber Essentials Plus (17%) certification, as are those in the professional, scientific and technical sector (31% and 15% respectively).
- Administration and real estate sector businesses are more likely than businesses on average to have ISO 27001 (21%).
- Businesses in the following sectors are more likely than average to have none of these three certifications, or not to know if they do: food and hospitality; health, social care and social work; retail and wholesale; and utilities and production.

Businesses that experienced a cyber incident in the last twelve months are more likely to have Cyber Essentials (22% vs. 15% of those that have not experienced an incident) and Cyber Essentials Plus (9% vs. 6%).

The qualitative research identified three different triggers for becoming certified. The reason mentioned most often by participants is that certifications are increasingly becoming a contractual requirement for working with public sector bodies and large companies.

"It became obvious that if we wanted to continue working with these people, we should get ISO 27001 accreditation. [Cyber Essentials] doesn't offer any more than what we get from ISO 27001, but certain things say you have to have Cyber Essentials, so we have that as well."

Business, Large, Administration and real estate

The other two drivers were a change in senior personnel, such as a new Chief Financial Officer (CFO) and having a new IT supplier. This could lead to organisations reviewing their whole approach to cyber security and deciding to become certified. Some of these participants felt that the process of obtaining a certification enabled their organisation to examine and improve their cyber security.

"It opened our eyes a bit. It allowed us to explore our security across many different assets. We had some of this in place, but it probably wasn't where it should have been. Getting that Cyber Essentials Plus in place allowed us to have that investment and spend it wisely on some of the areas that we felt there were gaps. It was difficult, but we passed it."

Business, Large, Professional, scientific and technical

6.2 Processes currently in place

The overwhelming majority of organisations say that they have various rules and controls already in place, with more than nine in ten organisations reporting that they have the following technical controls required to attain Cyber Essentials in place:

- 96% of both businesses and charities say they restrict IT admin and access rights to specific users
- 95% of businesses and 96% of charities have up-to-date malware protection across all their devices
- 94% of businesses and 92% of charities have firewalls that cover their entire IT network, as well as individual devices

- 92% of businesses and 94% of charities have security controls on their organisation's own devices.

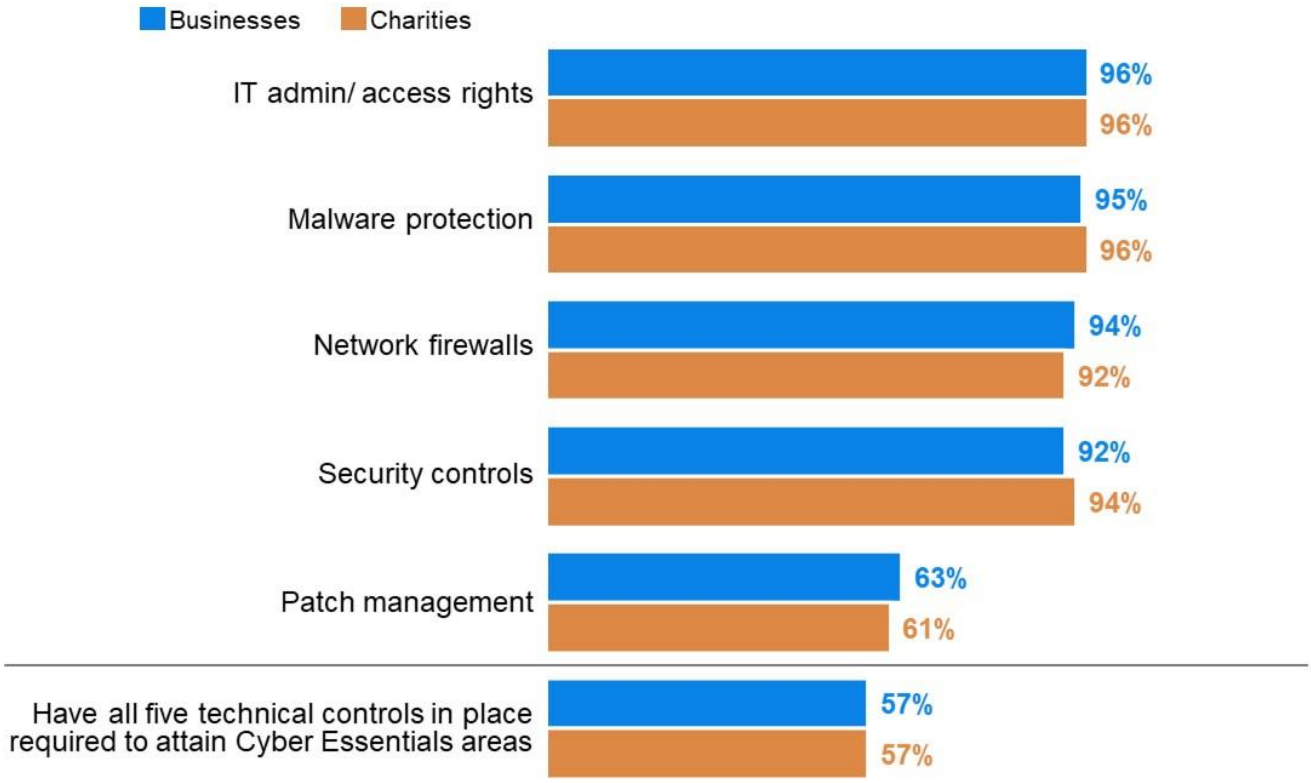
More than six in ten organisations (63% of businesses and 61% of charities) report having a policy to apply software security updates within 14 days.

Overall, more than half of businesses and charities (57% of each) have technical controls in place in all five of the areas required to attain Cyber Essentials. In addition, nearly two in three organisations (66% of businesses and 64% of charities) say they monitor user activity, while the vast majority of businesses (85%) and charities (87%) have specific rules for storing and moving files containing people's personal data.

Businesses are more likely than charities to back up data securely via a non-cloud service (70% vs. 64%), though usage of cloud services for secure data backup is similar (74% of businesses and 77% of charities). Large businesses (250+ staff) are more likely than medium businesses to have specific rules for storing and moving files containing people's personal data (89% vs. 84%).

Figure 6.2: Technical controls in place in the areas required to attain Cyber Essentials

And which of the following rules or controls, if any, do you have in place?



Base: All businesses (n=1,205); All charities (n=536). Don't know not shown.

Large businesses and medium businesses are similarly likely to have technical controls in place in each of five of the areas required to attain Cyber Essentials, except for restricting IT admin/access rights, which is more prevalent among large businesses (99% vs. 95% of medium businesses). There is also little difference between businesses and charities on these measures.

Businesses in certain industry sectors are more likely than average to have technical controls in place in all five of the areas required to attain Cyber Essentials: financial and insurance (76%), information and communications (71%), and professional, scientific or technical (also 71%). Businesses that have experienced a cyber security incident in the last twelve months, and those

experiencing an impact from such an incident, are also more likely to have technical controls in place in all five of the areas required to attain Cyber Essentials (62% of both groups, compared to 57% of all businesses). This pattern also emerged in the qualitative interviews where businesses that relied more heavily on digital technologies were more likely to have invested in the technical controls required to attain Cyber Essentials. For example, one transport business whose core business is less reliant on digital technology and had started as a farming business explained:

"You've still got that same person who is a farmer and doesn't like the look of any technology or computer. We're still trying to catch up on technological systems in filing and sharing information. Trying to change the culture of the business is difficult because of the people who are leading it, who are still in that old-school mind."

Business, Medium, Transport and storage

In addition, businesses whose board are informed more frequently on cyber security are more likely to have technical controls in place in all five of the areas required to attain Cyber Essentials (68% whose board receives at least monthly updates and 65% whose board receive at least quarterly updates, compared to 36% of those whose board never receive updates). This difference is also observed among charities, with 85% of charities whose board receives at least monthly cyber security updates having technical controls in place in all five of the areas required to attain Cyber Essentials, compared with just 34% of charities whose board never receive any cyber security updates.

Businesses that experienced a cyber incident in the last twelve months are also more likely to have technical controls in place in all five of the areas required to attain Cyber Essentials (62% vs. 50% of businesses not reporting an incident). This was supported by the qualitative interviews, where businesses explained that investment in cyber security is often triggered by an incident:

"It is not the priority. You rely on these things, and you don't take a second thought on it until it goes wrong. That is an issue for us as a business. It is not a priority that is discussed enough, only when something really goes wrong".

Business, Medium, Transport and storage

The qualitative interviews provided insight into how much of a driver acquiring cyber security certifications can be for establishing more robust security practices and embedding them across their organisations.

"The requirement to be Cyber Essentials Plus certified started a programme of work. It opened our eyes a bit. It allowed us to explore our security systems from across many different aspects: patching of systems, making sure our mobile devices are of a particular standard and making sure we are aware of all vulnerabilities across our servers, desktops and laptops. And also training… getting that Cyber Essentials Plus in place allowed us to have that investment and spend it wisely on some of the areas that we felt there were gaps."

Business, Large, Professional, scientific and technical

The qualitative interviews also provided insight into the motivation for acquiring certifications. Several businesses explained that it was a necessity to be able to bid for contracts with large public sector clients. Without this requirement, some businesses would not have invested to the same extent in cyber security because of the level of investment needed and concerns over whether the investment would be proportionate to the financial gains. Businesses pursuing Cyber Essentials certification to meet client procurement standards were positive about this requirement.

"We are driven quite heavily by [Regulator], which does actually make us better. They drive us down the cyber security route, it means you don't forget to do things. It is quite useful to have a demanding client like that".

Business, Medium, Construction

6.3 Monitoring and evaluation

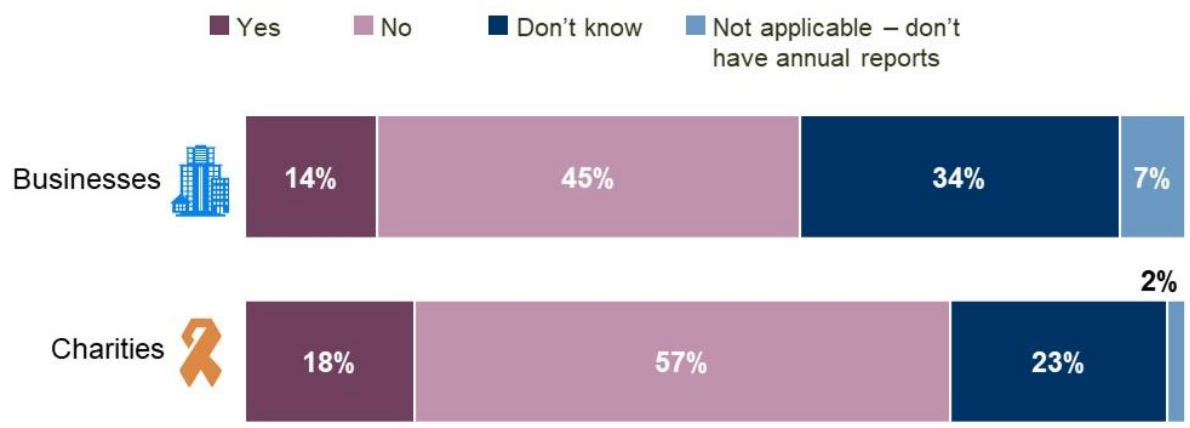
Annual reports

Overall, charities are more likely than businesses to state that cyber security was included in their organisation's most recent annual report (18% vs. 14%). Large businesses with 250+ employees are more likely than medium businesses to have included cyber security in their annual report (18% compared to 13%).

Around half of organisations say cyber security was not included in their organisation's most recent annual report, with this applying to more charities than businesses (57% vs. 45%). However, businesses are more likely than charities not to know whether their annual report mentions anything about cyber security (34% vs. 23%). This was supported by the qualitative interviews, where uncertainty was observed about the detail of what is and is not covered in annual reports.

Figure 6.3: Reporting on Cyber Security

Did you include anything about cyber security in your organisation's most recent annual report?



Base: All businesses (n=1,205); All charities (n=536).

There is a link between how engaged senior leadership is with cyber security issues and whether annual reports include anything about cyber security. Organisations with a board that receive regular information or updates about cyber security are more likely to include cyber security in their most recent annual report, with 25% of businesses and 36% of charities whose board receives updates on cyber security at least monthly reporting that cyber security was included in their last annual report.

Businesses in the information and communication sector (24%), construction (also 24%), and finance and insurance sector (23%) are the most likely to have included anything about cyber security in their annual reports.

During the qualitative interviews, several businesses indicated that their annual reports are typically aimed at shareholders, with a high-level view of performance measures and profitability. An in-depth look at key risks, such as cyber security, often does not fall into the scope of these reports. Charities discussed how their annual reports tend to focus on their main projects throughout the year and their main achievements, and therefore things like cyber security are not included because it would not fit the tone of the report.

“We tend to use our annual report more as a celebration of the kind of support we’ve offered to the community, so it doesn’t fit particularly well with the tone of what we do.”

Charity

The qualitative interviews also provided more insight into the type of detail that is covered in annual reports among the minority of organisations who do include coverage of cyber security. A number of organisations, both charities and businesses, suggested that cyber security might be covered in their annual report but under a larger section on digital infrastructure or as part of the risk register.

Identification of cyber security risks

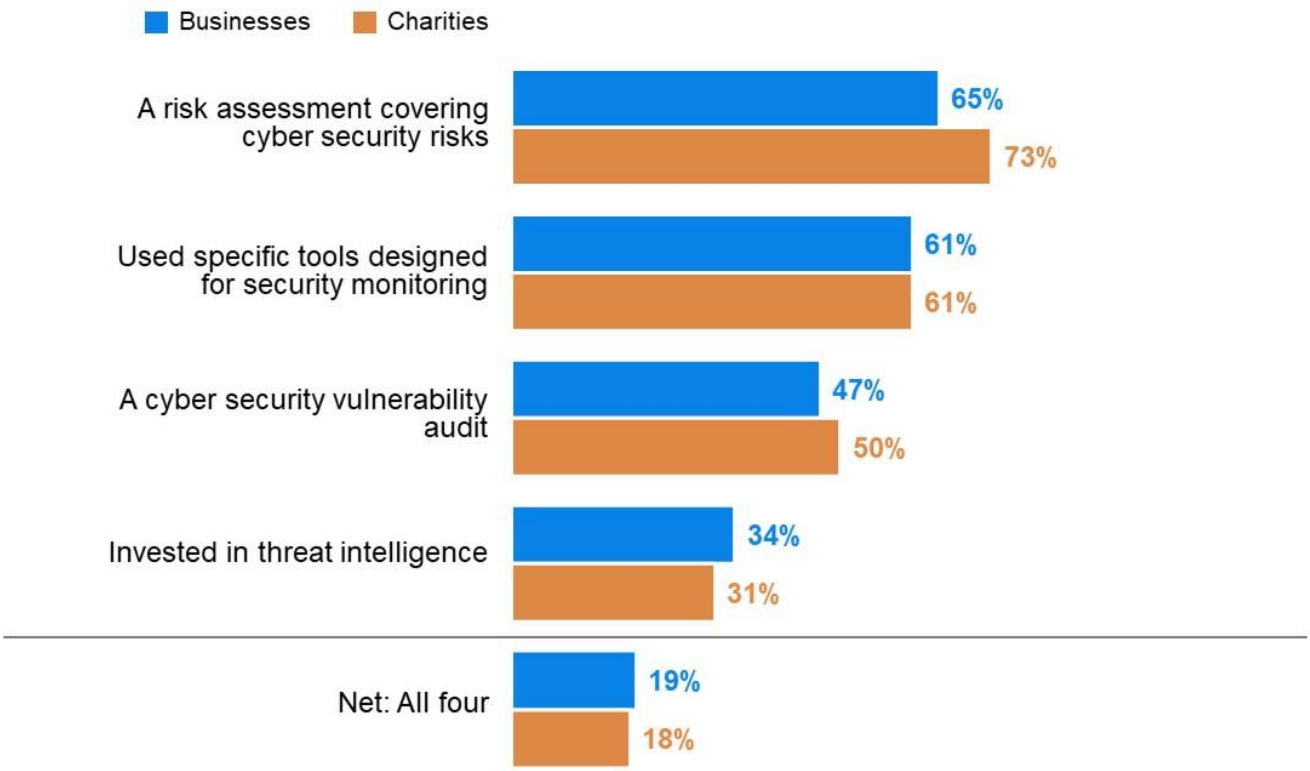
Having procedures in place to monitor and identify cyber security risks is crucial to make sure the correct systems are in place to deal with these risks. The vast majority of businesses and charities have taken at least one action in the last twelve months to identify such risks.

Conducting a risk assessment covering cyber security risks is the most commonly reported action, with charities more likely than businesses to have done this (73% vs. 65%). This is followed by having used specific tools designed for security monitoring (61% both of businesses and charities). Around half have completed a cyber security vulnerability audit (47% of businesses and 50% of charities), while around three in ten (34% of businesses and 31% of charities) have invested in threat intelligence.

Overall, businesses are more likely than charities to report not taking any of the four actions covered in Figure 6.3 (18% vs. 13%).

Figure 6.4: Procedures to identify cyber security risks in last twelve months

Which of the following, if any, have you done in the last twelve months to identify cyber security risks to your organisation?



Base: All businesses (n=1,205); All charities (n=536). Don't know not shown.

Large businesses with 250+ employees are more likely than medium-sized businesses to have conducted each of the procedures asked about. For example, large businesses (250+ staff) are much more likely to have invested in threat intelligence (46% vs. 31%) and used specific tools designed for security monitoring (74% vs. 58%).

Again, these findings indicate the importance of senior-level engagement with cyber security issues. Almost all businesses whose board discusses or receives updates on cyber security at least monthly report that they have taken at least one of the specified actions in the last twelve months (96% vs. 56% whose board never discuss/receive updates). They are particularly likely to have carried out a risk assessment covering cyber security risks, used specific tools designed for security monitoring, or conducted a cyber security vulnerability audit (83%, 76%, and 70% respectively). Similarly, businesses with board oversight or a designated staff member with responsibility for cyber security are likely to have taken procedures to identify risks (91% and 92% respectively, versus 82% of all businesses). The pattern is similar for charities.

Businesses working in the finance and insurance sector and the information or communications sector are the most likely to have undertaken these actions to identify cyber security risks.

At the beginning of each qualitative interview, organisations were asked about the top risks they feel are facing their organisation. The main concerns mentioned were inadequate user skills among staff, constantly evolving threats met by limited budgets and the challenge of maintaining protections and improving existing defences.

Awareness of cyber security risks among staff was one of the most frequently mentioned risks to the organisation, particularly in the context of being vulnerable to phishing emails and ransomware attacks or working from unsecured personal devices.

"Our biggest risks are our people. We've done great things in terms of training to make our staff aware of the risks out there, like phishing. The training helps them at work, but in their home life as well. We are all human; we sometimes make mistakes and click on the wrong thing. It's not only combatting the human error but also having those technical solutions just in case someone does fall foul of a phishing link."

Business, Large, Professional, scientific and technical

The constantly evolving nature of digital technology and therefore the emergence of new types of cyber security threats was also mentioned. Particularly among businesses and charities with limited IT budgets, maintaining protections or even just being aware of new threats was raised as a significant concern. Additionally, securing buy-in from key decision-makers was frequently mentioned when it comes to upgrading systems. One respondent particularly mentioned the issue of IT, and cyber security more specifically, not being recognised as a strategic priority among senior leadership.

"One of the problems I have is that I don't have great visibility and one of my priorities is to get visibility over what our risks actually are."

Charity

6.4 Improvements made over the last twelve months

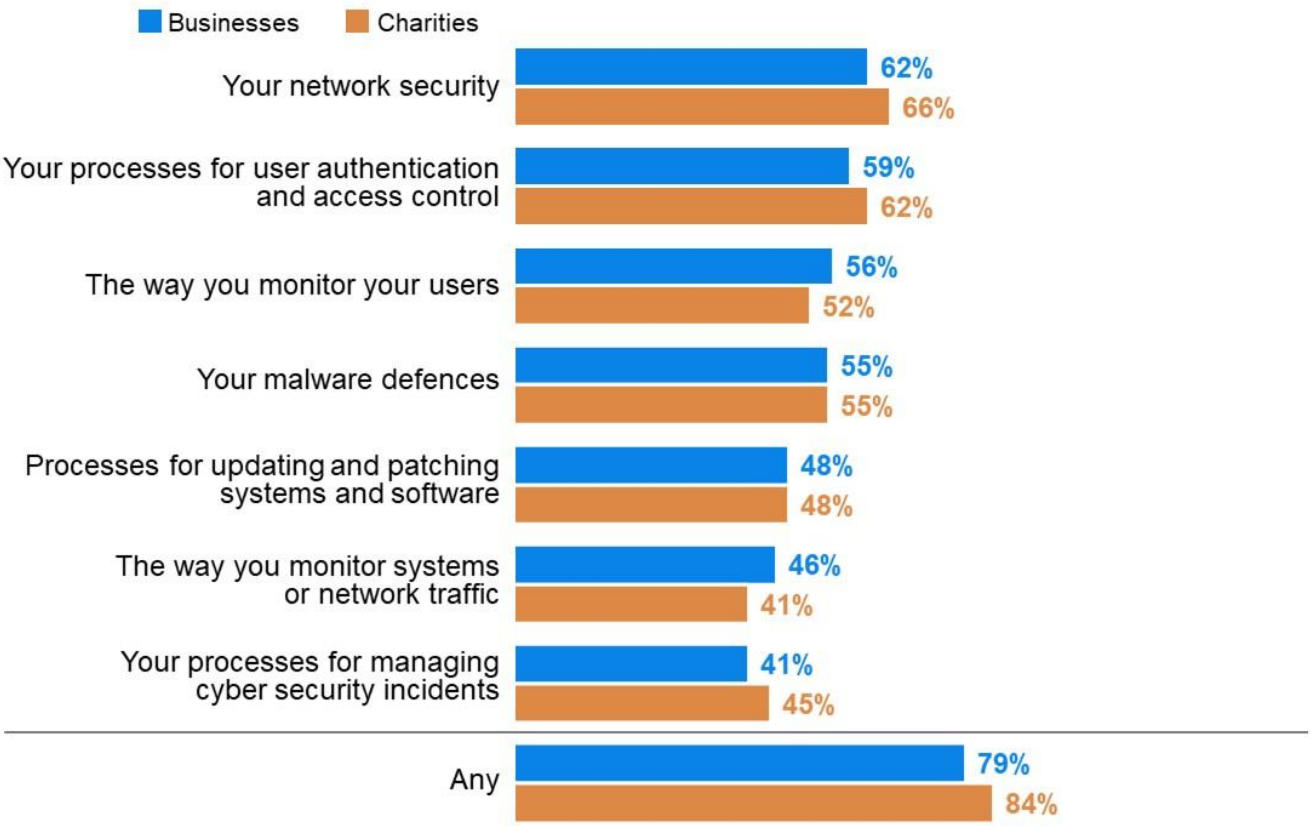
The survey covers a range of actions that organisations can take to expand or improve cyber security. Overall, findings show a strong desire across both businesses and charities to improve their cyber defences, with around four in five taking steps to expand or improve aspects of their cyber security in the last twelve months (79% of businesses and 84% of charities).

More than half of organisations report improving their network security (62% of businesses and 66% of charities), processes for user authentication and access control (59% of businesses and 62% of charities), and malware defences (55% of each). They are least likely to have improved or expanded the way they monitor their users (37% of businesses and 34% of charities).

Businesses are more likely than charities to have expanded or improved the way they monitor their systems or network traffic in the last year (46% vs. 41%).

Figure 6.5: Steps to expand or improve cyber security in last twelve months

In the last twelve months, has your organisation taken any steps to expand or improve any of the following aspects of your cyber security?



Base: All businesses (n=1,205); All charities (n=536). Don't know/ not applicable not shown.

Large businesses (250+ staff) are consistently more likely to have made improvements over the last twelve months. They are particularly likely to have improved their network security (72% vs. 60% of medium businesses). The qualitative interviews suggested that larger businesses have more resources to be able to invest in their cyber security and keep up to date with an ever-changing cyber security landscape.

"We could always do more, the question is how much money do we have to spend on anything different that's proportionate to the risk…We spend decent money on things like penetration testing, upgrading firewalls and that sort of stuff. I'm not sure we could do much more that's proportionate to our size."

Charity

Similarly, the qualitative interviews highlighted that charities and medium-sized businesses may not have the manpower to have a dedicated IT team, are even less likely to have someone with exclusive responsibility for cyber security and, as such, putting in place procedures to improve cyber security can be a challenge.

"This is not my background. I am on a massive steep learning curve. It is such a complicated area, there is so much out there and so many products. It is a minefield really. It is a massive area that is not simple and not clear, and the expertise is not out there to manage it in most small organisations. You can employ a digital manager and a cyber security manager and a data protection manager, but in [name of organisation] that's all me."

Charity

The survey findings also suggest that the experience of a cyber security incident may also drive action, with 90% of businesses and charities that experienced an incident (other than phishing) in the last twelve months reporting improvements to their cyber security, compared to 67% of businesses and 78% of charities that have not experienced a cyber security incident in this time.

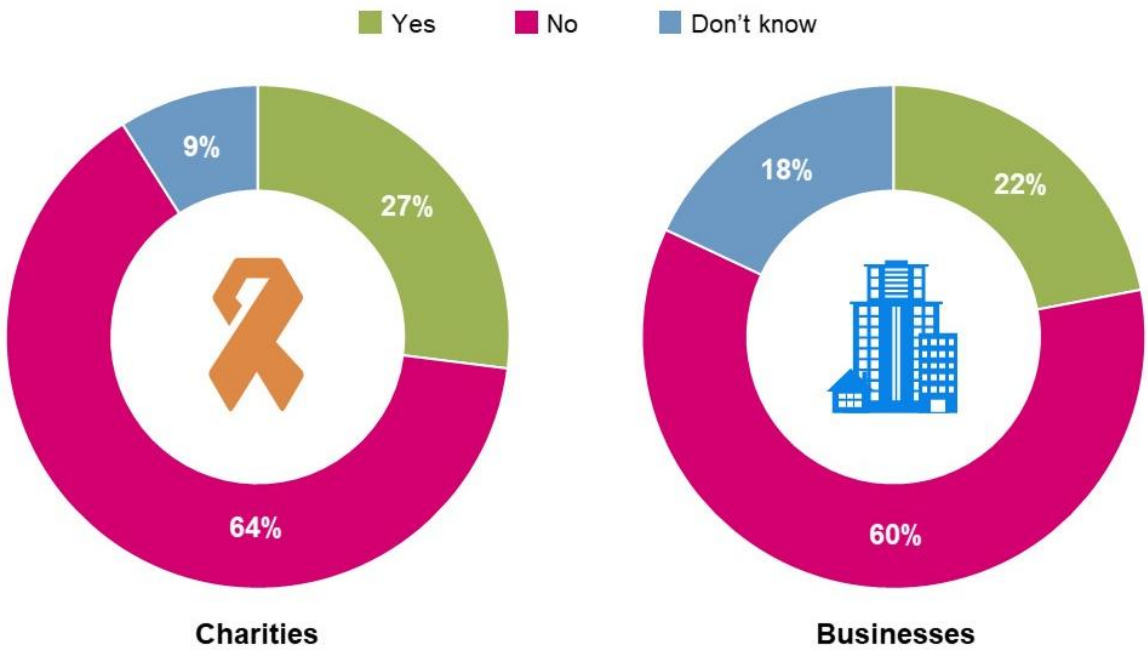
Certification also appears linked to the likelihood of taking measures to improve cyber security, likely as these measures are essential to maintain the level of certification. For example, organisations with ISO 27001, the Cyber Essentials standard or the Cyber Essential Plus standard are all more likely than organisations without these certifications to have taken the steps identified above.

6.5 Supplier risks

Charities are more likely than businesses to have carried out work to formally assess or manage the potential cyber security risks presented by their suppliers or partners in the last twelve months (27% vs. 22%). However, a far greater proportion of organisations have not taken any action to manage cyber security risks presented by their suppliers (60% of businesses and 64% of charities). Businesses are more likely than charities to say they are not sure whether this work has been carried out (18% vs. 9%).

Figure 6.6: Work to assess or manage the risks presented by suppliers

In the last twelve months, has your organisation carried out any work to formally assess or manage the potential cyber security risks presented by any of these suppliers/suppliers or partners?



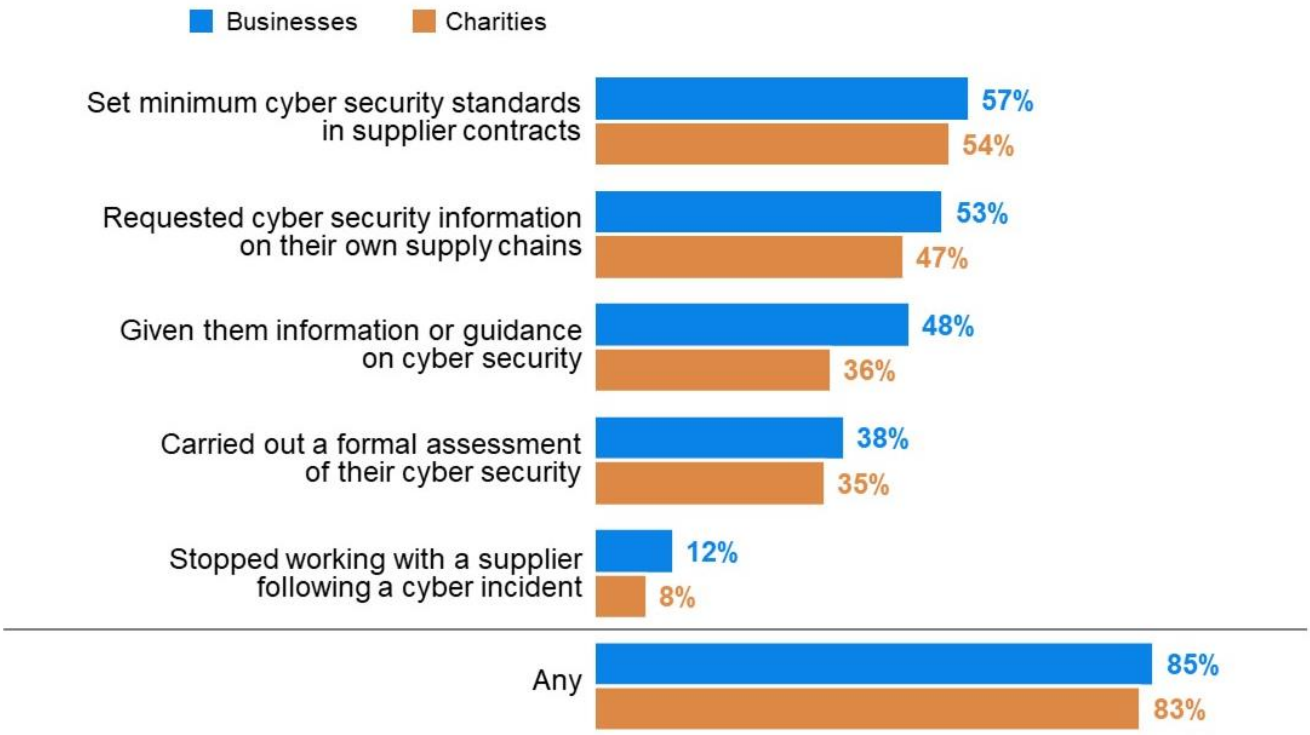
Base: All businesses (n=1,205); All charities (n=536).

Large businesses with 250+ employees are more likely to have carried out a supplier risk assessment than medium firms (33% vs. 20%). In addition, businesses with cyber security certification, those with board oversight and involvement, and those working in the information and communications and finance and insurance sectors are all also more likely than average to have carried out work to assess or manage supplier risk.

Organisations that had carried out supplier risk assessment were then asked about the work they have done with their suppliers during the last twelve months. Businesses and charities are both most likely to have set minimum cyber security standards in their supplier contracts (57% of businesses and 54% of charities), followed by requesting cyber security information on their supply chains (53% of businesses and 47% of charities). Businesses are more likely than charities to have given their suppliers information or guidance on cyber security (48% vs. 36%). Just over one in three (38% of businesses and 35% of charities) carried out a formal assessment of suppliers' cyber security, and one in ten (12% of businesses and 8% of charities) stopped working with a supplier due to a cyber incident.

Figure 6.7: Work done in last twelve months with suppliers to manage cyber security risk

Which of the following, if any, have you done with any of your suppliers/suppliers or partners in the last twelve months?



Base: All businesses (n=1,205); All charities (n=536). Don't know not shown.

Large businesses (250+ staff) are more likely to have set minimum cyber security standards in supplier contracts than medium businesses (70% vs. 52%).

As with other cyber security policies, organisations with any cyber security certifications and board involvement or oversight into cyber security are more likely to have taken steps to manage their supplier risks than organisations with no certifications, board involvement or oversight. This resonates with the qualitative research, where businesses without any cyber security certifications tended to be less likely to have vetted their suppliers on their cyber security protocols and procedures.

"We don't have [cyber security] on the list and one of the reasons for that is that I don't have any accreditations so for me to go back to my supply chain and ask for Cyber Essentials is a bit…!"

Business, Medium, Construction

Chapter 7 – Cyber incident management

This section explores the prevalence of written incident management processes at organisations, and what these may cover.

7.1 Processes

Around half of businesses and charities (51% of each) have written processes in place, such as an incident response plan, for managing cyber security incidents. Around two in five organisations (38% of businesses and 41% of charities) do not, and around one in ten (11% of businesses and 8% of charities) are unsure.

Written processes are more prevalent among large businesses (250+ staff) (60%), and businesses in the finance and insurance (75%), information and communications (72%) and professional, scientific and technical (62%) sectors.

Businesses with cyber security certifications are more likely to have written processes in place. This is particularly the case for those certified under Cyber Essentials Plus (85%), where the likelihood is higher compared to businesses with ISO 27001 (75%) and Cyber Essentials (74%) certification. Businesses where boards receive cyber security updates at least monthly are also more likely to have written processes (73%).

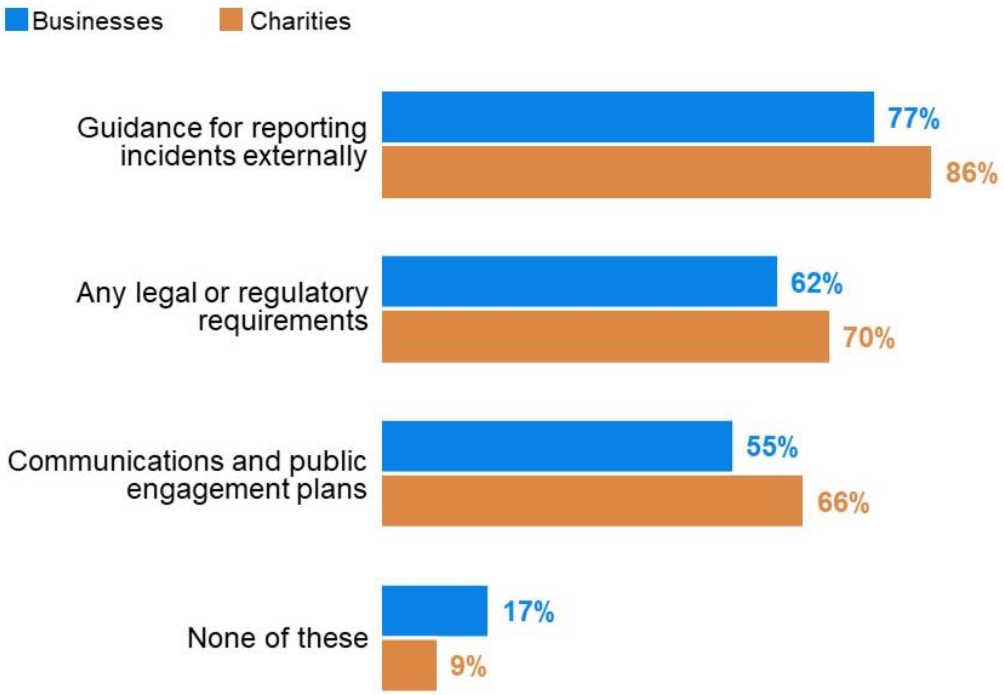
It is a similar position among charities. More than eight in ten charities (82%) with Cyber Essentials Plus certification have written processes in place, where the likelihood is higher compared to 66% of charities with ISO 27001 and 64% of charities with Cyber Essentials certification. Two-thirds (67%) of charities where boards receive cyber security updates at least monthly have written processes in place.

There is a link between experiencing a cyber security incident in the last twelve months and having written processes, with 54% of businesses and 55% of charities having plans in place (and 58% both of businesses and charities reporting a non-phishing incident), compared to 44% of businesses and charities that did not experience an incident.

Among those organisations with written incident management processes, these are most likely to cover guidance for reporting incidents externally, for instance to regulators or insurers (77% of businesses and 86% of charities). Around two-thirds (62% of businesses and 70% of charities) say their incident management processes cover legal or regulatory requirements, while communications and public engagement plans are covered by 55% of businesses and 66% of charities with processes in place.

Figure 7.1: Incident management processes that organisations have

Which of these, if any, is covered in your written incident management processes?



Base: All who have incident management processes: Businesses (n=643); Charities (n=272). Don't know not shown.

Coverage of legal or regulatory requirements is more likely among businesses in the finance and insurance sector (86%), and in businesses where boards receive at least monthly cyber security updates (75%), compared to businesses in general (62%).

Having legal or regulatory requirements as part of written incident management processes is also more common in organisations with cyber security certifications. For example, 79% of businesses that adhere to ISO 27001 include legal or regulatory requirements in their written incident management processes, compared to 57% of businesses without any certifications.

Businesses with any cyber security certification are also more likely to include communications plans in their written incident management processes. For instance, seven in ten businesses certified with the ISO 27001 (70%) or Cyber Essentials Plus (68%) standards include communications and public engagement plans, compared to 54% of businesses that do not have any certifications.

Cyber Essentials certified businesses are also more likely to cover guidance for reporting incidents externally than businesses on average (87% vs. 77% respectively). Businesses that experienced a cyber security incident in the last twelve months which impacted them are more likely to include all three types of guidance in their written processes.

Businesses (37%) are more likely than charities (28%) to have tested their written incident processes in the last twelve months, but for both types of organisations, testing has only been completed by a minority. However, among very large businesses, and businesses in the information and communications sector, a majority have done so (54% and 56% respectively).

There is a clear relationship between cyber security certification status and testing plans, although businesses with Cyber Essentials certification are less likely to have done so compared to those with ISO 27001 and Cyber Essentials Plus certification (44% vs. 55% and 60% respectively).

Testing is also more likely among businesses where the board discusses cyber security at least monthly (47%) and businesses that have experienced any cyber security incident in the past twelve months compared to those that have not experienced any incidents (41% vs. 30%).

The qualitative research found that many organisations are satisfied with an informal approach to responding to cyber incidents, and do not see the value of having a formal incident response plan. Typical comments from participants were that things worked very informally in their organisation, or that what needed to happen in the event of an incident was common sense. Some organisations without an incident plan simply relied on their IT consultants instead.

"The incident response plan would be one line – call the IT business support!"

Business, Medium, Transport and storage

Among organisations that do have a plan, it was clear from the qualitative research that the level of detail in these plans could vary widely. Some plans simply set out who incidents should be reported to, who should deal with them and who needs to be informed. Others were much more comprehensive, covering roles and responsibilities, communications and record keeping. A few organisations used more general incident response plans for IT or broader risk management.

"Because I am a one-man band, it all rests with me so, I keep it pretty simple. I am certainly not going to put in a whole incident response solution when it is only me on the other end of it. We have an incident response policy which is, by its nature, loose because there is such a huge array of incidents you can have, and invariably you would have the same people involved."

Business, Medium, Information and communications

The qualitative interviews reflect the absence of an accepted standard for record keeping. Some organisations keep detailed records of incidents or potential incidents, while others only record major incidents or rely on their IT consultants to keep records. Records are typically used to identify follow up actions and lessons learned or to review their risk strategy. The organisations that share information with insurers tend to only do so when reporting incidents, rather than routinely providing incident records.

Chapter 8 – Prevalence and impact of cyber incidents

This section explores the type and frequency of cyber incidents that organisations have experienced over the last twelve months. It also discusses the impact that these incidents have on organisations.

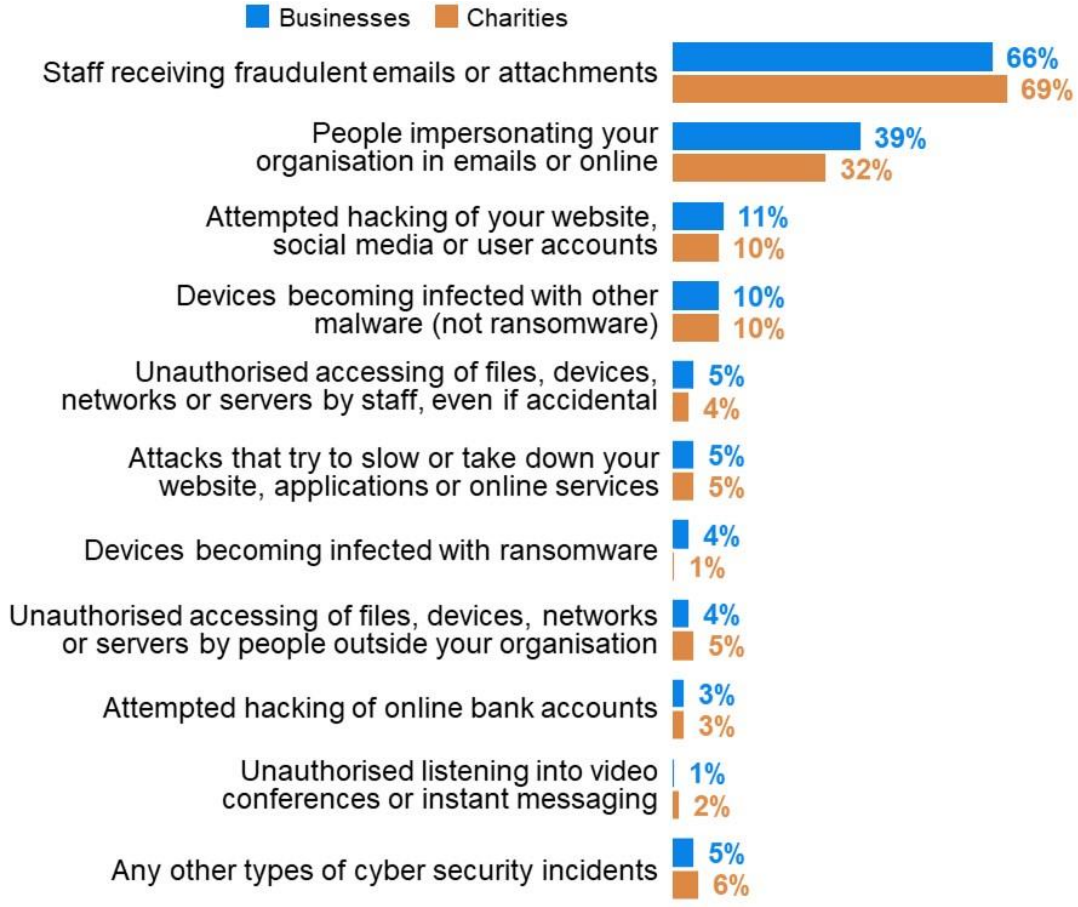
8.1 Experience of cyber incidents

The prevalence of cyber incidents ranges considerably, from just one per cent of businesses and two per cent of charities reporting unauthorised listening into video conferences or instant messaging to two-thirds (66% of businesses and 69% of charities) that say that staff received fraudulent emails or attachments in the last twelve months. Overall, more than seven in ten organisations (72% of businesses and 74% of charities) experienced at least one cyber security incident in the last twelve months, and around half (50% of businesses and 47% of charities) experienced an incident other than phishing.

Cyber incidents are more common among large businesses with 250+ employees. For example, almost half (48%) of these businesses report someone impersonating their organisation in emails or online, compared to 37% of medium businesses with between 50 and 249 employees.

Chapter 8.1: Types of cyber incident experienced in the last twelve months

Have any of the following happened to your organisation in the last twelve months? (% yes)



Base: All businesses (n=1,205); All charities (n=536). Don't know not shown.

Organisations with cyber security certification may be more aware of incidents, as a higher proportion of those with certifications report having experienced an incident over the last twelve months. For example, four in five businesses (79%) with the Cyber Essentials Plus standard

experienced a phishing incident in the last year compared to 66% of all businesses. Similarly, more than half (53%) of businesses with Cyber Essentials Plus say that people impersonated their organisation in emails or online compared to 39% of all businesses.

Related to this, organisations where the board is more involved in dealing with cyber security are also more likely be aware of an incident in the last twelve months. For instance, 14% of businesses whose board receives updates on cyber security at least every month report instances of devices becoming infected with malware compared to 4% of businesses whose board never receive updates on cyber security. This may indicate that organisations that are more engaged in cyber security are more likely to detect incidents, or that actual experience of incidents may drive this senior leadership involvement and investment in certifications.

Indeed, this resonates with some of the discussions in the qualitative interviews where organisations that had not experienced any serious cyber incidents explained that one of the main challenges in improving their cyber security processes and procedures was overcoming a lack of buy-in and interest from their board and senior management. They indicate that only a large incident with significant financial consequences would be reported to the board and possibly prompt their investment in stronger cyber security measures.

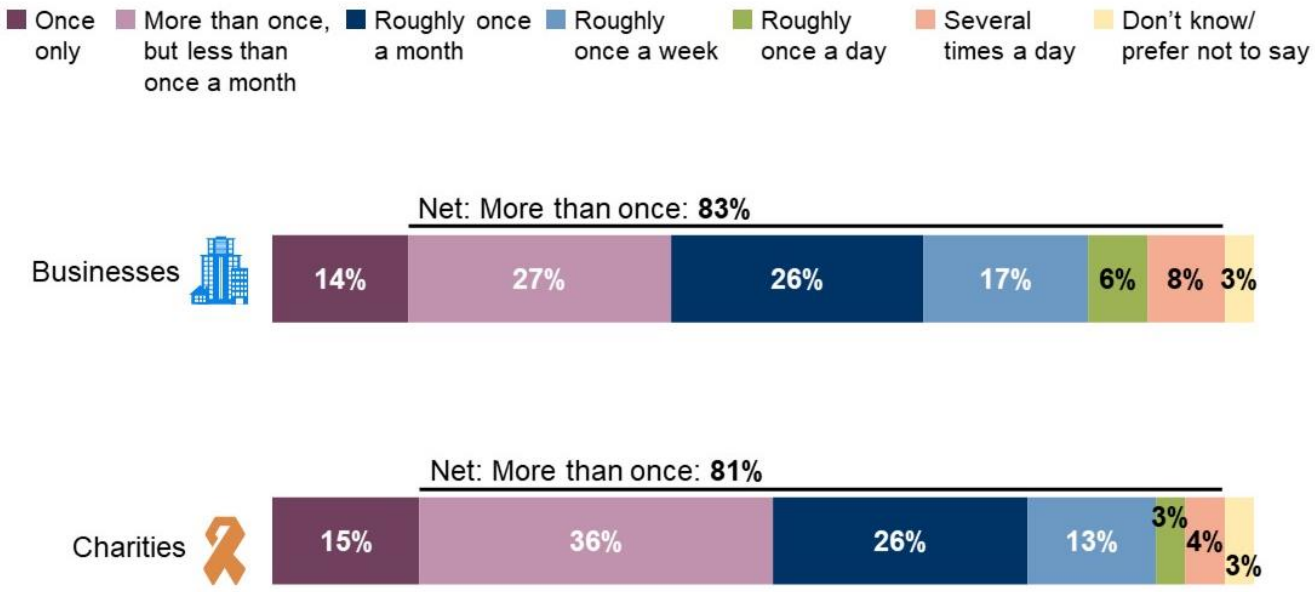
"Unless there is a really big issue that, you know, goes above and beyond £50,000 or something, then we wouldn't report that. If it is something like emails, we wouldn't report that".

Charity

The vast majority (83% of businesses and 81% of charities) that have experienced a cyber security incident in the last year say the incident(s) happened more than once, with just over half reporting that incidents occurred at least once a month (53%), and one-quarter (27%) reporting incidents at least once a week. Businesses are more likely than charities to have experienced more frequent incidents (30% compared to 20% once a week, and 56% compared to 46% once a month). Large businesses, however, are no more likely than medium businesses to experience frequent cyber incidents.

Figure 8.2: Frequency of cyber security incidents

Approximately, how often in the last twelve months did you experience any of the cyber security incidents you mentioned?



Base: All who have experienced any cyber security incidents in the last twelve months; Businesses (n=883); Charities (n=394).

Businesses that operate in the finance and insurance sector are more likely to cite at least weekly cyber incidents in the last year (53% vs. 30% of all businesses).

Even when phishing incidents are excluded, the vast majority of those organisations that experienced any incidents report them having taken place more than once in the last 12 months (79% of businesses and 83% of charities). When phishing is excluded, businesses are more likely than charities to experience cyber incidents. For example, 53% of businesses report that they experienced cyber security incidents other than phishing at least once a month compared to 43% of charities.

When phishing is excluded from instances of cyber incidents, businesses within the finance and insurance sector are no more likely than other sectors to report frequent incidents.

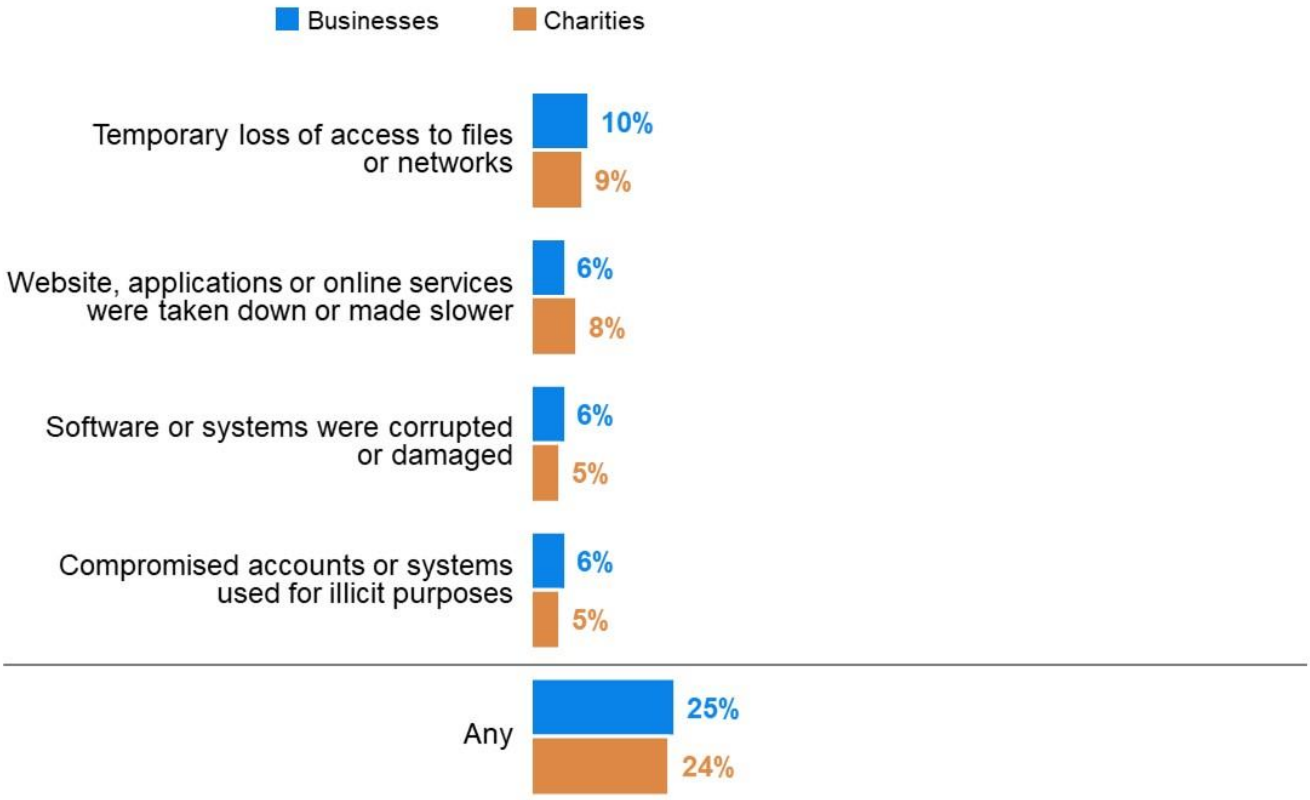
8.2 How are businesses affected?

Organisations that experienced any cyber security incidents over the last twelve months were asked about the outcomes of these incidents. Around a quarter of organisations (25% of businesses and 24% of charities) say they had experienced at least one negative outcome. The most common outcomes mentioned by at least 5% of organisations are:

- Temporary loss of access to files or network (10% of businesses and 9% of charities)
- Websites, applications or online services taken down or made slower (6% of businesses and 8% of charities)
- Software or systems corrupted or damaged (6% of businesses and 5% of charities)
- Compromised accounts or systems used for illicit purposes (6% of businesses and 5% of charities).

Figure 8.3: Outcome of cyber incident on organisation

Thinking of all the cyber security incidents experienced in the last twelve months, which, if any, of the following happened as a result?



Base: All who have experienced any cyber security incidents over the last twelve months; Businesses (n=883); Charities (n=394). Don't know not shown.

Large businesses with 250+ employees are more likely to be affected in certain ways than medium businesses. For example, they are more likely to have software or systems corrupted or damaged, and their accounts compromised, or systems used for illicit purposes (9% vs. 5% respectively for both outcomes).

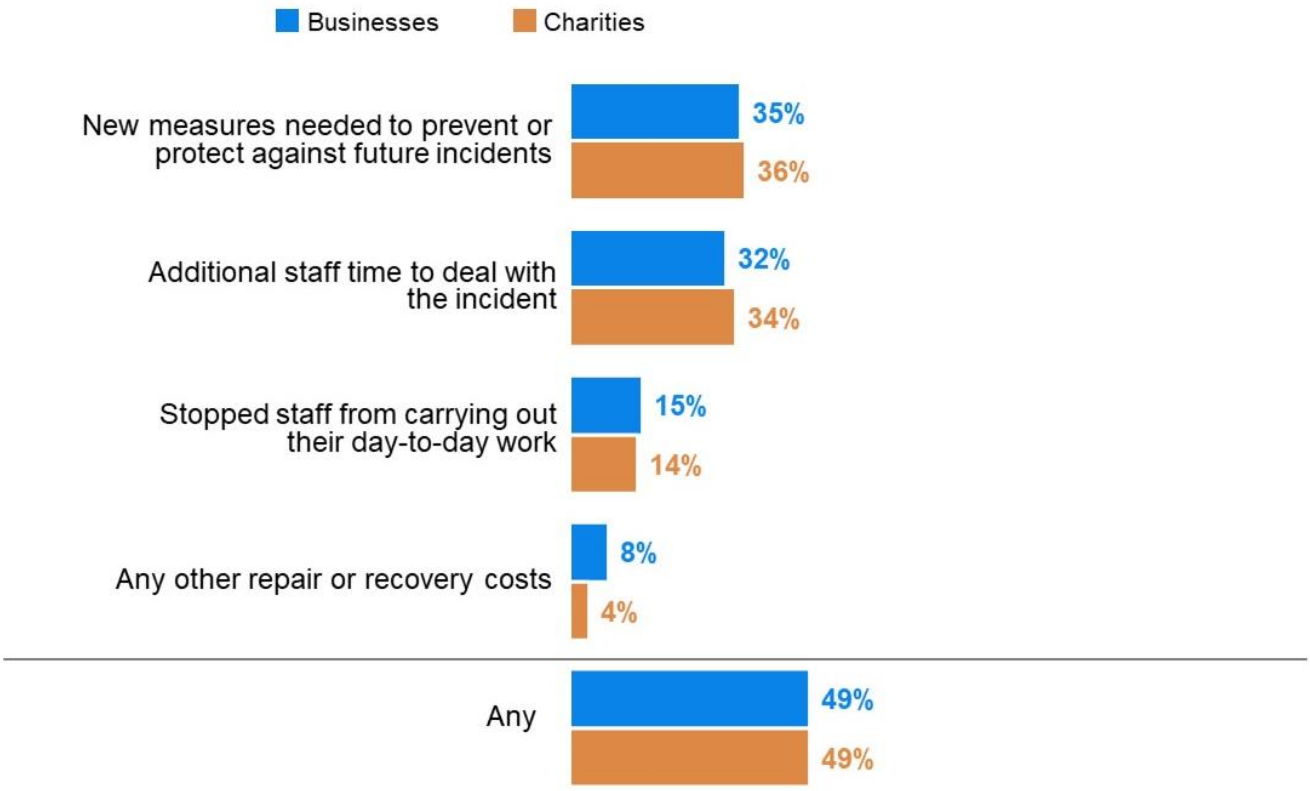
Even incidents that do not result in negative financial consequences or data loss can have an impact on organisations. Therefore, organisations that experienced a cyber incident in the last twelve months were also asked about the impact the incident(s) had on their organisation.

Figure 8.4 shows the most common impacts experienced as a result of a cyber incident cited by at least five per cent of organisations. It illustrates that around half (49% both of businesses and charities) were impacted in at least one of the ways listed. Just over one in three (35% of businesses and 36% of charities) say that new measures were needed to prevent or protect against future incidents, and a similar proportion (32% of businesses and 34% of charities) report needing additional staff time to deal with an incident or incidents.

Large businesses (250+ staff) are generally more likely than medium businesses to report that cyber incidents have an impact, and to indicate in particular that new measures are needed to prevent or protect against future incidents (43% compared to 33%).

Figure 8.4: Impact of incident on organisation

Have any of these incidents impacted your organisation in any of the following ways?



Base: All who have had any cyber security incidents over the last twelve months; Businesses (n=883); Charities (n=394). Don't know not shown.

8.3 Ransomware attack response policy

Four in ten organisations (41% of businesses and 40% of charities) report that they have a rule or policy not to pay ransomware payments in the case of ransomware attacks. However, a quarter (24% of businesses and 27% of charities) do not have a rule or policy on this, and the remaining third (35% of businesses and 32% of charities) are unsure of their organisation's ransomware policy.

Those who have more experience of cyber security incidents, who have invested in cyber security preventative measures, and who have a more informed senior leadership are more likely to have rules in place against ransomware payments. For example, businesses whose board receives updates on cyber security are more likely to have a policy against paying ransomware payments (52% of those whose board meets at least monthly). Almost half (45%) of businesses with all five cyber essentials in place have a rule against ransomware payments, and a similar proportion (49%) of businesses adhering to the Cyber Essentials standard have this approach to ransomware.

8.4 Time taken to restore business operations after cyber incident

The vast majority of incidents have a short-term impact on operations; nine in ten organisations (90% of businesses and 89% of charities) that experienced any incidents report that it took them less than a day to restore business operations back to normal. Around one in ten (8% of businesses and 10% of charities) say it took a day or longer, while three per cent of businesses and two per cent of charities say they were affected for a week or longer. Again, this resonates with the qualitative research where there were no mentions of recent cyber incidents that had had

a long-term impact on their business. Instead, participants placed a lot of emphasis on preventative measures to stop incidents in the first place and having procedures in place to minimise the impact of an incident so that it could be resolved quickly and have minimal disruption to the business.

There are very few differences in terms of business type, size, or preparedness to deal with cyber incidents. However, businesses operating in the food and hospitality sector are more likely to report that it took them a day or longer to restore operations (23% compared to 8% of businesses overall).

8.5 Financial cost of incidents

Following the approach taken by the Cyber Security Breaches Survey (CSBS), this survey has attempted to capture the cost of cyber security incidents faced in the last twelve months, and more granular questions breaking down different aspects of the cost of the single most disruptive incident that organisations recall facing in this period. Costs covered include short-term and long-term direct costs, staff time costs and other indirect costs.

Overall cost of incidents

Table 8.1 below shows the estimated costs organisations incurred from all the identified incidents over the last twelve months. When asked about cost, organisations are asked to bear in mind all the potential impacts.

Table 8.1: Average cost of all incidents identified in the last year[13]

	All businesses	Medium businesses	Large businesses	All charities
	Across organisations identifying any incidents			
Mean cost	£2920	£2160	£6500	£1878
Median cost	£0	£0	£34	£0
Base	770	538	232	365
	Only across organisations identifying incidents with an outcome			
Mean cost	£8410	£5530	£17010	£4420
Median cost	£1000	£600	£2280	£1425
Base	195	116	79	76

[13] The cost estimates in this section 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 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.

Costs associated with the most disruptive incidents

Tables 8.2 to 8.5 show cost estimates for the single most disruptive incident that organisations have identified in the last twelve months. Again, these are presented for all incidents, as well as those with an actual outcome, such as a loss of assets or data.

In the survey, we defined short-term direct costs as being any external payments that were made when dealing with the incident. This includes, as examples offered to respondents:

- any payments to external IT consultants or contractors to investigate or fix the problem
- any payments to the attackers, or money they stole.

Table 8.2: Average short-term direct cost of most disruptive incident in the last year

	All businesses	Medium businesses	Large businesses	All charities
	Across organisations identifying any incidents			
Mean cost	£1074	£1081	£1040	£302
Median cost	£0	£0	£0	£0
Base	811	560	251	374
	Only across organisations identifying incidents with an outcome			
Mean cost	£3245	£3320	£3025	£1124
Median cost	£0	£0	£2000	£0
Base	209	122	87	85

We defined long-term direct costs as external payments in the aftermath of the incident. The examples included in the survey were:

- any payments to external IT consultants or contractors to run cyber security audits, risk assessments or training
- the cost of new or upgraded software or systems
- recruitment costs if you had to hire someone new
- any legal fees, insurance excess, fines, compensation or PR costs related to the incident.

Table 8.3: Average long-term direct cost of most disruptive incident in the last year

	All businesses	Medium businesses	Large businesses	All charities
	Across organisations identifying any incidents			
Mean cost	£671	£570	£1140	£782
Median cost	£0	£0	£0	£0
Base	814	564	250	377
	Only across organisations identifying incidents with an outcome			
Mean cost	£1720	£1204	£3217	£720
Median cost	£0	£0	£0	£0
Base	211	124	87	85

We also asked about the costs of any staff time (i.e., indirect costs of the incident). This includes, for instance, how much staff would have got paid for the time they spent investigating or fixing problems caused by the incident. We explicitly asked respondents to include the cost of this time regardless of whether this duty was part of the staff member's job function or not.

Table 8.4: Average staff time cost of the most disruptive incident in the last year

	All businesses	Medium businesses	Large businesses	All charities
	Across organisations identifying any incidents			
Mean cost	£804	£722	£1190	£372
Median cost	£1	£1	£20	£4
Base	787	549	238	360
	Only across organisations identifying incidents with an outcome			
Mean cost	£2440	£2298	£2890	£755
Median cost	£190	£190	£200	£275
Base	201	122	79	80

Finally, we asked about other indirect costs related to incidents, including the following areas (offered as examples to respondents):

- the cost of any time when staff could not do their jobs
- the value of lost files or intellectual property
- the cost of any devices or equipment that needed replacing

Table 8.5: Average indirect cost of the most disruptive incident in the last year

	All businesses	Medium businesses	Large businesses	All charities
	Across organisations identifying any incidents			
Mean cost	£828	£591	£1940	£113
Median cost	£0	£0	£0	£0
Base	800	557	243	375
	Only across organisations identifying incidents with an outcome			
Mean cost	£3390	£2594	£5830	£365
Median cost	£0	£0	£0	£0
Base	201	120	81	81

The following key findings can be gleaned from these cost tables:

- The overall costs reported here (in Table 1) are in line with what was reported in the 2021 Cyber Security Breaches Survey.
- Short term direct costs are reported to be the highest among businesses. This is followed by indirect costs and staff costs.
- Among charities, long-term direct costs are reported to be the highest.
- Overall, businesses tend to identify higher costs than charities on average. This does not necessarily mean that charities face a lower risk – it could be that they tend to have a less comprehensive understanding of the cost implications, so report lower costs.

The median cost is typically £0 (nil) across businesses and charities – also a similar pattern to what is reported in the Cyber Security Breaches Survey. This reflects the fact that most incidents do not have any material outcome (a loss of assets or data), so do not always need a response. By contrast, the typical organisation that has dealt with a negative outcome from incidents does report non-negligible costs (a median cost across the year of £1000 for businesses overall). Organisations that experienced incidents but are fortunate enough not to lose data or assets, therefore, run the risk of systematically underappreciating the seriousness of cyber security incidents.

Conclusions

These findings represent the first wave in this three-year Cyber Security Longitudinal Survey. The publication provides an insight into how the cyber security of medium and large businesses, and large-income charities, is functioning now under the challenges posed by the pandemic, and a baseline against which to measure changes to see how investment and attitudes to cyber security evolve. The study will allow DCMS to conduct analysis around the link between organisations' cyber security behaviours and the extent to which they influence the impact and likelihood of experiencing an incident over time.

Reactive approach to cyber defences

Overall, both the baseline survey and qualitative research indicate that making any changes or improvements to an organisation's cyber security is often reactive rather than proactive**.** The survey findings consistently show a link between organisations having experienced an incident in the last twelve months, having cyber security prevention measures in place and processes for how to manage an incident. This could indicate organisations more engaged with cyber security are more likely to detect incidents, and/or that organisations tend to put measure in place after they experience an incident.

These findings are also supported by the qualitative interviews. Participants discussed how greater engagement with cyber security had been triggered by a cyber security incident or was required to secure public sector contracts, as evidence of meeting an accepted standard is often a prerequisite. Organisations, particularly medium businesses, are also more likely to hire consultants or outsource cyber security, and then leave everything up to them. In contrast, large organisations are more likely to have the financial means and cyber specialists to drive investment in cyber security.

Lack of board level engagement

The baseline survey also shows that board level engagement with cyber security is relatively low, with half of businesses (50%) and four in ten charities (40%) having one or more board members with oversight of cyber security risks. The qualitative interviews shed more light on the difficulties of engaging board members with cyber security, citing lack of IT skills and knowledge, age, and lack of training as barriers to engagement.

The interviews also highlighted that charities and business sectors that are not so closely related to information technology and finance are likely to face greater barriers to board engagement. However, the survey suggests that board engagement with cyber security can be an important factor in having effective cyber procedures and policies in place. It suggests a correlation between board-level engagement (having a board that receives updates on cyber security at least monthly) and having cyber security certifications, policies and procedures in place, as well as including information about cyber security in annual reports.

Areas of engagement

There are some areas of cyber security where organisations show a reasonable level of engagement, although there is still room for improvement in future waves:

- In terms of governance and planning, around seven in ten (69% of businesses and 73% of charities) have a Business Continuity Plan that covers cyber security
- More than half have an insurance policy that covers cyber security, with charities more likely than businesses to do so (66% vs. 53%)
- More than half of businesses and charities (57% of each) have in place technical controls in place for each of the five areas required to attain Cyber Essentials certification, with more

than nine in ten saying they restrict IT admin and access rights to specific users, have up-to-date malware across all their devices, firewalls that cover their entire IT network as well as individual devices, and security controls on their organisation's own devices
- In the last twelve months, around four in five (79% of businesses and 84% of charities) have taken some action to expand some aspect of their cyber security, and organisations are most likely to have expanded or improved their network security (62% of businesses and 66% of charities)

Across these areas, large businesses, and those in the information and communication and finance and insurance sectors, are consistently more likely to be outperforming smaller businesses and those in other sectors.

Areas for improvement

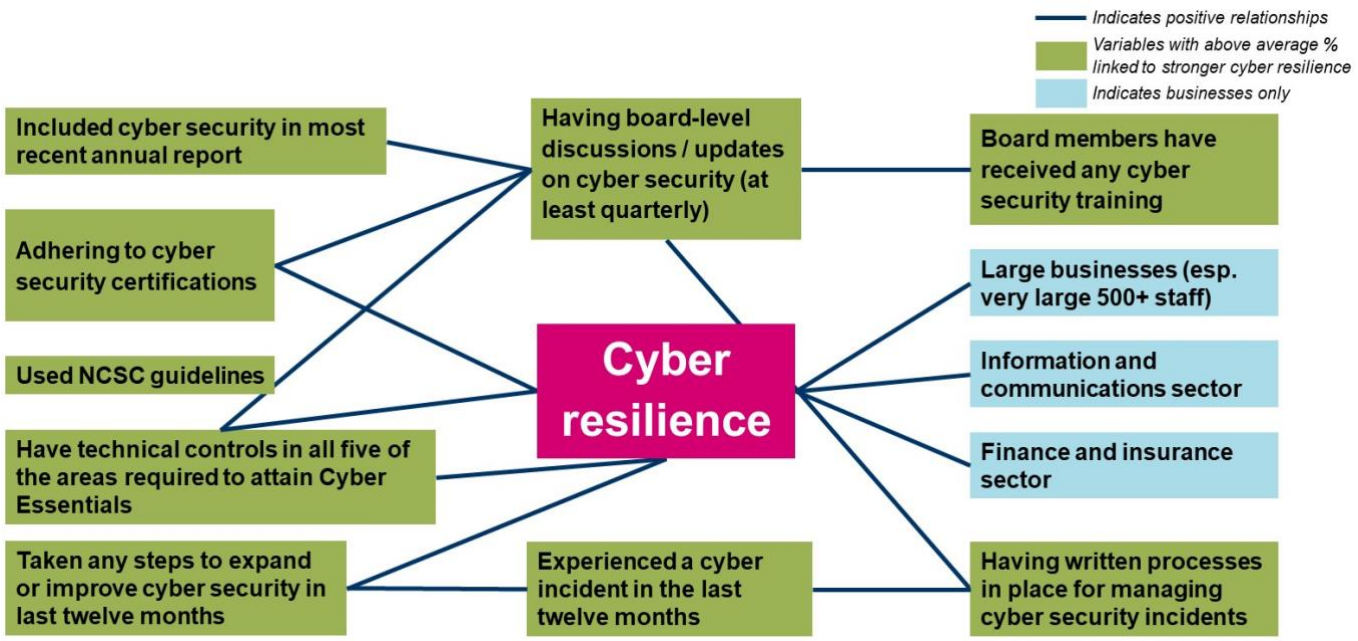
However, the results show that some organisations are still lacking many fundamentals of cyber risk management, and that there is considerable scope for further measures to be put in place:

- Only around three in ten (32% of businesses and 29% of charities) confirmed having cyber security certification in place (either Cyber Essentials, Cyber Essentials Plus and/or ISO 27001)
- Around three in five (60% of businesses and 64% of charities) did not carry out work to formally assess or manage the potential cyber security risks presented by suppliers in the last year
- Only six in ten organisations have patch management procedures in place (63% of businesses and 61% of charities). This is one of the technical controls required to attain Cyber Essentials certification
- Only around half (48% of businesses and 55% of charities) carried out cyber security training or awareness raising sessions over the last twelve months for those employees or volunteers not directly involved in cyber security. Only around three in ten organisations (35% of businesses and 28% of charities) reported that any of their board members have received any cyber security training
- A significant minority of organisations do not have a designated staff member responsible for cyber security who reports directly to the board

Overall, there are several areas where organisations of all sizes could potentially take more action, including around supply chain management, staff awareness and training, and actively assessing cyber security risks and seeking formal certifications.

Additionally, findings identified multiple drivers of increased cyber resilience such as increased board engagement with cyber security, adhering to certifications, or having written processes in place for managing cyber security incidents.

Figure 9.1: Factors driving improved cyber resilience



The second and third waves of the survey will provide further insight into these relationships and:

- their impact on improved resilience over time
- how changes and improvements in cyber security training, policies and processes evolve, and
- the extent to which those who have more robust processes in place are 1) protected from experiencing an incident over time, and 2) less impacted by incidents in terms of frequency, recovery times and costs etc.

Annex A: Summary of key findings

The below table provides an overview of headline survey findings by respondent group. Further detail can be found in the corresponding chapters.

Chapter / Measure	Businesses (no. of employees)			Charities
	Medium (50-249)	Large (250-499)	Very large (500+)	
Chapter 3: Board Involvement				
Organisation has one or more board members whose roles include oversight of cyber security risks	48%	55%	59%	40%
Board has discussed or received updates on the organisation's cyber security at least quarterly over the last 12 months*	43%	51%	55%	37%
Board received any cyber security training	33%	43%	48%	28%
Chapter 4: Sources of information				
Used information or guidance from the National Cyber Security Centre	21%	30%	37%	32%
External IT or cyber security consultants had a 'great deal / fair amount' of influence on actions on cyber security	47%	51%	46%	55%
Regulators for sector had a 'great deal / fair amount' of influence on actions on cyber security	20%	24%	27%	27%
Insurers had a 'great deal / fair amount' of influence on actions on cyber security	25%	33%	31%	30%
Changed any cyber security policies or processes as a result of: Another organisation in your sector experiencing a cyber security incident	12%	18%	29%	20%
Changed any cyber security policies or processes as a result of: Another organisation in your sector implementing similar measures	9%	14%	20%	14%
Chapter 5: Cyber security policies				
Has a Business Continuity Plan that covers cyber security in place to help manage cyber security risks	67%	68%	81%	73%
Has cyber security insurance	34%	34%	36%	20%
Carried out any cyber security training or awareness raising sessions specifically for any staff/staff or volunteers who are not directly involved in cyber security in the last twelve months	45%	51%	70%	55%
Chapter 6: Cyber security processes				
Organisation certified under the Cyber Essentials standard	18%	23%	26%	19%
Have technical controls in all five of the areas required to attain Cyber Essentials certification	16%	18%	25%	17%
Included anything about cyber security in most recent annual report	13%	14%	21%	18%
Taken any action to expand or improve some aspect of cyber security over the last twelve months	77%	84%	88%	84%

Taken steps to improve or expand network security over the last twelve months	60%	69%	74%	66%
Carried out a risk assessment covering cyber security risks over the last twelve months to identify cyber security risks to their organisation	63%	69%	76%	73%
Carried out work in the last twelve months to formally assess or manage the potential cyber security risks presented by suppliers	20%	26%	41%	27%
Chapter 7: Cyber incident management				
Have written processes for how to manage a cyber security incident	49%	55%	65%	51%
Chapter 8: Prevalence and impact of cyber incidents				
Experienced at least one cyber security incident – excluding phishing – in the last twelve months	49%	53%	64%	47%
Organisation makes it a rule or policy to not pay ransomware payments	40%	41%	40%	42%

Base (unless otherwise stated): All (n=1,741); All medium businesses (n=835); All large businesses (n=173); All very large businesses (n=197); All charities (n=536)

*Base: All excluding don't knows (n=1,447); All medium businesses (n=686); All large businesses (n=135); All very large businesses (n=153); All charities (n=473)

Annex B: Further information

The Department for Digital, Culture, Media and Sport would like to thank Ipsos MORI and Steven Furnell of the University of Nottingham for their work in the development and carrying out of the survey and for their work compiling this report.

This research report is accompanied by infographics and a technical report. These can be found at https://www.gov.uk/government/publications/cyber-security-longitudinal-survey-wave-one .

The responsible DCMS analyst for this release is Maddy Ell. The responsible statistician is Robbie Gallucci. For enquiries on this release, please contact us at evidence@dcms.gov.uk.

For general enquiries contact:

Department for Digital, Culture, Media and Sport
100 Parliament Street
London
SW1A 2BQ
Telephone: 020 7211 6000

For media enquiries only (24 hours) please contact the press office on 020 7211 2210.

DCMS statisticians can be followed on Twitter at @DCMSinsight.

Annex C: 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 1,205 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 2.8 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.[14]

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

	10% or 90%	30% or 70%	50%
1,205 businesses	±1.7	±2.6	±2.8
835 medium businesses	±2.0	±3.1	±3.4
370 large businesses	±3.0	±4.6	±5.0
536 charities	±2.5	±3.8	±4.1

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 for the subgroups that we have referred to several times across this report.

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

	10% or 90%	30% or 70%	50%
1,205 businesses	±2.2	±3.3	±3.6
835 medium businesses	±2.4	±3.7	±4.1
370 large businesses	±3.3	±5.0	±5.5
536 charities	±2.8	±4.3	±4.7

[14] In calculating these margins of error, the design effect of the weighting has been taken into account. This lowers the *effective* base size for businesses used in statistical significance testing. The overall effective base sizes are 1,075 for all businesses, 803 for medium businesses and 356 for large businesses.

4th Floor
100 Parliament Street
London
SW1A 2BQ