Understanding the state of cyber security in adult social care

Main Report

March 2025

Ipsos: Margaret Blake, Claire Lambert, Rachel Burkitt, Amun Rehsi, Sonja Schneuwly, Holly Brown

Institute of Public Care: Fiona Richardson, Paul Riley, Jonathan Gardam

Contents

Executive summary

This executive summary provides an overview of the main findings from a research project undertaken by Ipsos and the Institute of Public Care (IPC) at Oxford Brookes University, on behalf of the Department of Health and Social Care (DHSC).

Context

The Network and Information Systems Regulations (NIS Regulations) were introduced in 2018. Healthcare services are an essential service under the NIS Regulations. In 2023, DHSC and NHS England published 'A cyber resilient health and adult social care system in England: cyber security strategy to 2030'. This strategy provides the vision for protecting health and social care services that are increasingly leveraging digital technology to transform care from the disruptive impact of a cyber attack.

Significant efforts have been made over the last few years to improve both information security and cyber security across the sector through increased awareness of the Data Security and Protection Toolkit (DSPT) and support available through the Better Security, Better Care (BSBC) programme.

In this context, the project aimed to understand how cyber security is currently managed within the adult social sector and how cyber resilience can be strengthened. It also provides a baseline upon which knowledge and understanding can be monitored.

Methodology

The research started with a rapid evidence review and a scoping phase, which helped determine the remit and objectives of the project and refine the methodology.

The main phase used a mix of quantitative and qualitative research methods, with fieldwork taking place between December 2023 and April 2024. A survey with 575 regulated care providers in England was conducted, using a combination of online and telephone interviews. In-depth qualitative interviews were conducted, via Microsoft Teams, with:

- 15 care providers
- 10 technology suppliers
- 16 adult social care representatives and leaders

An online survey with technology suppliers was also conducted using an open link, but only achieved 9 responses despite repeated attempts to engage with this target audience through a range of different channels.

Economic analysis was conducted about the cost of cyber incidents reported by care providers in the survey. The project was guided by the regular input of a data end user group, established by DHSC.

Main findings

Threats and risks facing the adult social care sector

About 4 in 5 care providers (79%) had used some well-established approaches to identify cyber threats within the last 12 months (17% did not use any measures and 4% did not know if they had). The most

common approaches were risk assessments that include cyber security (62% reported carrying this out), testing staff awareness and response (41%) and/or carrying out cyber security vulnerability audits (38%).

Representatives and leaders raised concerns regarding care providers' ability to identify cyber threats, which they attributed to a lack of understanding of cyber security risks and of the likely impacts of incidents, a lack of dedicated staff resources to manage risks, and the limited information shared by technology suppliers about this.

Phishing was identified by representatives and leaders as the most common type of incident care providers are at risk from, with ransomware the most costly. Technology suppliers identified unauthorised accessing of files or networks as the greatest cyber risk facing care providers using their services or solutions, followed by malware, denial of service attacks and ransomware attacks.

There were concerns about a number of risk factors inherent to the sector that make care providers very exposed to cyber incidents. Low digital maturity, the sensitive financial information and personal data care providers hold, and the sector's reliance on a small number of technology suppliers contribute to this vulnerability.

Experience and impact of cyber incidents

Only a third of care providers reported experiencing a cyber incident or unsuccessful attack in the last 3 years (33%). As a comparison, in the 2024 Cyber Breaches Survey half of businesses (50%) and a third of charities (32%) reported experiencing a cyber security breach or attack in the last 12 months. There were some concerns about potential underreporting of attacks, with representatives and leaders suggesting that a lack of awareness and fear of reputational damage when disclosing incidents contributed to this discrepancy.

Of the care providers who had experienced an incident or attack:

- the most common type of incident was phishing (reported by 75% of providers who had experienced an incident) - this was followed by just over a third who had experienced people impersonating their organisation in emails or online (35%)
- the incidents or attacks had been fairly infrequent - within individual care providers, 2 in 5 incidents happened once only in the last 3 years (27%) or roughly once a year (14%)
- just under half of the attacks originated from a third-party organisation (44%), and 1 in 5 originated within the care provider's systems (21%)

Over half of the incidents reported did not have any impact such as loss of revenue, reputational damage, impact on staff or service users (52%). Overall, the most common type of impact was having to introduce new measures to prevent future breaches (28%) and commit additional staff time to deal with the attack (28%), which reflects and may also exacerbate current workforce pressures faced by care providers, as shown in Skills for Care's state of the adult social care sector and workforce in England. Similarly, over 3 in 5 incidents did not result in any outcomes for the care provider (63%). Loss of access to files or networks (11%), compromised accounts or systems used for illicit purposes (9%) and software or systems being corrupted or damaged (8%) were the most common for those who reported an outcome.

On average, care providers spent £2,575 dealing with cyber security incidents over the last 3 years. This average includes care providers who did not report any incident, and those who reported incidents but

said they did not incur any costs as a result. The figure is much higher when excluding those who did not report any incident over the last 3 years: care providers who reported at least one incident incurred an average cost of £9,528 dealing with this or these incidents over the last 3 years. The median was £0 and the highest cost of incidents reported by an individual provider over the past 3 years cumulatively stood at £900,080, indicating a large range of possible costs. When excluding care providers who did not incur any costs as a result of the incident or 'near miss', the average cost incurred by care providers over the past 3 years stands at £24,064, with a median cost of £650.

The vast majority of incidents (89%) resulted in actions being taken by the care provider - for example, carrying out training and/or communications to staff (61%) or reviewing or updating their cyber policies and procedures (50%).

Awareness and perceptions of cyber security in the adult social care sector

Self-reported knowledge about good cyber security practices was high among care providers (90% reported they know a great deal or fair amount about it). The qualitative interviews confirmed that there had been a significant rise in awareness of cyber security issues in the sector, as a result of the:

- BSBC programme
- DSPT and its inclusion in the Care Quality Commission (CQC) Single Assessment Framework
- adoption of digital technology
- cyber incident affecting the software supplier, Advanced, in August 2022 that had been a wake-up call for many in the sector

Over 4 in 5 care providers agreed that their organisation knew where to go for advice and expertise on cyber security (82%). Access to cyber security expertise was typically accessed through contracts with cyber security organisations (46%), ad hoc access to specialists (31%), and internal expert team (27%) or individual (21%). However, insights from the qualitative interviews suggested that some care providers relied heavily on policies and procedures without a full grasp of cyber security risks. This surface-level understanding meant exposure to cyber security risks, and the potential impact of cyber incidents were underestimated.

The majority (90%) of care providers consider cyber security a high priority, and it is recognised as an important issue for the leaders of care providers. However, competing priorities and limited resources pose challenges. Misconceptions about data sensitivity, risk levels and reliance on external cyber security teams or technology suppliers could hinder adequate prioritisation and leadership.

In terms of the wider workforce, three-quarters (77%) of care providers agreed their frontline staff have the digital skills they need to securely use the digital technology or systems adopted by their organisation. However, concerns about staff digital skills were raised in relation to high staff turnover, varying digital literacy levels across the workforce (also shown in Adult social care technology innovation and digital skills reviews) and the perception that cyber security is not something that care workers typically consider as part of their role.

Policies, procedures and practices

Care providers reported that they have implemented a wide range of policies, procedures, rules and controls in their organisation to promote cyber security. For example:

- a majority (82%) had established a formal policy or policies covering cyber security risks, and/or a business continuity plan that covered cyber security (80%)
- a majority of care providers taking the expert routing through the questionnaire had a broad range of technical rules and controls in place to help minimise the risk of cyber security breaches (such as strong password policies, restricted access, up-to-date malware protection): 55% had 11 to 15 rules and controls, 35% had 6 to 10, and only 10% had 1 to 5 of the 15 rules or controls listed

The majority (around three-quarters) reported that they provide staff with a wide range of training offers on cyber security, and a similar proportion (75%) agreed that they knew the cyber security risks associated with 'enterprise connected devices'.

As such there was a high level of confidence among care providers in the procedures and policies their organisation had in place to ensure cyber security. Where there was uncertainty, this related to:

- concerns around human error
- the changing landscape in terms of technological advances and advances in cyber crime
- the lack of resources, time and capacity to dedicate to cyber security

Still, representatives and leaders expressed some concerns regarding the robustness of these procedures and policies, their implementation, and the quality of the cyber security training provided to staff.

Furthermore, some risky behaviours and practices seemed to be fairly common. In the survey around a third of care providers reported that things like sharing organisational devices (39%), staff using their own devices for work (33%) or sharing email addresses (30%) were happening fairly or very frequently. In the qualitative interviews, all audiences thought that these practices were widespread, linking them back to low digital skills, lack of awareness of cyber risk and lack of resources (for example, to buy extra licences or devices).

Responding to future cyber incidents

Care providers showed a high level of confidence in their organisation's ability to deal with a future cyber incident, with the proportion feeling very confident higher among care providers who did not report any incident over the last 3 years (36%, as opposed to 25% among those who did).

Care providers' high level of confidence in their ability to deal with a future cyber incident was driven by the policies and procedures they had in place, including:

- written guidance on who to notify (75%), assigned roles and responsibilities (72%), and guidance on when to report incidents externally (64%)
- business continuity plans covering cyber security (80%) and incident response plans (61%) - over half of care providers have both (53%)
- back-ups - the majority reported that they backed up their data (81%), with over half reporting that this happened once a day or more (56%). Nearly all (96%) care providers were confident their back-ups were usable and complete

- insurance - just under two-thirds (64%) reported being insured against cyber security risks in some way

Still, some concerns were raised in the qualitative interviews (particularly from representatives and leaders) around the strength of some of these measures. This again included an over-reliance on policies and procedures that was not backed up by practical knowledge and experience. More specifically, there were concerns about weaknesses common in business continuity plans (for example, underestimating the time it can take to recover from an attack) and back-ups being inadequately implemented.

In terms of actions in the event of an incident, care providers reported that they would notify a range of organisations - in most cases CQC (80%), the Information Commissioner's Office (ICO) (73%), their insurance company (73%) and/or the local authority (71%), though in practice they explained that who they would notify would depend on the nature of the incident.

Technology suppliers also reported a range of measures in place to respond to an incident - and though there is a low base size it appears that the procedures in place are widespread. They were also confident in their cyber incident response and recovery arrangements.

Technology suppliers' approaches to cyber security and risks

Technology suppliers generally had a strong awareness of cyber security, current and emerging threats, and its importance within the adult social care sector.

They mentioned a range of characteristics to demonstrate their cyber maturity and resilience, including:

- senior leadership on cyber security
- high prevalence of business continuity plans
- formal policies covering cyber security
- high take-up of various rules and controls associated with cyber security

All or most participating technology suppliers used third-party cyber services such as IT system monitoring and threat detection, and penetration testing. Technology suppliers also reported high levels of confidence in their digital supply chain.

Maintaining a good reputation, and the likely commercial impact of an incident were the main drivers for good cyber security governance, practices and supply chain arrangements.

Relationship between care providers and technology suppliers

In practice, ownership for cyber security risks is a mixed responsibility between care providers and technology suppliers. As care providers are ultimately accountable for their data, they see themselves as responsible for assuring themselves of the cyber resilience of their digital arrangements.

However, lack of in-depth cyber expertise and resources to dedicate to cyber security mean care providers rely heavily on their technology suppliers. They place a significant amount of confidence in their technology suppliers having appropriate cyber security measures in place. This led technology suppliers and sector representatives and leaders to think that care providers assumed that their

technology suppliers were fully responsible for cyber security - which did not reflect care providers' views.

When purchasing technology, there was also high confidence among care providers in their commissioning staff's ability to purchase safe and secure technology. Technology suppliers confirmed that cyber security is increasingly considered when technology is purchased, in particular by large care providers.

Two-thirds of care providers (68%) agreed that they would be prepared to trade functionality, or pay more, to receive high quality cyber security when purchasing digital technology. Still, technology suppliers mentioned that in practice, buying decisions are mostly based on price and functionality rather than cyber security. The care providers who took part in the qualitative interviews confirmed this.

There appears to be limited ongoing monitoring of cyber security risks by care providers after the contracting process. This is due to lack of time, size of organisation (too small to have bargaining power), and not knowing what checks to carry out.

Looking at the support offered to care providers by their technology suppliers, this tends to be at the set-up stage and focused around functionality rather than cyber security. In the event of an incident on the supplier side, support would be offered to the care provider in the form of back-up data, electronic forms and so on, so the organisation can continue to operate offline. Support when the care provider is the victim of a cyber incident would be offered on a goodwill basis rather than on a formal basis.

Improving cyber resilience

Research participants viewed the DSPT as useful for raising awareness of cyber security and driving up the adoption of basic controls. However, DSPT compliance was not viewed as an accurate measure of cyber resilience in the sector. It was thought that some care providers treated DSPT completion as a 'tick box', and that meeting DSPT standards did not necessarily equate with depth of knowledge and engagement with cyber security issues. Mixed and conflicting suggestions were made for the future of the DSPT, ranging from simplification (to make it more proportionate to the mix of care providers in the sector) to greater inclusion of Cyber Essentials requirements and external verification of the self-assessment.

Barriers to improving cyber security primarily focused on costs (mentioned by 49%) followed by time and capacity to dedicate to this (34%). They included the cost of updating out of date and legacy digital systems, the time for staff to invest in training and learning about cyber security, and the cost of working with a cyber security supplier providing the level of expertise needed.

Suggestions for improving cyber resilience varied, and focused on:

ensuring all care providers are aware of the range of support options available to them (for example, from the BSBC programme)

- education and awareness raising across all staff
- supporting care providers financially
- strengthening requirements and assurances for care providers and technology suppliers to promote safer cyber practices

- central co-ordination of cyber resilience testing and incident response
- the role of technology suppliers in supporting and upskilling their customers

All audiences generally supported a national reporting function for cyber security incidents in adult social care where the incident could potentially impact care delivery. This was on the grounds that the function should facilitate sector learning and that providers would not be identifiable in any publicly shared information. Linking the reporting of incidents to a cyber incident response co-ordination offer would encourage the reporting of incidents.

Subgroup analysis

Some fairly distinct groups emerged from the analysis of the survey with care providers, regarding their:

- leadership on cyber security
- awareness and understanding of cyber security risks
- monitoring of risks
- adoption and implementation of cyber security measures

In terms of size, providers with 50 or more staff were more likely than smaller providers to back up their data once a day or more, use a secure back-up system contracted elsewhere, and report cyber incidents. They were also more likely to have various cyber security controls and risk management arrangements in place. However, on certain questions such as confidence about having appropriate measures in place, responses were similar regardless of size.

Looking at the type of service provided, home care providers were more likely than average to say that cyber security is a very high priority for their owners, directors or senior management (61% versus 51%), and to strongly agree that there is strong leadership in cyber security planning in their organisation (48% versus 40%). They were also more likely to strongly agree their staff have the digital skills needed to securely use the digital technology or systems adopted by their organisation (47% versus 41%), and to strongly agree with a range of statements about cyber security training for staff.

Some care providers demonstrated a high level of engagement with cyber security. They reported a strong understanding of cyber security principles and had implemented comprehensive policies and procedures to protect their organisations. These care providers usually had many of the following in common:

- a business plan and/or formal policies specifically addressing cyber security
- 11 to 15 rules and controls in place to ensure good ‘cyber hygiene’
- specific cyber security insurance
- regular data back-ups
- a complete cyber incident response plan
- Cyber Essentials or other nationally recognised certifications

- access to cyber expertise from the BSBC programme

In particular, access to cyber security expertise provided by BSBC through the Digital Care Hub was consistently associated with better cyber security practices, when compared with the average. For example, care providers who said they accessed this source of expertise:

- had better awareness of the likely impact of a cyber incident
- were more likely to have various rules, controls, policies and procedures in place to manage cyber security day-to-day and respond to incidents
- were more positive about training and staff awareness on cyber security

A small group of care providers is further behind. In the survey, they did not appear to engage well with cyber security overall, and showed limited awareness of the cyber security risks faced by care providers and the likely impact of cyber security incidents. These care providers tended to have many of the following in common:

- they lacked formal policies or business continuity plans covering cyber security
- they only had 1 to 5 rules and controls in place
- they did not back up their data or backed them up infrequently
- they did not have cyber security insurance
- they did not have a cyber incident response plan
- they had ad hoc access to cyber expertise with an external specialist

This is demonstrated by the association between the sub-groups listed above: for example, 44% of care providers with 1 to 5 rules and controls reported that they do not back up their data, and over half of care providers with no cyber security insurance do not have any cyber incident response plan (55%). These care providers with minimal or no cyber security measures in place are particularly vulnerable to cyber threats, but tended not to realise their vulnerability or could not afford to prioritise cyber security.

Many more care providers fell between these 2 extremes, having implemented some cyber security policies and procedures while also reporting some areas for improvement.

Evidence of good practice was found among providers of all sizes and types, and so was limited engagement with cyber security. Rather than size, and types of services, it is leadership on cyber security, and access to cyber expertise, which appear to have most influence care providers' awareness and understanding of cyber security and their adoption and implementation of cyber security practices.

01

Introduction

1 Introduction and methodology

This chapter outlines the background and objectives of the research, and the methodology used. It also provides notes on the presentation and interpretation of data, and acknowledgements to those who have supported the research.

1.1 Background and objectives

This report presents the findings of a project aiming to develop an accurate understanding of the state of cyber security risks in the adult social care sector. It was commissioned by the Department of Health and Social Care (DHSC) and NHS Transformation Directorate. The project was conducted by Ipsos in partnership with the Institute of Public Care (IPC) at Oxford Brookes University between July 2023 and May 2024.

The objectives of the research were to:

- provide a baseline of knowledge and understanding about cyber security and risks associated with cyber security in the adult social care sector and its supply chain
- establish levels of cyber resilience among adult social care providers and technology suppliers to the sector, and how this varies by organisation type, by exploring:
  - what actually happens in the sector in relation to cyber security practices (beyond the information reported in Data Security Protection Toolkit)
  - occurrence of cyber incidents
  - how organisations deal with incidents and recovery
  - interest in and need for additional support and training
- quantify the costs, impact and value of cyber security considering costs (including losses from incidents) and impacts for public sector, care providers, technology suppliers and individuals drawing on care and support, to make the case for government spending and investment in cyber resilience

The findings of the research will be used by DHSC to:

- understand the appropriate balance of risk between government and providers of adult social care services and their supply chain
- inform the way in which cyber security is assured within adult social care providers
- inform the development of a national or regional support offer to the sector and potential interventions to improve resilience in terms of prevention and support to recover when incidents occur, building on the current DSPT and activities of BSBC
- provide the economic case for investment in cyber resilience by government
- establish an approach which could be replicated for gathering similar evidence in future and which is consistent with other sources of data such as the cyber breaches survey and NHS reporting

approaches to cyber security, and which aligns with frameworks such as the DSPT and the Cyber Assessment Framework (CAF)

1.2 Methodology

The project involved a scoping phase, a workshop with stakeholders, surveys and depths interviews with care providers and technology suppliers, depth interviews with adult social care representatives and leaders, and economic analysis on the costs of cyber incidents. The project benefited from the input of a Data End User Group at various stages.

Scoping phase

The scoping phase was conducted between July and September 2023. It aimed to:

- confirm the objectives and scope of the research
- confirm the approach and methodology
- inform the content of surveys and the discussion guides for the depth interviews
- confirm the sample design for the surveys with care providers, and approaches to recruitment of the depth interviews
- identify an approach to measuring costs and impact of cyber and data protection incidents in the sector and the benefits of alternative scenarios with improved cyber security
- summarise existing knowledge to scope and steer the research.

In order to achieve these aims, the following actions were undertaken as part of the scoping phase:

- an inception meeting between DHSC, Ipsos and IPC
- a rapid evidence review (RER)
- ten in-depth scoping interviews with core stakeholders in the sector, plus a targeted conversation with DHSC about the project's objectives
- a meeting with the Data End User Group conveyed by DHSC
- review of existing data held within NHS England and DHSC.

Inception meeting

Ipsos, IPC and DHSC reviewed the aims of the project and discussed specific research questions in more detail, discussed the core stakeholders involved, identified background documents to review and discussed which organisations should be in scope for the research.

Rapid evidence review

IPC carried out a RER which summarised the academic literature, grey literature and online practices within the UK in the last 5 years regarding cyber resilience of the adult social care sector. Though the brief was UK related, due to the international nature of the perpetrators and actors, some relevant lessons from international literature were captured.

There are no central repositories of provider and supplier information for many aspects of the adult social care system. Furthermore, there are only limited academic studies specifically focused on cyber security in the adult social care sector. Data and evidence were therefore gathered from various sources, and from studies that related to specific attributes relevant to the sector, for example, studies undertaken regarding small and medium sized enterprises across a range of sectors, to inform an initial picture of the adult social care provider cyber landscape. Findings from the RER helped with the design and plan of the research.

In-depth scoping interviews

Ten in-depth interviews were conducted with stakeholders who could comment on cyber security or building cyber resilience in the adult social care sector. Ipsos, IPC and DHSC jointly identified potential participants across the sector, using their contacts and networks. The interviews were carried out by Ipsos and IPC in August 2023. They lasted between 45 minutes to one hour and took place via Microsoft Teams.

Expert workshop

At the end of the scoping phase, an expert reference group was convened to discuss the objectives of the research, the content of the questionnaires for the 2 surveys, and ways to engage the sector. The workshop included sector experts and leaders, and the workshop took place on Microsoft Teams on 27 September 2023.

Qualitative and quantitative methods

The research employed a mixed-methods approach, including quantitative surveys with care providers and technology suppliers, and in-depth interviews with care providers, technology suppliers and leaders and representatives of the sector.

- within care provider organisations, the research focused on individuals in charge of cyber security within a care provider organisation or individuals who were responsible for buying digital technology or services for a care provider organisation.

- within technology suppliers, the research focused on individuals able to discuss the cyber security of their organisation and of the technology products or services they supply to the adult social care sector.

- leaders and representatives of the sector were individuals with in-depth understanding of cyber security issues in adult social care. They included care provider umbrella organisations, organisations supporting or representing the cyber security sector, ICS or local authority, technology suppliers, BSBC local support organisations (LSOs), and national organisations overseeing or supporting the sector. The input of sector leaders and representatives was important for understanding the wider context and issues such as support and monitoring of cyber security

Across these audiences, several themes were covered:

1. attitudes, knowledge and awareness of cyber security: including gaps in understanding, perceived importance of cyber security, digital skills, prioritisation and leadership on cyber security

2. practices and behaviours: including risky practices, policies, advice and guidance for staff, organisation culture and barriers to improving cyber resilience

3. threats and risks: including understanding the landscape, reporting and impact of incidents and preparedness

4. support for care providers: including awareness of, use and access to support

5. technology suppliers: supply chain management and supplier perspectives

Care providers survey

The care providers survey used a mixed mode approach (online and telephone). A sample of care providers was selected from the BSBC register of adult social care providers which is based on the CQC list of regulated providers. Sampling was conducted at parent organisation level and selected providers were invited to take part in this research. The BSBC sample did not include email addresses for care providers. The survey was disseminated in 2 ways:

- Ipsos shared the ODS codes of the care providers sampled with the DSPT team. They sent out survey invitations and reminders by email to those who had completed the DSPT, using the last login (email) from that organisation on the DSPT. The DSPT team did this on behalf of Ipsos, which did not have access to their email addresses

- for the rest of the sample, Ipsos sent out survey invitations and reminders by email to a sample of providers who had not completed the DSPT (or for whom the DSPT team did not have a valid email address), using email addresses DHSC had obtained from the Care Quality Commission (after DHSC administered an opt out)

Telephone interviews were conducted by Ipsos, with people who did not respond to the online survey.

In total, 575 care providers participated in the survey between 14 February and 4 April 2024: 327 participants took part online and 248 participants took part by telephone. The average interview length was about 50 minutes over the phone and 33 minutes online. 207 of the interviews were completed from the CQC contacts and the rest were from the DSPT contacts.

The questionnaire made a distinction between ‘learners’ and ‘experts’ in cyber security, which was used for routing purposes. This ensured that people were asked questions that were relevant and appropriate to their role and level of cyber security knowledge.

Experts were defined as those who were in charge of cyber security, who were responsible for buying digital technology products and services (including commissioning or purchasing digital care rostering or care management software, or digital care records or planning systems) or those who reported knowing a great deal or fair amount about good practice in cyber security for their organisation.

Learners were defined as those who were not solely or were not at all in charge of cyber security, were not responsible for buying digital technology products and services or those who did not know very much or knew nothing at all about good practice in cyber security for their organisation or those who preferred not to say.

The profile of the interviews achieved with care providers was broadly aligned with the population profile (care providers in the BSBC register). The sample profile and weighting approach are detailed in the technical report.

Technology suppliers survey

The technology supplier survey was conducted online. There is no comprehensive sampling frame of technology suppliers in adult social care, but the Technology Enabled Care Services Association (TSA), the Care Software Providers Association (CASPA) and techUK agreed to disseminate the survey invitation with an open link to their contacts, on behalf of Ipsos and IPC.

The contact details of technology suppliers on the NHS assured solutions list were publicly available, so Ipsos sent them an email invitation with a unique link to the survey.

IPC and Ipsos carried out a number of engagement activities to communicate the survey to the sector and demonstrate the importance of taking part. These are listed in the technical report. Despite this, there was a much lower than anticipated uptake for the technology suppliers survey. Reasons for this are detailed in the next chapter. In total, 9 participants took part in the online survey between 31 January and 4 April 2024, and the average completion time was around 28 minutes.

The data for technology suppliers are unweighted, owing to a lack of a sample frame against which to wait and the small number of responses.

Depth interviews

Due to the complex subject matter, depth interviews were valuable for understanding how organisations deal with cyber security, the barriers and challenges they face, and how these could be overcome. Depth interviews were carried out with 16 representatives and leaders of the sector, 15 care providers and 10 technology suppliers. They were conducted on Microsoft Teams between 5 March and 26 April 2024.

Recruitment of sector representatives and leaders

Ipsos and IPC suggested a list of names and/or organisations of adult social care sector leaders and representatives, and DHSC were invited to comment and add their own contacts.

Recruitment of care providers

The depth interviews with care providers were recruited from those who took part in the survey and gave permission for recontact for further research conducted as part of this project. Quotas were set based on size, location and DSPT status in addition to quotas by incidents and awareness of cyber security reported in the survey. These can be found in the technical report.

Recruitment of technology suppliers

The research had been designed so that technology suppliers would be invited to take part in a qualitative interview if they gave permission for recontact when participating in the survey.

Due to the small number of survey responses, most technology suppliers who took part in the depth interviews had not completed the survey. The recruitment approach for recruitment was altered so that:

- IPC contacted suppliers in their network and from the NHS assured solutions list, to encourage them to take part in a depth interview
- IPC liaised with TSA and CAPSA asking them to endorse the research, encourage people to participate in a way that suited them (a depth interview and/or the survey), and contact IPC if they could participate in a depth interview

1.3 Data end user group

DHSC convened a data end user group which included cross government contacts in the analytics community, with a clear business interest in the findings and outputs. The group were asked to provide the necessary steering and insights to enable the project to serve the wider needs of DHSC and NHS England. The group met 5 times over the course of the project.

1.4 Analysis and interpretation

Depth interviews

The interviews were transcribed. Data from the interviews were summarised in a grid which set out the data each interview had provided against each of the interview topics and research questions. Responses to these were analysed thematically.

Interviewers from Ipsos and IPC met twice over the fieldwork period to share and brainstorm findings from their interviews, identify emerging findings and patterns, and compare and contrast the findings across the 3 audiences. At the analysis stage, findings from the qualitative interviews were triangulated with those from the surveys.

Unlike quantitative surveys, qualitative methods are not designed to provide statistically reliable data on the population of interest, rather they are designed to be illustrative and exploratory and include the range and diversity of experience in the population of interest. These methods are design to address questions about ‘how’ and ‘why’. In this report qualitative findings are presented thematically rather than quantified.

Verbatim comments from the interviews have also been included in this report. These should not be interpreted as defining the views of all participants but have been selected to provide insight into a particular issue or topic expressed at a particular point in time.

Technology suppliers survey

In light of the small number of responses from technology suppliers, their survey responses have been reported in numbers rather than in percentages. The findings from this group primarily focuses on the qualitative evidence collected.

Care providers survey

The report comments on differences in the data between different sub-groups of care providers. A difference has to be of a certain size in order to be statistically significant and only differences which are statistically significant at the 95% confidence interval are commented on in this report. In addition to being statistically significant, only sub-group differences which are interesting and relevant to the research questions are commented on in the report to ensure that the report contains a coherent narrative.

At the data processing stage, some derived variables were compiled using information provided in the survey. These are listed in the technical report. Some of these derived variables were used extensively for sub-group analysis as they showed significant difference:

- number of rules or controls in place within the care provider organisation (1 to 5, 6 to 10, or 11 to 15 rules and controls). This is based on a question asking care providers which rules and controls their organisation had in place, from a list of 15, to ensure good cyber hygiene (RULES)

- whether the care provider had experienced at least one cyber incident, attack or near miss over the last 3 years, or none. This is based on a question asking care providers which types of cyber incidents, from a list of 11, they had experienced (TYPE)
- whether the care provider has a full cyber incident response plan, a partial one, or no such plan. This derived variable is based on 2 questions asking if the care provider has a cyber incident response plan (INCIDENCE), followed by one asking about its features, from a list of 5 (CYBER_DOC)

Survey participants were permitted to give a 'don't know' or 'prefer not to say' answer to most of the questions. Unless otherwise specified in the report, these responses are included in the analysis. These responses are referred to in the report where they form a large enough proportion to be of substantive interest.

Where percentages do not sum to 100, this is due to computer rounding, the exclusion of 'don't know' categories, or participants being able to give multiple answers to the same question.

Cost analysis of cyber incidents

This was conducted using survey data from care providers. The economic analysis focuses on relevant examples that demonstrate the economic impacts of cyber incidents, rather than attempting to quantify the total economic impact of all such incidents. Specifically, it looks at cyber incidents which are experienced particularly often by organisations in the adult social care sector: phishing incidents, incidents of others impersonating organisations in emails or online, and incidents of computers becoming infected with malware.

The economic analysis pursues 2 objectives, namely to:

- estimate the impacts and costs of a select number of types of cyber security incidents
- identify associations with best practice and experience with cyber breaches and use to estimate the costs of alternative scenarios related to improved data security and cyber resilience

1.5 Comparisons with National Breaches Survey results

Some survey questions were similar or identical to questions asked in the Cyber Security Breaches Survey. Where appropriate, findings are compared with the 2024 Cyber Breaches Survey results

The survey conducted with care providers for this project and the Cyber Breaches Survey were both aimed at the person in charge of cyber security within the organisation.

1.6 Acknowledgements

Ipsos and IPC would like to thank all of those who participated in the research and shared their views.

A range of organisations have supported the conduct of the research and we are very grateful for their input:

- the BSBC team for their advice and guidance re. the sampling of care providers
- the DSPT team, for the mail out of the survey with care providers
- CASPA, TSA and Tech UK for endorsing and disseminating the research with technology suppliers

- members of the Data End User group, for providing valuable input to shape and guide the research: NHS England, BSBC, DSPT and Government Actuary's Department and DHSC

1.7 Glossary

ASL – Assured solutions list

BSBC – Better Security, Better Care

CQC – Care Quality Commission

DSCR – Digital social care records

DSPT – Data Security Protection Toolkit

EUD – End user devices

IaaS – Infrastructure as a service

ICB – Integrated care board

ICO – Information Commission Officer

ICT – Information, communication and technology

LSOs – Local support organisations

NCSC – National Cyber Security Centre

PaaS – Platform as a service

RER – Rapid evidence review

SaaS – Software as a service

SME – Small and medium size enterprises

VPN – Virtual private network

02

Context

2 Background and context

This chapter first provides the background for the research, summarising what is already known about cyber security in adult social care and the progress that have been made. It then details the profile of the care providers and technology suppliers who contributed to the research, to set the context of the findings provided in the next chapters.

Summary

The achieved sample profile of the 575 care providers who took part in the survey is in line with the profile of the population of adult social care providers by type of services provided, region, DSPT status, and size. Data were weighted and the survey is representative of regulated care providers in England.

The care providers survey was usually completed by people for whom cyber security was part of their role (79%) or a core part of their role (16%).

Over half of care providers in the survey said their organisation used both digital and paper systems (57%) to store information, and 38% used mainly digital system. Using digital technology to support day-to-day business activities was common, with 4 in using Digital Social Care Records (DSCR) (81%), and around 3 in 5 using financial accounting software (62%), digital reporting systems (62%) and digital rostering (58%).

Fewer technology suppliers than hoped for participated in the research despite a range of avenues to secure wider involvement being tried. The challenges faced in engaging with this audience included the lack of a named sample, technology suppliers feeling there was duplication of effort due to the significant work they had undertaken to evidence the DSCR standards for the Assured Solutions List, the length of the online questionnaire, and the potential consequences of the survey for the sector more generally.

The vast majority of the 16 technology suppliers who took part in the research were small and medium size enterprises (SMEs) and participants held a mix of roles spanning senior leadership, governance and cyber security. Most had operated in the sector for at least 5 years and all but one provided Software as a Service (SaaS). Between them these 16 technology suppliers provided solutions to around a tenth of adult social care providers in England.

2.1 Background to the research

The UK Cyber security breaches survey 2024 identified a continued high level of threat with half of businesses (50%) and around a third of charities (32%) experiencing some form of cyber security breach or attack in the last 12 months. The UK is the third most targeted country for cyber-attacks, behind only the USA and Ukraine. The National Cyber Security Centre (NCSC) highlighted digital supply chains in health and adult social care as an attack vector and therefore a major area of cyber risk in terms of both probability of a cyber incident occurring and the impact size for care providers.

The Network and Information Systems Regulations (NIS Regulations) were introduced in 2018. Healthcare services are an essential service under the NIS Regulations. In 2023, the Department of Health and Social Care and NHS England published, 'A cyber resilient health and adult social care system in England: cyber security strategy to 2030'. The health and adult social care specific strategy provides the vision for protecting health and social care services that are increasingly leveraging digital

technology to transform care from the disruptive impact of a cyber-attack. One of the strategy's 5 pillars is 'defend as one'. There are significant challenges to achieving cyber resilient health and social care services on a 'defend as one' basis, including:

- being a complex ecosystem with many systems interdependences
- adult social care being provided by a mix of public, private and third sector organisations funded by either local authorities, the NHS or private individuals (self-funders), or a mix of these funding sources
- adult social care comprising around 18,000 regulated care provider organisations who are commonly SMEs
- potential differences between sub-sectors of adult social care, with care providers operating in one or more of: homecare, live-in care, extra care, supported living, shared lives, care homes, or nursing homes

What is known about current cyber exposure in adult social care is:

- there are indications of lower levels of cyber maturity in adult social care providers than in healthcare, and differing levels of cyber maturity across care providers, but not a robust baseline
- the 'Adult Social Care Technology and digital skills review' commissioned by NHSX identified a consensus among registered managers and others with responsibility for developing the digital skills of staff that there were gaps in the digital skills of the frontline workforce. The types of skills thought to need improvement were predominantly basic digital skills. This provides a degree of exposure when the main attack vectors identified by the NCSC related to basic cyber hygiene controls and practices, and in particular with end user devices (EUDs)
- there have been improvements in both information security and cyber security across the sector through the rollout of the DSPT and awareness raising through the BSBC programme. The proportion of care provider locations who are DSPT compliant was at 70% as of April 2024. This compares with under 5% in June 2019 and over 50% by the end of 2022
- the Care Quality Commission's (CQC) new Single Assessment Framework's explicitly references the DSPT under the 'well led' quality question. This now provides an impetus for the 30% of care providers who are neither compliant nor approaching standards with DSPT to become so. CQC has also issued good practice guidance for providers relating to the use of digital care records which includes specific references to the DSPT as a core standard
- the ICO data security incident trends reporting tool recorded 42 cyber related reported incidents for adult social care during 2023. This is across a care provider base of around 18,000 organisations (with 27,000 locations) and compares with 178 reported incidents in healthcare
- the adult social care sector remains under considerable pressure from rising demand for care (including rising levels of people with substantial or complex care needs, high staff vacancy rates and turnover in the sector, rising costs and longer-term issues related to how social care is funded. This means that while cyber resilience is increasingly important, the capacity of care providers in the sector to focus on this issue may be limited by other compounding pressures

The rest of this chapter details the profile of the care providers and technology suppliers who participated in the research.

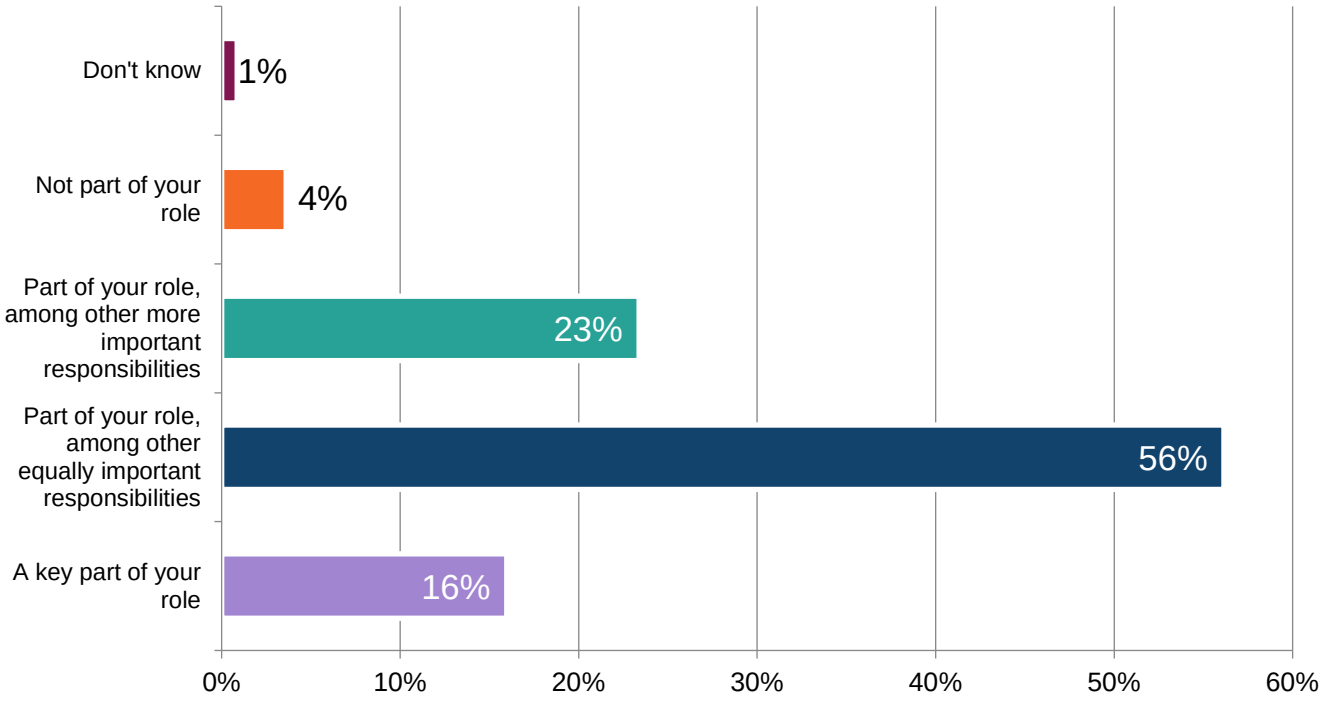
2.2 Profile of care providers who participated in the survey

The achieved sample profile of care providers was broadly in line with the profile of the population of adult social care providers by type of services provided, region, DSPT status, and size. The unweighted sample profile can be found in the technical report.

Job roles and responsibilities

Participants' roles and responsibilities were relevant to the aims of the survey: for one in 6 (16%), cyber security responsibility was a core part of their role, with a further 56% for whom it was part of their role among other equally important responsibilities. For just under a quarter of participants (23%), cyber security was part of their role among other more important responsibilities – this rose to a third of participants working for a care home provider (33%). Only 4% of participants indicated that cyber security was not part of their role. Responsibilities for the commissioning or purchasing of digital technology followed a similar pattern.

Figure 1: Cyber security as part of participants' roles and responsibilities



Base: Care providers (575)

The most common job role participating in the survey was registered manager (53% of respondents). Two in 5 participants had a job role covering compliance (39%) and for a third their job role fell into cyber security or information security (34%). A similar proportion reported being the owner (32%) or having a job role covering communications (32%), finances and accounts (30%) or human resources (30%). Just under 3 in 10 mentioned a job role covering IT infrastructure (28%) or commissioning and procurement (28%).

For routing purposes, the questionnaire made a distinction between ‘experts’ and ‘learners’ in cyber security (see definition on page 16). Only 17 care providers met the definition of ‘learners’ (weighted figure), with the remaining 558 classified as ‘experts’.

Size of organisations

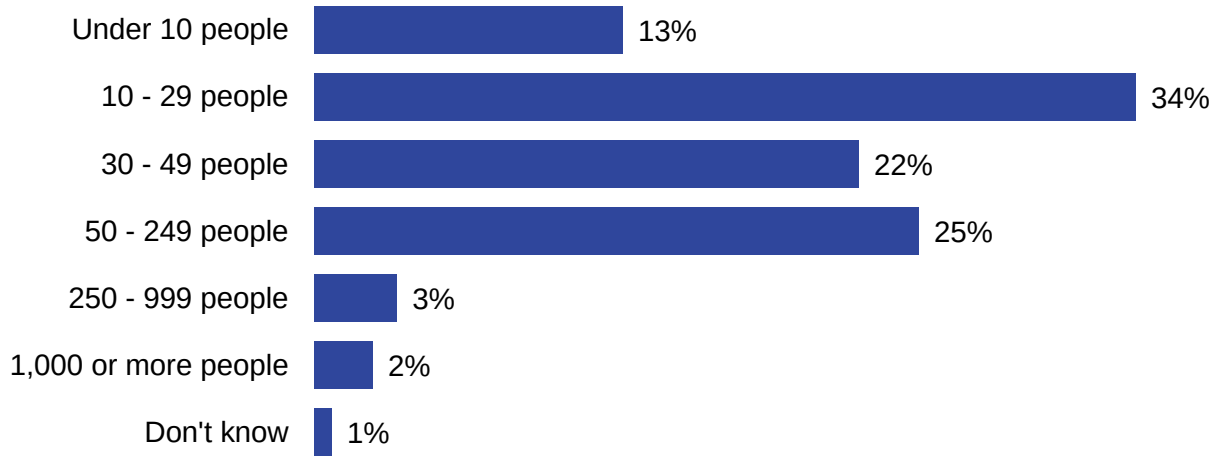
Three-quarters of participants (75%) reported that their work responsibilities covered one care setting, location, service or franchise, with the rest covering 2 or more. The number of care settings or locations is related to the size of the organisations that took part. Using the profiling information provided by BSBC for the sampling, 83% of care providers that took part in the survey had one location only (weighted figure). The variable on number of locations (settings) was used for weighting purposes.

Table 1: Number of care settings of participating care providers (sample information)

	% of care providers (weighted profile)
1 care setting	83%
2 care settings	8%
3 care settings	3%
4 or more care settings	6%

Related to this, the vast majority of the organisations surveyed were Small and Medium-size Enterprises (SMEs): 94% of the 575 participants said the care settings, locations, services or franchises they were responsible for employed less than 250 staff, including nearly half (47%) who employed less than 30 staff.

Figure 2: Number of staff care providers employed across all their care settings or locations (weighted profile)



Base: Care providers (575)

Regions

A good geographical coverage was achieved across the survey. The table below shows the regional profile of the achieved sample after weighting, using information appended to the sample at the sampling stage (the unweighted profile can be found in the technical report). A minority of participating care providers (5%) had care settings in more than one region. This variable was used to weight the data.

Table 2: Weighted regional profile of care providers

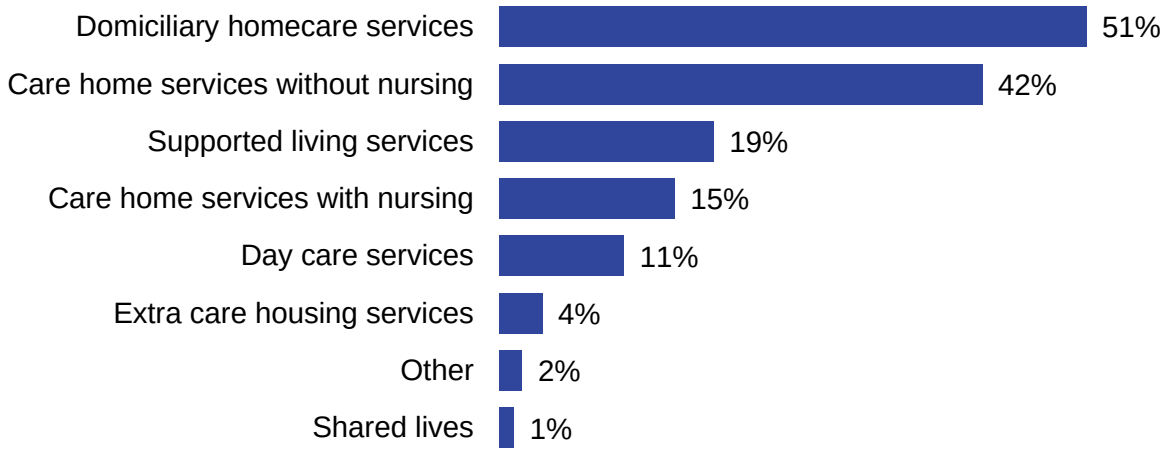
	% of care providers (weighted profile)
North East	3%
North West	11%
Yorkshire and The Humber	8%
East Midlands	9%

	% of care providers (weighted profile)
West Midlands	11%
East of England	11%
London	13%
South East	17%
South West	11%
Multiple regions	5%

Care services provided

Participating care providers represented the full range of adult social care and support services, dominated by the provision of homecare services (51%) and care home services (42% without nursing and 15% with nursing) – in line with the population profile. One in 4 (19%) provided supported living services.

Figure 3: Type of care services provided (weighted profile)



Base: Care providers (575)

Please note that people could choose multiple answers to this question if their organisation provided 2 or more care services. Organisations providing services exclusively for people aged 18 or under were screened out at the start of the survey.

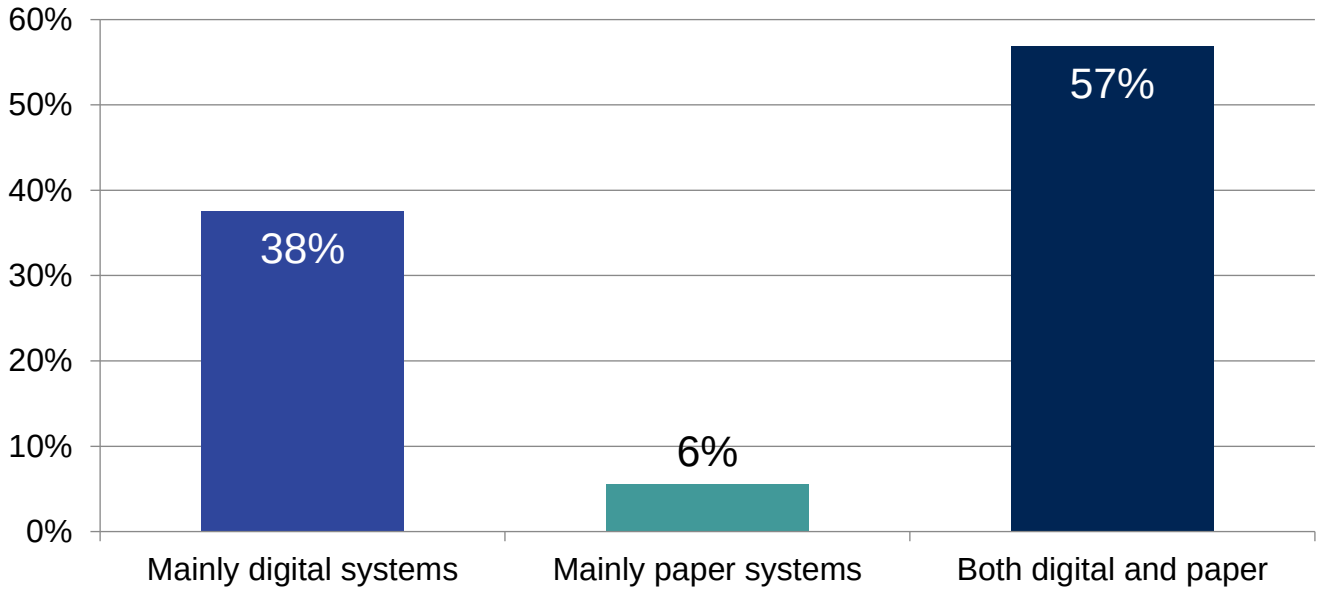
Use of technology

Nearly all participating care providers had access to the internet (99%), used laptops (92%), desktop computers (80%), or smartphones (79%). Tablets were slightly less frequently mentioned (69%). Smartphones were more frequently mentioned by community-based services, such as homecare (91%) and supported living (88%), compared with care home services (68%). Conversely, 81% of organisations providing care home services used mobile tablets, versus only 60% of organisations providing homecare services.

Information storage

Over half of participating care providers said they used both digital and paper systems (57%) to store information, while just under 2 in 5 used mainly digital systems (38%) – rising to nearly half among those providing homecare services (46%) or supported living services (47%). Using mainly digital systems was also more common among care providers that had access to an internal cyber security expert team (44%) or employing 50 or more staff (56%). Only a minority of care providers (6%) used mainly paper systems to store information.

Figure 4: Types of systems used to store information

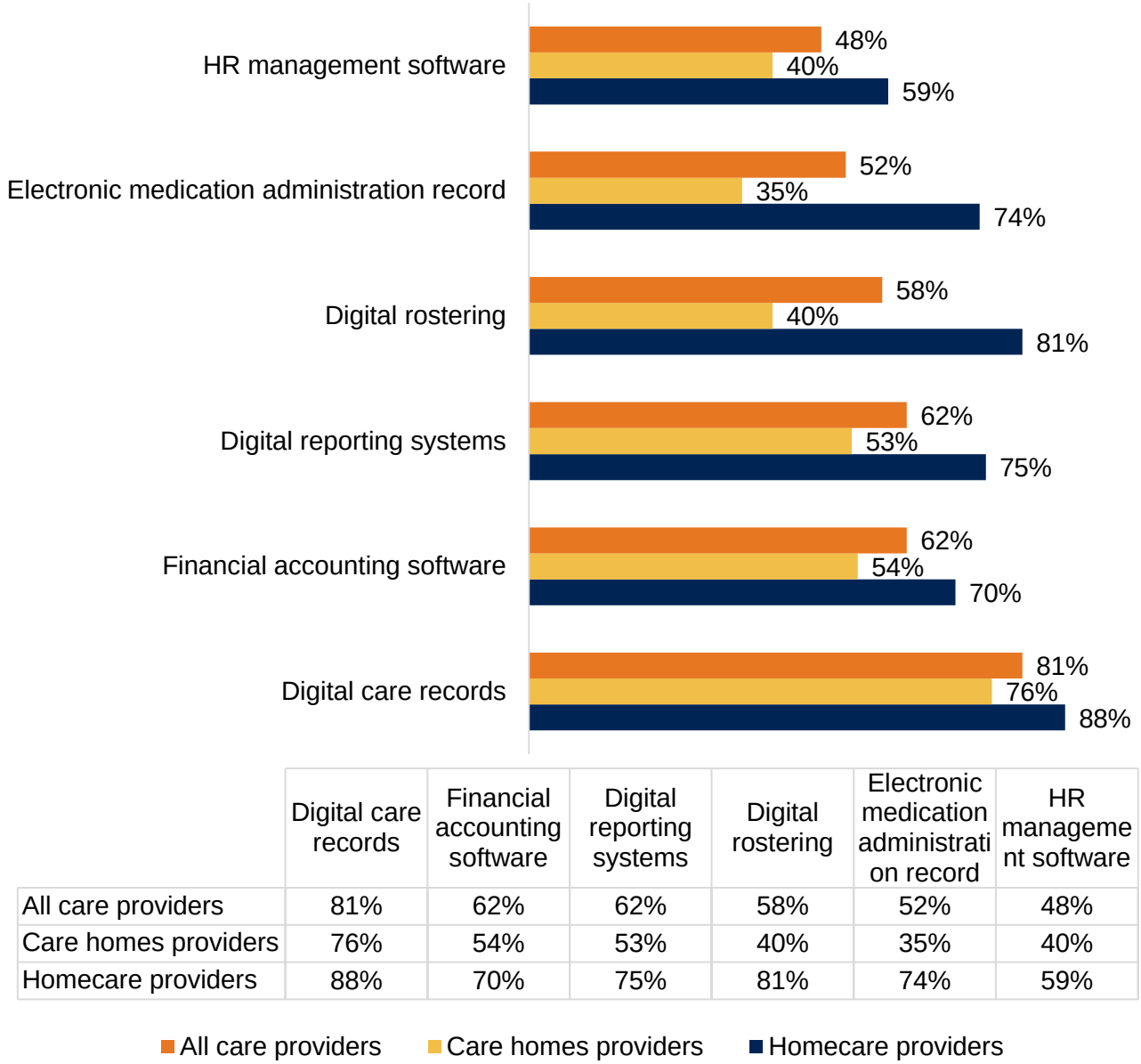


Base: Care providers (575)

Use of digital technology products for business and day-to-day management

Looking at the digital technology used by care providers to support its business and day-to-day management activities, digital care records were the most widely used type of technology, mentioned by 4 in 5 participants (81%). Financial accounting software (62%), digital reporting systems for management (62%) and digital rostering (58%) were all mentioned by approximatively 3 in 5 participants. Half of participants mentioned their organisation used electronic medication administration record (eMAR) or HR management software (52% and 48% respectively). Remarkably, one in twenty (6%) of participants said their organisation did not use any of the digital technology listed – in line with the proportion whose organisation mainly used paper systems to store information.

Figure 5: Care providers' use of digital technology to support their business and day-to-day management activities



	Digital care records	Financial accounting software	Digital reporting systems	Digital rostering	Electronic medication administration record	HR management software
All care providers	81%	62%	62%	58%	52%	48%
Care homes providers	76%	54%	53%	40%	35%	40%
Homecare providers	88%	70%	75%	81%	74%	59%

Base: Care providers (575) including 296 care home providers and 296 homecare providers.

Use of these digital technology was more common in organisations providing homecare services, and less common in those providing care home services (with or without nursing). For example, 40% of care home participants used digital rostering versus 81% of homecare participants. It was also more common in organisations employing 50 or more people to have digital care records in place (91% versus 86% with between 30-49 staff members) and for those accessing cyber security expertise from an internal team or a contracted external organisation.

DSPT status

Information was compiled at the sampling stage about the DSPT status of care providers, based on all the care settings or locations covered by each provider. This shows that over half of participants worked for care providers where all care settings or locations met DSPT standards when the sample was drawn in January 2024 (53%, rising to 64% among care homes), and a further 5% worked for care providers

where all care settings or locations were approaching DSPT standards. Three in 10 worked for care providers where none of the care settings or locations were registered with the DSPT (30%, rising to 42% among providers of homecare services), and a minority of one in twenty (4%) worked for care providers where DSPT status differed between settings. This variable was used to weight the data.

Table 3: DSPT status of participating care providers

	% of care providers (weighted profile)
Approaching Standards	5%
Standards Met	53%
Standards Exceeded	1%
Differ (defined as settings have different DSPT status)	4%
Not individually registered	30%
Not published	7%

When asked about their DSPT status as part of the survey, participants were more likely to report meeting or exceeding DSPT standards than the sample information showed. This is examined in chapter 6 on practices and behaviours.

2.3 Profile of care providers who participated in qualitative interviews

The 15 care providers who took part in a depth interview held a range of roles spanning senior leadership, operations management, business development, back-office, technology, and cyber security. Cyber security and resilience were core parts of 5 participants' roles, with one of these specialist roles created as a consequence of the provider experiencing a ransomware attack. The table below provides more details about the profile of the care provider organisations represented in the qualitative research.

Table 4: Profile of care providers who took part in the qualitative interviews

Quota and Profile	Number of Interviews
East Midlands Region	2
East of England Region	2
London Region	1
North East Region	1
North West Region	1
South East Region	3
South West Region	3
West Midlands Region	1
Yorkshire and The Humber Region	1
Experts	11
Learners	4
Care home services with nursing	4
Care home services without nursing	2
Domiciliary homecare services	5
Supported living services (excluding extra care housing)	2
Day care services	2
Care provider with 2 or 3 locations	3
Care provider with 4 or more locations	1
Care provider with one location.	11
Fully digital care provider	8
Paper only care provider	N/A
Care provider using paper and digital systems	7
Care provider who has not completed, not registered, published the DSPT	6
Care provider where DSPT compliance differs between settings	1
Care provider who has Approaching Standards on the DSPT	2
Care provider who has Standards Met on the DSPT	5
Care provider who has Standards Exceeded on the DSPT	1
Care provider who has experienced a cyber incident in the last 3 years	8
Care provider who has no experience of a cyber incident in the last 3 years.	7
Care provider who has no back-ups for data	5
Care provider who has back-ups	7
Care provider who where it is unknown whether they have back-ups	3

2.4 Research with technology suppliers

Fewer technology suppliers than hoped for participated in the survey and the qualitative interviews despite a range of avenues to secure wider involvement being tried, which are detailed in the technical report. The challenges faced in engaging with technology suppliers included:

- lack of named sample, meaning the survey had to be conducted using an open link approach
- technology suppliers feeling there was duplication of effort due to the significant work they had undertaken to evidence the DSCR standards for the Assured Solutions List not being accessed by this research
- technology suppliers having already responded to other research project requests
- long questionnaire – one technology supplier specifically fed back that they did not complete the survey because it was too long
- potential consequences of the survey – concern that any gaps identified would become expectations on the technology supplier to build into their offer without additional funding to do so

There were 16 participants in the technology supplier research: 3 participants completed both the survey and a depth interview, 6 participants completed the survey only, and 7 participants took part in a qualitative interview but did not complete the survey. Due to the limited number of participants in each research method, comments and observations have been made across the group as a whole.

Roles and responsibilities

The technology suppliers who took part in the research held a mix of roles spanning senior leadership, technology, governance and cyber security. Cyber security and resilience were a core part of 3 participants roles. Only one participant did not have cyber or IT security as part of their role.

Organisational context

Participating technology suppliers were commonly SMEs: 15 of the 16 technology suppliers met the SME criteria of less than 250 staff. Four of them had less than 10 staff.

14 of the technology suppliers' main base was in England. One technology supplier's main base was international and one was in another part of the United Kingdom.

There were commonly several years' experience of developing and supplying technology to the adult social care sector amongst the participants. 12 of the 16 technology supplier participants had operated in the sector for 5 or more years.

The products offered by technology supplier participants were Software as a Service (SaaS), with the exception of one organisation who was a supplier in the sector of services supported by technology. SaaS is application software hosted on the cloud and used over an internet connection by way of a web browser, mobile app or thin client. The SaaS provider is responsible for operating, managing and maintaining the software and the infrastructure on which it runs, with the application licensed on a subscription basis. 11 of the 16 participants provided care management systems and were members of CASPA. This reflected the agreed focus of participant recruitment.

About the technology suppliers

While being a small number of participants, the technology suppliers appeared to provide solutions to around a tenth of adult social care providers and engaged with a cross-section of sub-sectors. 12 of the 13 technology supplier participants who indicated the size of their adult social care customer base had more than 100 customers, with 2 of these participants having more than 1,000 customers. Six of the 7 technology supplier participants who shared the proportion of their business related to adult social care had more than 80% of their business in the sector. All participants supplied technology to independent care providers and 11 of the 16 participants supplied to local authority and/or NHS care providers. At least 11 of the 16 participants supplied technology to each of the sub-sectors of homecare, extra care and/or supported housing, and residential and/or nursing homes.

All 8 technology suppliers who took part in a depth interview stated their motivation for operating in the adult social care sector was purely a commercial one based upon identified gaps in the market and having relevant knowledge of the sector.

03

Threats and risks within the adult social care sector

3 Threats and risks facing the adult social care sector

This chapter explores the cyber risks facing adult social care providers. It focusses on the approaches care providers take to identify cyber security risks, the types of incidents they are most at risk from, and some of the risk factors inherent in the sector.

Summary

The most common approaches care providers reported using to **identify threats** is through risk assessments that include cyber security (62% reported carrying this out), testing staff awareness and response (41%) and/or carry out cyber security vulnerability audits (38%). The other ways to identify threats like penetration testing, and using specific tools for monitoring were less common. One in 6 care providers had not used any of the approaches listed in the survey to identify cyber security risks over the last 12 months.

Phishing was thought to be the main **type of incident care providers are at risk from**, and representatives and leaders thought that ransomware was the most costly. Technology suppliers identified unauthorised accessing of files or networks as the greatest cyber risk facing the adult social care sector.

There were concerns about a number of **risk factors** inherent to the sector that make care providers very exposed to cyber incidents. Low digital maturity, a poor understanding of risk and the likely impact of an incident, the sensitive financial information and personal data care providers hold, and the sector's reliance on a small number of technology suppliers contribute to this vulnerability.

3.1 Identifying threats

In the survey, care providers reported using a range of approaches to identify cyber security risks, in particular risk assessments (mentioned by 62%), testing staff awareness and response (for example via mock phishing exercises) (41%) and cyber security vulnerability audits (38%). A third of care providers used specific tools designed for security monitoring, such as Intrusion Detection System (32%).

One in 6 (17%) care providers said they did not use any of the approaches listed in the survey to identify cyber security risks, rising to around a third among those with no business continuity plan covering cyber security (36%), no formal policies covering cyber security (31%) and no cyber incident response plan (32%).

Figure 6 Approaches used by care providers to identify cyber security risks within the last 12 months

Base: Care providers (575)

Care providers' take up of measures to identify cyber security risks is higher than the data from the 2024 Cyber Breaches Survey, where only 3 in 10 businesses had undertaken cyber security risk assessments (31%, versus. 26% of charities) or said they had security monitoring tools in place (33%, versus. 23% of charities).

Care providers with a specific cyber security insurance policy were more likely to have conducted the following, compared to those with no cyber security insurance:

- a risk assessment covering cyber security risks (68% versus 50%)
- a cyber security vulnerability audit (57% versus 29%)
- used specific tools designed for security monitoring, such as Intrusion Detection Systems (49% versus 21%)
- used or invested in threat intelligence (35% versus 14%)
- penetration testing (32% versus 13%)

In addition, those with an internal cyber security expert team or individual, those accessing cyber expertise through a contract with an external organisation, from the BSBC programme or from digital support teams at an integrated care board (ICB) were more likely than average to have used many of the measures listed to identify cyber risks. This was reflected in the mean number of responses they gave: those accessing expertise from BSBC mentioned 3 responses on average, compared with 2 among all care providers taking part in the survey (mean number of mentions of 3.03 versus 2.08).

Care providers with 11 to 15 rules and controls in place were more likely to have used all the measures listed to identify cyber risks, compared with those with 6 and 10, or 1 to 5 rules and controls, as reflected by the mean number of responses provided by these groups (2.9, 1.22, 0.62 respectively, compared with 2.08 on average).

Finally, the mean number of approaches mentioned to identify cyber security risks was higher among care providers who experienced at least one type of incident over the last 3 years, compared with those who had not experienced any (2.36 versus 2.01).

Penetration testing

In the qualitative interviews, some care providers referenced penetration testing they had undertaken. They noted that this testing served multiple purposes:

- it helped the organisation understand how the workforce would react to a breach
- it kept the workforce aware of the organisation's cyber security policies and procedures
- it reminded the workforce to stay vigilant to potential breaches
- it highlighted to staff next steps in case of a potential breach

Three care providers in the qualitative interviews discussed carrying out penetration testing as an activity to identify weaknesses in their systems and prepare for a potential attack. All reported that this was an annual exercise. For example, one care provider explained they carry out 'cyber incident drills' once a year. In their small team this comprised of announcing an incident (verbally) and working through response plans together in a meeting setting. Two care providers discussed this being carried out by their security partner on a yearly basis. The penetration testing had given them confidence to deal with a cyber incident in future.

"Annually, we tend to have an external penetration test, social engineering engagement, so mock phishing exercises, things like that." – Care Provider

Another activity being carried out to identify cyber threats involved a care provider working with their technology supplier to run simulated phishing attacks. The test involved checking whether their email system would block the fraudulent link to prevent staff from accessing it and sharing personal data. In one test, the email system blocked the link, however, a member of staff forwarded the email to their personal email address, accessed the link on their personal device and shared their credentials. The participant provided this as an example of the attitudes they had observed within the care workforce; people try to be helpful, without sufficient scepticism about potentially fraudulent emails (attitudes and behaviours are discussed further in chapter 5 and 6).

"This goes back to this idea that people in social care want to be helpful and have this bit of naivety so, when you put that with a not great level of computer awareness, they'll say, 'I've had a message from somebody that seems to be important. The system won't let me answer it. I'll send it to my home address and do it that way." – Representative and Leader

Confidence in care providers' ability to identify threats

Representatives and leaders in qualitative interviews expressed some concerns around care providers' limited ability to identify cyber security threats. They attributed this to:

- providers' lack of understanding around cyber security risks and impacts more generally (discussed in chapter 5)
- among smaller care providers, the lack of dedicated staff resource to manage cyber security risks (discussed in chapter 10 about barriers)
- the (limited) transparency of technology suppliers and how much information they share with the care providers they work with. One representatives and leader noted that the cyber security breach that impacted the health and care software supplier Advanced in 2022, was not immediately

communicated to customers. There was a feeling from one representative and leader that a lack of communication from technology suppliers resulted in care providers not having an accurate understanding of how secure their systems were

"When the last cyber-attack happened, providers had been told by the supplier that everything was all safe and secure and I guess they kind of took their word for it. I don't think it's really possible for a provider to do proper due diligence, unless they've got an expert involved." – Representative and Leader

3.2 Types of incidents care providers are at risk from

Technology suppliers were asked to consider the types of cyber security risks their customers in the adult social care sector were most at risk from, in relation to the use of the technology, solution or service they supplied them with. They considered that the greatest cyber risk was the unauthorised access of files or networks by people outside their organisation, with 5 out of 8 technology suppliers reporting this in the survey.

Three out of 8 technology suppliers reported that computers becoming infected with other malware, denial of service attacks and computers becoming infected with ransomware were the other risks for their customers using their technology, solution, or service.

Table 5: Most likely cyber security risks faced by care providers using their technology, solution or service, according to technology suppliers

	Total (8 technology suppliers)
Unauthorised accessing of files or networks by people outside your organisation	5
Computers becoming infected with other malware (for example viruses or spyware)	3
Denial of service attacks, defined as attacks that try to slow or take down your website, applications or online services	3
Computers becoming infected with ransomware	3
Unauthorised accessing of files or networks by staff, even if accidental	2
Hacking or attempted hacking of online bank accounts	1
Phishing attacks, defined as staff receiving fraudulent emails, or arriving at fraudulent websites	1
Takeovers or attempts to take over your website, social media accounts or email accounts	1
Prefer not to say	2

Technology suppliers stated their main cyber vulnerabilities related to EUD configuration, ensuring timely application updates and patches, and staff behaviours and practices. The main risks were therefore ransomware, distributed denial of service (DDoS), unauthorised access of files, and phishing attacks. A successful ransomware attack was viewed as the costliest incident and phishing was the most frequent form of attack. The technology suppliers stated that a significant impact risk would be their Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) provider being subject to a cyber incident and availability being lost, though this was viewed as much lower probability of occurring. The main cyber

security risks facing the adult social care sector were also discussed with representatives and leaders in the qualitative interviews. According to representatives and leaders, phishing was the most common threat care providers were at risk from, and ransomware the most costly. For example, one participant said of insurance claims related to cyber crime, that a third related to business email compromises, another third related to cyber-crime, and less than a fifth were a ransomware attack.

“Everybody we talk to in the membership has had phishing attacks. It's just prolific really. So I think at that level they're as exposed as any other organisation in a way.” – Representative and Leader

Risk factors

The RER indicated that there are a set of characteristics of the adult social care sector which both increase and decreases cyber security threat levels, compared to other sectors, in particular: the highly fragmented sector, with care services provided by many private small and medium enterprises (SMEs), a core of corporate chains, and to a lesser degree third sector organisations and local authorities.

Representatives and leaders in the qualitative interviews agreed that care providers are very exposed to cyber incidents. This was linked to a range of factors inherent in the sector – and discussed throughout this report. This includes, a lack of time and capacity, lack of in-depth understanding of cyber security, the use of unsecure and personal email accounts, old hardware and legacy systems. These were all felt to contribute to the sector being vulnerable to threats. In particular, representatives and leaders felt the following factors put care providers at risk:

- the sector’s low digital maturity (as discussed throughout this report – particularly in chapter 5), which made it more vulnerable to external threats, despite the sector not being targeted more than others

"We talk a reasonable amount about organisational maturity, and I don't think we're at that level of maturity where the organisation realises that the data drives the organisation. Not the organisation drives the data. And I think, because of that, the risks are seen in a fairly superficial way." – Care Provider

- poor understanding of the risks, and the impact of the risks associated with cyber security (for example care providers underestimated how drastically a cyber incident could impact their business, see section 4.4)

“I think most of the providers are worried about, you know, is somebody going to send a spam email that actually asks them to make a payment for something for a couple of thousand pounds. That's going to hit them quite hard. But if all their systems are down, and they're going to be offline for a couple of weeks, I don't think they'd even have thought about it”. – Representative Leader

- the nature of the sensitive financial and personal data that care providers hold making them attractive to hackers

- the small number of technology suppliers within the sector, meaning the same solutions, for example, those on the Assured Solutions List, may be used by a large number of care providers. This led to the concern that if one technology supplier was victim of a cyber breach, this could impact a large number of organisations. In addition, one representative and leader was aware of cyber criminals specifically targeting technology suppliers with a wide reach across the sector, to cause maximum impact

"What we have seen is some groups will target mainly service providers or people who provide a platform because then they've got a chance to affect a much larger group of entities. So, loads of social care entities could be hit simultaneously as a result of an incident without there being anything to do with themselves" – Representative and Leader

- the motivations of technology suppliers working in the adult social care sector (see section 2.4), which could be perceived as 'fertile market', leading technology suppliers to prioritise financial gain over cyber secure solutions. This was also mentioned in the context of smaller care providers who may lack negotiating power to ensure that the systems they procure offer security as well as a good value for money

Technology suppliers and sector representatives and leaders also noted that care providers, particularly smaller ones, can underestimate the likelihood and impact of them or their digital supply chain being the victim of a cyber incident. For example:

- care providers may not be aware of the degree of operational dependency on a technology supplier. This can be compounded if the care provider uses multiple modules or applications for different functions from the same provider

- there are a number of vulnerabilities for care providers in relation to their information, communications and technology (ICT) setup, particularly if they are running applications on local servers, and configuration and use of ECDs (Enterprise Connected Devices). These would be dealt with in-house by a care provider or through contracted ICT service suppliers rather than the technology suppliers involved in this research

"Smaller care providers who typically have much less awareness, view that a cyber incident is unlikely to happen to them, and don't believe there will be too much cost or interruption to their business involved. They underestimate both the impact on service delivery, for example, ensuring correct administering or mediation, and the full cost of restoring systems and retrieving data." – Representative and Leader

04

Experience and impact of cyber incidents

4 Experience and impact of cyber incidents

This chapter explores care providers' experience of cyber incidents and the impact of these incidents. It first looks at the type and prevalence of the incidents experienced, the impact they had, and the estimated cost of these incidents. It then explores care providers' views of a hypothetical severe cyber incident and the potential impact this could have on their organisation and on the people they support. Finally, it provides the findings of the economic analysis on the costs of the 3 most prevalent types of incidents and looks at the impact of best cyber practices on the likelihood of experiencing an incident and the costs resulting from it.

Summary

Only a third of care providers reported experiencing a cyber incident or unsuccessful attack in the last 3 years (33%). There was a suggestion by representatives and leaders that this represented an underreporting of incidents due care providers not being aware of incidents that had happened, and/or the fear of reputational damage when disclosing incidents.

Of the care providers who had experienced an incident or attack:

- The most common type of incident was phishing (reported by 75% of providers who had experienced an incident). This was followed by just over a third who had experienced people impersonating their organisation in emails or online (35%).

- The incidents or attacks had been fairly infrequent – 41% of incident types reported by providers had happened once only in the last 3 years or roughly once a year Phishing attacks were the most frequent types of incidents, with over a third of phishing attacks (35%) being experienced at least once a month in the last 3 years.

- Just under half of the attacks originated from a third-party organisation (44%), and one in 5 originated within the care provider's systems (21%).

In terms of the impact on the care provider, over half of the incidents reported did not have any impact such as loss of revenue, reputational damage, impact on staff or service users (52%). Overall, the most common type of impact was having to commit additional staff time to deal with the attack (28%) and introduce new measures to prevent future breaches (28%). Only one in 7 incidents resulted in staff stopping their day-to-day work (15%). Similarly, over 3 in 5 incidents did not result in any outcomes for the care provider such as loss of files, damaged systems, or stolen money (63%). Incidents involving ransomware, malware or denial of service resulted in a greater number of overall impacts and outcomes for the care provider. Phishing attacks were the least likely to result in any of the impacts or outcomes included in the survey.

Looking at the costs, care providers spent an average of £2,575 to deal with cyber security incidents over the last 3 years. This figure includes organisations that did not report any incident (and therefore did not report any costs). Organisations that reported at least one incident over the last 3 years spent an average of £9,528 dealing with this or these incidents. The majority of organisations participating in the survey did not report any costs, however (median being £0), but the highest cost reported over the past 3 years cumulatively stood at £900,080, indicating a large range of costs is possible.

The vast majority of incidents (89%) resulted in actions being taken by the care provider. Three in 5 (61%) incidents resulted in the care provider carrying out training and/or communications to

staff, and half (50%) resulted in the care provider reviewing or updating their cyber policies and procedures.

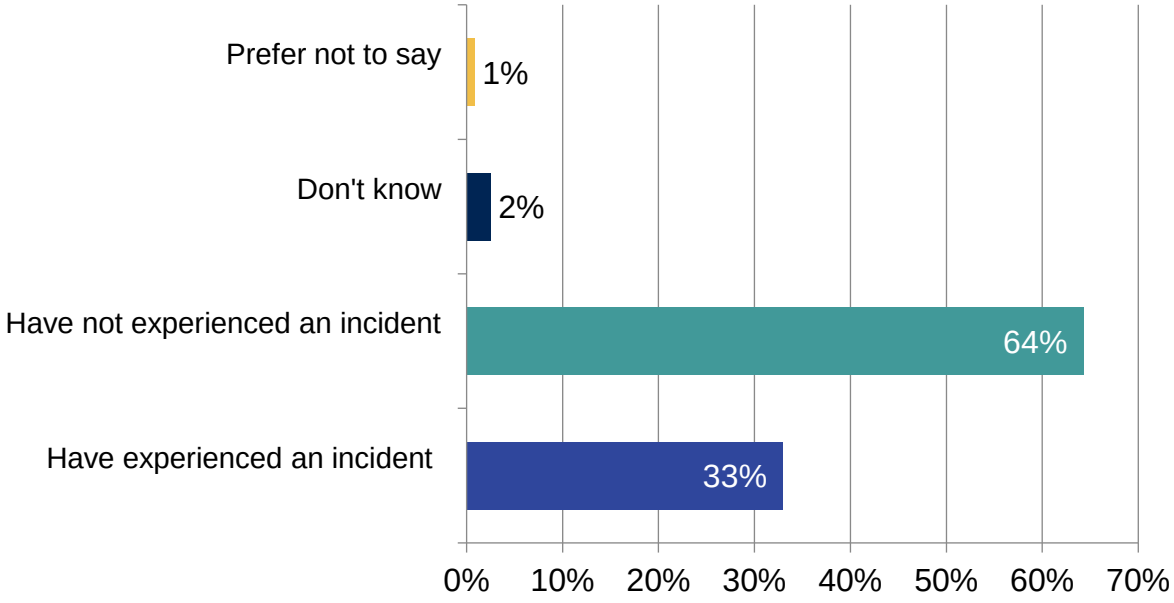
Care providers were asked about a hypothetical scenario where a severe cyber incident locked them out of their digital systems. In the qualitative interviews, care providers who were largely reliant on digital systems recognised that the impact could be large and widespread. In the survey, over 4-tenths (44%) of care providers estimated that it would take less than a day before this type of incident would impact service users. However, the majority (93%) of care providers were confident they would be able to avoid harm to service users if they experienced a severe cyber incident, including over half (55%) who were very confident.

4.1 Incidents experienced

Prevalence of incidents and near misses

In the survey, care providers were presented with a list of cyber incidents and asked if their organisation had experienced any of them in the last 3 years. Nearly two-thirds (64%) of care providers reported that their organisation had not experienced any incidents or unsuccessful attacks (for example near misses) in the last 3 years, compared to just over one-third (33%) who had.

Figure 7: Care providers' experience of cyber security incidents or unsuccessful attacks in the last 3 years



Base: Care providers (575)

For comparison, half of businesses (50%) and a quarter of charities (32%) reported in the 2024 Cyber Security Breaches Survey having experienced some kind of cyber security breach or attack in the last 12 months (note that the timeframe for the Cyber Breaches Survey question was shorter).

The proportion of care providers saying they have not experienced any incidents or unsuccessful attacks over the last 3 years was higher than average among organisations with fewer than 30 staff (87% for under 10 staff, 76% for 10 to 29 staff), organisations with only 1 to 5 rules or controls in place (79%), and those who do not back up their data (82%) (Note there is some overlap between some of these groups: 44% of care providers with 1 to 5 rules and controls in place do not back up their data (compared with

8% on average)). It is not possible to say whether they genuinely did not experience any incidents, or whether they did not actually identify those that happened.

The proportion of care providers who said they have not experienced a cyber incident over the last 3 years was also higher among those with a complete cyber incident response plan (73%), and among those exceeding DSPT standards (73%).

Care providers with ad hoc access to an external specialist were slightly more likely than average to report at least one incident over the last 3 years (40% did, compared with 33% on average).

In the qualitative interviews, there was some doubt expressed by representatives and leaders about the accuracy of these reported incidents. They were not surprised that a third reported that they had experienced an incident, but suggested that this was underreporting the number of attacks happening in practice. They felt that care providers may not be aware when incidents have occurred (hence low reporting). It was also suggested that the risk of reputational damage could hold back some care providers from honestly answering this question.

Types of incidents experienced by care providers

Of the care providers who had experienced incidents or unsuccessful attacks in the last 3 years, three-quarters (75%) had experienced phishing attacks – defined in the survey as staff receiving fraudulent emails or being directed to fraudulent websites. This was followed by just over-third (35%) who had experienced people impersonating their organisation in emails or online and just over one in 5 (22%) had experience of computers becoming infected with other malware (for example viruses or spyware), or an attempt to do so.

Figure 8: Types of incidents experienced by care providers in the last 3 years

Base: Care providers who have experienced a cyber security incident in the last 3 years (184)

In the 2024 Cyber Breaches Survey, among those who had experienced an incident, phishing was the most common type of breach and attack reported (84% for businesses and 83% for charities). This was followed by others impersonating organisations in emails or online (35% and 37%) and viruses or other malware (17% and 14%).

In qualitative interviews with care providers, technology suppliers and representatives and leaders, phishing attacks were thought to be the most common type of cyber security incident experienced in the adult social care sector. There was also a view that staff in the sector had at least a broad understanding of what phishing was, as it is discussed both inside and outside of the workplace, particularly in relation to personal digital services such as online banking. However, it was also identified as a difficult threat to manage and mitigate as it could target any staff member. Phishing attacks could also be highly sophisticated. For example, one care provider had received a phishing attack that looked like an Office 365 portal login, which was very convincing. Others suggested phishing attacks tended to be easy to spot due to mistakes such as poor spelling and incorrect company details.

Most costly incidents reported

Care providers which had reported more than 3 types of incidents were asked which 3 types were the most costly. For the questions about frequency of incident (presented in the next section) providers were asked about all types (if they experienced up to 3) or the 3 most costly types of incident if they experienced more than 3 types. Following the question about frequency, for questions about outcomes, impacts and costs providers were asked to think about the most costly incident of each type they had experienced (up to 3 types).

This means that data are reported about the most costly incidents experienced by each provider. Providers which experienced 3 or fewer types of incident and only had one incident of each type were reporting on all their incidents. Providers which experienced more than 3 types and/ or had more than one incident of each type would be reporting on their most costly incidents.

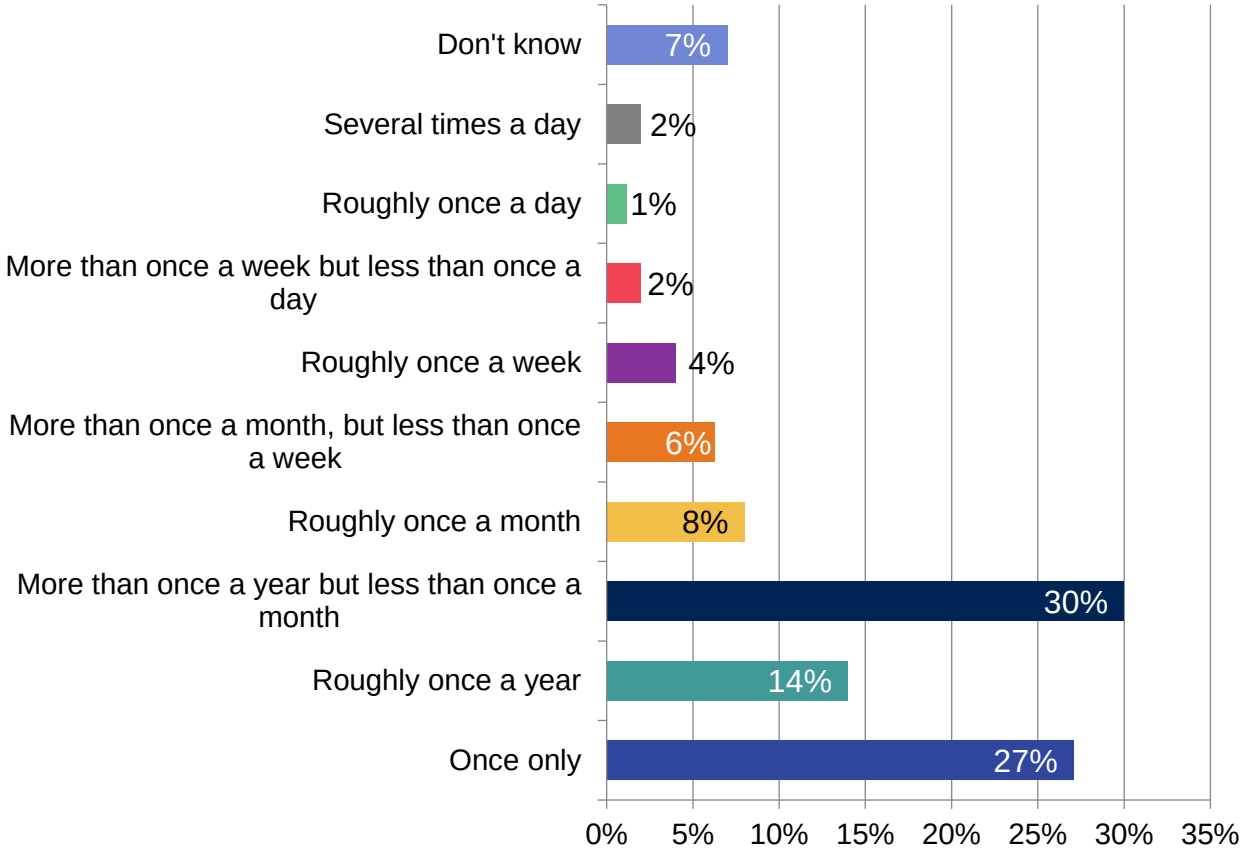
It should be noted that providers were asked about near misses as well as successful attacks. For providers which experienced successful attacks as well as near misses, since the focus was on the most costly, we expect they would be reporting on the successful attacks rather than near misses. However, providers which had only experienced near misses or had fewer than 3 types of successful incident were reporting on near misses in the questions which followed.

The mean number of types of incident reported by providers which reported any incidents was 1.9. Only 20 of the 184 providers reporting any incidents reported more than 3 types and were asked about which types were most costly.

Frequency of incidents identified

For each type of incident (up to the 3 most costly per provider) reported in the last 3 years care providers were asked how often incidents of this type happened. Looking at the frequency of the incidents reported by care providers, a quarter of incident types reported by providers happened once only (27%) in the last 3 years, and one in 7 types occurred roughly once a year (14%). Three in 10 incident types occurred more than once a year but less than once a month (30%). Around in one 10 incident types occurred once a week or more frequently (9%).

Figure 9: Frequency of cyber security incident types experienced by care providers in the last 3 years



Base: 292 incident types reported by 184 care providers

Phishing attacks were the most frequent types of incidents. Over a third providers (35%) which had reported phishing attacks as among their 3 most costly types of incident experienced this type of attack at least once a month in the last 3 years. Half of providers (49%) reporting ransomware, malware and denial of service attacks as among their most costly types of incident reported that each of these types of incident was experienced once only in the last 3 years. Just over 2 in 5 providers (44%) reporting the impersonation of an organisation in emails or online as one of the 3 most costly types of incidents, reported that this type of incident happened more than once a year but less than once a month.

Origin of incidents

Care providers classified as ‘experts’ were asked about the origin of the most costly incident(s) they reported (each provider could report up to 3 incidents focussing on the most costly types if they had experienced more than 3 types and the most costly of each type if they had experienced more than one incident of any type). Of the 289 most costly incidents reported on by experts in the survey, two-fifths (44%) originated in a third-party organisation (for example a technology supplier, internet provider or local authority), and one in 5 originated within the care provider’s systems (21%). For 3 in 10 incidents (31%), the origin was unknown.

4.2 Outcomes and impacts of incidents

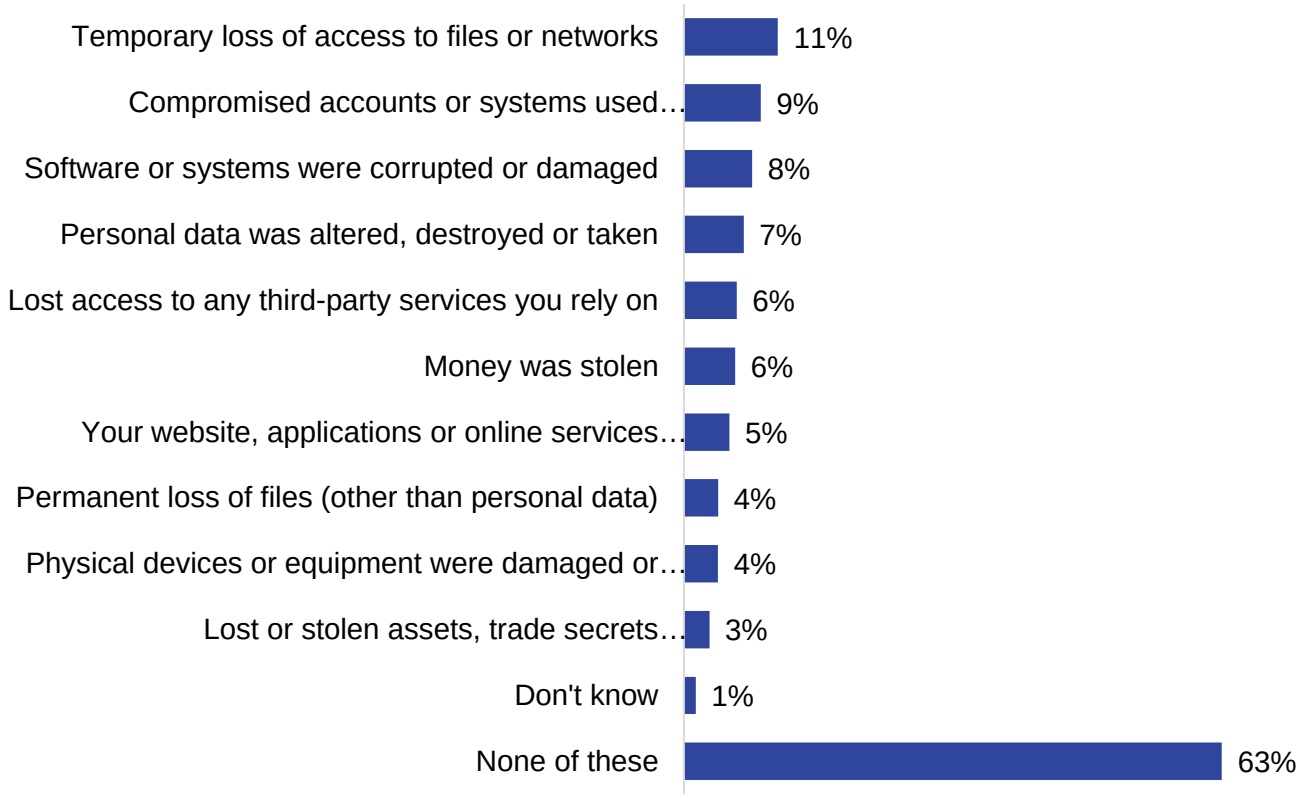
Outcomes of the incidents experienced

In the survey, care providers were asked to consider the outcome of the 3 most costly cyber incidents they experienced in the last 3 years. Across the most costly incidents reported on, the most common

outcomes were temporary loss of access to files or networks (11%), compromised accounts or systems used for illicit purposes (9%), damaged or corrupted software or systems (8%), and personal data being altered, destroyed or taken (7%). Over 3 in 5 of the most costly incidents (63%) did not result in any of the outcomes listed in the question.

For comparison, the 2024 Cyber Breaches Survey found that among the 50% of businesses that experienced a breach or attack, just over one in 7 (13%) experienced at least one negative outcome, such as a loss of money or data. Among the 32% of charities who identified a breach or attack, around one in 8 (12%) experienced negative outcomes. This compares to 36% of care providers which reported an incident reporting at least one negative outcome.

Figure 10: Outcomes of cyber incidents at care providers



Base: 292 incidents reported by 184 care providers classified as experts

Ransomware, malware or denial of service incidents resulted in more impacts overall (mean number of mentions of 1.64 of outcomes compared with 0.63 across all types of incidents reported on). The impacts faced as a result of these types of incidents included:

- temporary loss of access to files or networks (32% versus 11% across all types of incidents)
- software or systems being corrupted or damaged (28% versus 8% across all types of incidents)
- personal data being altered, destroyed or taken (22% versus 7% across all types of incidents)
- lost access to any third-party services (17% versus 6% across all types of incidents)

- website, applications or online services being taken down or made slower (17% versus 5% across all types of incidents)
- permanent loss of files (12% versus 4% across all types of incidents)
- physical devices or equipment being damaged or corrupted (19% versus 4% across all types of incidents)

Still, one-quarter (25%) of the combined ransomware, malware, denial of service incidents resulted in none of the impacts included in the survey. As above, phishing attacks were the most likely incident to result in none of the listed impacts (79% versus 63% across all types of incidents).

Incidents occurring in care providers that had an internal cyber expert team were more likely than average to result in a range of outcomes (mean number of 1.24 outcomes, compared with 0.63 on average), including the temporary loss of access to files or networks (21% versus 11% average), software or systems being corrupt or damaged (26% versus 8% average), personal data altered, destroyed or taken (14% versus 7% average), permanent loss of files (11% versus 4%), and physical devices or equipment being damaged or corrupted (9% versus 4%). It is likely that having access to an internal expert team on cyber security allowed for the full range of outcomes to be identified when these incidents occurred.

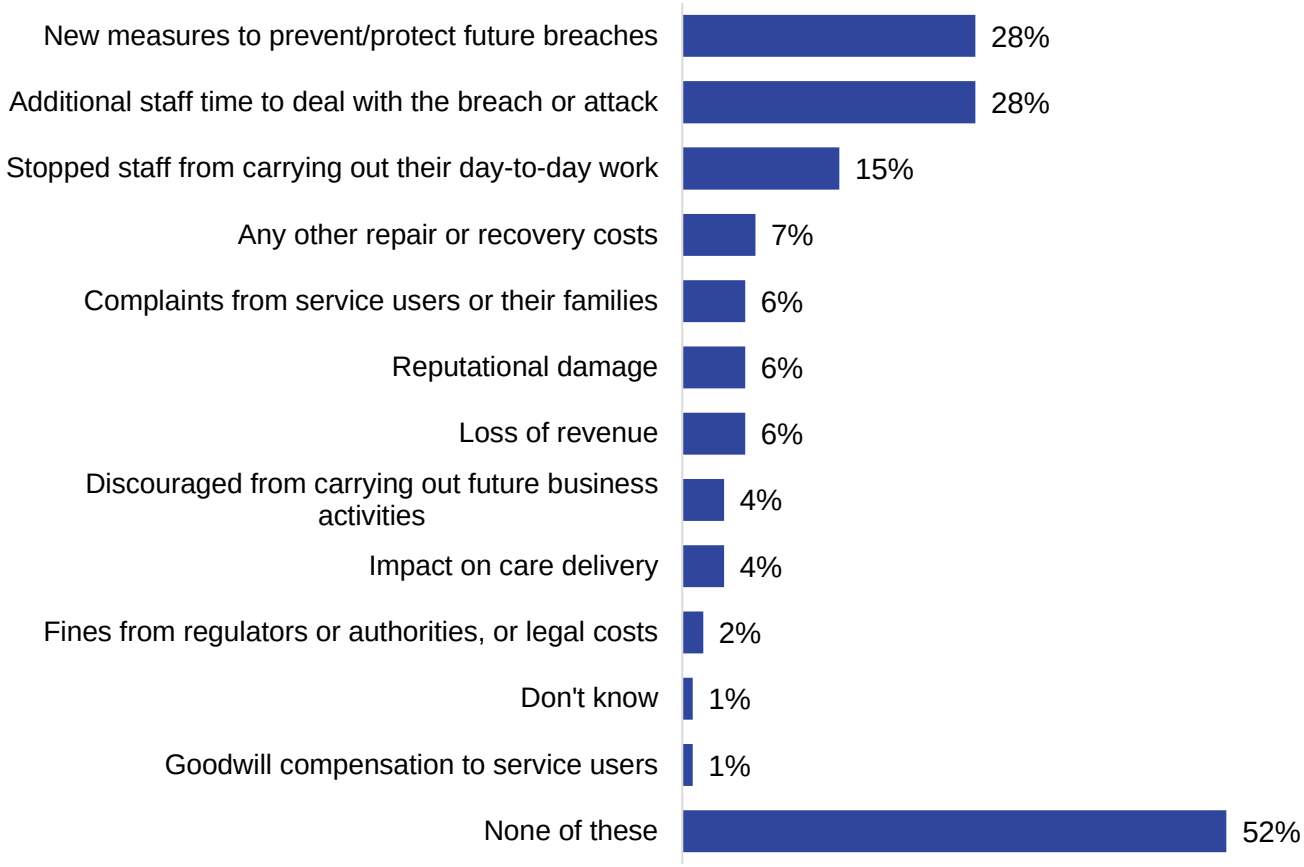
Qualitative interviews with representatives and leaders confirmed that while phishing was the most common type of incident, ransomware attacks were the most damaging for care providers. This was due to ransomware attacks rendering digital systems inaccessible until a ransom is paid.

“The most frequent ones we see are normal business email compromises, so phishing attacks. Normally that's in relation to cyber crime, transferring money from an entity to a third party. Around 33% of incidents that we see are business email compromises. Another 32% is cyber crime. Ransomware attacks are not necessarily the most frequent, so you're looking at late-teens, early-20s for that but the big actual financial impact is ransomware attacks.” – Representative and Leader

Impacts on care providers

In the survey, care providers were asked if the incidents they had experienced had impacted their organisation, using a list of possible impacts. Half of the most costly incidents reported on did not have any of the impacts listed on the question (52%). Over a quarter of the incidents reported on required additional staff time to deal with the breach or attack, or to inform service users or stakeholders (28%), and the same proportion required creating new measures to prevent or protect against future breaches or attacks (28%). One in 7 incidents reported on stopped staff from carrying out their day-to-day work.

Figure 11: Impacts incidents have on care providers



Base: 292 incidents reported on by 184 care providers

Incidents involving ransomware, malware or denial of service resulted in a greater number of overall impacts: only a third of incidents of these types reported on by providers did not have any impact (34% versus 52% on average across incidents of all types). These incidents were more like than average to have the following impacts:

- preventing staff from carrying out their day-to-day work (31% versus 15% across all types of incidents)
- loss of revenue (13% versus 6% across all types of incidents)
- other repair and recovery costs (18% versus 7% across all types of incidents)

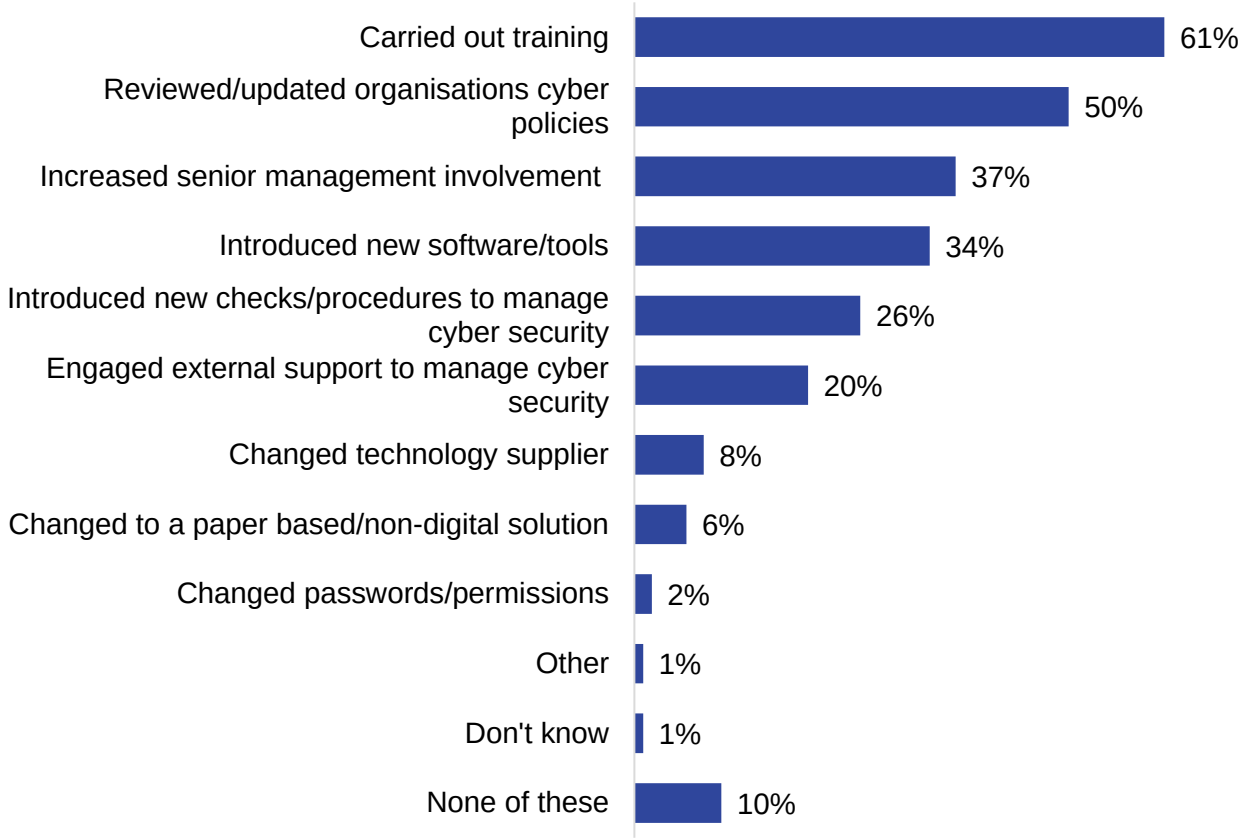
Phishing attacks were the least likely to result in any of the impacts included in the survey, with two-thirds (66%) of phishing attacks reported on not resulting in any impact, compared to the average (52%).

Data from the 2024 Cyber Breaches Survey found almost a quarter of businesses (24%) and two-fifths of charities (41%) that have had any breaches or attacks report being impacted in at least one of the ways noted above. This compares to 47% of care providers reporting an impact from any of the up to 3 most costly incidents they reported on. In the Cyber Breaches Survey, the 2 most common impacts are the same as the top 2 reported by care providers (additional staff time, and new measures).

4.3 Actions taken to prevent future breaches or attacks

Care providers who had experienced a cyber security incident were asked what they had done since then to prevent, or protect their organisation from, further breaches like the one they had experienced for up to 3 most costly incidents (of different types). The vast majority of incidents which were reported on (89%) resulted in actions being taken. Three in 5 (61%) incidents reported on resulted in the care provider carrying out training and/or communications to staff and half (50%) resulted in the care provider reviewing or updating their cyber policies and procedures.

Figure 12: Actions taken to prevent or protect care providers from further breaches



Base: 292 incidents reported on by 184 care providers

Many of the actions listed were more likely to take place where the incident occurred in organisations which had:

- at least 11 rules or controls in place (67% for training, 57% for reviewing organisation's policies or procedures, 40% for introduced new software or tools, 24% for engaged external support)
- Cyber Essentials or other nationally recognised certification (72% for training, 62% for reviewing organisation's policies or procedures, 49% for introduced new software or tools, 37% for introduced new checks and procedures)
- a complete incident response plan (79% for training, 78% for reviewing organisation's policies or procedures, 52% for increased senior management oversight, 44% for introduced new checks and procedures)

This was reflected by the larger mean number of mentions per provider of preventative actions following an incident in these groups of care providers (2.78, 3.14 and 3.64 respectively, compared with 2.44 across all incidents).

Actions taken to prevent future attacks or breaches depended on the type of incident faced. Those who had experienced impersonation in emails or online, takeover of website or social media reported they were more likely to increase senior management oversight and involvement in cyber security (52% versus 37% average). Ransomware, malware or denial of service attacks caused organisations to introduce new software and/or tools (48% versus 34% average), engagement with external support to manage cyber security (35% versus 20% average) and changes to the technology supplier (21% versus 8% average).

Data from the 2024 Cyber Breaches Survey found that among those that identified any breaches or attacks, two-thirds of businesses (59%) and a similar proportion of charities (70%) reported taking action to prevent further breaches – this is lower than in our survey (89% of reported incidents resulted in preventative actions). In the 2024 Cyber Breaches Survey a slightly larger proportion of businesses made technical changes (for example to firewalls, admin access or antivirus software) (30%), compared to internal management changes (for example to training or staffing) (24%). The reverse was true for charities, where 33% made internal management changes and 24% made technical changes.

In the qualitative interviews, discussion of specific incidents was limited as very few participants had experienced a significant incident (beyond a spam email that was quickly dealt with). The following examples were provided.

Example one: In a large care provider organisation, a new employee attempted to divert a senior manager's salary into a different account. The employee impersonated the senior manager via email and contacted the organisation's HR team, asking them to update their bank details. The HR team explained how the bank details could be changed on the system but the employee managed to convinced the HR team to update the details on their end. The HR team did update the bank details. However, the emails were flagged to the data protection manager before the next payment cycle which prevented the payment from being made.

The organisation estimated that this incident had costed the organisation £1,500 in staff time dealing with the incident, assistance from the payroll team and the data protection manager. Time was also spent training HR staff to make it clear that bank account details should not be updated based on an email. It was noted that if the incident had been successful the cost would have been considerably more expensive as the senior manager's salary would have been paid out twice.

"Had it been successful it would've [cost] more like £15,000, it would've been 10 times the impact at least because we would've had to essentially pay the senior staff member their wages twice, we would've had to write off the stolen money, and there would've been much more accounting and all the team follow up." *Care Provider*

Example 2: In 2023, a small homecare provider experienced an inability to access its digital financial data including its backup files and subsequently received a ransomware message. It is believed the data system was infected by malware likely due to a staff member "clicking on online links".

At the time of the incident, cyber security was not considered a high priority and it was not a significant consideration in the procurement of digital systems to help run its care management and back-office systems. Staff only had basic digital skills and the business was still reliant in part on paper systems.

The homecare provider sought support from its local authority commissioner and while helpful in terms of identifying sources of information and advice, the homecare provider handled the response internally. As there was no loss of personal data, the incident was reported to the police only, but no further action was taken as there was no contact with the criminals who sent the ransomware message. The homecare provider noted the DSPT team had been helpful in framing its recovery and supported greater openness amongst other care providers in sharing their experiences for mutual benefit and support.

The incident resulted in the loss of financial data which the provider was still in the process of recovering from over 12 months later, rebuilding its financial data records "from scratch".

“It was COVID time, so we were accessing all of our systems remotely. Some files were getting changed, but we just thought people were changing things because they're not that computer literate. The next week, all the files had different extensions and we couldn't access anything. Interestingly enough, they actually got into our backups as well.” *Care Provider*

4.4 Potential impact of a severe cyber incident on an organisation

In the survey and qualitative interviews, care providers were asked to imagine that their organisation experienced a severe cyber incident that locked them out of their digital systems, including any digital records, reporting systems and electronic medication administration record (eMAR) systems. They were then asked some questions about the potential impact of this hypothetical incident.

In the qualitative interviews, the level of impact predicted largely depended on how reliant the services were on digital technology. For example, care providers working largely digitally felt the impact could be large and widespread. These care providers recognised that this could result in: carers not being able to identify where their next address is (as rotas were not backed up by paper); having to make manual adjustments to ensure staff are paid properly; information about medications being out of date; potentially commissioners losing confidence in the service. One care provider felt that even if their digital systems went down for as little as 30 minutes, this could have a critical impact on their business.

“It would be quite a severe impact. We’d really, really struggle. Families won’t be updated and I think work would grind to a halt. That would have a massive impact on us. It could have a big impact as well if the commissioning agents caught wind of it. They’d be less confident in sending service users for assessment." – Care Provider

Others working largely with paper, felt the impact might be minor for ‘back-office’ staff, but the incident would be unlikely to impact care workers and service users.

“Things like sending emails to commissioners, family, friends, the company [might be impacted]. It could be things like accessing the documentation, the individual historic documentation, information, but that would be purely from a computer system perspective. Like in lots of care homes, people would continue.” – Care Provider

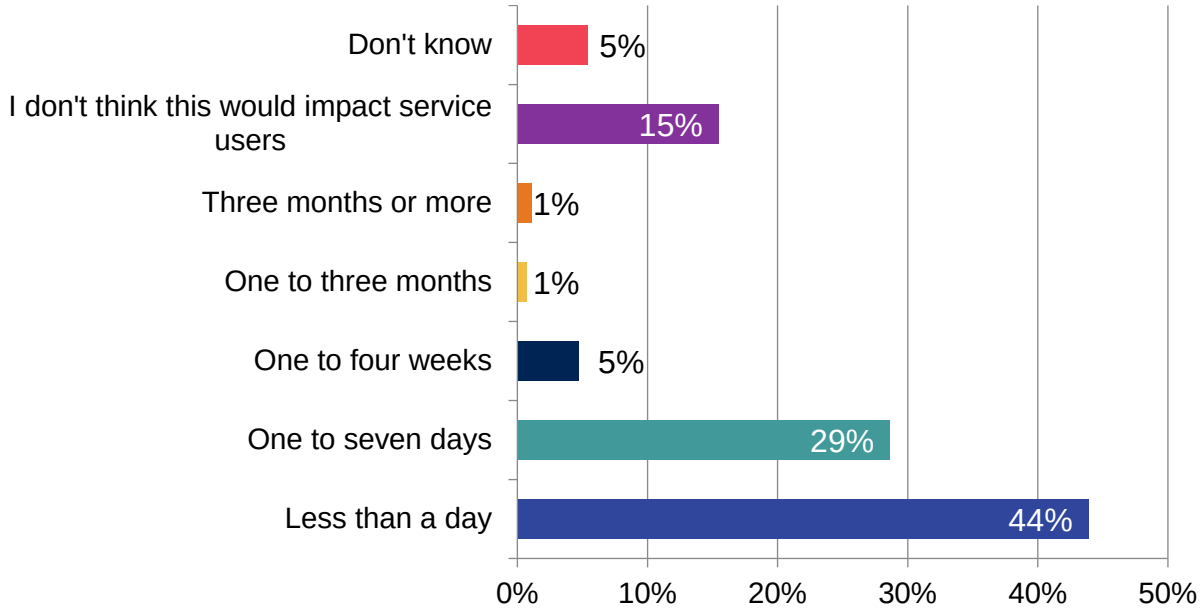
There was some indication that care providers in the qualitative interviews could be underestimating the impact of this hypothetical incident. For example, one care provider felt that because they worked across 3 separate systems, the event of all systems being unavailable would be unlikely. They therefore felt the likelihood and impact of such an event would be limited. On further discussion, it was apparent that the organisation’s rotas were only available on one system, so if that system was affected that could cause issues for their business (with care workers not being able to access their schedule).

"We've got information stored on [Microsoft] Teams that we've got stored on Birdie and CarePlanner. So, they would have to break into 3 individual systems for us to be completely wiped out of the information." – Care Provider

Length of time before the incident impacts service users

Care providers were asked in the survey to estimate how long it would take until a hypothetical severe incident could result in an impact on service users. Impact was defined as missed episodes of care, missed prescription renewals, diverted staff time impacting time spent with people. Over four-tenths (44%) of care providers estimated that it would take less than a day. Three-tenths (29%) said service users would be impacted one to 7 days after the incident. One in 7 (15%) didn't think this severe incident would impact their service users, rising to one in 5 (20%) among care providers with fewer than 30 members of staff.

Figure 13: Estimated time it would take for a severe cyber incident, which locked care providers out of all their digital systems, to impact service users



Base: Care providers (575)

Participants from homecare services were more likely than average to report that service users would be impacted in less than a day (49% versus 44%), and also more likely than care home providers and supported living providers (38% and 34% respectively).

Those more likely than average (44%) to say the severe incident would impact their service users in less than a day tended to be care providers already well versed into cyber security, for example:

- those who access cyber expertise from BSBC (57%) through the Digital Care Hub or with an internal cyber security expert team (53%)
- those with a complete cyber incident response plan (55%)
- those who say they exceed DSPT standards (59%)

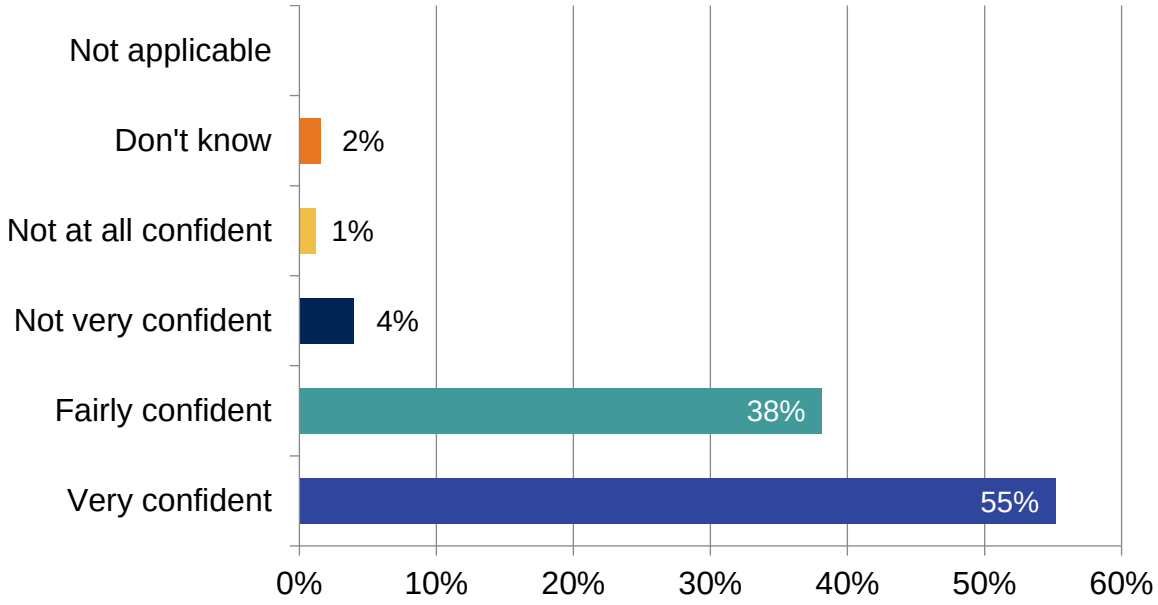
In contrast, care providers with one location only, or with fewer than 30 staff members, were more likely to think such incident would not impact their service users (17% and 20% respectively, compared with

15% on average). This could point to possible overconfidence in their ability to cope with a severe incident.

Avoiding harm to service users

The majority (93%) of care providers were confident they would be able to avoid harm to service users if they experienced a severe cyber incident, including over half (55%) who were very confident. Examples of harm could include missed medications or medical appointments, harms through lack of access to care records or poor staffing levels, and delays in hospitalisation. Only 5% said they were not confident.

Figure 14: Confidence that a care provider would be able to avoid harm to service users in the event of a severe cyber security incident



Base: Care providers (575)

Feeling very confident that the organisation would be able to avoid harm to service users in the event of a severe cyber incident was more common than average (55%) among certain groups:

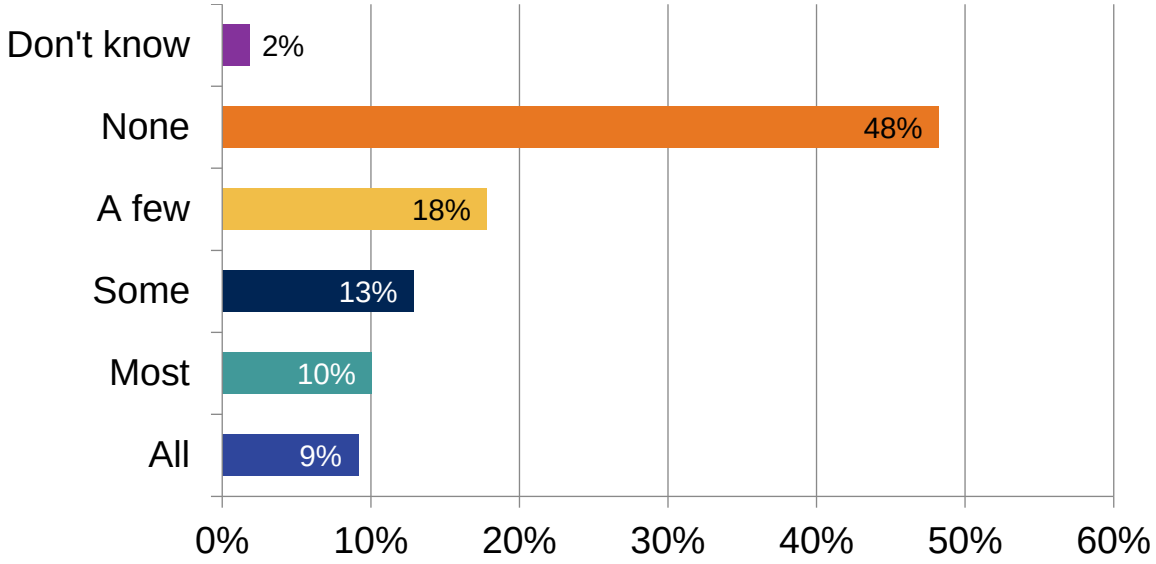
- those with an internal expert individual (65%) or with access to digital support teams at their ICB (74%)
- those with 11 to 15 rules or controls in place (60%)
- those who said they exceeded DSPT standards (63%)
- those with a business plan covering cyber security (58%)
- those with a complete incident response plan (64%)
- those with one location only (58%)
- those who said they have not experienced a cyber security incident in the last 3 years (61%)

Services users at a high risk of harm

Almost half (48%) of care providers reported that none of their service users would be at a high risk of harm in the 4 weeks following a severe cyber incident. Harm was defined as missed medications or

medical appointments, harms through lack of access to care records or poor staffing levels, and delays in hospitalisation. Conversely, 9% said all service users would be at risk of harm and just over one-in-10 (13%) reported that some would be at risk of harm.

Figure 15: Estimated number of service users who would be at risk of harm in the event of severe cyber incident



Base: All care providers who estimated a severe cyber incident would impact on service users in under 4 weeks (445)

Those saying none of their service users would be at high risk of harm during the first 4 weeks after the incident included:

- care homes providers (52% of them said so), compared to those working in homecare services (43%)
- organisations with fewer than 50 staff members (57% said of them so) compared to those with 50 or more staff (30%)
- care providers who accessed cyber security expertise through the digital support teams at an ICB (60%, compared with 48% on average)
- care providers who had not experienced an incident over the last 3 years (59%), compared to those who had (28%)

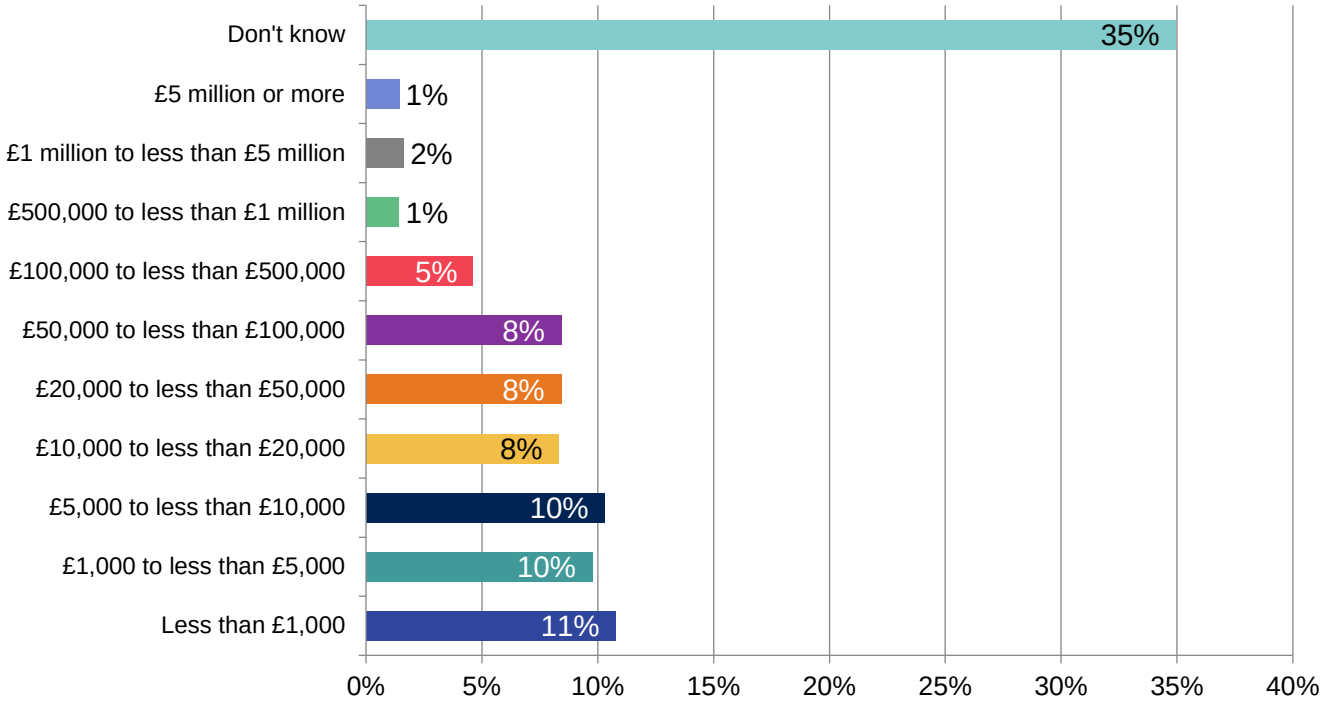
Financial impact

Turning to financial impact, over one-third (35%) of care providers did not know what degree of financial impact their business could shoulder before it would lose its viability, if a serious cyber incident was to occur.

Just over one-tenth (11%) reported they would only be able to shoulder less than £1,000.

One-tenth (10%) of care providers thought they would be able to shoulder between £1,000 and £5,000 and a further one-tenth (10%) of care providers stated would be able to shoulder between £5,000 and £10,000 before they would lose viability.

Figure 16: Estimated financial impact a business could shoulder, before it would lose its viability as a care provider, following a severe cyber incident



Base: Care providers (575)

Care providers employing fewer than 10 people across their care settings (24%), those without cyber security insurance (21%) and those with only 1 to 5 rules and controls in place (21%) were more likely to report that they would only be able to shoulder less than £1,000 before they would lose viability as a care provider (11% average).

Risks to care delivery if an incident occurred within the supply chain

In the survey, technology suppliers reported that a cyber security incident would most likely impact their ability to deliver their technology, solution or service to customers, and their reputation, with 7 of the 8 participating technology suppliers reporting each of these. Six in 8 technology suppliers reported a loss of data or intellectual property, and costs to recover from the incident as other likely impacts.

If a cyber incident was to occur, there was no consensus among technology suppliers regarding their ability to implement a short-term workaround lasting between one and 7 days if their technology, solution or service was not available to customers: 4 thought it could be done fairly easily, and 4 thought there would be some or great difficulty. The same lack of consensus was also observed when asking about longer workaround of 2 or more weeks: 4 technology suppliers thought it could be done very or fairly easily and 4 thought it would involve great difficulty.

4.5 Estimated costs of the incidents identified

In the survey, twenty care providers reported that their organisation had experienced more than 3 types of incidents in the last 3 years. They were asked which 3 types were the most costly. Phishing attacks, people impersonating their organisation in emails or online, and computers becoming infected with other

malware (for example viruses or spyware) received the largest number of mentions (16, 11 and 7 respectively, out of 20).

The survey then captured the costs of the different types of cyber security breaches or attacks on organisations in turn. Care providers which had experienced more than 3 types of incidents were asked to focus on the 3 most costly types. When a care provider had experienced a specific type of incident more than once over the last 3 years, they were asked to answer questions on costs thinking of the single most disruptive breach or attack of this type the organisation faced in the last 3 years. This means that providers with up to 3 types of incident and no more than one of each type were reporting on all their incidents. Those with more than 3 types or more than one incident of the same type were reporting on their most costly incidents. Across the 184 providers who had experienced an incident or near miss, 289 incidents were reported on at the cost questions. Only care providers classified as experts were asked detailed cost questions.

Different aspects of the cost were captured. These are detailed below.

Cost of staff time: First, care providers were asked about the costs of any staff time spent responding to an attack. This included, for instance, how much staff would have got paid for the time they spent investigating or fixing any problems caused by the breach. For half of the incidents reported on (50%), no cost of this kind was incurred, rising to 62% for phishing incidents but dropping to a third for ransomware, malware and denial of service attacks (34%).

Across the 289 incidents reported on by care providers in the survey where this kind of cost was incurred and could be provided, the average costs of staff time spent responding to the incident was £1,148, and the median was £250.The maximum cost of staff time a care provider reported spending responding to an incident was £20,000 and this was incurred as a result of a denial of service attack.

Payment made to attackers or stolen by attackers: Care providers were then asked for the approximate value of any payments made to attackers, intentionally or unintentionally, or stolen by attackers. Of the 289 incidents reported on, 83% did not involve any cost of this kind, and for a further 8% of incidents the respondent didn’t know if this type of cost had been incurred and/or how much it was. Looking at the 22 incidents where this kind of cost was incurred, the mean amount was £24,108 and median £500. The 2 most costly of these related to an incident involving unauthorised accessing of files or networks by staff for which only a range of costs was provided (£100,000 to less than £500,000 in payment made to or stolen by attackers), and an impersonation of the organisation by emails or online which resulted in payment made or stolen by attackers of £120,000.

Cost of incident response: Three-quarters of incidents reported did not incur any payments when the incident was being dealt with and in the aftermath, for example to external IT consultants, incident response, legal fees, and new post incident activities which they would not otherwise have undertaken. These costs may include actions taken by organisations following incidents to reduce the risks of future incidents. For a further 10% of incidents, the care provider didn’t know if such costs at been incurred or how much they were. Of the 39 incidents reported on where these costs were incurred and could be provided, the average cost was £13,083 and the median was £500. The maximum cost a care provider reported spending responding to an incident was £120,000 for an incident involving impersonation, and another provider estimated spending between £100,000 and £500,000 in incident response for unauthorised access of files by staff. These are the same 2 incidents that also incurred the highest payment to or stolen by attackers.

Cost of damage and disruption: The final cost care providers were asked about related to the value of any damage or disruption during an incident. This could have included the cost of any time when staff could not do their jobs, the value of lost files or intellectual property or the cost of any devices or equipment that needed replacing. No such costs were incurred for 7 in 10 incidents reported (71%) and for a further 11% the care provider could not say if these costs were incurred or how much they amounted to. The average costs of damage and disruption across the 44 incidents for which these costs were incurred and could be provided was £8,440 (mean £350), with a small number of incidents incurring very high costs. The maximum cost of damage and disruption reported were for 2 incidents involving unauthorised access of files and networks by staff. One provider incurred costs of damage and disruption of £15,000 as a result and the other estimated that the cost were between £100,000 and £500,000 (it was the same incident that also incurred this range of costs for payment to attackers and incident response).

4.6 Economic impact and cost analysis

Estimating the costs of cyber incidents of different types and overall

This section estimates the impacts and costs of cyber security incidents for care provider organisations, overall and disaggregated by specific types of incidents where data is available. In order to avoid burden during the survey, providers were asked for details about up to 3 incidents (focussing on the most costly) even if they had experienced more than 3. There was also flexibility about how detailed the information they provided was. The economic analysis involved making some assumptions and estimations based on the information given by providers. The box below provides further information about this for readers who would like more detail.

Detailed information on data and assumptions for economic analysis

Care providers which had experienced more than 3 types of incident were asked to report on the 3 most costly types of incidents they had experienced and then within each type the most costly individual incident. Most providers were reporting on all their types of incident as only a small number (20) had experienced more than 3 types. Care providers regarded as 'expert' reported on 4 different aspects of cost for the most costly of each type of incident. They were initially asked for the precise cost but it they were unable to provide this, they were asked for a range. 'Experts' which had experienced more than 3 types of incident were also asked about overall costs of any other incidents over the last 3 years not reported on individually. Note that if a provider had experienced more than one incident of a particular type but fewer than 3 types of incident they were not asked this overall question. Care providers regarded as 'learners' were just asked an overall question for the costs of up to 3 incidents using ranges (not split into 4 types).

The answers to these questions were used to derive a total cost of incidents for the provider over the last 3 years, adding up across cost types, and using an imputed value within each range for providers which answered using the ranges rather than a precise value (based on the median for providers which had given a precise value within that range, or the mid-point if no other costs within that range had been provided).

The average cost resulting from cyber security incidents for care providers over the last 3 years is £2,575. This figure includes care providers who did not report any incidents and care providers who reported at least one incident but whose cost was 0. The majority of organisations participating in the survey did not any incidents or did not report any costs, however (median being £0), but the highest cost reported over the past 3 years cumulatively stood at £900,080, indicating a large range of costs possible.

Excluding those organisations who did not experience a cyber security incident, average costs of cyber security incidents experienced over the past 3 years can be calculated as £9,528. This means that care providers who reported at least one incident over the last 3 years spent an average of £9,528 dealing with this or these incident(s). The median however is still £0.

Finally, if looking only at organisations which experienced incidents which incurred a cost (thus removing any incidents that reported a cost of £0, whether these be incidents that could be categorised as 'near misses' or incidents that simply did not result in any costs), the average cost of these over the past 3 years stands at £24,064, with a median cost of £650.

Table 6: Overall cost resulting from all incidents

	Number of care providers	Mean cost	Median cost	Minimum cost	Maximum cost	Std. Deviation for cost
Cost resulting from incidents (all)	514	£2,575	£0	£0	£900,080	41,272
Costs resulting from incidents for impacted organisations	139	£9,528	£0	£0	£900,080	79,155
Costs resulting from incidents which incurred any costs for impacted organisations	55	£24,064	£650	£5	£900,080	125,122

Looking at the most costly incidents, there were 8 incidents reported in the survey with estimated costs of £10,000 or higher. These are listed in the table below. They are various types of incidents, with 3 incidents related to unauthorised access and 3 caused by impersonation. None of the 8 most costly incidents were caused by ransomware. Note that the providers who reported these incidents sometimes reported additional incidents for which they also incurred costs over the last 3 years.

Table 7: Cost incurred by care providers for the 8 most costly incidents reported

	Cost of staff time dealing with the incident	Approximate value of any payments made to attackers, intentionally or not, or money stolen by attackers	Payments made when the incident was being dealt with for example external IT consultant, incident response, legal fees, new post-incident activities	Value of any damage or disruption	Estimated total costs of the incident incurred by the care provider who reported it
impersonation	£4,000	£0	£6,000	£0	£10,000
impersonation	£750	£6,000	£0	£6,000	£12,750

	Cost of staff time dealing with the incident	Approximate value of any payments made to attackers, intentionally or not, or money stolen by attackers	Payments made when the incident was being dealt with for example external IT consultant, incident response, legal fees, new post-incident activities	Value of any damage or disruption	Estimated total costs of the incident incurred by the care provider who reported it
malware	£10,000	£0	£3,000	£500	£13,500
unauthorised access by outsiders	£10,000 to less than £20,000	£0	£0	£0	£15,000
Denial of service	£20,000	£0	£0	£0	£20,000
unauthorised access by staff	£15,000	£0	£0	£15,000	£30,000
impersonation	£0	£120,000	£120,000	£3,000	£243,000
unauthorised access by staff	£80	£100,000 to less than £500,000	£100,000 to less than £500,000	£100,000 to less than £500,000	£900,080

Where information was provided in ranges a mid-point was used to create the estimated overall costs.

Sufficient data was available to provide more specific estimates of the impacts and costs of 3 types of cyber security incidents. For each of these incident types, the average cost to an organisation experiencing such an incident was calculated and, while not quantified, estimates regarding other impacts are also provided. The 3 types are:

- phishing: phishing attacks, defined as staff receiving fraudulent emails, or arriving at fraudulent websites, whether successful or not
- impersonation: people impersonating the respondent's organisation in emails or online
- malware: computers becoming infected with other malware (for example viruses or spyware), or an attempt to do so

The average cost of these 3 types of incidents are provided below in summary form. More detail on each is provided in the following sections. Reported figures account for the fact that many providers did not incur any cost from an attempted incident. These costs are calculated based on costs for a specific incident (up to 4 types of cost) with an annual cost calculated based on the reported frequency for that

type. The number of incidents per year assumed for each level of frequency is outlined in the next section.

Phishing incidents can be estimated to result in an average cost of £2,531 per year per organisation (across all organisations, including those not experiencing this type of incident). This calculation is driven by a high incidence rate of on average 8.95 phishing incidents or attempts per organisation per year, with average costs per impacted organisation of £283 per incident. It is worth noting that the cost data on which these estimates are based on the most costly phishing incident experienced by each organisation. Since many phishing incidents incur no cost and the incidence rate is high, it is likely that the average cost per year per organisation is an over-estimate of costs incurred across the sector.

Incidents of people impersonating the organisation in emails or online can be estimated to result in an average cost of £5,630 per year per organisation (across all organisations, including those not experiencing this type of incident). While the annual incidence rate of incidents of impersonation per organisation calculated is lower (0.85) than of phishing incidents, high average cost per incident of £6,624 increases the financial impact of such attacks. It is worth noting that the average costs per incident for this type is influenced by some occurrences of high costs. These costs could be outliers, however they could simply reflect the wide range of potential costs of an incident and the sometimes very high costs. The sample is too small to determine whether the incidence of very high costs in our sample for these types of incidents is representative.

Malware incidents resulted in an average cost of £182 per year per organisation (across all organisations, including those not experiencing this type of incident), driven by a low incidence rate of 0.16 incidents per year per organisation and average cost per incident of £1,139 resulting from malware incidents reported by impacted care providers.

4.7 Phishing incidents

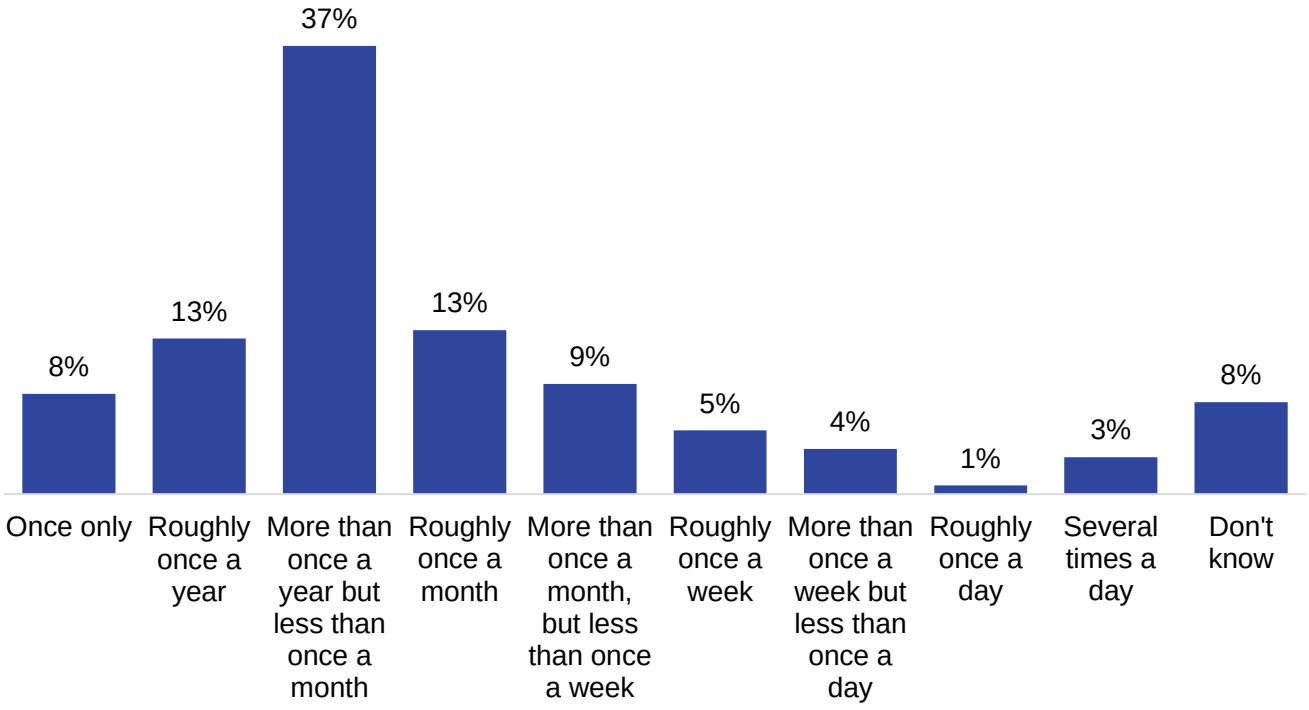
Incidence of phishing incidents

Phishing attacks (defined as staff receiving fraudulent emails or arriving at fraudulent websites) was the type of incident most commonly experienced by care providers responding to the survey, with 24% (139) reporting their organisation had experienced them over the past 3 years, whether successful or not. 73% (420) of all participants stated that they did not experience a phishing incident over the past 3 years, with the remaining 3% responding ‘Don’t know’, ‘Prefer not to say’.

Figure 17 further shows the frequency of phishing incidents in organisations that had experienced them, and where this type of incident was one of the 3 most costly types of incidents experienced by that provider over 3 years.

Please note that the base size is smaller than the number of care providers who reported experiencing phishing incidents as not all of them qualified for the detailed questions on the frequency, costs and impact of the incident. The same consideration applies to the other 2 types of incident included in the economic analysis.

Figure 17: Frequency of phishing incidents experienced in the last 3 years



Base: 134 care providers who reported having experienced phishing incidents in the last 3 years. Values do not add up to 100% due to computer rounding.

On the basis of these data and using the assumptions laid out in the methodology section, an approximate annual incidence rate of 8.95 phishing incidents per organisation can be calculated.

Cost of phishing incidents

The average cost of individual phishing incidents reported by care providers over the last 3 years was £283 (providers reported on the most costly phishing incident if they experienced more than one). Costs per incident varied between £0 and £7,500 (standard deviation = £896). However, the majority of incidents incurred no cost, with the median being £0. This indicates that the majority of reported incidents were unsuccessful phishing attempts. Considering only incidents that incurred a cost (values above £0), the average costs of individual phishing incidents experienced over the past 3 years was £960. It is important to note that this excludes not only unsuccessful attempts, but also potentially excludes successful attempts that simply did not incur any costs.

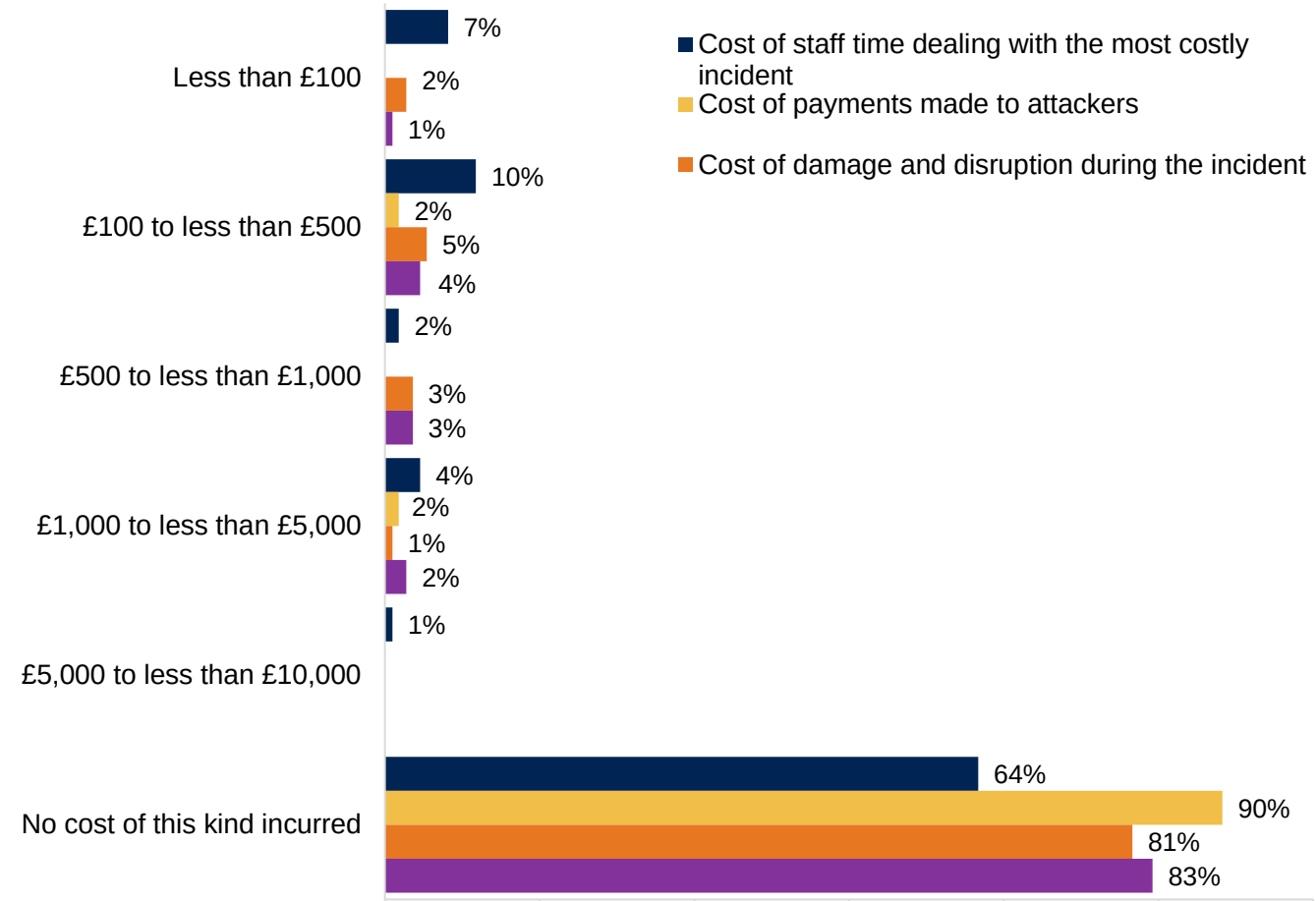
Table 8: Overall per incident costs resulting from phishing incidents

	Number of care providers	Mean cost	Median cost	Minimum cost	Maximum cost	Std. Deviation for cost
Costs resulting from phishing incidents	112	£283	£0	£0	£7,500	896

Multiplied with the annual incidence rate calculated above, this can be estimated to result in costs of £2,531 per year per organisation (across all organisations including those which did not experience this type of incident). It is worth noting that the cost data on which these estimates are based on the most costly phishing incident experienced by each organisation. Since many phishing incidents incur no cost and the incidence rate is high, it is likely that the average cost per year per organisation is an over-estimate of costs incurred across the sector.

When looking at the individual cost categories which make up the total (average) cost of a phishing incident experienced by care providers, it emerges that most of the costs resulting from phishing incidents were cost of staff time dealing with the incident. Less than one-fifth of respondents who experienced a phishing incident reported any costs associated with payments made to attackers or costs resulting from damage or disruption during or in the aftermath of the incident.

Figure 18: Cost incurred as a result of a phishing incident



	No cost of this kind incurred	£5,000 to less than £10,000	£1,000 to less than £5,000	£500 to less than £1,000	£100 to less than £500	Less than £100
Cost of staff time dealing with the most costly incident	64%	1%	4%	2%	10%	7%
Cost of payments made to attackers	90%		2%		2%	
Cost of damage and disruption during the incident	81%		1%	3%	5%	2%
Cost of damage and disruption after the incident	83%		2%	3%	4%	1%

Base: 133 care providers experiencing phishing incidents and providing cost data, considering the most costly incident of this type they experienced.
Categories not shown include '£10,000 to less than £20,000', '£20,000 to less than £50,000', '£50,000 to less than £100,000', '£100,000 to less than £500,000', '£500,000 to less than £1 million', '£1 million to less than 5 million', '£5 million or more'. Categories 'Don't know' and 'Prefer not to say' also not shown.

Beyond direct costs, few other impacts were reported by care providers experiencing phishing incidents. A majority (69%) of respondents experiencing a phishing incident did not report any impacts.

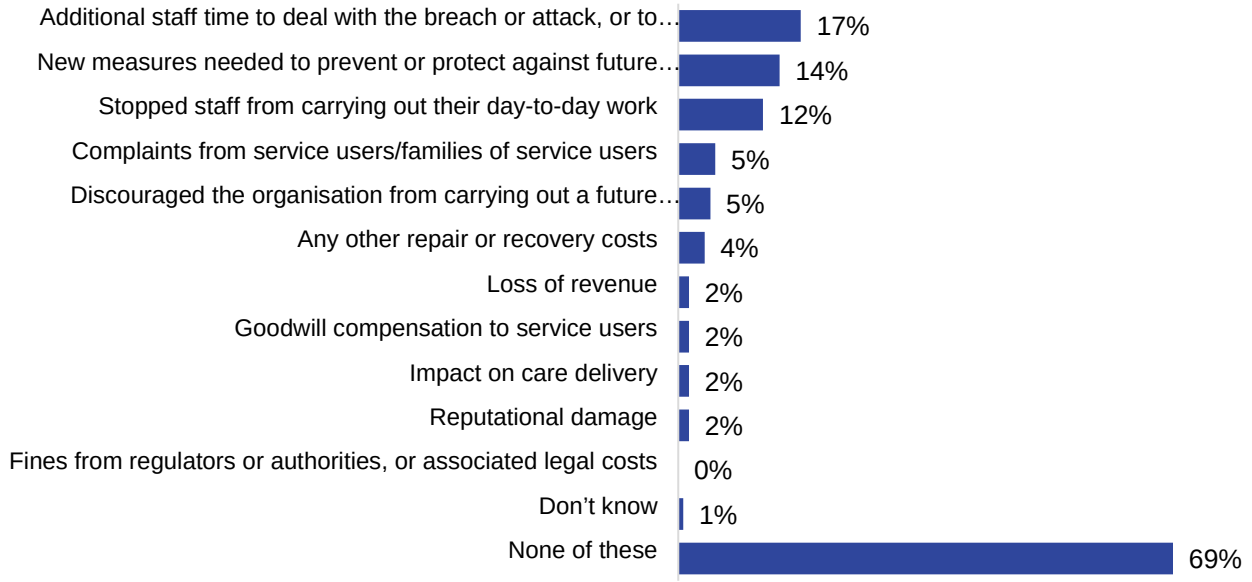
17% of respondents who had experienced a phishing incident reported that it required additional staff time to deal with the breach or attack, or to inform service users or stakeholders, and 12% reported that it stopped staff from carrying out their day-to-day work. This is in line with the findings above, highlighting the impact on staff time.

14% of respondents who had experienced a phishing incident reported new measures needed to prevent or protect against future breaches or attacks as an impact.

Few care providers who experienced a phishing incident reported it impacted on their services or business. 2% reported loss of revenue as an impact, 2% reported reputational damage, and 2% reported an impact on care delivery. 5% reported complaints from service users and/or families of service users and 2% reported that the incident resulted in goodwill compensation being given to service users. 5% reported that the incident had discouraged them from carrying out a future business activity they were intending to do.

4% of care providers who had experienced a phishing incident reported that it resulted in repair or recovery costs.

Figure 19: Thinking about the phishing incident, has this impacted your organisation in any of the following ways, or not?



Base: 134 care providers having experienced phishing incidents over the last 3 years, considering the most costly incident of this type they experienced

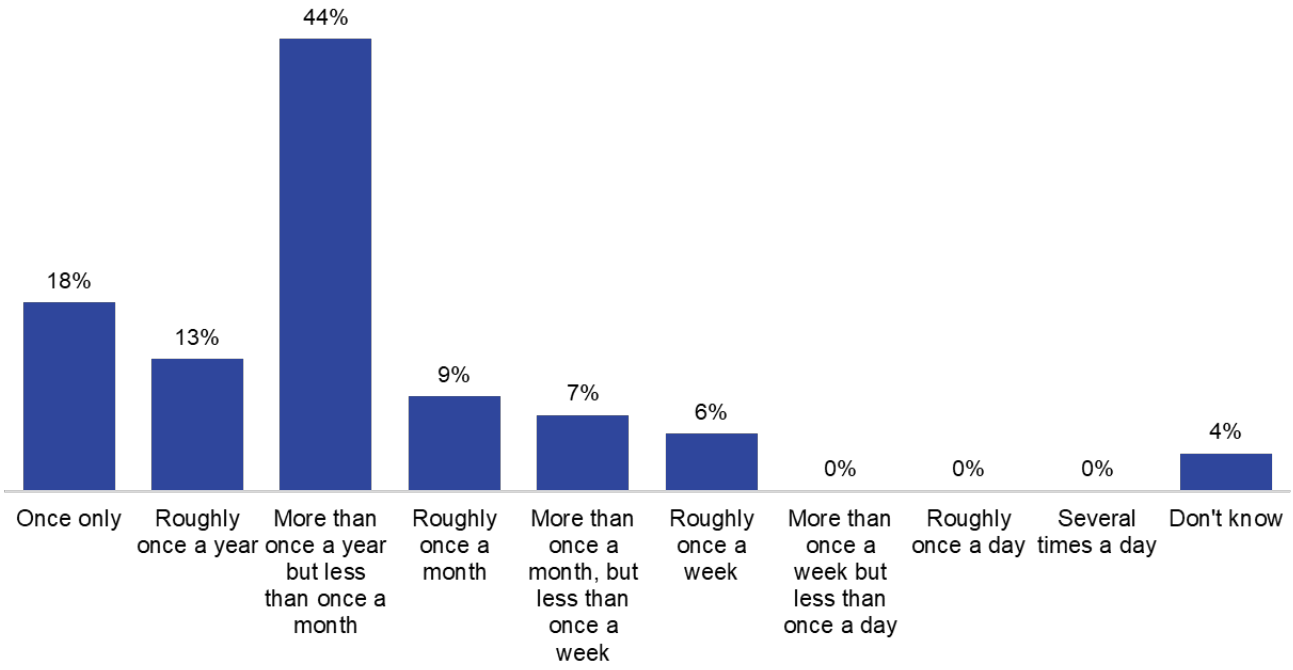
4.8 Incidents of impersonation in emails or online

Incidence of impersonations

The second most common type of incident experienced within the last 3 years by care providers in the survey (whether successful or not) was their organisation being impersonated in emails or online. This was experienced by 63 participants (11% of the sample). 86% (496) of all participants stated that they did not experience an incident of impersonation over the past 3 years, with the remaining 3% responding 'Don't know' or 'Prefer not to say'.

Figure 20 shows the frequency of impersonation incidents, for 55 care providers who were asked about it (please note that respondents were only asked to report on the frequency of incidents experienced for the 3 types of incidents which incurred the greatest costs).

Figure 20: Frequency of incident involving people impersonating the care provider's organisation in emails or online in the last 3 years



Base: 55 care providers reporting having experienced incidents of someone impersonating their organisation in emails or online.
Values do not add up to 100% due to 'Don't know' answers.

On the basis of reported frequency and following the assumptions laid out in the methodology section, an approximate annual incidence rate of 0.85 incidents of people impersonating the organisation in emails or online per organisation can be calculated.

Cost of impersonation incidents

The average cost of incidents of impersonation reported by care providers over the last 3 years was £6,624 per incident. Costs per incident varied between £0 and £243,000 (standard deviation =£36,573). The median was £0. Considering only incidents that incurred a cost (values above £0), the average costs of individual impersonation incidents experienced over the past 3 years was £153,400, with the lowest cost incident reported at £850. It is important to note that this excludes not only unsuccessful attempts, but also potentially excludes successful attempts that simply did not incur any costs.

Table 9: Overall per incident costs resulting from impersonation incidents

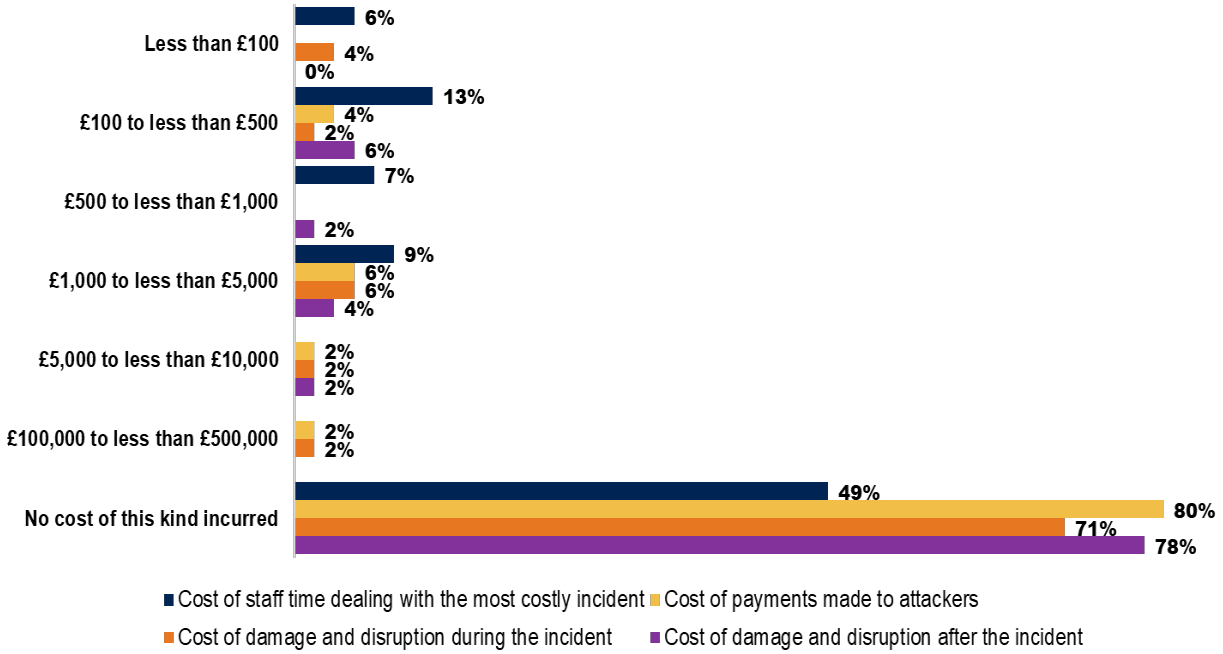
	Number of care providers	Mean cost	Median cost	Minimum cost	Maximum cost	Std. Deviation for cost
Costs resulting from impersonation incidents	44	£6,624	£0	£0	£243,000	36,573

Multiplied with the annual incidence rate calculated above, this can be estimated to result in costs of £5,644 per year per organisation (across all organisations including those which did not experience this type of incident).

However, it is important to note that the high variation in costs provided between individual cases (especially considering the small sample size) heavily influences the average cost. In particular, one case (the highest cost estimate provided, £243,000) is almost 20 times higher than the next-highest cost experienced. With this case removed, the average cost experienced per incident would amount to £1,127, and the average annual cost per organisation would stand at £958.

Figure 21 below shows the individual cost categories which make up the total (average) cost of an incident of people impersonating the organisation in emails or online experienced by care providers. As can be seen, costs arising from staff time spent dealing with the incident tend to be lower (below £5,000 per incident), with the big drivers to high costs for this type of incident being the cost of payments made to attackers and the cost of damage and disruption during the incident or in its aftermath.

Figure 21: Cost incurred by care providers as a result of an impersonation incident



	No cost of this kind incurred	Less than £100	£100 to less than £500	£500 to less than £1,000	£1,000 to less than £5,000	£5,000 to less than £10,000	£100,000 to less than £500,000
Cost of staff time dealing with the most costly incident	49%	6%	13%	7%	9%		
Cost of payments made to attackers	80%		4%		6%	2%	2%
Cost of damage and disruption during the incident	71%	4%	2%		6%	2%	2%
Cost of damage and disruption after the incident	78%		6%	2%	4%	2%	

Base: 55 care providers experiencing incidents of someone impersonating their organisation in emails or online. and providing cost data, considering the most costly incident of this type they experienced.

Categories not shown include ‘£10,000 to less than £20,000’, ‘£20,000 to less than £50,000’, ‘£50,000 to less than £100,000’, ‘£100,000 to less than £500,000’, ‘£500,000 to less than £1 million’, ‘£1 million to less than 5 million’, ‘£5 million or more’. Categories ‘Don’t know’ and ‘Prefer not to say’ also not shown.

Higher proportions of care providers reported other direct impacts as a result of incidents of people impersonating their organisation (via email or online) than in the case of phishing incidents.

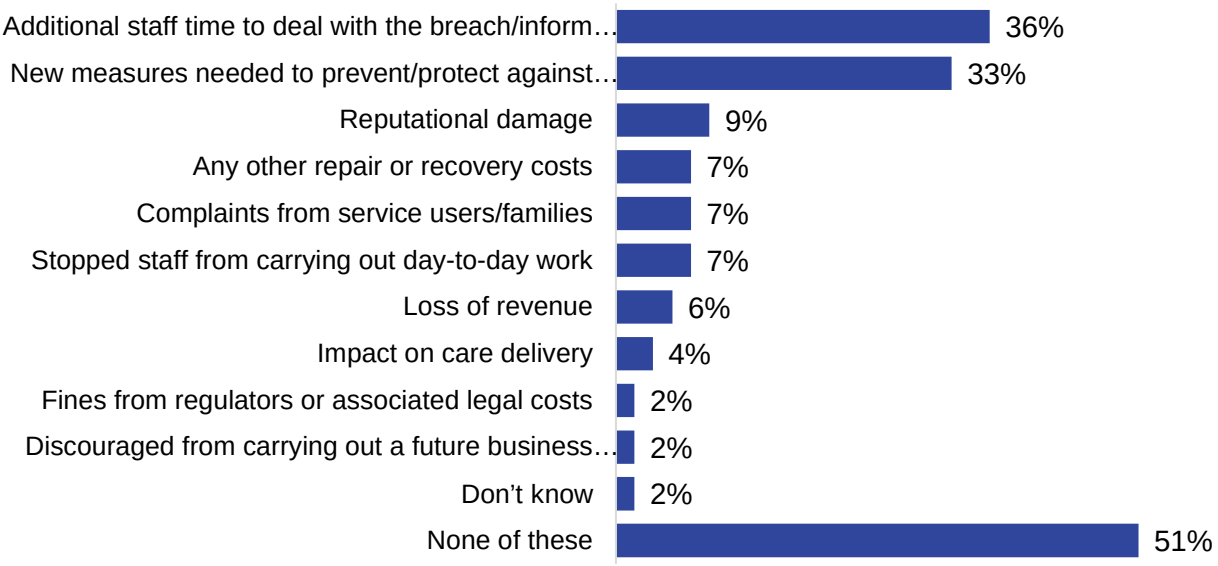
Over a third (36%) of respondents who had experienced an incident of impersonation reported that they it required additional staff time to deal with the breach or attack.

A third (33%) of respondents who had experienced an incident of impersonation reported new measures needed to prevent or protect against future breaches or attacks as an impact.

9% reported experiencing reputational damage as a result of the impersonation attack, and 7% reported complaints from service users and/or families of service users.

7% of respondents who had experienced a phishing incident reported that it resulted in repair or recovery costs.

Figure 22: Thinking about the impersonation incident, has this impacted your organisation in any of the following ways, or not?



Base: 55 care providers having experienced an incident of impersonation, considering the most costly incident of this type they experienced

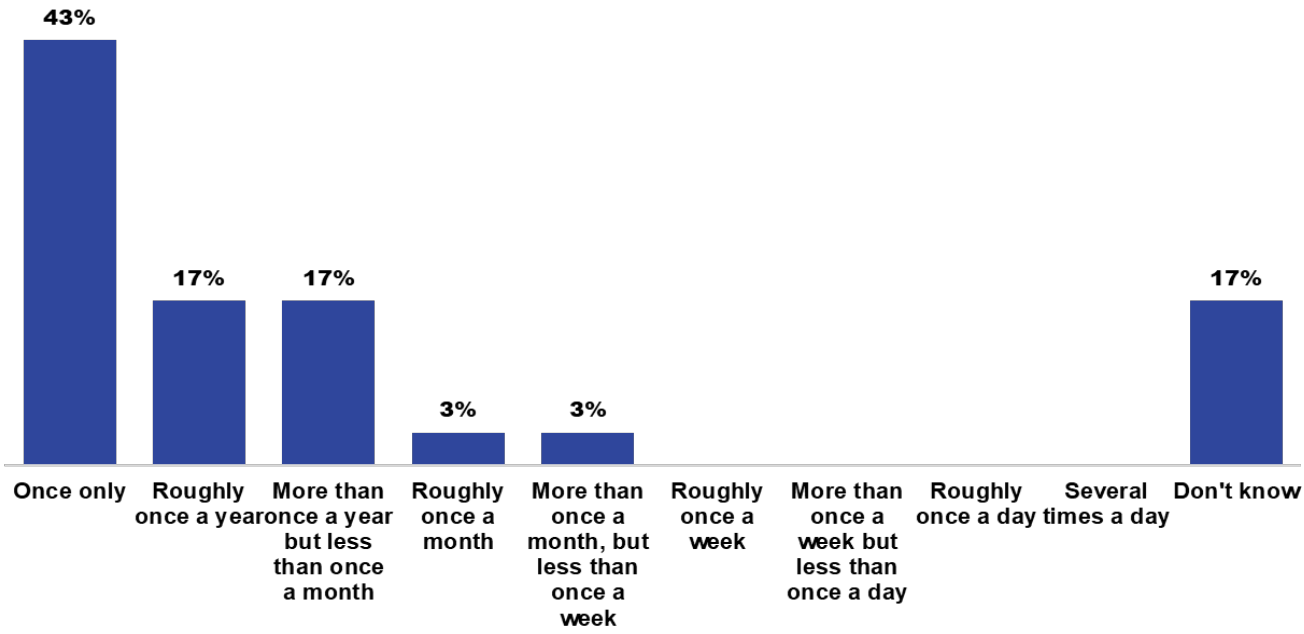
4.9 Malware incidents

Incidence rates of malware incidents

The third most common incident type reported by care providers responding to the survey were incidents of computers becoming infected with other malware (for example, viruses or spyware) or an attempt to do so. 7% (n=40) of participants had experienced such an incident (or an attempt) in the past 3 years. 90% (519) of participants did not experience such an incident over the past 3 years, with the remaining 3% responding 'Don't know' or 'Prefer not to say'.

As can be seen in Figure 23 incidents of computers becoming infected with other malware or an attempt to do so are rare, with 43% of care providers who experienced them saying it only occurred once in the last 3 years and 17% reporting it happened once a year.

Figure 23: Frequency of malware incident in the last 3 years



Base: 30 care providers having experienced a malware incident. Values don't add up to 100% due to 'Don't know' answers.

Following the assumptions laid out in the methodology section, an approximate annual incidence rate of 0.16 incidents of computers becoming infected with other malware or an attempt to do so per organisation can be calculated.

Cost of malware incidents

The average per incident cost of a malware incident reported by care providers over the last 3 years was £1,139. Costs varied between £0 and £13,500 (standard deviation = £2,877). The median was £50. If looking only at incidents that incurred a cost above £0, the average costs per incident increase to £2,183. It is important to note that this excludes not only unsuccessful attempts, but also potentially excludes successful attempts that simply did not incur any costs. Only 12 incidents incurred a cost of more than £0 so the resulting costs should be treated as indicative.

Table 10: Overall per incident costs resulting from malware incidents

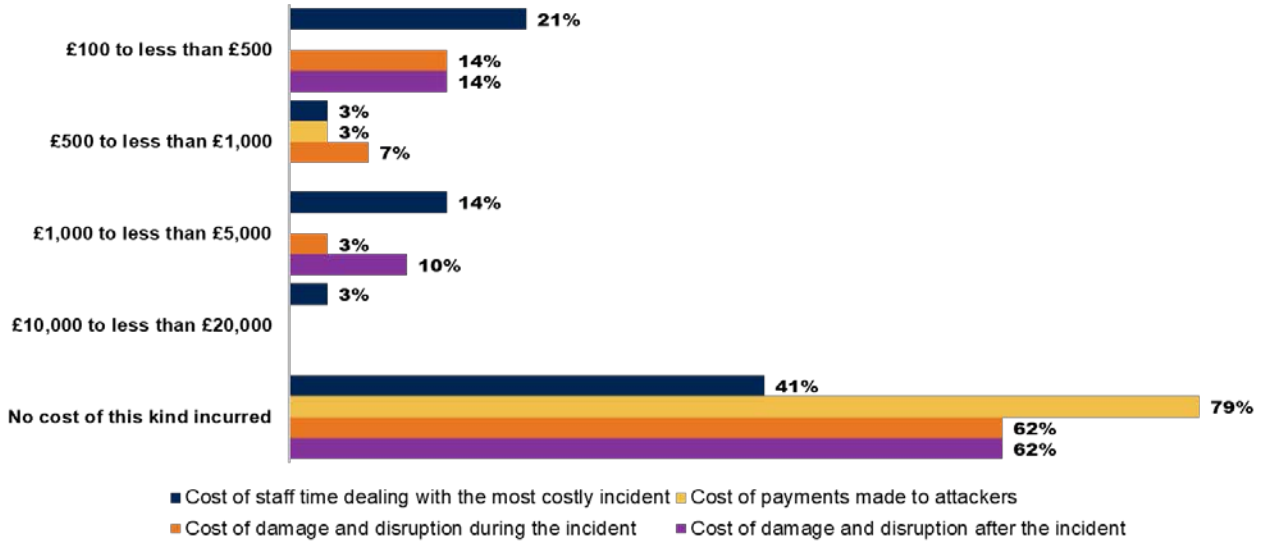
	Number of care providers	Mean cost	Median cost	Minimum cost	Maximum cost	Std. Deviation for cost
Costs resulting from malware incidents	23	£1,139	£50	£0	£13,500	2877

It is important however to highlight that the estimate of average cost is based on a very small number of observations and as such should be treated as indicative. This applies to all further estimates and cost data presented in this section.

Multiplied with the annual incidence rate calculated above, this type of incident can be estimated to result in costs of £182 per year per organisation (across all organisations including those which did not experience this type of incident).

When looking at the individual cost categories which make up the total (average) cost of a malware incident experienced by care providers, no clear driver to costs is noticeable.

Figure 24: Cost incurred by care providers as a result of a malware incident



	No cost of this kind incurred	£100 to less than £500	£500 to less than £1,000	£1,000 to less than £5,000	£10,000 to less than £20,000
Cost of staff time dealing with the most costly incident	41%	21%	3%	14%	3%
Cost of payments made to attackers	79%		3%		
Cost of damage and disruption during the incident	62%	14%	7%	3%	
Cost of damage and disruption after the incident	62%	14%		10%	

Base: 30 care providers having experienced malware incidents, considering the most costly incident of this type they experienced

Categories not shown include 'less than £100", "£5,000 to less than £10,000", "£20,000 to less than £50,000', '£50,000 to less than £100,000', '£100,000 to less than £500,000', '£500,000 to less than £1 million', '£1 million to less than 5 million', '£5 million or more'. Categories 'Don't know' and 'Prefer not to say' also not shown.

Beyond direct costs, most care providers (60%) who had experienced a malware incident reported other impacts.

Over a third (37%) reported that they it required additional staff time to deal with the breach or attack, or to inform service users or stakeholders, and 23% reported that it stopped staff from carrying out their day-to-day work.

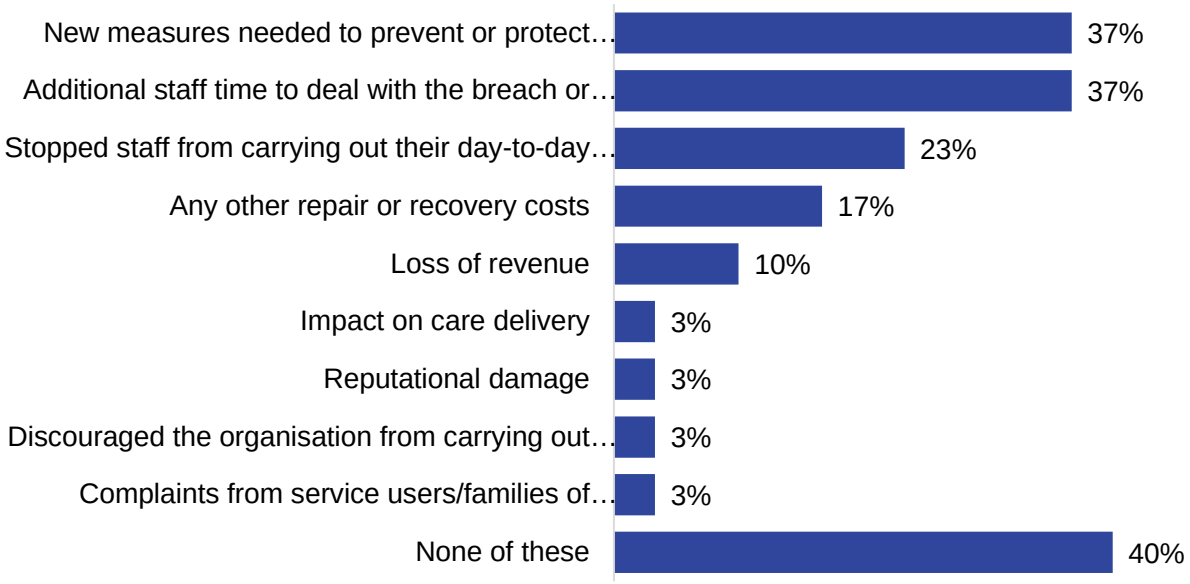
Over a third (37%) reported new measures needed to prevent or protect against future breaches or attacks as an impact.

17% reported that it had resulted in repair or recovery costs.

Only a few respondents who had experienced a malware incident reported an impact on their service or business activities with 3% reporting each of these: an impact on care delivery, complaints from service users and/or families of service users, reputational damage and a loss of revenue.

No fines or goodwill compensation being given to service users were reported.

Figure 25: Thinking about the malware incident, has this impacted your organisation in any of the following ways, or not?



Base: 30 care providers having experienced a malware incident. Participants, considering the most costly incident of this type they experienced

4.10 Estimating costs and savings of alternative scenarios based on best practice

A regression analysis was conducted to estimate the relationship between a range of best practices (policies, behaviours and systems in place) and the likelihood of experiencing a cyber security incident.

The majority of best practices reported by care providers did not have a statistically significant relationship with the likelihood of an organisation experiencing a cyber security incident.

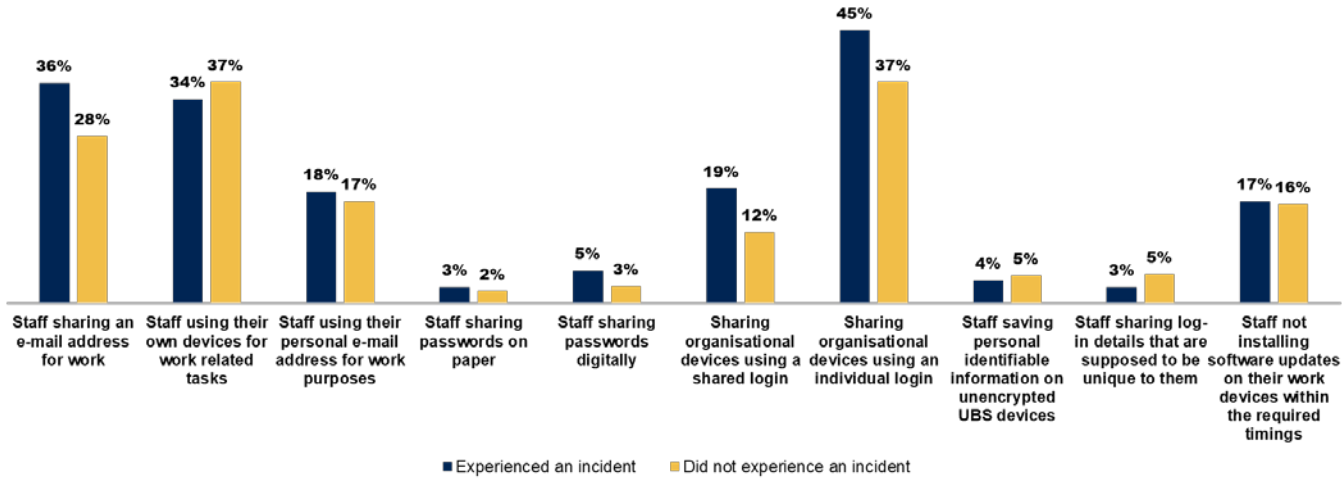
The exception to this is the frequency of occurrence of different (negative) staff behaviours. Based on an aggregated index score that represented a range and frequency of 'bad practices' within an organisation (such as staff sharing an e-mail address for work purposes, or staff sharing passwords on paper or digitally with each other), a higher score was associated with an increased likelihood of that organisation experiencing a cyber security incident, by 1.3% for each point increase in the index score. This was significant at the 5% level. This suggests, that discouraging staff from such behaviours carries potential for reducing risks of an incident.

78% of organisations that did not report any of these 'bad' practices occurring did not experience a cyber security incident over the past 3 years. However, over one-fifth (22%) of organisations that indicated that all specified 'bad' staff behaviours were occurring 'not at all frequently' still experienced a cyber security incident. By comparison, 39% of care providers who reported either high frequency of certain behaviours occurring, or a breadth of behaviours occurring to at least some level of frequency (receiving a score of at least 10 on the derived variable) experienced an incident.

A closer look at the individual behaviours reported, comparing those organisations that did experience an incident with those that did not, reveals that prevalence of most behaviours is equally common in both types of organisations. Staff sharing an e-mail address for work, sharing organisational devices using a

shared login and sharing organisational devices using an individual login was slightly more prevalent amongst organisations that have reported experiencing an incident.

Figure 26: Share of care providers having experienced or not having experienced an incident reporting behaviours occurring frequently



	Experienced an Incident	Did not experience an incident
Staff sharing an e-mail address for work	36%	28%
Staff using their own devices for work related tasks	34%	37%
Staff using their personal email address for work purposes	18%	17%
Staff sharing passwords on paper	3%	2%
Staff sharing passwords digitally	5%	3%
Sharing organisational devices using a shared login	19%	12%
Sharing organisational devices using an individual login	45%	37%
Staff saving personal identifiable information on unencrypted USB devices	4%	5%
Staff sharing log-in details that are supposed to be unique to them	3%	5%
Staff not installing software updates on their work devices within required timings	17%	16%

Base: 575 Care providers

When repeating the regression analysis to explore the impact of the individual best practices separately on the likelihood of an incident occurring, only one practice had a statistically significant effect: sharing organisational devices using a shared login.

Attempts to estimate the relationship between best practices and more granular frequency (incidence rates per incident type) did not yield any statistically significant results, likely due to the limited data available.

4.11 Estimating the impact of 'best practices' on cost

When attempting to estimate the relationship between the costs resulting from cyber security incidents as reported by care providers and a range of best practices, most of the practices did not have any statistically significant relationship with costs.

As for the analysis of likelihood of incidents occurring, a regression on costs of cyber incidents (or attempts) over the past 3 years reported by care providers, regardless of type (excluding 'Don't know' answers) did not show any significant relationships with the exception that increased frequency of certain (negative) behaviours is associated with increased costs of incidents. The regression results indicate that for each point increase in the index score for frequency of 'bad' behaviours, costs of incidents (cumulative, over the past 3 years) increased by £7,320 per organisation. This finding was statistically significant at the 5% level.

81% of organisations that did not report any of these 'bad' staff behaviours occurring reported not experiencing any costs (this includes organisations that did not experience a cyber security incident, and thus had no resulting costs). However, similarly almost three-quarters of care providers who reported either high frequency of certain behaviours occurring, or a breadth of behaviours occurring to at least some level of frequency (receiving a score of at least 10 on the derived variable) also said they did not incur any cost from cyber security incidents over the past 3 years (whether they experienced an incident or not).

The same analysis was conducted separately for the costs per phishing incidents, malware incidents and incidents of people impersonating the organisation in emails or online per organisation. As with the analysis of associations with overall costs (not disaggregated by incident type), most practices did not show any significant effect. While some weak trends did emerge in terms of associations between practices and cost per incident type, as described below, these should be interpreted with caution due to the low sample sizes for these analyses.

The number of measures taken over the last 12 months to identify cyber security risks in the organisation was found to have a positive relationship with the cost of phishing incidents, if they had occurred. Each additional identification measure taken (for example, conducting a cyber security vulnerability audit, a risk assessment covering cyber security risks, or penetration testing) was associated with an increase in costs of £498 per incident occurring ($p=0.638$). While a negative correlation could be expected, the direction of the relationship cannot be assessed and thus it is possible that the (higher) number of identification measures taken could in fact represent organisations' reaction to having experienced a phishing incident in the first place.

When looking at the cost from phishing incidents per organisation overall (thus including those who did *not* report a phishing incident), the estimated correlation between cost and number of different identification measures taken increases to an extra £554 for each additional identification measure taken. This finding is statistically significant at the 5% level. A likely explanation to this is that organisations having experienced (potentially costly) other types of incidents (considering the fact that other types of incidents had higher average costs) within the last 3 years responded with implementing several different identification measures to prevent such an incident happening again.

The number of good practices when contracting suppliers was found to have a relationship with the cost of incidents of people impersonating the organisation in emails or online per organisation. A unit-increase in the number of good practices when contracting suppliers was associated with an increase in costs of such incidents by £14,070 ($p=0.0993$). It should be noted that reported costs for impersonation

incidents varied considerably; removing the highest outlier from the analysis reduces the estimated increase in cost associated with a unit-increase in the number of good practices to £1,176.

As above, directionality (causation) of the relationship between these variables cannot be assessed on the basis of the data, and as such it can be hypothesised that practices when contracting suppliers changed (and thus 'best practice' is reported) after a costly incident happened.

When looking at the cost from incidents of people impersonating the organisation in emails or online per organisation overall (including those who did *not* report such an incident and thus did not report any cost), the same relationship was slightly smaller: a unit-increase in the number of good practices when contracting suppliers was associated with an increase in costs of such incidents of £9,973 (p=0.0935). An increase in staff training good practice was associated with an increase in the cost expected from a malware incident. A unit-increase in the number of good practices related to staff training was associated with an increase in costs of such incidents by £1,530 (p=0.0972). As above, however, the same hypotheses related to the directionality of the relationship between the variables can be assumed.

When looking at the cost of malware incidents (including those who did not report such an incident and thus did not report any cost), there were no associations with practices.

05

Awareness and perceptions of cyber security in the adult social care sector

5 Awareness and perceptions of cyber security in the adult social care sector

This chapter focusses on awareness and perceptions of cyber security among care providers. It first looks at knowledge of cyber security and access to expertise. It then focusses on organisational culture around cyber security.

Summary

There is a high level of self-reported knowledge of cyber security among care providers (90% reported they know a great deal or fair amount about it), and a recognition this has grown in recent years. However, the qualitative interviews highlighted some nuance around these high levels of knowledge – including some misconceptions around exposure to cyber risks and the likely impact of incidents, and concerns over the extent of cyber security knowledge and how widespread it is across the workforce.

Access to cyber security expertise varies; high proportions of care providers reported that they know where to go to access advice and expertise on cyber security (82%). The most frequently cited source of expertise was the use of external contracts with cyber security organisations (46%) and ad hoc access with external specialists (31%). Just over a quarter of care providers said they have their own internal expert (27%).

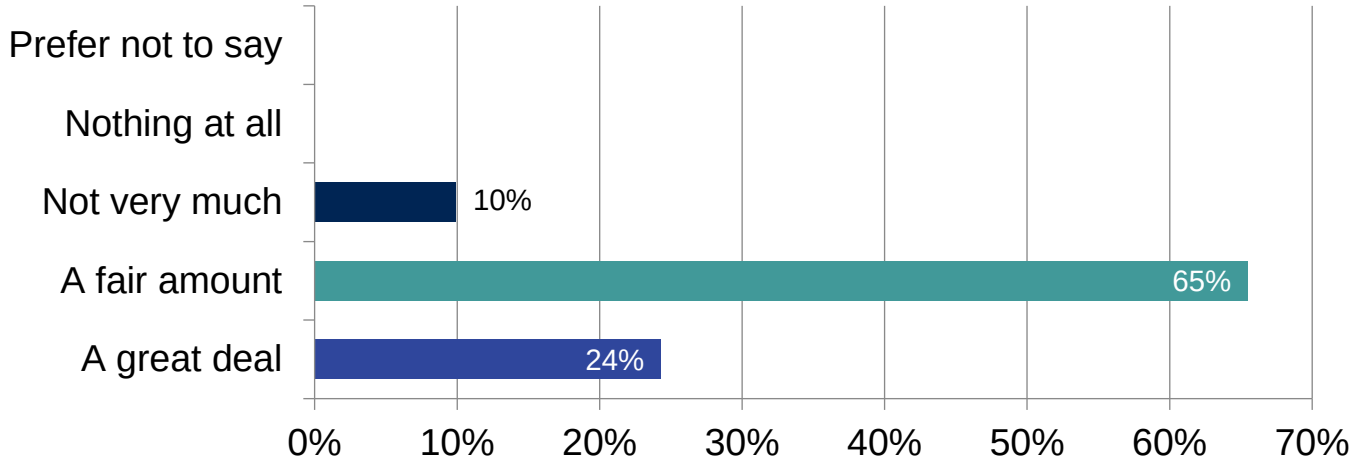
In terms of organisational culture around cyber security, in the survey cyber security is seen as a high priority for care providers (90% reported that it is a high priority), and there was agreement that good leadership and oversight of cyber security is in place within the majority of care provider organisations (around three-quarters of care providers agreed that there is strong leadership in cyber security planning and a cyber security strategy and vision). However, the qualitative discussions highlighted that providers faced many competing priorities, and sometimes lacked the resources required to commit to good cyber security practices.

In terms of the wider workforce, three-quarters agreed that their staff have the digital skills to securely use their digital technology or (77%). Again, the 3 audiences taking part in the qualitative interviews appeared less confident about this, pointing **to a low level of digital skills among some of the workforce.** This was identified as a major barrier to good cyber practices throughout this research.

5.1 Care provider knowledge and awareness

A high level of awareness of cyber security best practice was reported in the care provider survey. Nine in 10 care providers reported that they know a great or fair amount about good practice in cyber security for an organisation like theirs (90%). This includes a quarter (24%) who reported a great deal of knowledge. Only 10% said they do not know very much. This is related to the job responsibilities of respondents: the survey was aimed at the person responsible for cyber security and/or the commissioning of digital technology products or services within care provider organisations (see Chapter 2), and only 4% of respondents said cyber security was not part of their role.

Figure 27: How much care providers feel they know about good practice in cyber security for care providers



Base: Care providers (575)

Participants were more likely to report that they have a great deal of knowledge of cyber security if their organisation had mainly digital systems (31% versus. 24% on average); had an internal expert team (43%) or internal expert individual (32%); and had experienced an incident in the last 3 years (32%).

In the qualitative interviews participants generally reported that they themselves had a high level of awareness, which is to be expected as they were usually responsible for cyber security and/or the commissioning of digital technology products or services within their organisation. They defined cyber security predominantly in terms of information security – including maintaining secure digital systems and sharing information safely. Keeping networks secure, protecting service users' information, maintaining access to information that is stored digitally, monitoring internet traffic, protecting the organisation from phishing emails and hacking were all mentioned as features of cyber security.

"I would think of 2 aspects. One would be the keeping information secure in the sense of it not falling into the wrong hands…The other aspect of security is the danger that data could be compromised. It could be removed, disappear, our access to it could be hindered." – Care Provider

In the qualitative interviews, care providers reported that their awareness had grown in recent years, and they were still on this 'learning curve'. This was also noted in the interviews with representatives and leaders and technology suppliers who recognised that there had been good progress recently in raising awareness and improving approaches to cyber security in the adult social care sector. The main drivers for the increasing profile of cyber security reported in these interviews included:

- increasing use of digital systems within a care provider organisation
- recent initiatives like the Data Security Protection Toolkit and the BSBC programme
- people using digital technology in their day-to-day lives

"There has been a huge amount of work done through the BSBC programme and that has transformed the landscape in the context of that so I think for many organisations now they have an awareness of cyber security that they wouldn't have had without that programme." – Representative and Leader

However, representatives and leaders were more nuanced about care providers' knowledge and awareness of cyber security. Their experience was that it was variable, and that the barriers to gaining a comprehensive understanding of cyber security could be multifaceted. The nuances surrounding knowledge of cyber security included:

- the depth of knowledge around cyber security. Some representatives and leaders, technology suppliers, and digital leads in the care provider interviews suggested that getting policies and procedures in place was relied upon, but that a deeper understanding of cyber risks was lacking. Knowledge of cyber security was described as 'surface-level'. This is due to a range of contextual issues: cyber security is relatively new, priorities for care providers are diverse, resources are limited, and there are workforce considerations (see section 5.3 below)

- the level of risk and impact of a cyber incident. Representatives and leaders thought that there was good awareness of immediate issues such as theft of money, but poor awareness of the high risk of cyber threats, and the extent of damage that a cyber incident can cause (defined as system failures lasting significant periods of time). This is covered in more detail in chapter 4

- knowledge of the range of issues cyber security involves. Representatives and leaders, and some care providers, were concerned that although people in the sector can exhibit some knowledge of aspects of cyber security, they lack a sufficiently detailed and holistic view of data, cyber risk, and how these pertain to different aspects of their organisation

- the extent to which knowledge is widespread across the workforce. There was a strong view among all audiences that knowledge of cyber security was often concentrated with specific individuals (for example digital leads or owners and managers) rather than widespread across the workforce – many of whom may lack the digital skills to work in a cyber secure way (see section 5.3 below)

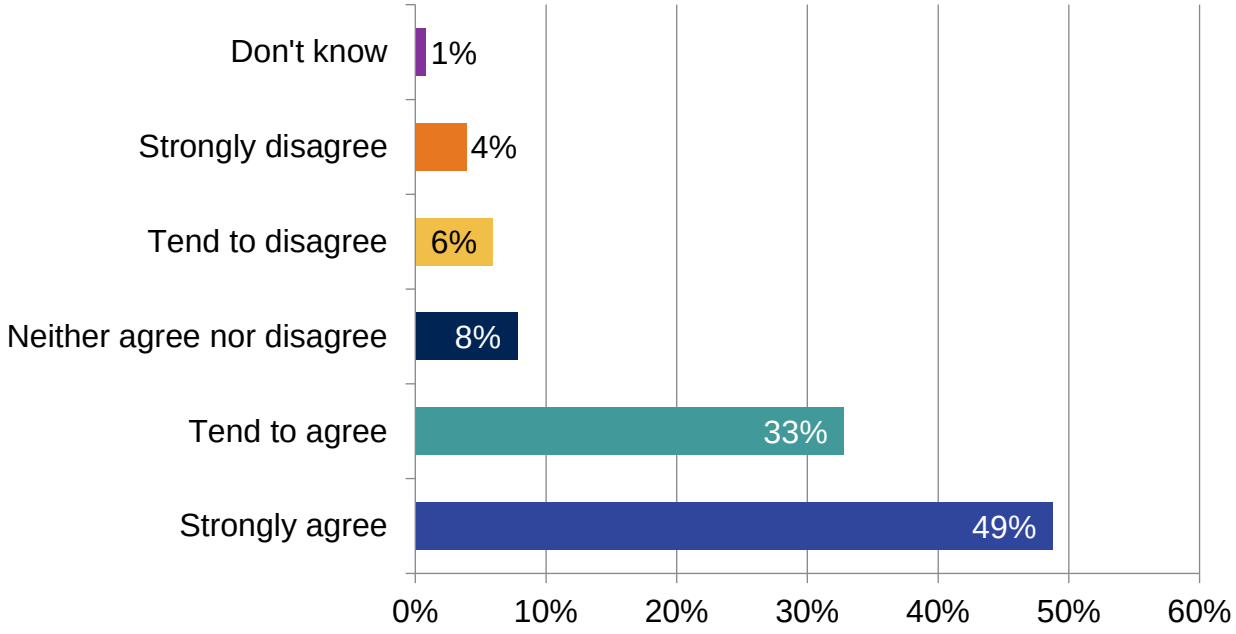
- the extent to which knowledge is widespread across the sector. There was consensus that knowledge is variable across the sector. This variation is not clear-cut – for example, one participant in the representative and leader interviews said they had observed that there are digitally mature homecare providers and some with 'absolutely nothing' in place to cover cyber security, with nothing 'in-between'. However, there was a strong view among representatives and leaders, and technology suppliers, that some smaller providers were much further behind larger organisations because they did not have the infrastructure in place to drive cyber security policies and practices. Participants noted there will be exceptions to this – for example, small but highly digital care providers. This variation between small and large providers is not observable in the survey data – suggesting the variation is more complex than a split between small and large providers

"I find people have a fairly surface-level knowledge, but don't really feel comfortable around the detail…[they] might have some things, like a basic policy around their IT support or some basic incident response policy. But if you ask in detail, you know, how are you managing mobile devices, or how are you talking to your staff about this? I don't necessarily see that as much." – Representative and Leader

5.2 Access to cyber expertise

In the survey, over 4 in 5 (82%) care providers agreed that their organisation knows where to go for advice and expertise on cyber security. This includes almost half (49%) who strongly agree. One in 10 (10%) disagreed.

Figure 28: Whether an organisation knows where to go for advice and expertise on cyber security

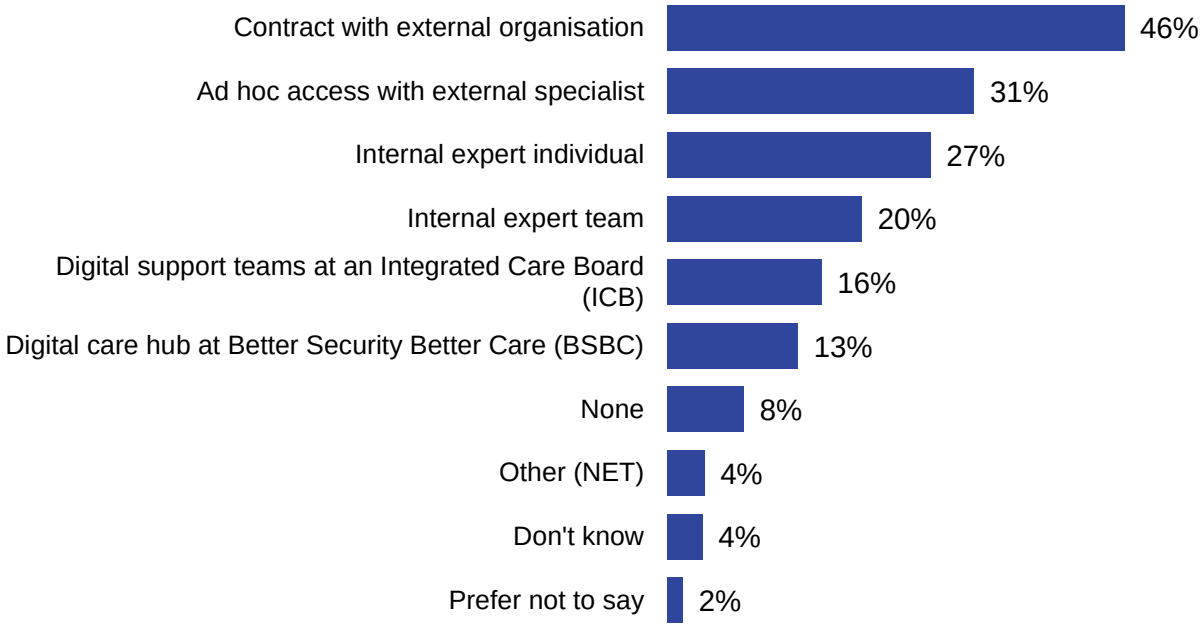


Base: Care providers (575)

Care providers who report having at least 11 rules or controls in place for cyber security (out of the 15 rules and controls asked about in the survey) were more likely than average to agree that they knew where to access expertise (91%). Those with an incident response plan were also more likely to agree to this (95%).

Care providers were asked how they accessed cyber security expertise. The source of expertise most frequently cited was the use of external contracts with cyber security organisations (46%) and ad hoc access with external specialists (31%). Just over a quarter of care providers said they have their own internal expert (27%) and one in 5 have an internal expert team (20%). A smaller proportion of care providers reported using digital support teams at an ICB (16%) or the BSBC programme (13%).

Figure 29: Types of cyber security expertise in care providers



Base: Care providers (575)

Accessing cyber security expertise via an external organisation or specialist is more common among some groups of care providers:

- access to external expertise increases with the number of staff a care provider has. For example, among organisations with fewer than 10 people, a third (33%) have a contract with an external organisation and less than one in 5 (19%) have ad hoc access to an external specialist, compared with 50% and 42% respectively for organisations with over 50 people
- access to external expertise is higher than average among care providers that have experienced at least one type of cyber incident over the least 3 years: 54% of them reported accessing cyber security expertise through a contract with an external organisation (versus 46% on average) or 39% reported ad hoc access with an external specialist (versus 31% on average)

Care providers who report having at least 11 rules or controls in place for cyber security (out of the 15 rules and controls asked about in the survey), and those who have Cyber Essentials or other nationally recognised certification, were more likely than average to say they access cyber expertise through a contract with an external organisation and/or internally (through an internal expert individual or team) as well as through BSBC at the Digital Care Hub.

Access to cyber security expertise was not covered in detail in the qualitative interviews. Two care providers talked specifically about a data security partner they had commissioned to oversee the organisation's cyber security policies and approach. These suppliers were working with the care provider to set up the management of cyber security procedures in the organisations, were advising them on how to improve cyber resilience, what they needed to do to complete the DSPT, and carrying out penetration testing.

"We've been talking to a data specialist company…to help us along the way…We've also got an IT guy that we've used for the last 6 or 7 years in house that is helping us set things up, and he's helped quite a lot." – Care Provider

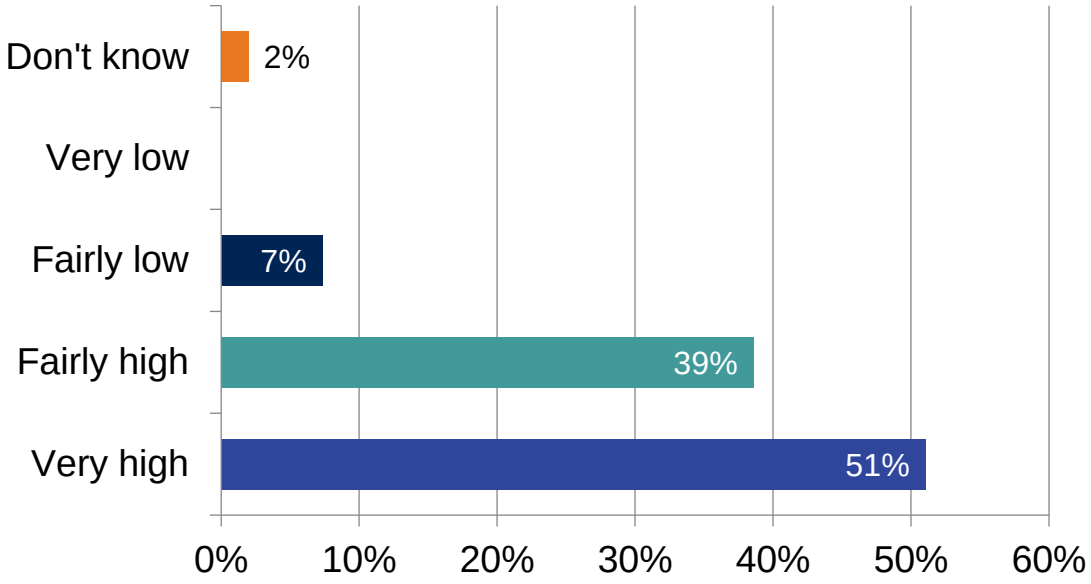
5.3 Culture around cyber security

Organisational culture was explored in the research in several ways: though exploring the extent to which cyber security is a priority for care providers, the leadership approach to cyber security within care providers, and views of the wider workforce's awareness and understanding of cyber security. This is explored below. Specific organisational practice and procedures in relation to cyber security within care provider organisations and how these are followed by the workforce is explored in the next chapter.

Prioritisation of cyber security

The overwhelming majority (90%) of care providers reported that cyber security is a high priority for their organisation's owners, directors and senior management, including over half (51%) who said it is a 'very high priority'. Just 8% stated it was a low priority. For comparison, in the 2024 Cyber Breaches Survey, 62% of organisations in the health, social care and social work sector reported that cyber security is a 'very high priority' for their directors, trustees, and other senior managers.

Figure 30: Cyber security's level of priority for owners, directors or senior management at care providers



Base: Care providers (575)

Homecare and supported living providers were more likely to state that cyber security is a very high priority for their organisation's owners, directors and senior management (61% and 64% respectively) compared to those from care homes (43%) or day care services (40%). Organisations with mainly digital systems were also more likely to state it is a very high priority (58%), and so were those with Cyber Essentials or other nationally recognised certification (61%), those with at least 11 rules or controls in place (60%), and those with a complete cyber incident response plan (65%).

In the survey, care providers were also asked if they agreed or disagreed with the statement 'my organisation has more important priorities than cyber security'. Responses to this statement were split; approximately a third agreed (34%) that their organisation had more important priorities than cyber security and the same proportion disagreed (34%).

Care homes providers were more likely to agree that their organisation has more important priorities than cyber security (40% versus. 34% overall), while homecare providers were more likely to disagree (39% versus. 34% overall).

Disagreement that their organisation has more important priorities than cyber security was higher than average (34%) among the same groups identified earlier: those with 11 to 15 rules and controls in place (39%), those with Cyber Essentials or other nationally recognised certification (44%), those with a complete cyber incident response plan (48%), and those with a business continuity plan covering cyber security (37%).

In the qualitative interviews, there was general agreement from all audiences that cyber security is an increasingly important priority, but could be overshadowed by several other equally important, or arguably more important, priorities. In the context of limited financial resources, and multiple competing complex priorities and challenges, care providers reported that it can be difficult to dedicate the time and capacity needed for cyber security, or land messages about the importance of cyber security practices among staff. Technology suppliers noted that their experience was that there is wide variation in care provider prioritisation of cyber security (which reflects wide variation in digital skills and adoption of digital technology in the sector in general).

"Trying to get the cyber security message to somebody that is, you know, worried about somebody with a complex set of needs that is about to be kicked out on the street, is a challenge." – Technology Supplier

Some misconceptions around data, who is responsible for it, and the level of risk posed to care providers were also apparent in the interviews when discussing the question of prioritising cyber security. This was commented on by representatives and leaders, and exhibited in some of the interviews with care providers. These misconceptions could result in cyber security not being prioritised as much as it should be in the sector. For example:

- assumptions were made in the interviews about what types of data are at risk from cyber attack. For example, one care provider said that cyber security is a ‘medium priority’ for their organisation because they are not a bank which handles a large amount of sensitive data (defined as financial data). This was also discussed by a participant in the representative and leader discussions – who said that social care data is not always seen as being as sensitive as NHS data because its less ‘clinically urgent’. There is therefore potential for care providers to underestimate the level of risk they face from cyber attacks

"I'd say, it's a medium priority because we're not a financial organisation. We don't store enough. If it was a bank, for example, it'd be at the very top of the agenda. But because we're a nursing home and we've got service users' records, we do our best to keep it secure." – Care Provider

- the potential impact of cyber incidents that care providers could face was often underestimated. This was an observation from representatives and leaders, but also demonstrated in the interviews with care providers. For example, one care provider did not think they would ever be prevented from accessing any of their information stored digitally because they stored information on different digital platforms

- assumptions were made that IT teams or technology suppliers are responsible for cyber security. There was an overreliance stated in the interviews with care providers (and observed in the interviews with representatives and leaders) on the IT team, and/or technology suppliers to

oversee and manage data and cyber threats (as discussed in chapter 9). There was a tendency for cyber security to be seen as something that is outsourced and/or managed by a separate team or individual, and not part of the day-to-day running of the care provider

"[it is a] very high priority, but…I don't worry about it, per se, because a lot of our [digital] systems, the control is with them" – Care Provider

There was some scepticism among the representatives and leaders interviewed that the high proportion of care providers reporting that cyber security is a high priority did not reflect their experiences of engaging with care providers. This was also reflected in the interviews with technology suppliers. As with knowledge and awareness of cyber security, these participants reported variation in terms of the extent to which it is prioritised equally across the whole organisation, across the sector, and the extent to which prioritising it indicates a comprehensive understanding of cyber security. Again, they reported that large providers have the expertise, manpower and capacity to prioritise it (along with dedicated teams responsible for it), unlike smaller providers who may see this as a priority in principle but may not have the means to put it in practice. Again, this difference between large and small providers is not reflected in the survey data and may suggest the differences are driven by more than just size.

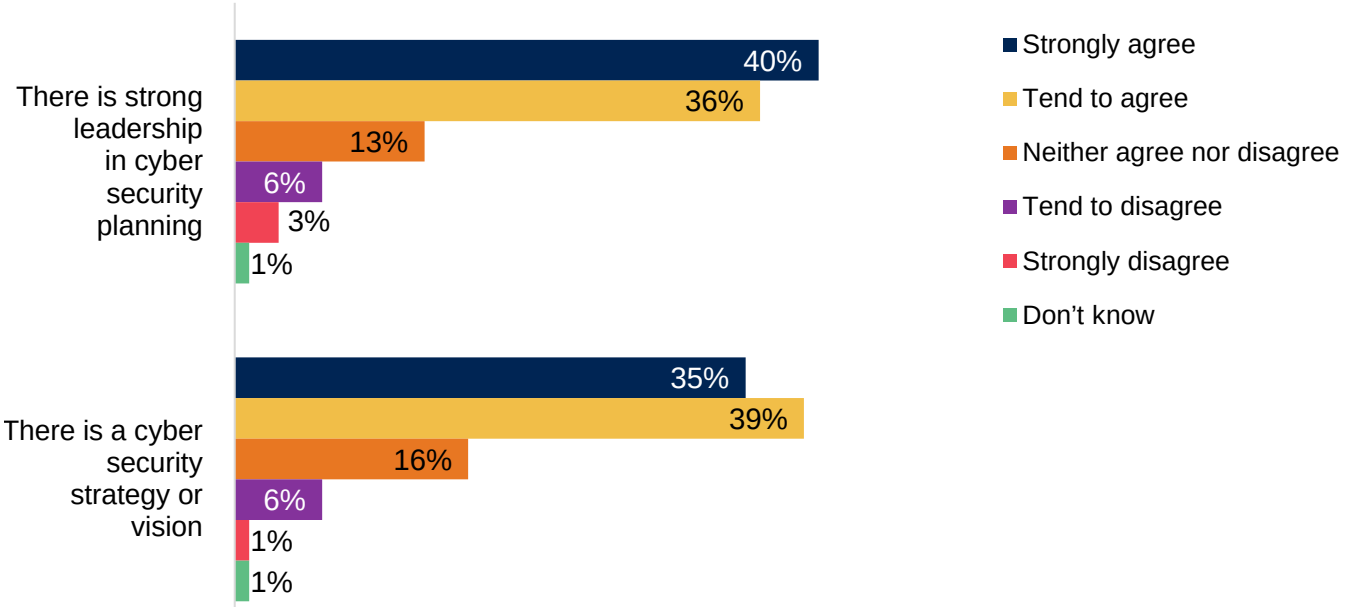
"Your big providers, really, they've got a whole suite of staff who have these responsibilities. But 85% of the sector is SMEs, and if you look at that job description of a registered manager who, ultimately, this falls on their lap. Not an awful lot of registered managers came into social care because they were interested in digital, let alone cyber." – Representative and Leader

Leadership and oversight

In the survey, care providers were asked if they agreed or disagreed with the statements: 'there is strong leadership in cyber security planning in my organisation', and 'there is a cyber security strategy or vision in their organisation'.

Around three-quarters of care providers agreed that there is strong leadership in cyber security planning within their organisation (76%), including 2 in 5 (40%) who strongly agreed. Less than one in 10 disagreed (9%). Findings are similar for the second statement: three-quarters (74%) agreed that there is a cyber security strategy or vision in their organisation (74%, including 35% who strongly agreed); and fewer than one in 10 disagreed with this statement (8%).

Figure 31: Extent to which care providers think there is strong leadership in cyber security planning and a cyber security strategy of vision at their organisation



	There is a cyber security strategy or vision	There is strong leadership in cyber security planning
Strongly agree	35%	40%
Tend to agree	39%	36%
Neither agree nor disagree	16%	13%
Tend to disagree	6%	6%
Strongly disagree	1%	3%
Don't know	1%	1%

Base: Care providers (575)

Agreement with these 2 statements was higher among some sub-groups previously noted:

- for both statements, agreement was higher among care providers that have access cyber security expertise via an internal expert team or individual, or a contract with an external organisation, compared with those with ad hoc access to an external specialist (Table 11)
- care providers that have 11 to 15 rules and controls in place on cyber security were also more likely to agree (88% on leadership, 85% on vision) compared with those with 1 to 5 rules or controls only (47% agreed on leadership, 51% on vision)
- homecare providers were also more likely to *strongly* agree with both statements (48% for leadership, 40% for vision or strategy, compared with 33% and 32% respectively for care home providers)
- agreement was higher than average among those with a complete incident response plan (94% for leadership, 88% for vision or strategy), those with Cyber Essentials or other nationally recognised certification (87% and 86% respectively), those a business continuity plan covering cyber security

(80% and 76% respectively), those with formal policies covering cyber security (79% and 78% respectively), and those who back up their data (78% and 77% respectively)

Table 11: Extent to which care providers agree the following exists within the organisation by type of cyber security expertise available to the organisation

	Total	Internal expert team	Internal expert individual	Contract with external organisation	Ad hoc access with external specialist	BSBC (BSBC) Digital Care Hub	Digital support teams at an ICB
Agree - strong leadership in cyber security planning	76%	88%	85%	83%	76%	81%	81%
Agree - cyber security strategy or vision	74%	89%	82%	80%	74%	84%	85%

Views of leadership around cyber security were explored in the qualitative interviews among care providers who were not in leadership roles. There was recognition that cyber security is generally recognised as an important issue by the leadership team. However, cyber security was not seen as something the leadership team were heavily involved with; there was awareness of it, but it had to be balanced with many competing priorities. There were some exceptions to this – for example, very small providers where the owner or leader had taken a particular interest in cyber security. The importance and priority given to cyber security was sometimes prompted by experience of cyber incidents.

"But yes, that cybersecurity role was created because of the hack" – Care Provider

The same concerns were raised around there being a surface-level understanding of cyber security rather than a comprehensive understanding of the issues and risks. As one data security manager described; data is not seen as an asset in the way other assets are (like the organisation's finances). It therefore does not receive the same level of scrutiny; for example, there was no IT representation to the board, and cyber security did not feature in their board reports.

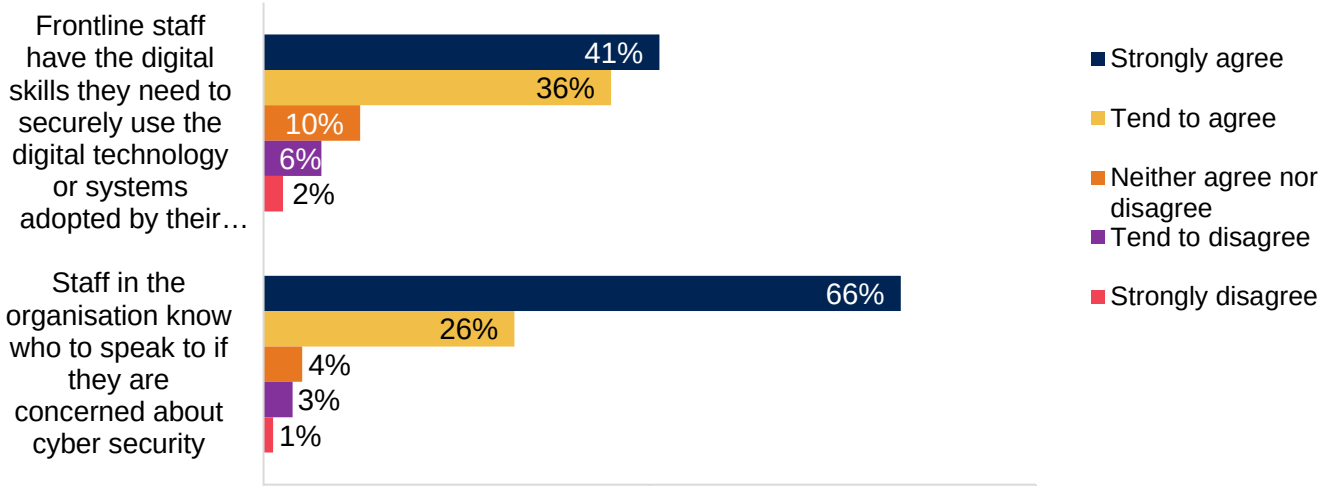
"It just feels like technology and security are not seen as 'what we do'. And wearing my data protection officer hat, I would say that data isn't fully understood to be a major asset of the organisation. We still think in terms of bricks and mortar." – Care Provider

The wider workforce

In the survey, just over three-quarters (77%) of care providers agreed that their frontline staff have the digital skills they need to securely use their digital technology or systems. Only 9% disagreed with this statement. Similarly, three-quarters of care providers agreed with the statement 'Our staff have the digital skills they need to use Enterprise Connected Devices securely', and only 8% disagreed.

The survey also explored views on whether staff within the care provider organisation know who to speak to if they are concerned about cyber security. Over 9 in 10 (92%) care providers agreed with the statement that staff in their organisation know who to speak to.

Figure 32: Extent to which frontline staff have the digital skills they need to securely use the digital technology or systems and whether they know who to speak to if they are concerns about cyber security



	Staff in the organisation know who to speak to if they are concerned about cyber security	Frontline staff have the digital skills they need to securely use the digital technology or systems adopted by their organisation
Strongly agree	66%	41%
Tend to agree	26%	36%
Neither agree nor disagree	4%	10%
Tend to disagree	3%	6%
Strongly disagree	1%	2%

Base: Care providers (575)

Sub-group differences are in line with earlier findings. Homecare providers were more likely to agree their frontline staff have the digital skills they need to securely use their digital technology or systems (83%, including 47% who strongly agree), compared with providers of care home (73%), supported living (75%) and day care services (68%).

Agreement was more common than average among those with at least 11 rules and controls in place (86% for staff digital skills, 95% for staff knowing who to speak to), those who access cyber security expertise via BSBC at the Digital Care Hub (88% and 97% respectively) or at an ICB (88% and 98% respectively). These sub-group differences are also observed for the statement ‘our staff have the digital skills they need to use Enterprise Connected Devices securely’.

In the qualitative interviews with care providers, participants who were positive about the workforce’s ability to use technology securely gave the following reasons for their confidence:

- the care provider had been digital for a long time, allowing them to develop digital skills and awareness around cyber security

- there was faith that staff had good access to information about cyber security and there were effective training programmes in place
- their workforce was familiar with cyber security issues when using digital technology outside work, which had made it quick and easy to train the staff in cyber security practices for work purposes. This typically happened when their workforce was young
- the small size of the organisation meant they were able to easily communicate with their staff, with access to digital systems restricted to a small number of people
- there was low staff turnover meaning rules, policies and procedures could be embedded

"There's only myself and one other person who are involved in the care home and we both work for that organisation. So, we understand what to share and what not to share, or the type of information we share and who it's going to is important…I think we're quite clued up." – Care Provider

However, there was some discussion of features in the care workforce that might inhibit a comprehensive understanding of cyber security – especially in larger organisations. These were discussed by both representatives and leaders, and some care providers (particularly those who were in a role related to digital infrastructure and/or cyber security), and included:

- acknowledgement that cyber security is not something all care workers will necessarily consider as part of their role (due to competing priorities, and the nature of their work)
- a lack of digital skills within the workforce. This was raised in this research as a barrier, but also has been explored in depth in previous research conducted by Ipsos and IPC for NHSX which found that a significant minority of the workforce did not feel confident about their digital skills. The age of the workforce was raised as a particular barrier. Access to and use of digital technology (and relevance to many care workers' roles) was also identified as a major barrier to developing digital skills (in this research and in the NHSX research), as discussed in chapter 2

"I think it's something that the younger generation are more aware of than the older generation, if I'm being honest. I think they understand it better." – Care Provider

- high levels of staff turnover in the sector, and (for a minority of the workforce) low levels of English. These can make it challenging to instil a consistent and robust organisational approach to cyber security

These reasons led to the view that understanding of cyber security risks related to the use of digital technology at work may be patchy in large proportions of the adult social care workforce. However, this was also coupled with confidence among some care providers taking part in the research that the policies and procedures in place protected their organisation – and the staff – from cyber security risks. This could potentially represent an overreliance on cyber security systems, and underestimation of the risk that human error poses to care provider organisations. This tendency to rely on systems and underestimate human error was also observed in the interviews with representatives and leaders. We explore this in more depth in the next chapter.

06

Policies and practices around cyber security within care providers

6 Policies and practices around cyber security within care providers

This chapter explores the policies and practices care providers have in place to manage cyber security, such as accreditations, governance arrangements, rules and controls for good cyber hygiene. It also looks at the common behaviours that sit alongside these policies that could put organisations at risk.

Summary

Care providers reported that they have implemented a **wide range of policies, procedures, rules and controls** in their organisation to improve cyber security. For example:

- A majority (82%) had established formal policy or policies covering cyber security risks, and/or a business continuity plans that covered cyber security (80%).

- A majority of care providers who qualified as experts had a broad range of technical rules and controls in place to help minimise the risk of cyber security breaches (such as strong password policies, restricted access, up-to-date malware protection): 55% had 11 to 15 rules and controls, 35% had 6 to 10, and only 10% had 1 to 5 of the 15 rules or controls listed.

There is overlap between some of these groups: care providers with only 1 to 5 rules and controls in place are less likely than average to have formal policies covering cyber security or cyber insurance.

The majority (around three-quarters) reported that they provide staff with a wide range of training offers on cyber security, and a similar proportion (75%) agreed that they knew the cyber security risks associated with ECDs Enterprise Connected Devices.

There was a **high level of confidence** among care providers in the procedures and policies their organisation had in place to ensure cyber security. Where there was uncertainty, this related to concerns around human error, the changing landscape in terms of technological advances and advances in cyber crime, and the lack of resources, time and capacity to dedicate to cyber security.

Still, representatives and leaders expressed some **concerns regarding the robustness of these procedures and policies, their implementation, and the quality of the cyber security training provided** to staff.

Some risky behaviours and practices also seemed to be fairly common. In the survey around a third of care providers reported that things like sharing organisational devices (39%), staff using their own devices for work (33%) or sharing email addresses (30%) were happening fairly or very frequently. In the qualitative interviews, all audiences thought that these practices were widespread, linking them back to low digital skills, lack of awareness of cyber risk and lack of resources (for example to buy extra licences or devices).

6.1 Policies and governance arrangements

Policies and accreditations

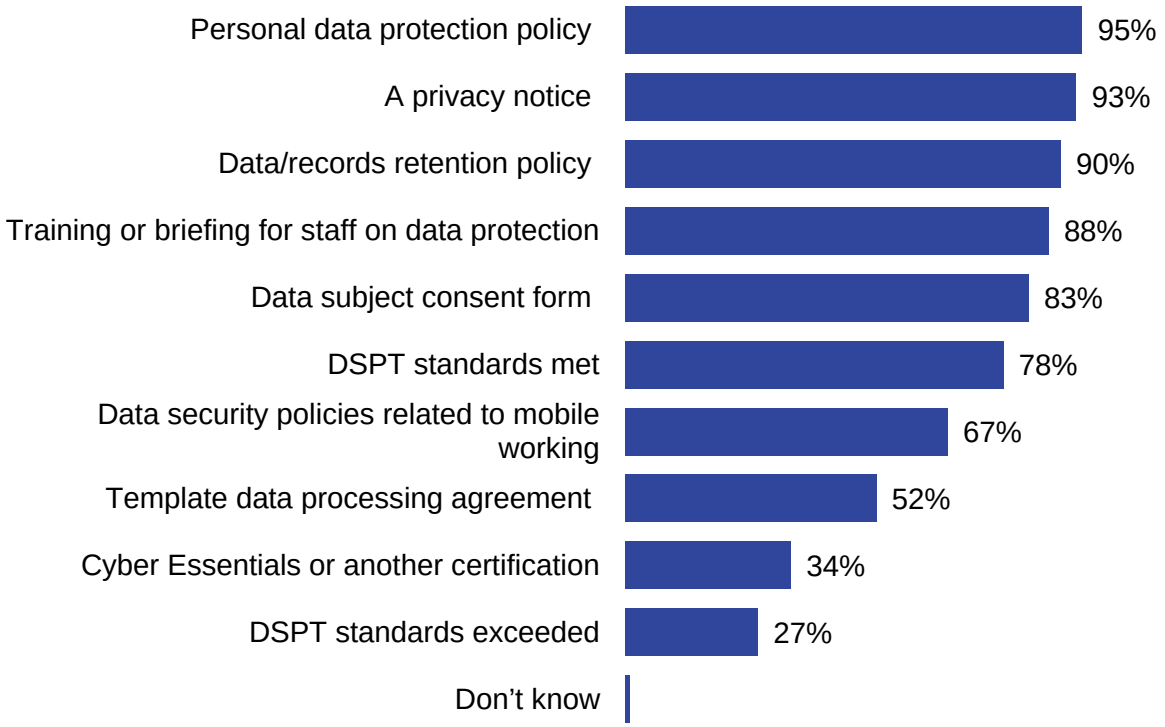
In the survey, care providers were asked about the policies and procedures their organisation had in place. The vast majority reported that they had a personal data protection policy (95%), a privacy notice

(93%) and a data and/or records retention policy (90%) in place – policies they would be expected to have. A slightly lower proportion reported that they had training or briefing for staff on data protection and data security issues (88%) or that they had a data subject consent form (83%), or data security policies related to mobile working (67%, rising to 78% among homecare providers and 76% among supported living providers).

Looking at accreditations, three-quarters said their organisation met the DSPT (DSPT) standards (78%), and just under 3 in 10 said they exceeded DSPT standards (27%). This is higher than indicated by the information provided by the BSBC sample (see Table 3 in chapter 2), which could be due to the complexities and nuances around the completion and status of the DSPT: it can be completed at parent organisation level and/or at location level, and there are a number of status categories in addition to 'Standards Met' and 'Standards Exceeded' which were not listed in the questionnaire ('not individually registered', 'approaching standards', 'entry level', 'not published').

Only 2 care providers did not have any of the policies, procedures or accreditations listed in the question.

Figure 33: Types of policies, procedures or accreditation in place at care providers



Base: Care providers (575)

Many of these policies and accreditations were more common than average among care providers that accessed cyber security expertise via the BSBC programme, and/or the Digital support teams at an ICB, for example:

- personal data protection policy and a data retention policy (100% and 98% respectively among those accessing expertise via their ICB)
- training and briefing for staff on data protection and data security issues (95% among those accessing expertise via BSBC, 98% of those accessing it via their ICB)

- DSPT standards met (88% among those accessing expertise via BSBC, 89% among those accessing it via ICB)
- DSPT standards exceeded (48% and 45% respectively)

Those accessing cyber security expertise through a contract with an external organisation or an internal expert individual were also more likely than average to report having many of these policies or accreditation in place. Care providers with ad hoc access with an external cyber security specialist were less likely than those accessing other forms of cyber security expertise to report having some of these policies and accreditations, in particular those with Cyber Essentials or other nationally recognised certification (only 32% of them did, compared with 50% among those with an internal expert team and 55% of those accessing expertise via BSBC).

Most of these policies and accreditations were less common than average among care providers with no cyber security insurance, only 1 to 5 rules or controls in place, those with no business plan covering cyber security, and those without a cyber incident response plan. Note that there is a significant overlap between these groups: for example, 44% of care providers with 1 to 5 rules and controls reported that they do not back up their data, and over half of care providers with no cyber security insurance do not have any cyber incident response plan (55%).

Governance and risk management

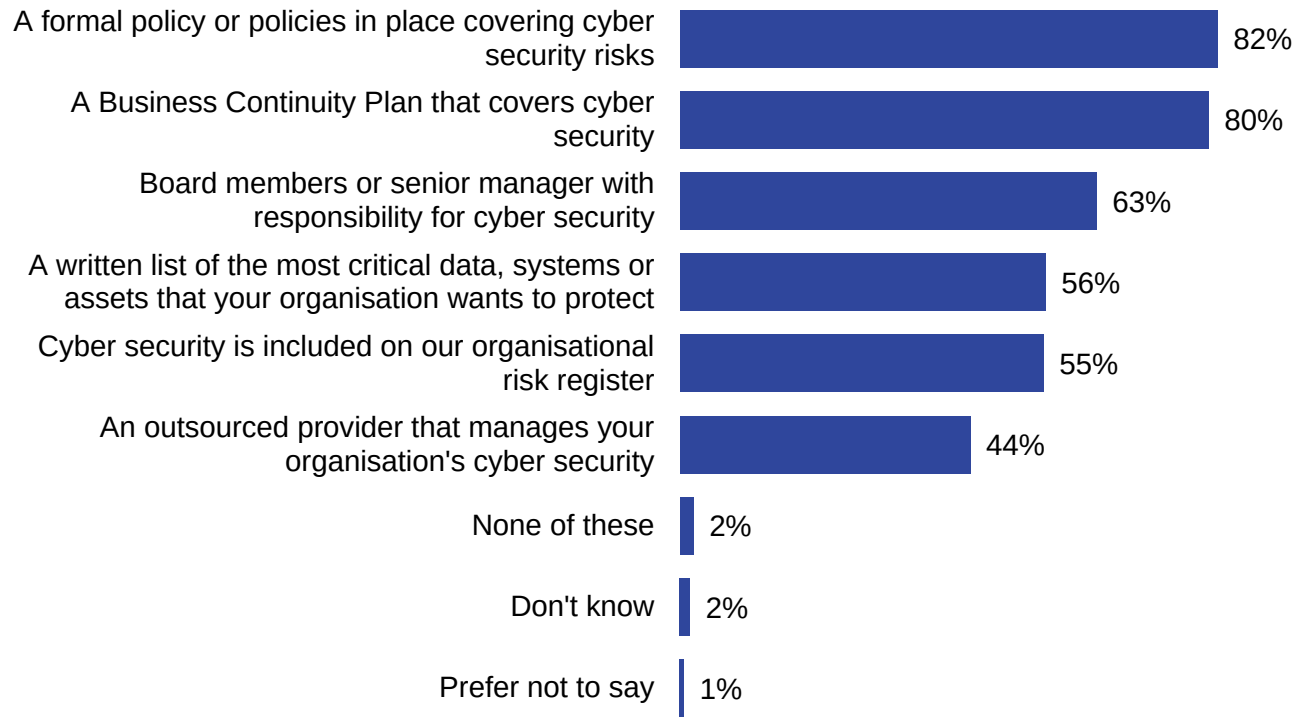
In the survey, care providers reported that a number of governance and risk management arrangements were in place in their organisation. A majority (82%) had established formal policy or policies in place covering cyber security risks, and/or a business continuity plans that covered cyber security (80%).

For comparison, the 2024 Cyber Security Breaches survey found a third of businesses (33%) and charities (32%) had formal cyber security policies in place. To note, these policies may be part of a wider policy within the organisation, such as the IT policy. A similar proportion of businesses (31%), and a smaller proportion of charities (22%) had a business continuity plan that covers cyber security. This is much lower than among care providers, and the difference could be accounted for by the fact that care providers must have specific policies in place on data security and business continuity to meet DSPT standards.

Two in 3 providers had board members or senior managers with responsibility for cyber security (63%), and over half had a written list of the most critical data, systems or assets that their organisation wants to protect (56%). The same proportion (55%) reported that cyber security was included in their organisational risk register, and over 2 in 5 (44%) used an outsourced provider to manage their organisation's cyber security.

A minority (2%) did not have any of the governance or risk management arrangements listed in the question, rising to 5% among care providers with no cyber incident response plan, 7% among those with no cyber security insurance and/or no back-up, and 11% among those with only 1 to 5 rules or controls in place.

Figure 34: Types of governance or risk managements arrangements in place at care providers



Base: Care providers (575)

Looking at other sub-group differences, formal policies covering cyber security risks, business continuity plans covering cyber security, and outsourcing the organisation's cyber security to a provider were more common among care providers with 50 or more staff. Other differences are in line with those previously observed, with the following groups all more likely than average to report having most risk management arrangements in place: those insured for cyber security, those with back-ups, those with at least 11 rules or controls in place, those meeting or exceeding DSPT standards and those Cyber Essentials or other nationally recognised certification.

6.2 Rules and controls in place around cyber security

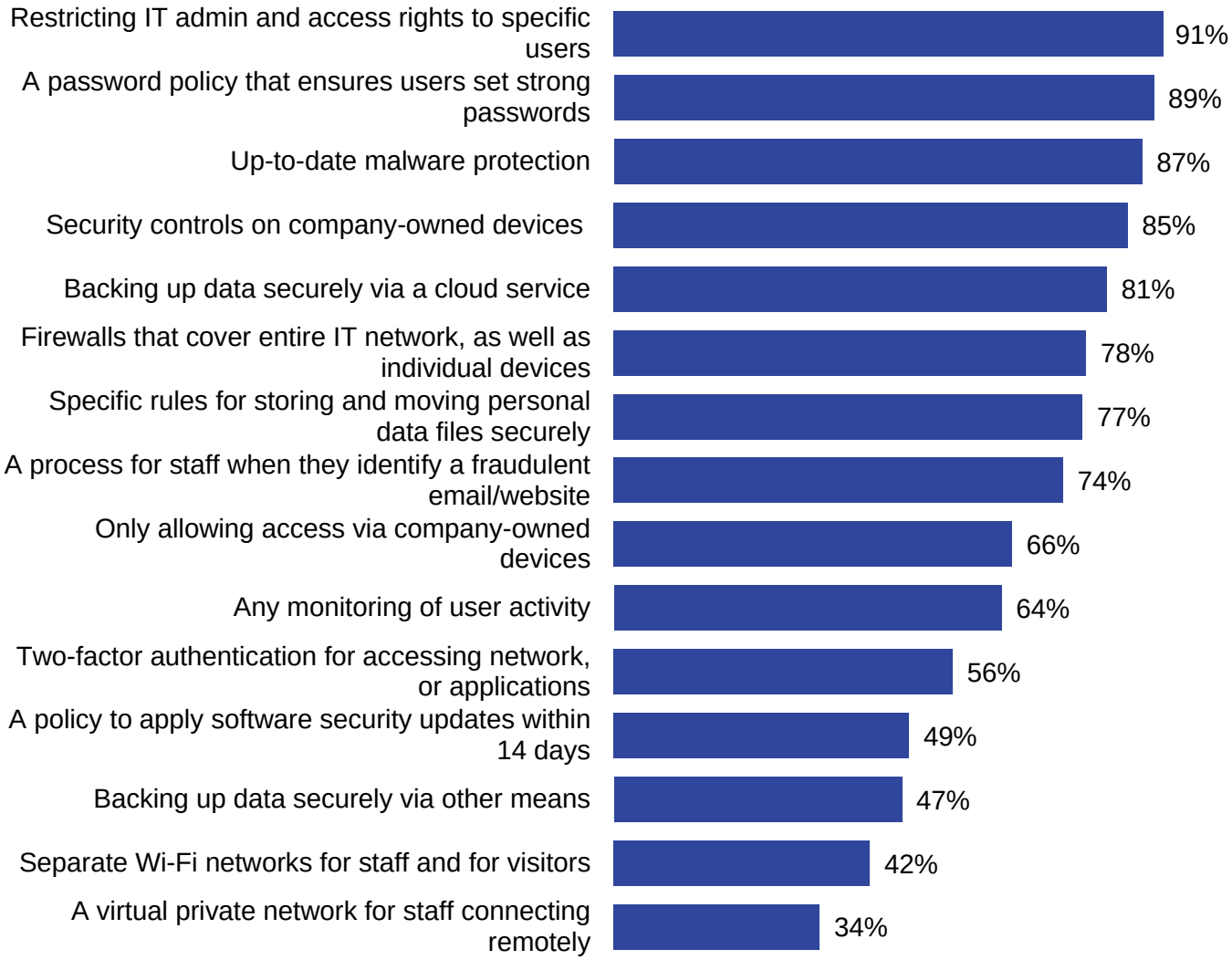
Care providers taking the 'expert' routing through the questionnaire were asked about the range of technical rules and controls in place in their organisation to help minimise the risk of cyber security breaches. Many of these rules and controls were taken from the Cyber Security Breaches Survey. A majority of these care providers had a broad range of rules and controls in place: 55% had 11 to 15, 35% had 6 to 10, and only 10% had just 1 to 5 of the 15 rules or controls listed.

The most frequently deployed rules or controls involved restricted IT admin and access rights to specific users (91%), password policies that ensures users set strong passwords (89%), up-to-date malware protection (87%), security controls on company-owned devices (85%), and secure back-up of data via a cloud service (81%). The least common rules and controls were around use of Virtual Private Networks (VPNs) (34%), separated Wi-Fi networks for staff and visitors (42%), backing-up data via other means (not a cloud) (47%), and a policy to apply software security updates within 14 days (49%).

These are broadly in line with the findings from the 2024 Cyber Breaches Survey, where the most frequently deployed rules or controls were updated malware protection (83% among businesses and

65% among charities) and password policies (72% among businesses and 54% among charities), and the least common rules were applying software updates (32% among businesses and 18% among charities) and use of VPNs (34% among businesses and 20% among charities).

Figure 35: Types of rule or controls in place at care providers



Base: All care providers classified as experts in the questionnaire (559)

Looking at sub-groups, organisations with 50 or more staff and those that use mainly digital systems are more likely than average to report having many of the rules and controls listed in place. Those with a cyber security insurance, a business continuity plan and/or formal policies covering cyber security, and those with a complete cyber incident response plan are also more likely than average to report having many of the rules and controls listed in place.

The low uptake of VPNs (virtual private networks) was reflected in an interview with a technology supplier, who felt that while some care providers were beginning to understand the importance of utilising VPNs, the quality of the services they were accessing was an issue.

"Some customers have got VPNs, but they're not very good ones, and they don't know how to configure them. We'll install VPNs for people, just at cost price, and we don't want to particularly make money out of it, but we'd prefer people to have VPNs. Again, very small take-up." – Technology Supplier

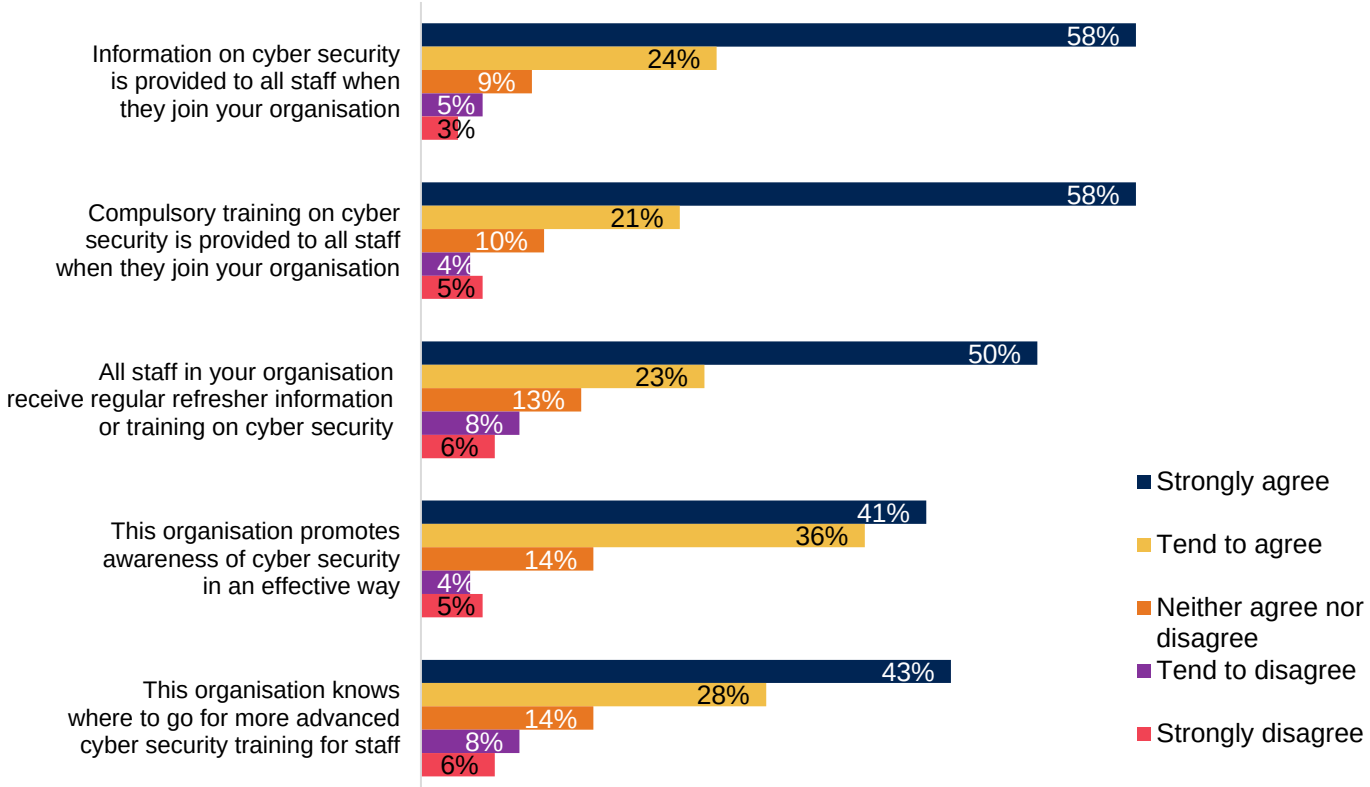
A very small number of care providers did not meet the definition of experts (16). They were asked a shorter question, about their confidence that the rules or controls their organisation had for cyber security were appropriate. 11 of them said they were very or fairly confident that their organisation had appropriate rules and controls, and 5 were not very confident.

6.3 Training for staff

In the survey, care providers were asked 5 attitudinal statements on staff awareness and training in relation to cyber security.

When asked whether staff were provided with compulsory training on cyber security when they joined the organisation, the majority (79%) agreed, including 3-fifths (58%) who strongly agreed. Only 9% disagreed. Views on the statement 'Information on cyber security is provided to all staff when they join your organisation' followed a similar pattern, with 82% who agreed and 8% who disagreed. A slightly lower proportion agreed with the statements 'this organisation promotes awareness of cyber security in an effective way' (77%), 'all staff in your organisation receive regular refresher information or training on cyber security (annually or more often)' (72%), and 'this organisation knows where to go for more advanced cyber security training for staff' (72%).

Figure 36: The extent to which care providers offer different types of cyber security training and awareness raising



	This organisation knows where to go for more advanced cyber security training for staff	This organisation promotes awareness of cyber security in an effective way	All staff in your organisation receive regular refresher information or training on cyber security	Compulsory training on cyber security is provided to all staff when they join your organisation	Information on cyber security is provided to all staff when they join your organisation
Strongly agree	43%	41%	50%	58%	58%
Tend to agree	28%	36%	23%	21%	24%
Neither agree nor disagree	14%	14%	13%	10%	9%
Tend to disagree	8%	4%	8%	4%	5%
Strongly disagree	6%	5%	6%	5%	3%

Base: Care providers (575)

Strong agreement with each of these 5 statements was more common among homecare providers (62% on information on cyber security, 63% on compulsory training, 54% on regular refresher, 48% on promoting awareness in an effective way and knowing where to go for more advanced training) compared to care home providers and compared with the average. Strong agreement was also more common among care providers who accessed cyber security expertise from BSBC at the Digital Care Hub, compared with the average.

Agreement with the statements was also higher than average among the following groups:

- care providers with one location or setting
- those with a business plan and/or formal policies covering cyber security

- those with 11 to 15 rules and controls in place
- those with cyber security insurance
- those who back up their data
- those with a cyber incident response plan
- those with Cyber Essentials or other nationally recognised certification

As mentioned earlier, there is a significant overlap between many of these groups.

In the qualitative interviews, training was frequently mentioned by care providers as a aspect of how they raise awareness and upskill their workforce around cyber security. Training was offered on induction and some care providers also discussed providing annual refresher training. One care provider noted that as a result of near misses they had experienced with cyber security incidents, they ran specific staff training focussing on areas for improvement.

"[As a result of an incident] there's been more training for HR, the policy has been tightened up. Hopefully the procedures have also been tightened up" – Care Provider

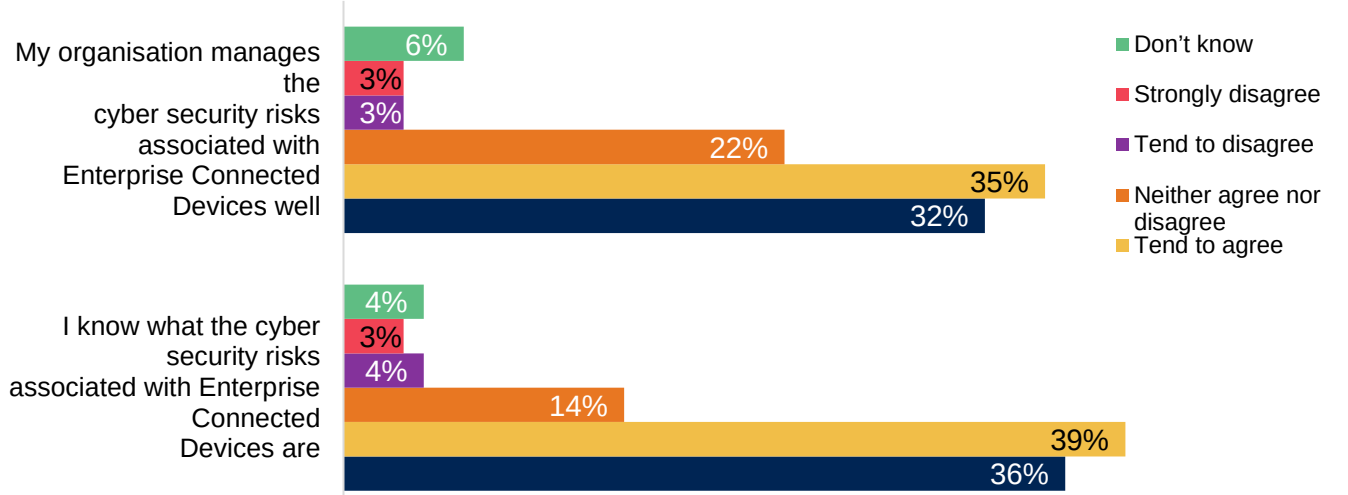
However, there was some scepticism about the effectiveness of training expressed in a few interviews with representative and leaders, who described the training as a 'tick-box' exercise. They were concerned that training was heavily geared to meeting requirements – for example of the DSPT, rather than embedding a comprehensive understanding of good cyber security practices within the workforce. Barriers to accessing training were mentioned – these are explored further in chapter 9.

"An awful lot of the systems that are in place around things like annual cyber security training are largely geared around ticking boxes and demonstrating you've done the things you should do, more so than actually being really good at helping people to understand what the risks are." – Representative and Leader

6.4 Enterprise Connected Devices

In the survey, care providers were asked about the risks associated with Enterprise Connected Devices (ECDs), which they may use. ECDs include computers, laptops, tablets, mobile phones used for work purposes in addition to technology that is used to provide care, such as personal alarms, and monitoring equipment with sensors. Three-quarters (75%) agreed that they knew the cyber security risks associated with ECDs, and 7% disagreed. A slightly lower proportion (67%) agreed that their organisation manages the cyber security risks associated with ECDs well, and one in twenty (6%) disagreed.

Figure 37: Extent to which care providers know the cyber security risks associated with ECDs and how well their organisation manages these ECD risks



	I know what the cyber security risks associated with Enterprise Connected Devices are	My organisation manages the cyber security risks associated with Enterprise Connected Devices well
Don't know	4%	6%
Strongly disagree	3%	3%
Tend to disagree	4%	3%
Neither agree nor disagree	14%	22%
Tend to agree	39%	35%
Strongly agree	36%	32%

Base: Care providers (575)

Sub-group differences for these 2 statements follow the same pattern previously mentioned, with care providers that back up their data, have a cyber incident response plan, have 11 or more rules or controls in place, have a business plan and/or formal policies covering cyber security, or access expertise through BSBC at the Digital Care Hub, all more likely than average to agree with the statements.

6.5 Confidence in procedures and policies

In the qualitative interviews, care providers were asked whether they were confident in their organisation's approach to cyber security. Care providers gave the following reasons for confidence in their policies and procedures:

- they had never experienced an attack, indicating that their practices were robust
- they had built their policies and procedures up over time and had seen progress in implementing these in recent years
- they were working with an external supplier to oversee their approach to cyber security
- they had leadership buy-in into cyber security that indicated to them it was being taken seriously
- the training provided to staff meant they felt they were doing everything they could to raise awareness of policies and procedures

"We try and make things fairly common knowledge for our staff so they do have the means to be able to try and do the best that they can for the organisation to keep things safe" – *Care Provider*

However, uncertainty was also expressed in the qualitative interviews as to how robust organisational practices were. Reasons care providers doubted the resilience of their approaches included:

- human error was seen as the biggest risk when working with technological devices. Participants noted that that regardless of how secure the systems were, the policies or controls in place, staff were central to ensuring systems are not compromised
- advances in technology, and advances in cyber-crime, were ongoing, so it was difficult to keep up with various developments
- lack of time, capacity and/or knowledge. Some were concerned there were gaps in their practices but unsure of how they needed to better protect themselves, or did not have the resources required to improve their cyber security

"I would say I've probably got about 80% confidence in [our policies and procedures]. I think the policies and procedures themselves are reasonably good and correct. It's around the application and enforcement of those policies and procedures." – Care Provider

"It's not been a priority. It's just been a small part of my job and I've not even really been able to assess the risk. So, my gut feeling is we haven't got enough in place." – Care Provider

Representatives and leaders, and technology suppliers, also expressed some concern about the robustness of care providers' approaches to cyber security. Their concerns focussed on the following things:

- how good the policies and procedures were (for example, whether business continuity plans went far enough)
- the application of policies and procedures, due to a lack of technical ability. For example, they said that the right policies may be in place, but they had observed a lack of deeper understanding to apply them in a comprehensive way
- the nature of the policies and procedures – for example, one participant said that the emphasis tends to be avoiding the loss of data rather than empowering staff and service users to use digital technology safely

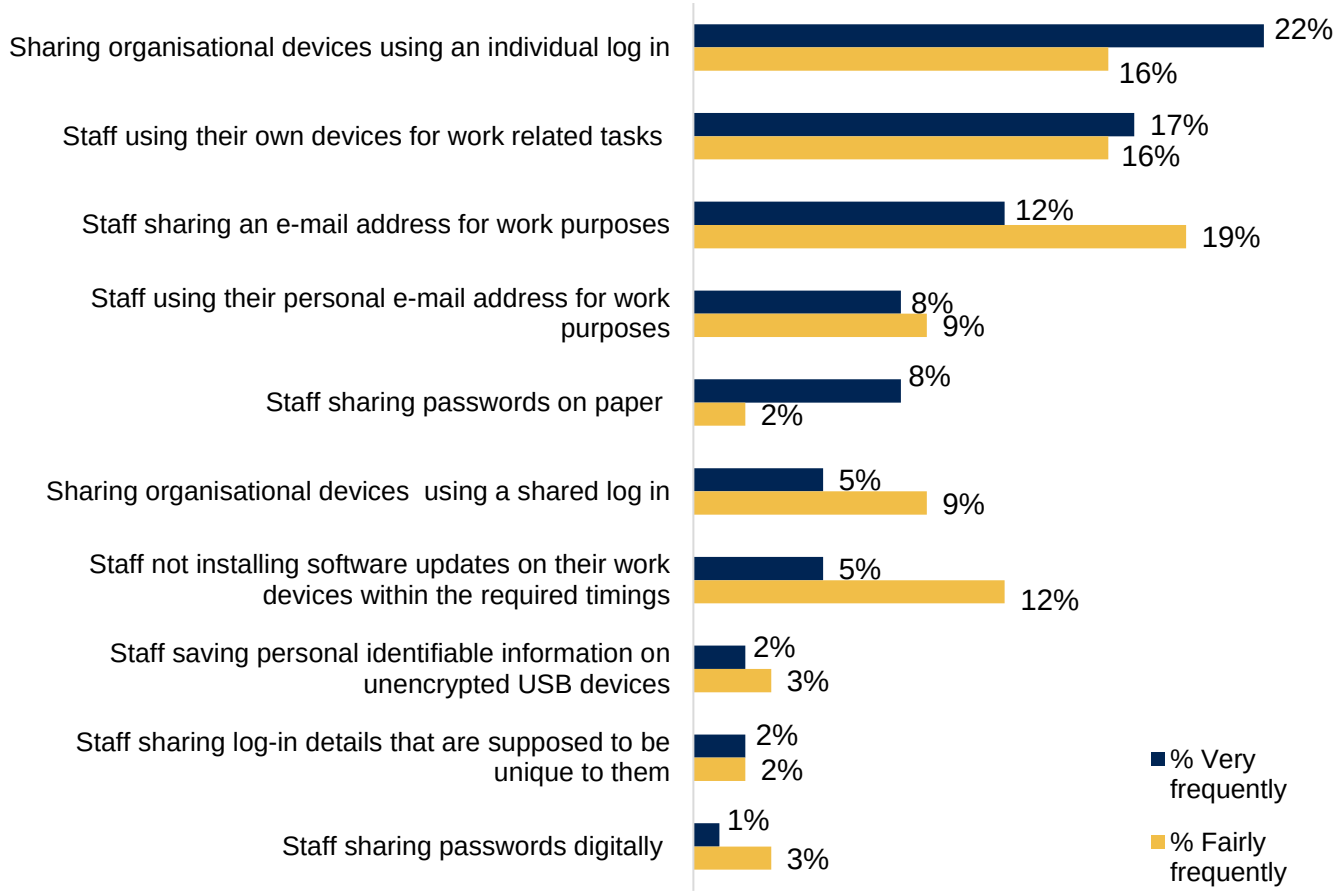
"What all the emphasis is on, is about keeping the organisation systems safe and secure so that you are not going to lose the data you hold on the people you support. But you're also responsible for those people and if those people are not supported to use digital systems, then they've got a new level of disadvantage." – Representative and Leader

6.6 Risky behaviours and practices

In the survey, care providers were asked to estimate how frequently or infrequently certain risky practices happened within their organisation. The risky practices most likely to be estimated as happening very or fairly frequently were staff sharing organisational devices (for example smartphone or laptop) using an individual log in (39% saying this happened very or fairly frequently), staff using their own devices (for example smartphone, laptop or home computer) for work related tasks (33%) and staff sharing an e-mail address for work purposes (30%).

Some risky practices were far less widespread, with less than one in twenty estimating these happened very or fairly frequently in their organisation. They were: staff sharing passwords on paper (3%) or digitally (4%); staff sharing log-in details that are supposed to be unique to them (4%); and staff saving personal identifiable information on unencrypted USB devices (4%).

Figure 38: How frequently different risky practises happen at care providers



	Staff sharing passwords digitally	Staff sharing log-in details that are supposed to be unique to them	Staff saving personal identifiable information on unencrypted USB devices	Staff not installing software updates on their work devices within the required timings	Sharing organisational devices using a shared log in	Staff sharing passwords on paper	Staff using their personal e-mail address for work purposes	Staff sharing an e-mail address for work purposes	Staff using their own devices for work related tasks	Sharing organisational devices using an individual log in
% Very frequently	1%	2%	2%	5%	5%	8%	8%	12%	17%	22%
% Fairly frequently	3%	2%	3%	12%	9%	2%	9%	19%	16%	16%

Base: Care providers (575).

Notable differences can be observed based on the type of services provided: 3 in 10 providers of homecare services thought that staff using their own devices (for example smartphone, laptop or home computer) for work related tasks happened very frequently (29%), as opposed to 5% among care home providers and 14% among supported living providers. In contrast, a third of care home providers (32%) thought that sharing organisational devices (for example smartphone or laptop) using an individual log in

happened very frequently, compared with only 15% of homecare providers and 20% of supported living providers.

The common risky practices that were reported in the qualitative interviews with care providers, representatives and leaders, and technology suppliers largely reflected the survey responses. Participants described the use of personal own devices at work, which could be a particular problem with confidential information remaining on devices once a staff member left the organisation. Sharing passwords and email log-ins across multiple people was also a common practice discussed in the interviews. This was particularly in relation to NHSmail – as a limit is placed on the number of NHS email addresses care providers receive, organisations often share an email address among staff. Alternatively, some care providers kept one shared device logged into the NHS email address that staff could access. A technology supplier also provided an example of staff saving passwords to care systems on the browsers of shared devices. This allowed staff to share logins when completing work related tasks.

"At my last organisation, we had something like 3,500 employees, but only 1,200 licenses for company emails. And so, there were loads of staff wandering around without a company email and sending information." – Representatives and Leader

Participants also highlighted some further behaviours that could put organisations at risk:

- discussing and sharing confidential information across digital platforms, for example sharing photographs on WhatsApp. A representative and leader said there was an assumption that because WhatsApp is encrypted it is safe to share sensitive information on
- opening and responding to fraudulent emails (phishing), which was noted as a common issue and one that was difficult for organisations to oversee and mitigate
- staff accessing social media on the same devices they were using for work, with concern that bugs could be transferred from social media onto organisational software

"I think there's a little bit too much of freely discussing or just sending stuff around, downloading stuff...I suppose poor data hygiene is the bad practice that we see most often." – Care Provider

The causes of these 'risky behaviours' related to the cost of implementing some of these cyber controls (such as buying licences for all staff), and to the attitudes, knowledge and awareness around cyber security present in the sector. For example, it was felt that data, cyber security and safe digital practices were not fully understood by some of the workforce, and therefore not suitably prioritised. Furthermore, it was suggested that there were some things that put the wider care workforce at risk of a cyber breach. This included:

- insufficient scepticism about fraudulent emails – participants suggested that there is not enough curiosity or questioning around the source or motivations behind some suspect emails (for example, emails asking for donations or bank details, or offering vouchers)
- low awareness that staff themselves could be the target of a cyber-attack (not just the organisation as whole), and therefore the 'weak link' within the organisation
- staff working remotely, and dispersed across different locations, particularly in people's homes and using personal devices
- lack of digital skills

“Some members of staff are quite ignorant and could be taken in by some sort of scam. I mean, it did happen with our finances a while back, although the bank did reimburse us, but someone phoned and impersonated the bank and managed to extort some money from us.” – Care Provider

Behaviours that might put the care provider organisation at risk were not just mentioned in relation to the frontline workforce. There was also an example of push-back from leadership to implement robust policies and procedures. A care provider gave an example of trying to roll out a 2-factor authentication policy across the organisation’s system but not being able to due to resistance from the senior management team. There was no additional cost in adding the 2-factor authentication, but the senior management team felt the extra steps required to log into the system was inconvenient. Technology suppliers reported similar situations in their interactions with care providers.

“We'd like to do a lot more security on the system, but we get a lot of kickback, it's, 'Could you make it easier for our carers to log on? Do they actually have to log in? Can they just have PIN number? Can they set their own PIN number?' and '6 digits is too big, can it be 4?' So, we get this all the time, and we're saying, 'No,'” – Technology Supplier

07

Responding to cyber incidents

7 Responding to cyber incidents

This chapter looks at care providers' ability to deal with a cyber incident. It looks at their confidence in their ability to respond, and at the policies and procedures care providers have in place, including business continuity plans and incident response plans, back-ups, insurance, and ransom policies. It also looks at technology suppliers' assessment of their ability to respond to an incident.

Summary

There was a high level of confidence from care providers about their organisation's ability to deal with a future cyber incident. This was driven by the policies and procedures they had in place, including:

- Written guidance on who to notify (75%), assigned roles and responsibilities (72%), and guidance on when to report incidents externally (64%).

- Business continuity plans covering cyber security (80%), and incident response plans (61%). Over half of care providers have both (53%).

- Back-ups – the majority reported that they backed up their data (81%), with over half reporting that this happened once a day or more (56%). Nearly all (96%) care providers were confident their back-ups were usable and complete.

- Insurance – just under 2 thirds (64%) reported being insured against cyber security risks in some way.

Some concerns were raised in the qualitative interviews (particularly from representatives and leaders) around the strength of some of these measures. This included an overreliance on policies and procedures that was not backed up by practical knowledge and experience. More specifically, there were concerns about weaknesses common in business continuity plans (for example underestimating the of time it can take to recover from an attack), and back-ups being inadequately implemented.

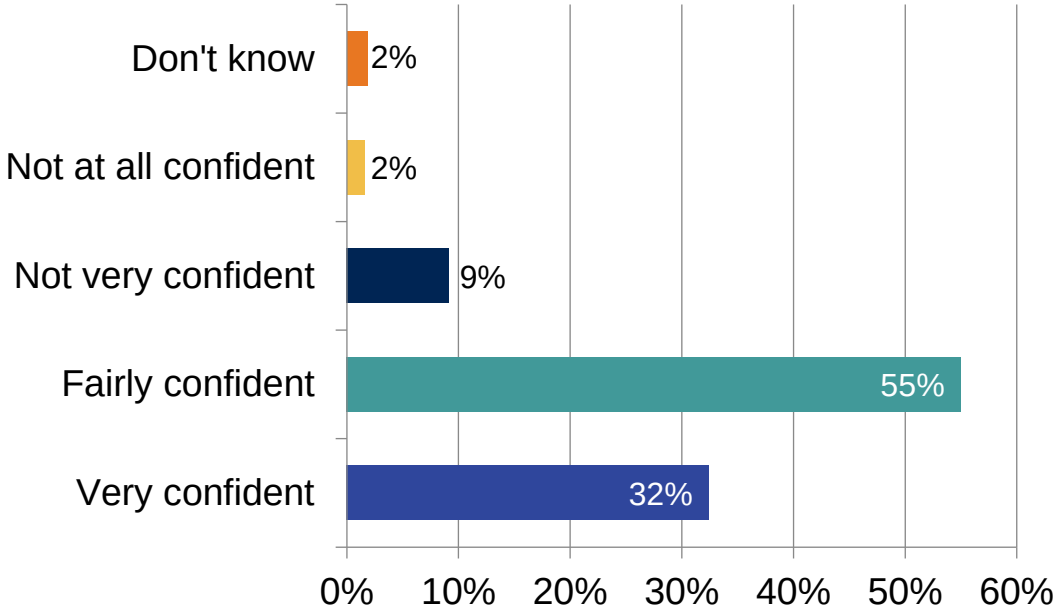
In terms of actions in the event of an incident, care providers reported that they would **notify a range of organisations**; in most cases the Care Quality Commission (CQC) (80%), the Information Commissioner's Office (ICO) (73%), their insurance company (73%) and/or the local authority (71%), though in practice they explained that who they would notify would depend on the nature of the incident.

Technology suppliers also reported a range of measures in place to respond to an incident – and though there is a low base size it appears that the procedures in place are widespread. They were also confident in their cyber incident response and recovery arrangements.

7.1 Care providers' confidence in their ability to deal with a cyber security incident

In the survey, care providers were asked how confident or not they felt in their organisation's ability to deal with a future cyber security incident. Nearly 9 in 10 said they were confident, including a third (32%) who were very confident. Only one in 10 were not confident.

Figure 39: Confidence in organisation's ability to deal with a future cyber security incident



Base: Care providers (575)

There was a higher proportion of people feeling not very or not at all confident among those who had no cyber incident response plan (17%), did not back up their data (27%), did not have a business continuity plan and/or formal policies covering cyber security (19% and 21% respectively), or only had 1 to 5 rules and controls in place (31%).

Having experienced at least one incident over the last 3 years made a small difference to the level of confidence reported, with only a quarter of care providers who had experienced an incident feeling very confident (25%), and two-thirds feeling fairly confident (65%), as opposed to 36% and 51% respectively for those who did not report any incident in the last 3 years.

When care providers were asked in the qualitative interviews whether they would feel confident responding to an incident, their responses largely focussed on the policies and procedures they had in place to respond to an incident (rather than – for example – their knowledge and expertise, or experience). Specifically, they were confident because:

- they had a business continuity plan in place to support their response
- their systems were backed up that would allow them to continue to access the information they needed
- they had drilled for a cyber-attack through penetration testing
- they had a technology supplier they were confident in

"I'm always trying to protect us from not being 100% reliant on any system, so if any system went down I feel we're covered with a good backup, because like I said to you I've got paper files, I've got that information, I've got paper files for the health and safety and fire, care planning, etcetera, medication." – Care Provider

However, there was some doubt cast in the qualitative interviews (from representatives and leaders, and some individuals working as digital and/or cyber security leads within care providers), that there was some misunderstanding of the types of threats facing care providers, and the level of impact it could have. This was again linked back to the same themes discussed throughout this report – low digital maturity, lack of time and capacity to engage with cyber security, and limited experience of cyber incidents.

Procedures in place to respond to an incident

High proportions of care providers have procedures in place to respond to an incident. This includes three-quarters (75%) who reported that they have written guidance on who to notify if they experience a cyber security incident. A similar proportion (72%) have roles or responsibilities assigned to specific individuals during or after an incident. Just under 2 thirds (64%) have guidance around when to report incidents externally.

Less than half had the following in place: guidelines for incident management structures and issues escalation (50%), guidelines for incident identification, technical remediation or logging (46%), templates for debriefs or incident management discussions (37%), or external communication and public engagement plans (29%).

Fewer than one in 10 care providers had none of the outlined actions in place (7%), and a further 3% didn’t know what they had in place.

In comparison to the 2024 Cyber Breaches Survey, larger proportions of care providers report that they have each of these things in place than the UK businesses and charities that responded to that survey.

Care providers with one location were slightly more likely to report having several of these measures in place including: written guidance on who to notify (77% versus 75% overall), a formal incident response plan (62% versus. 61%), templates for debriefs (38% versus. 37%) and external communication and public engagement plans (31% versus. 29%). Though small, these differences are statistically significant.

Care providers with no cyber security insurance, and those with 10 or fewer rules and controls, were less likely to have many of these measures in place for when they experience a cyber security incident. In line with previous findings, having these measures in place is more common among those accessing cyber expertise from the BSBC programme or from a digital support team at an ICB, compared with the average.

Incident response and business continuity plans

Four in 5 (80%) care providers reported that they had a business continuity plan covering cyber security, and 3 in 5 (61%) reported that they had an incident response plan. Over half of care providers (53%) had both.

Providers who reported having a business continuity plan covering cyber security were asked a follow up question about its features. Over 4 in 5 reported that this plan was approved at senior level (88%), that it was a written document (87%), that it could be used in the event of a loss of digital systems (85%), and/or that it was well understood among the people who need to know about it (82%). Around half said that it was tested and updated every 6 months and each time there was a change to the responsible staff (52%).

All these features were more common among care providers with at least 11 rules and controls in place, and among those with a complete cyber incident response plan.

Looking at the features of cyber incident response plan, the pattern of responses is remarkably similar. Of those who reported that they have an incident response plan, the majority of care providers reported that it was approved at a senior level (88%), could be used in the event of loss of digital systems (85%), and that it was well understood across the people who need to know about it (84%). Just over half (51%) reported that there was regular testing and updating of their cyber incident response plans. All these features were more common among care providers with at least 11 rules and controls in place. Care providers who accessed cyber expertise from BSBC mentioned a higher than average number of features (mean of 4.30, compared with 3.85 among all participating care providers).

Of the care providers who do not have a cyber incident response plan and/or a business continuity plan (47% of providers were in this case), the leading reason, reported by a third, was that their organisation was too small for these plans to be worthwhile (35%). Around one in 5 also stated that their organisation didn't have the time or resource for this activity (19%) and/or they didn't understand what an incident response plan would offer or when it would be used (19%). One in 6 (15%) reported that this wasn't a priority for their organisation's leadership. Just over one in 10 said that this wasn't relevant to them (13%). A small number of care providers said that they were currently working on the creation of these plans (4%). Just under one in 5 (18%) did not know whether their organisation had this or these plan(s).

Compared with the average, care home providers were more likely to mention that these plans were not relevant to them (20% versus 13%) and/or that this was not a priority for their organisation's leadership (19% versus 15%).

In the qualitative interviews, business continuity plans were mentioned by care providers largely with reference to reasons for feeling confident about the organisation's ability to deal with an incident. In the representative and leaders interviews, concern was raised about an overreliance on the documents and policies surrounding cyber security, without comprehensive understanding of what experiencing a cyber-attack is likely to entail underpinning this. One of the weaknesses they had seen was the length of time recovery plans covered (24 hours for example rather than a longer period). They were concerned that this left care providers exposed because the impact of a cyber incident could last much longer.

"Providers will say that their business continuity plan covers all aspects but isn't not enough - this isn't a flood, this isn't a fire, this isn't something you can physically repair tomorrow. This is all of your data being stolen, exfiltrated and you can't get access to the systems you need." – Representative and Leader

Back-ups

As reported in section 6.2, in the survey the vast majority of care providers reported that their organisation backed up their data via a cloud (81%) or other means (47%). Among those who reported backing-up their data securely via means other than a cloud service, three-quarters (75%) stored back-ups on on-premises servers or hard-drives. Nearly two-thirds (62%) had paper copies stored securely and over half had their enterprise systems (for example MS Office) or a secure back-up system contracted elsewhere (54% and 51% respectively).

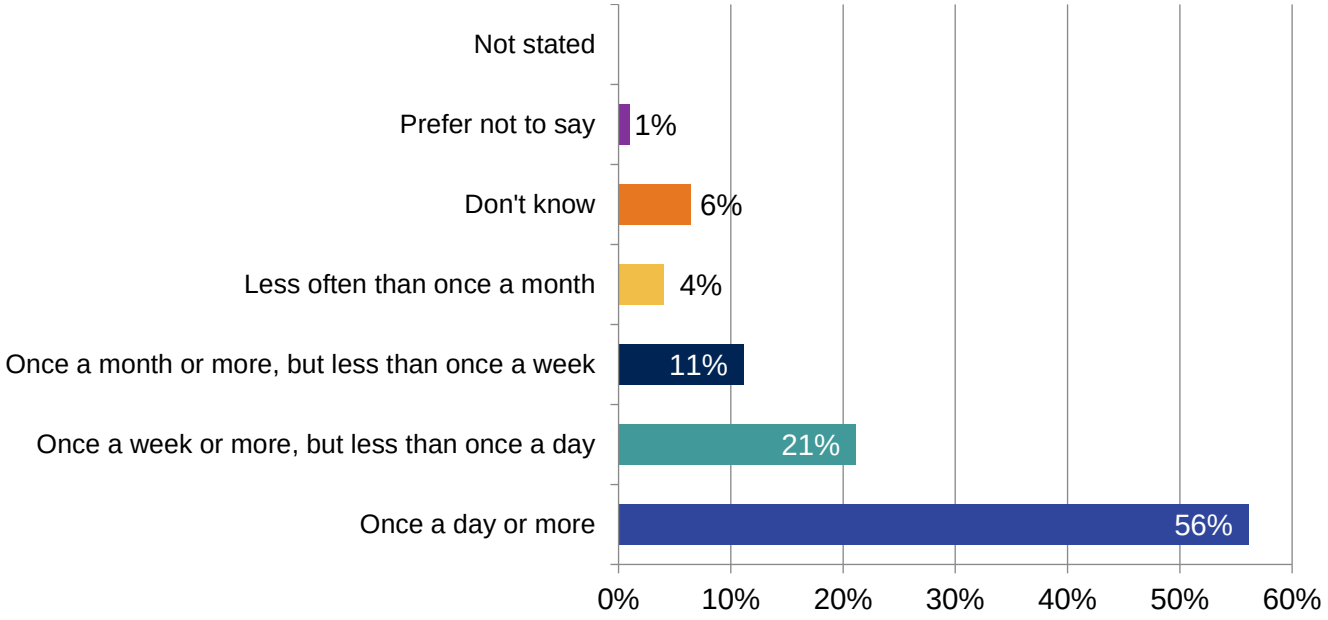
The type of back-ups differed slightly between the size of care provider. Only a quarter (26%) of care providers with fewer than 10 members of staff used a secure back-up system contracted elsewhere, compared to over half (60%) of care providers with 50 or more staff members.

There was some disparity between types of care services. Three-fifths of homecare providers used secure back-up systems contracted elsewhere (59%) or their enterprise systems (60%), compared with just over half on average (51% and 54% respectively). Care homes were not significantly different from the average with 44% using secure back-up systems contracted elsewhere and 49% using enterprise systems.

Means of backing up data varied based on the type of cyber expertise accessed: leaving aside cloud services, paper copies stored securely was the most common means of back up for those accessing cyber expertise from the BSBC (84%), while those accessing cyber expertise from an internal expert individual or an ad hoc access with external specialist favoured on-premises server or hard-drive (82% and 83% respectively) as a means of backing up their data.

Over half (56%) of care providers who back-up their data reported that this happened once a day or more. A fifth (21%) back-up data once a week or more, but less often than once a day. One in 10 (11%) back-up data once a month or more, but less often than once a week.

Figure 40: Frequency of care providers backing up their data



Base: Care providers classified as experts (512)

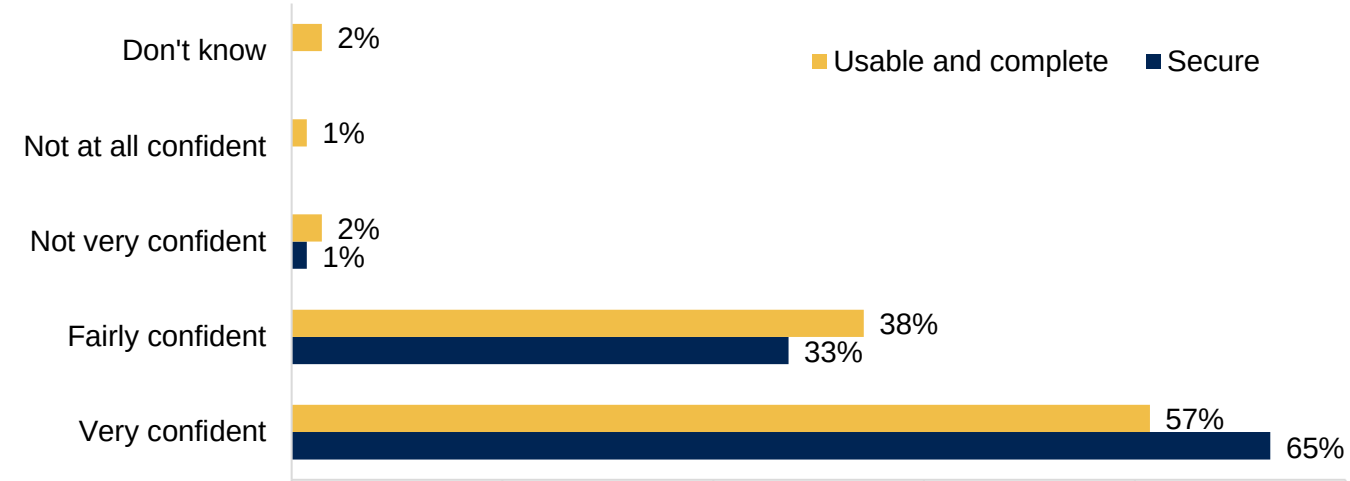
Backing up data once a day or more was a practice more common than average (56%) among certain groups of care providers, namely: organisations which had a cyber security contract with an external organisation (62%) or ad hoc access to an external specialist (61%), those with at least 50 staff (70%), and those who had experienced at least one type of cyber incident over the last 3 years (69% backing up once a day or more).

Nearly all (96%) care providers were confident their back-ups were usable and complete. Of this, three-fifths (57%) were very confident in their back-ups. Fewer than one in twenty (3%) were not confident in their back up.

There was some variation among service types, nearly all (99%) of homecare providers were confident in their back-ups, compared with 93% of care home providers and 93% of day care providers.

In addition, nearly all (98%) care providers were confident their back-ups were secure. Just over two-thirds (65%) were very confident their back-ups were secure, rising to nearly three-quarters (71%) of care providers with between 11 and 15 rules and procedures in place.

Figure 41: Care providers' confidence that their back-ups are usable and complete, and secure



	Very confident	Fairly confident	Not very confident	Not at all confident	Don't know
Usable and complete	57%	38%	2%	1%	2%
Secure	65%	33%	1%	0	0

Base: Care providers classified as experts (512)

When back-ups were discussed in the qualitative interviews, it was mainly in terms of paper back-ups or making sure that they are not solely reliant on one digital system (in case it went down). However, participants acknowledged limitations of this approach, including its time-consuming nature, potential for outdated information, and vulnerability to physical damage or loss. Another issue observed in the qualitative interviews with care providers, was that not everything was always being backed up (whether digital or paper). There was one example of a homecare provider that, through the course of the interview, identified that they did not store any paper versions of rotas and care plans, and therefore would not have access to this information if their digital systems all went down.

In the interviews with representatives and leaders, it was suggested that a poor understanding of back-ups could lead them to be inadequately implemented. For example, a cyber attack may not be identified before a bug is shared onto a back-up platform and hence infects the back-ups. It was suggested that care providers needed to continuously save back-up data, and save different versions of back-ups, to ensure they would be able to access their data if there was an incident – but this was not happening consistently in the sector.

"The failing is how quick is the organisation to detect and respond to a failure (cyber security attack) and make sure that they're not, simply, sharing that across their estate, including their backup platforms." – Representative and Leader

Cyber insurance

Just under 2 thirds of care providers (64%) report being insured against cyber security risks in some way, including just over one in 8 (12%) who said they have a specific cyber security insurance policy and

just over half (52%) who reported having cyber security cover as part of a broader insurance policy. This compares to 14% who stated they were not insured against cyber security breaches or attacks. Around one in 5 said they did not know if their organisation held cyber insurance (22%).

For comparison, larger proportions of care providers report being insured against a cyber security breach compared to businesses and charities responding to the 2024 cyber breaches survey (64% versus. 43%), with larger proportions also reporting a specific cyber security insurance policy (12% versus. 8% of businesses and 5% of charities).

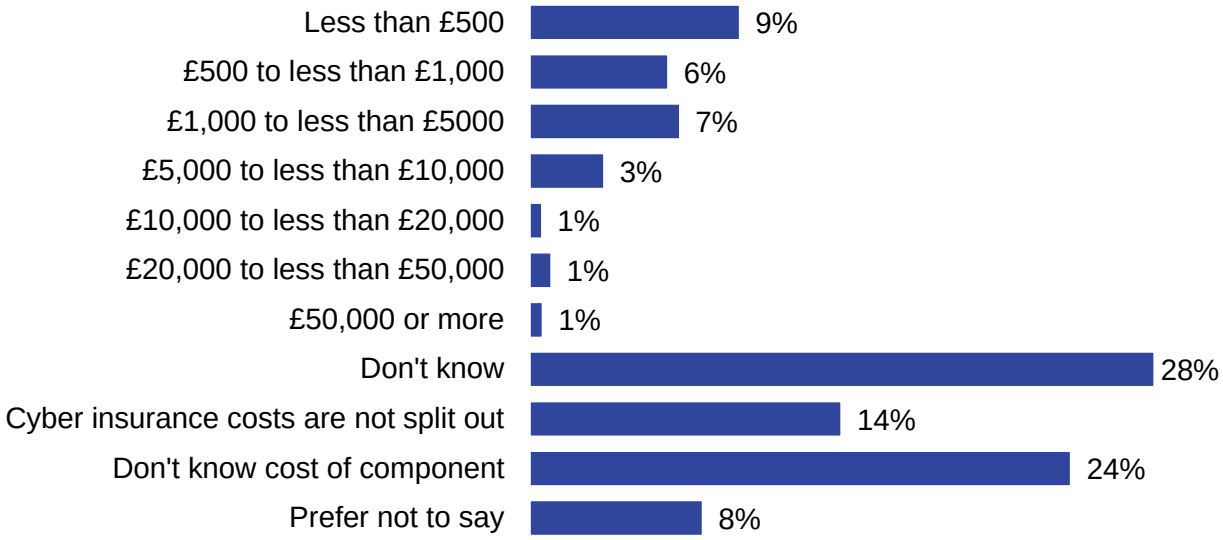
Key sub-groups are similar to those previously observed:

- over a quarter of care home providers do not know if they have cyber insurance (27%) – far more than providers of other types of services. In contrast, over a fifth of supported living providers (22%) and one in 7 homecare providers (15%) have a specific cyber security insurance, compared with 12% of providers on average
- those with no cyber incident response plan (20%) were also significantly more likely to report having no insurance compared those with complete (9%) or partial (11%) plans
- lack of cyber insurance is more common among care providers with no business plan covering cyber security (24%), compared with the average (14%) and compared with those with a business plan (11%)
- lack of cyber insurance is also more common among those with only 1 to 5 rules and controls in place (27%), compared with those with 6 to 10 (15%) or 11 or more rules and controls (11%) in place
- providers who access cyber expertise through a contract with an external organisation and the BSBC are more likely to report having cyber insurance (72% and 74% respectively, compared with 64% on average)

Almost all care providers with cyber security insurance reported that they had never made a claim for cyber security breaches (99%).

A quarter of care providers who said they had cyber insurance (26%) were able to say how much they paid for it, either providing the exact amount or a range. The average (mean) amount spent on cyber insurance reported in the survey was just over £5,270. The median cost of cyber insurance reported by care providers was £750. Around one in 10 (9%) said that it cost them less than £500, 6% said it cost them between £500 and £1,000, and 7% said it costs them between £1,000 to £5,000. Many care providers who had cyber insurance were not able to say: just under 3 in 10 (28%) did not know how much their organisation paid for cyber insurance, a quarter (24%) did not know the cost of the component of cyber risk within their policy, and a further 14% stated that the cost of cyber insurance was not split out in their policy.

Figure 42: Amount care providers pay for cyber insurance



Base: Care providers who have a specific cyber security policy (370)

The mean cost of cyber insurance was higher among care providers who had experienced at least one type of cyber incidents over the last 3 years (£10,226), compared with those who had not experienced any (£2,046).

Reasons for not having cyber insurance were explored in the qualitative interviews. Among representatives and leaders, it was felt that some smaller care providers did not have cyber insurance policies because they were deterred by the cost. Another barrier mentioned was a lack of understanding of the impact a cyber incident could have and how much it could cost. A participant in these interviews reported that the uptake of cyber insurance in the sector is relatively low compared to other industries, leaving many providers potentially exposed to significant financial burdens in the event of an incident.

"Smaller care providers often underestimate the cost of cyber incident response and recovery, and therefore can be reluctant to buy cyber insurance, when the actual cost of a cyber incident can often be in tens of thousands of pounds." – Representative and Leader

In the 2 interviews with care providers where insurance was mentioned – this was in the context of it giving them confidence that they would be prepared to deal with a cyber incident.

Reporting an incident

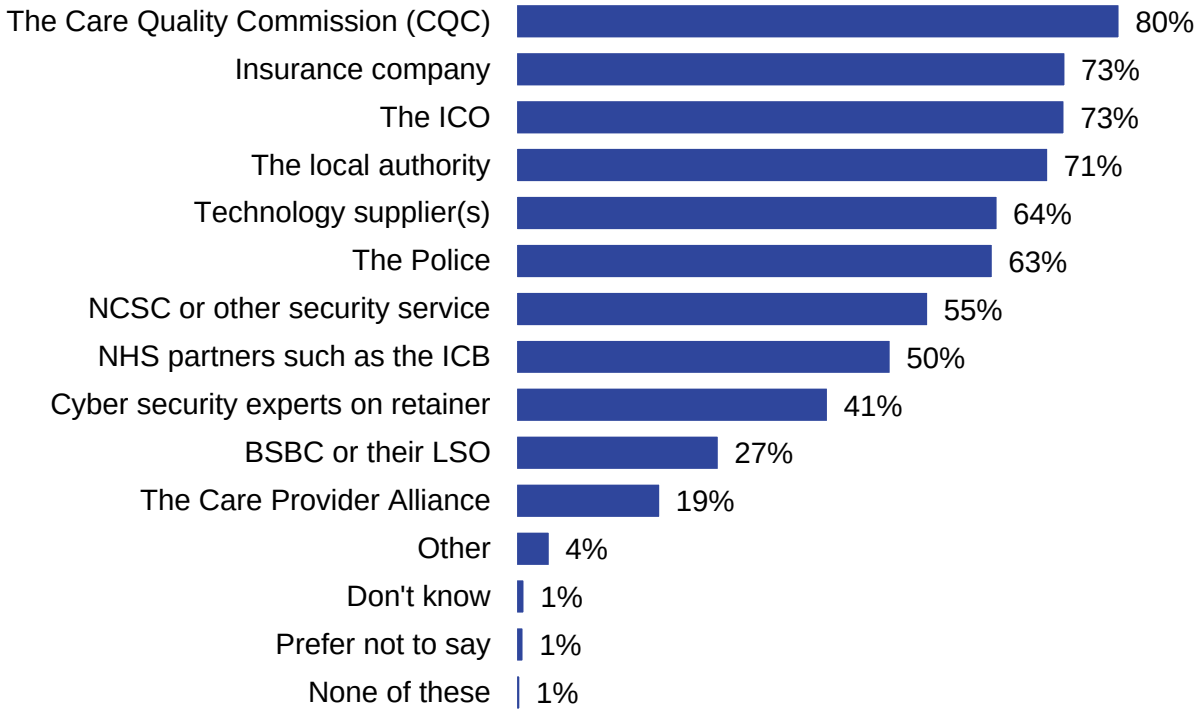
Care providers were presented with a list of organisations, asking them which of them they would inform in the event of an incident. The majority of care providers stated that they would report it to the Care Quality Commission (CQC) (80%). Around 7 in 10 also stated that they would inform the Information Commissioner's Office (ICO) (73%), their insurance company (73%) and/or the local authority (71%).

Around 3 in 5 stated that they would inform technology suppliers (64%), the police (63%), National Cyber Security Centre or other security service (55%). Half (50%) stated that they would inform NHS partners such as the ICB, and around 2 in 5 (41%) said they would inform cyber security experts they have on retainer.

Around a quarter (27%) said they would inform BSBC or their local support organisation. Only around one in 5 (19%) said they would inform the Care Provider Alliance.

Note that this question was prompted: in practice, when faced with an incident, care providers may not necessarily think of informing all the organisations they said they would inform when looking at the list.

Figure 43: Organisations care providers would inform in the event of a cyber incident



Base: Care providers (575)

Providers with just one location were more likely than the average to say they would report the incident through several of these routes including cyber security experts they have on retainer (44% versus, 41%), NHS partners such as the ICB (52% versus. 50%), the CQC (82% versus. 80%), the Care Provider Alliance (20% versus. 19%), the Police (66% versus. 63%) or the National Cyber Security Centre or other security services (58% versus. 55%).

Care providers with more than 11 rules or controls in place were also more likely than average to inform all of these organisations, as were care providers with complete incidence response plans, and those with formal policies covering cyber security.

Accessing cyber expertise through the BSBC or an ICB was associated with a higher than average proportion of people saying they would report the incident to 9 of the organisations listed.

Hypothetically, in the qualitative interviews care providers explained that if they experienced an attack, the type of attack they experienced would determine which organisation(s) they would report it to. For example, if it were:

- a data breach, they would report it to the Information Commissioner's Office (ICO)
- a ransomware attack, then to the police

In any case, the care providers who took part in the depth interviews suggested that their commissioners (local authorities or the ICB) would also be informed.

"I would obviously report to things like the ICO. So, I would have to report it to people like local authorities, so I would have to report it to our commissioners in ICB." – ***Care Provider***

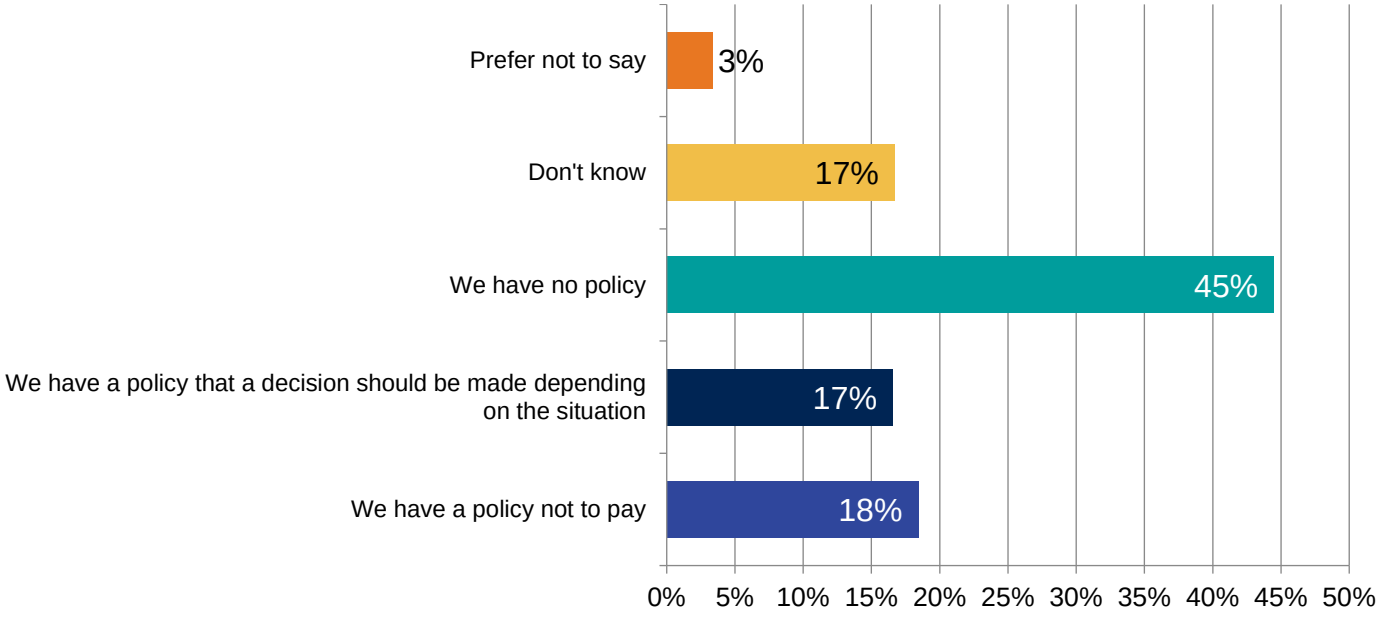
There were some barriers to reporting a cyber incident mentioned in the qualitative interviews with representatives and leaders. One said that fear of reputational damage could discourage care providers from reporting incidents. Another said that fear of fines or inspections could also discourage care providers. Reporting of incidents is explored further in chapter 10.

"[Reporting incidents] makes them really vulnerable. What they worry about is fines from the ICO. Bear in mind, again, I draw the parallels with safeguarding a lot. If you have a serious safeguarding incident, that will trigger a CQC inspection. The last thing they want to do is trigger a CQC inspection." – Representative and Leader

Policy on ransoms

In the survey, over 2 in 5 (45%) care providers said they have no policy on paying ransoms. Just under one in 5 (18%) said they have a policy not to pay a ransom, and a similar proportion (17%) said they have a policy that a decision should be made depending on the situation. The same proportion (17%) said they didn't know if they had a policy or what it was.

Figure 44: Policies care providers have on paying ransoms



Base: Care providers classified as experts (559)

Sub-group differences are broadly aligned with those previously observed:

- care home providers were significantly more likely to report having no ransom policy compared to providers with no care homes (53% versus. 37%)
- not having a policy on paying ransom is more common among those with no cyber incident response plan (60%), those with no business plan covering cyber security (55%), and those with only 1 to 5 rules and controls in place (63%), compared with the average (45%)

7.2 Technology suppliers' policies and procedures in case of incidents

Technology suppliers recognised that even with a range of preventative measures in place, they were still vulnerable to a cyber incident. Policies and procedures in case of incidents were therefore considered as important as prevention and detection. In the survey, technology suppliers reported the following procedures and policies in place to help respond to an incident:

- 8 in 9 stated that they had a disaster recovery capability for the ICT infrastructure
- 7 in 9 reported having roles or responsibilities assigned to specific individuals during or after an incident, a formal incident response plan, guidelines for incident identification, technical remediation or logging, guidelines for incident management structures (for example meeting groups) and issues escalation (for example to directors) and or cyber insurance
- 6 in 9 reported having written guidance on who to notify for example Cyber Incident Signposting Service (CISS) and insurers, guidance around when to report incidents externally, for example to regulators or insurers and or a disaster recovery capability for the data within the system, such as an air-gapped backup
- Fewer reported having external communications and public engagement plans (5) and or templates for debriefs or incident management discussions (3)

The characteristics of the cyber incident response plans reported by the 7 technology suppliers who had them, were largely consistent between technology suppliers. Six stated that their cyber incident response plan was a written document, was well-understood by those that need to know about it, was approved at a senior level and it could be used in the event of loss of digital systems. Five stated that the plan was tested and updated every 6 months and each time there was a change to the responsible staff. Just one technology supplier said that none of these applied to their cyber incident response plan. In the qualitative interviews, technology suppliers also commonly mentioned sharing some of their knowledge and know-how on cyber incident response plans with small care providers to guide them in developing their own plans.

"We guide smaller care providers more…this includes guidance on business continuity plans." – Technology Supplier

ICT infrastructure testing happened once a year at minimum for the majority of technology suppliers. The majority reported that they tested their ICT infrastructure disaster recovery capability once a year or more, but less than once every 6 months (5). Two technology suppliers reported that they tested their ICT infrastructure disaster recovery capability once every 6 months or more, but less than monthly. Just one technology supplier said they didn't know the frequency of these tests.

8 in 9 of the technology suppliers said they backed up their data once a day or more. The remaining one preferred not to say. Most of the technology suppliers explained that it takes 24 hours or less, but more than one hour to access back-up data (6). Two also stated that it could be accessed in one hour or less.

In the qualitative interviews, while the technology suppliers confirmed the ICT infrastructure testing and data backup reported in the survey responses, it was stated that a full operational test of their cyber incident continuity arrangements was not possible due to the potential disruption and cost to the organisation. This meant there was often strong emphasis on testing discrete elements of the overall arrangements, for example undertaking penetration testing and conducting mock phishing attacks.

These were procured from appropriately accredited third parties. These were regarded as core measures to conduct as they largely explored one of the main cyber vulnerabilities: staff behaviour and practices. How frequently these measures were undertaken varied from quarterly to annually. All technology suppliers gained insights each time the measures were undertaken, both from a technical control point of view and in terms of staff practices and awareness. The latter fed into individual and collective staff awareness raising and training plans. Recognising the value of penetration testing, it was suggested that ensuring care providers undertook penetration testing would be a high impact, low-cost route to increasing the cyber resilience of the sector.

"We introduced software that sends bogus phishing attacks to staff to test their reaction." – Technology Supplier

5 in 9 technology suppliers had a specific cyber security insurance policy and 3 in 9 said they had cyber security cover as part of a broader insurance policy. None of these 8 technology suppliers had ever made an insurance claim for cyber security breaches. However, in the qualitative interviews they confirmed their awareness of the response and recover support available through the insurer.

4 of the technology suppliers in the survey preferred not to say what their policy on paying ransoms was. 2 explained that they had a policy that a decision should be made depending on the situation, one said they had a policy not to pay and none said they had a policy to pay.

7.3 Technology suppliers' confidence in ability to deal with incidents

In the qualitative interviews, technology suppliers were confident in their cyber incident response and recovery arrangements, and those of their Platform as a Service (PaaS) and/or Infrastructure as a Service (IaaS) suppliers in particular. Implementing the measures and controls required to gain certifications and/or accreditations such as Cyber Essentials Plus or ISO27001, and keeping up to date on emerging threats, were viewed as part of minimising their cyber risk and justification for their confidence. Most technology suppliers stated they kept up to date on emerging cyber threats through reviewing publicly available information and receiving updates from their contracted experts, such as penetration testing suppliers. As mentioned in section 8.2, technology suppliers reiterated that they were less confident in relation to their staffs' behaviours and practices, with a resultant focus on awareness raising and training.

"The cyber security risks are our staff's practices, and hence a strong focus on awareness raising and training, and the platform and infrastructure we use for our SaaS." – Technology Supplier

Several technology suppliers were very confident in their organisation's ability to identify the need for, and respond to, critical patches required (7) and adapt to the findings of external cyber risk reviews or third-party penetration testing (6).

Most technology suppliers (6) reported that they were fairly confident in their organisation's ability to protect and secure their corporate data and systems; protect and secure their portfolio of products, services and customers' data; identify new cyber security threats, risks and issues; and respond promptly to new cyber security threats, risks and identified issues.

Feeling not very confident in their organisation's ability to identify new cyber security threats, risks and issues; respond promptly to new cyber security threats, risks and identified issues; and log security issues and decisions and communicate them appropriately to leaders; was only mentioned once.

08

Technology suppliers' approaches to cyber security and risks

8 Technology suppliers' approaches to cyber security and risks

This chapter provides findings on technology suppliers' culture and attitudes to cyber security, their governance arrangement and risk management policies. Small sample sizes mean that numbers rather than percentages are reported.

Summary

Technology suppliers generally had a strong awareness of cyber security, current and emerging threats, and its importance within the adult social care sector.

They mentioned a range of characteristics to demonstrate their cyber maturity and resilience, including senior leadership on cyber security, high prevalence of business continuity plans, formal policies covering cyber security, and high take up of various rules and controls associated with cyber security. All or most participating technology suppliers used third-party cyber services such as IT system monitoring and threat detection, and penetration testing. Technology suppliers also reported high levels of confidence in their digital supply chain.

Maintaining a good reputation, and the likely commercial impact of an incident, were the main drivers for good cyber security governance, practices and supply chain arrangements.

8.1 Organisational culture and attitudes to cyber security

Technology suppliers reported that they recognised the potential impact of cyber attacks on both care providers and their own businesses, particularly in the context of Software as a Service (SaaS) solutions. They were confident in their cyber security arrangements but recognised that they could still be victim of a cyber incident, and consequently the importance of response and recovery arrangements.

Technology suppliers also said that they were aware of the evolving threat landscape and the need to stay ahead of emerging risks. The Advanced Computer Software Group incident served as a further prompt for many technology suppliers to review and strengthen their security measures. However, there were some concerns about the ability to fully test and validate their cyber security arrangements due to the potential disruption to operations.

There was some scepticism expressed by the sector leaders and representatives around technology suppliers' approach to cyber security. There was more confidence that suppliers on the Assured Solutions List (ASL) would have the appropriate organisational culture and management around cyber security in place, but recognition that its scope is limited. Representatives and leaders had concerns that those outside the ASL, particularly smaller start-up companies, would be less focussed on implementing a robust cyber resilience approach. They also noted that that technology suppliers are commercial organisations so might prioritise sales rather than producing a safe and fit-for-purpose product. Another concern was around care providers being locked into their technology supplier due to potentially high costs and the length of time it can take to switch, and that this lack of flexibility could hinder their ability to adapt to evolving cyber security threats and adopt better solutions.

8.2 Governance, leadership and risk management within technology supplier organisations

Technology suppliers mentioned a range of characteristics to demonstrate their cyber maturity and resilience.

In terms of leadership on cyber security, they indicated that:

- they all had a Board member or senior manager with responsibility for cyber security. Cyber security was considered a high priority in their organisation with regular review mechanisms in place, such as monthly senior management review of cyber risks report
- there was high recognition of the negative impact on reputation, and commercial impact of this, in the event of a cyber incident and how it is responded to and recovered from in terms of minimising impact for care provider customers

In terms of governance of cyber risks and incidents:

- all technology suppliers who participated in the research had a business continuity plan that covered cyber security, and all have formal policy or policies in place covering cyber security risks
- 8 out of 9 technology suppliers in the survey had cyber security included on the organisation's risk register and a written list of the most critical data, systems or assets that their organisation wanted to protect
- 6 technology suppliers tested and updated the business continuity plan at least every 6 months

Participating technology suppliers had in place a range of rules and controls. All of them used the following basic hygiene controls:

- up-to-date malware protection
- firewalls that cover their entire IT network, as well as individual devices
- restricting IT admin and access rights to specific users
- a password policy that ensures users set strong passwords

8 of 9 of technology suppliers also used the following hygiene controls:

- a policy to apply software security updates within 14 days
- security controls on company-owned devices (for example laptops)
- backing up data securely via a cloud service
- an agreed process for staff to follow when they identify a fraudulent email or malicious website

Seven technology suppliers had a virtual private network (VPN), and 6 used 2-factor authentication when people accessed their network or applications, specific rules for storing and moving personal data files securely, and monitoring of user activity. Less common rules and controls were separate wi-fi networks

for staff and visitors (4 mentions), only allowing access via company owned devices (3 mentions) and backing up data securely via other means than a cloud service (3 mentions).

"A key aspect is ensuring the basic hygiene factors, as per Cyber Essentials, are in place and practices and controls reflect this." – Technology Supplier

The technology suppliers accessed a range of cyber security expertise. These included:

- 7 out of 9 had an internal expert individual and 4 had an internal expert team.
- 3 had ad hoc access with an external specialist and 2 had a contract with an external organisation.

In addition, all of them were aware of the range of National Cyber Security Centre (NCSC) guidance, resources and tools on cyber security.

All or most participating technology suppliers used third-party cyber services, including:

- company IT system monitoring and threat detection (9 mentions)
- product monitoring and threat detection (8 mentions)
- email threat detection (8 mentions)
- penetration testing of the organisation by third party specialist (8 mentions)
- penetration testing of products by third party specialist (7 mentions)

In the qualitative interviews, technology suppliers highlighted the importance of staff training on cyber security and how staff behaviours and practices were one of their main vulnerabilities, for example falling foul of a phishing attack. They showed a strong commitment to cyber security related training.

"Very regular training sessions are provided to staff to educate and then reiterate sound cyber security practices and how these benefit their every day life and not just their work environment." – Technology Supplier

Reflecting this, all 9 technology suppliers in the survey either tended to agree or strongly agreed to the following cyber security training related statements:

- information on cyber security is provided to all staff when they join your organisation
- compulsory training on cyber security is provided to all staff when they join your organisation
- all staff in your organisation receive regular refresher information or training on cyber security (annually or more often)
- this organisation promotes awareness of cyber security in an effective way
- this organisation knows where to go for more advanced cyber security training for staff
- this organisation knows where to go for advice and expertise on cyber security

8.3 Technology supplier measures undertaken to ensure supply chain

In the survey, 7 out of 9 technology suppliers had reviewed the potential cyber risks presented by their immediate supply chain. Only 3 out of 9 had reviewed the cyber security risks presented by their wider supply chain, defined as their suppliers' suppliers.

Most technology suppliers agreed or strongly agreed with the following digital supply chain statements:

- I am confident that the technology we use has appropriate cyber security measures in place (8 out of 9 participants)
- I trust my digital product and services suppliers to act responsibly towards us if they experienced a catastrophic cyber incident (8 out of 9 participants)
- when purchasing digital technology, commissioning staff in my organisation know what to look out for to ensure the technology is safe and secure (7 out of 9)
- when we purchase digital products or services, we would be prepared to trade functionality, or to pay more, to receive high quality cyber security (6 out of 9)
- when purchasing digital technology, products and services, data security considerations are built into the contracting process (7 out of 9)
- when purchasing digital technology, products and services, interoperability considerations are built into the contracting process (8 out of 9)

When contracting with their suppliers, all 8 technology suppliers who agreed that data security considerations were built into the contracting process were able to identify measures they had taken to establish the cyber resilience of their digital supply chain. These included setting minimum security requirements (7 mentions); requiring security certification, such as Cyber Essentials, or ISO27001 (7 mentions); and seeking evidence or assurance that the supplier meets contractual requirements (7 mentions).

8 technology suppliers had cyber insurance cover as part of their cyber security risk mitigation approach (one respondent did not know) – this compared to 2 in 3 (64%) of care providers.

Despite these measures, sector representative and leaders raised a concern regarding the lack of transparency for care providers of the cyber security arrangements through the technology suppliers' technology stack. The technology stack refers to the SaaS on Platform as a Service (PaaS) on Infrastructure as a Service (IaaS) arrangements. This would be particularly pertinent with the 15% of technology providers the RER identified as not evidencing their arrangements. The research was not able to secure interviews with this group of technology suppliers.

"As a result of the Cyber Essentials work, we shifted from (another) system to an Azure based PaaS as this was preferred by NHS from a security point of view." – Technology Supplier

The measures technology suppliers have in place to respond to a cyber incident are discussed in chapter 7.

8.4 Technology suppliers' products and services reducing cyber security risks

Technology suppliers stated that the main way their products reduced cyber security risks for care providers was through being SaaS applications. Through this route, the application and the data are cloud-based and subject to the cyber security measures of the technology supplier and their PaaS and/or IaaS providers, which enable controls such as prompt and automatic implementation of patches and/or upgrades, greater access controls, and detection and stopping of attacks that may come from a care provider's affected ICT infrastructure. When a similar application runs on the care provider's own or contracted ICT infrastructure, it is reliant on their own cyber security arrangements, which will generally be less robust. One technology supplier did also offer supply of configured EUDs, set-up of a Virtual Private Network (VPN) and other ICT infrastructure measures to give a broader cyber resilience but this was rarely taken up by care providers. This was due to care providers either not recognising the need for these measures or not wishing to pay for them.

"The nature of our product as a SaaS ensures a degree of resilience." – Technology Supplier

7 out of 9 technology suppliers stated that their technology and/or solutions positively reduced cyber security risks to their customers via unauthorised accessing of files or networks by staff, even if accidental; and unauthorised accessing of files or networks by people outside an organisation.

6 out of 9 technology suppliers cited other types of cyber security breaches or attacks and 5 mentioned denial of service attacks, defined as attacks that try to slow or take down a website, applications or online services.

Just one technology supplier said that their technology and/or solutions positively reduced cyber security risks to their customers via hacking or attempted hacking of online bank accounts, people impersonating an organisation in emails or online and phishing attacks, defined as staff receiving fraudulent emails or arriving at fraudulent websites; and takeovers or attempts to take over their website, social media accounts or email accounts.

09

Relationship between care providers and technology suppliers

9 Relationship between care providers and technology suppliers

The chapter explores views on where the responsibilities for cyber risks in the digital supply chain does and should lie, and care providers' confidence in the cyber security of the technology products and services they use. It also looks at how cyber security affects the selection of a supplier and the contracting process, and the on-going support offered by technology suppliers including when cyber security incidents occur.

Summary

In practice, ownership for cyber security risks is a mixed responsibility between care providers and technology suppliers. As care providers are ultimately accountable for their data they see themselves as responsible for assuring themselves of the cyber resilience of their digital arrangements. However, lack of in-depth cyber expertise and resources to dedicate to cyber security mean care providers rely heavily on their technology suppliers. They place a significant amount of confidence in their technology suppliers having appropriate cyber security measures in place. This led technology suppliers and sector representatives and leaders to think that care providers assumed that their technology suppliers were fully responsible for cyber security – which did not reflect care providers' views.

When purchasing technology, there was also high confidence among care providers in their commissioning staff's ability to purchase safe and secure technology. Technology suppliers confirmed that cyber security is increasingly considered when technology is purchased, in particular by large care providers.

Two in 3 care providers (68%) agreed that they would be prepared to trade functionality, or pay more, to receive high quality cyber security. Technology suppliers mentioned that in practice, buying decisions are mostly based on price and functionality, rather than cyber security, and the care providers who took part in the qualitative interviews confirmed this.

There appears to be limited ongoing monitoring of cyber security risks by care providers after the contracting process, due to lack of time, size of organisation (too small to have bargaining power), and not knowing what checks to carry out.

Looking at the support offered to care providers by their technology suppliers, this tends to be at the set-up stage and focussed around functionality rather than cyber security. In the event of an incident on the supplier side, support would be offered to the care provider in the form of back-up data, electronic forms so the organisation can continue to operate offline. Support when the care provider is the victim of a cyber incident appears to be offered on a goodwill basis rather than on a formal basis.

9.1 Responsibility for cyber security and accountability

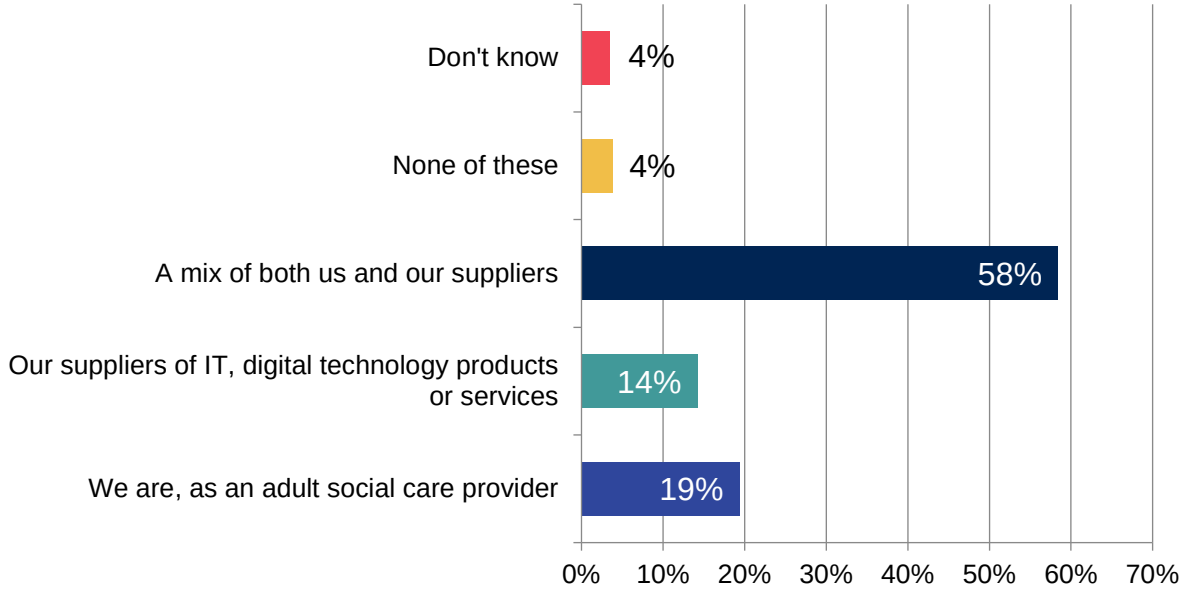
Participants were asked where responsibility for cyber security lies in practice, and where it should lie with care providers, technology suppliers, or a mix of both.

Where responsibility lies in practice

In the survey with care providers, responsibility in practice for cyber risks in care providers' digital supply chain was stated as being a mix between the care provider and their technology suppliers by 3 in 5

(58%) of care providers. Only 14% stated that cyber security was their technology suppliers' responsibility.

Figure 45: Where care providers felt primary responsibility for outsourced IT and digital technology lie in practice



Base: Care providers (575)

Looking at sub-groups, there are some differences in the proportion stating cyber security is a shared responsibility:

- smaller care providers with under 10 staff also had a lower proportion stating it was a shared responsibility (44%) and had a corresponding greater proportion in stating that it was their own responsibility (29%)
- higher proportions of care providers with access to external support stated it is a shared responsibility (67% for contract with external organisation and 68% for ad hoc access to external expert)
- lower proportions of care providers with 1 to 5 rules and controls (35%) stated it is a shared responsibility, compared to those with 11 to 15 rules and controls (64%)
- the proportion who stated cyber security was a mixed responsibility was also lower among care providers who did not have either formal policies or a business continuity plan covering cyber security (43% and 45% respectively)

In contrast, technology suppliers (in the survey and qualitative interviews) and sector representatives and leaders shared a common view that care providers frequently assumed that their technology suppliers were fully responsible for cyber security.

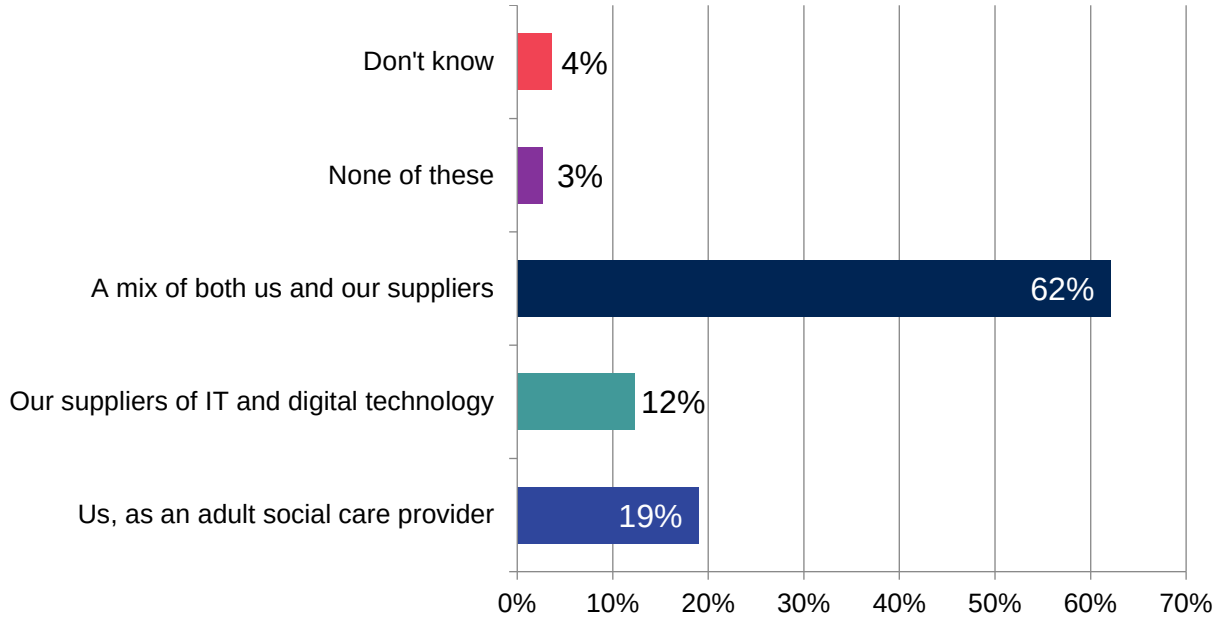
"Still a significant number of care providers regard cyber security as the sole responsibility of the solution supplier and expect this to have been addressed rather than undertaking any due diligence to ensure this is the case." – Technology Supplier

While this appears to contradict the views expressed by a majority of care providers in the survey (only 14% of them said cyber security was their technology suppliers' responsibility), this discrepancy could be accounted for by the nuances around how care providers fulfil their responsibility, with care providers relying heavily on technology suppliers and trusting them to provide cyber secure solutions, and therefore not necessarily undertaking appropriate levels of due diligence. What may be regarded as trust by care providers may be perceived as passing of responsibility by technology suppliers. It was suggested that this reliance had increased with the greater use of SaaS by care providers, for example with care management and back-office systems. Care providers' high level of confidence in the cyber security of the technology products and services used is detailed in section 9.2 below.

Perceptions of where responsibility should lie

In the survey, care providers' view on where responsibility for cyber risks *should* lie was very similar to their view of current actual responsibilities. Three in 5 (62%) stated a mix of responsibilities between the care provider and their technology suppliers would be appropriate. Only 12% stated that it was their technology suppliers' responsibility.

Figure 46: Where care providers felt primary responsibility for outsourced IT and digital technology should lie



Base: Care providers (575)

Sub-group differences were very similar to the differences in the responsibilities in practice question detailed above.

Similarly, technology suppliers (in the qualitative interviews and survey), agreed that responsibility for cyber risks in care providers' digital supply chain should be a mix of responsibilities between the care provider and their technology suppliers. The sector representatives and leaders interviewed concurred with this view.

Still, across the qualitative interviews there was recognition that even in an environment of accepted mixed responsibilities, the ultimate accountability lay with the care provider.

"I think it's everybody's responsibility. Ultimately it will be mine, because I'm the registered person" – Care Provider

Sector representatives and leaders and technology suppliers also shared the perception that care providers are ultimately accountable for their data and therefore responsible for assuring themselves of the cyber resilience of their digital arrangements. This was evidenced by the Care Quality Commission (CQC) focus on cyber security through its 'Well-Led' theme, which reinforces the responsibility and accountability of care providers.

Challenges around taking ownership of cyber security

In the qualitative interviews, some challenges were mentioned which affected how responsibility was shared and fulfilled in practice.

Care providers consistently indicated in the interviews that while recognising they had ultimate accountability, they relied significantly on their technology suppliers to ensure their cyber resilience. This related to their Information, Communication and Technology (ICT) service suppliers as well as their technology suppliers (as defined for this research). The technology suppliers and sector representatives and leaders interviewed shared this view, particularly in relation to smaller care providers.

"I suppose (cyber security responsibility is) a little bit with everybody…because…ultimately it's us that have bought the software but we're relying on that [sic] the supplier has everything." – Care Provider

Aligned and effective collaboration across the digital supply chain was thought to be required to reduce cyber security risk as a whole, and participants noted that this needed to be done in the context of a system understanding of respective responsibilities and accountabilities. A challenge in achieving this was the somewhat low cyber security maturity, capacity and capability in the sector, and care providers facing competing priorities. To compensate for this, technology suppliers felt that greater emphasis was being put on them to proactively address and evidence their cyber resilience.

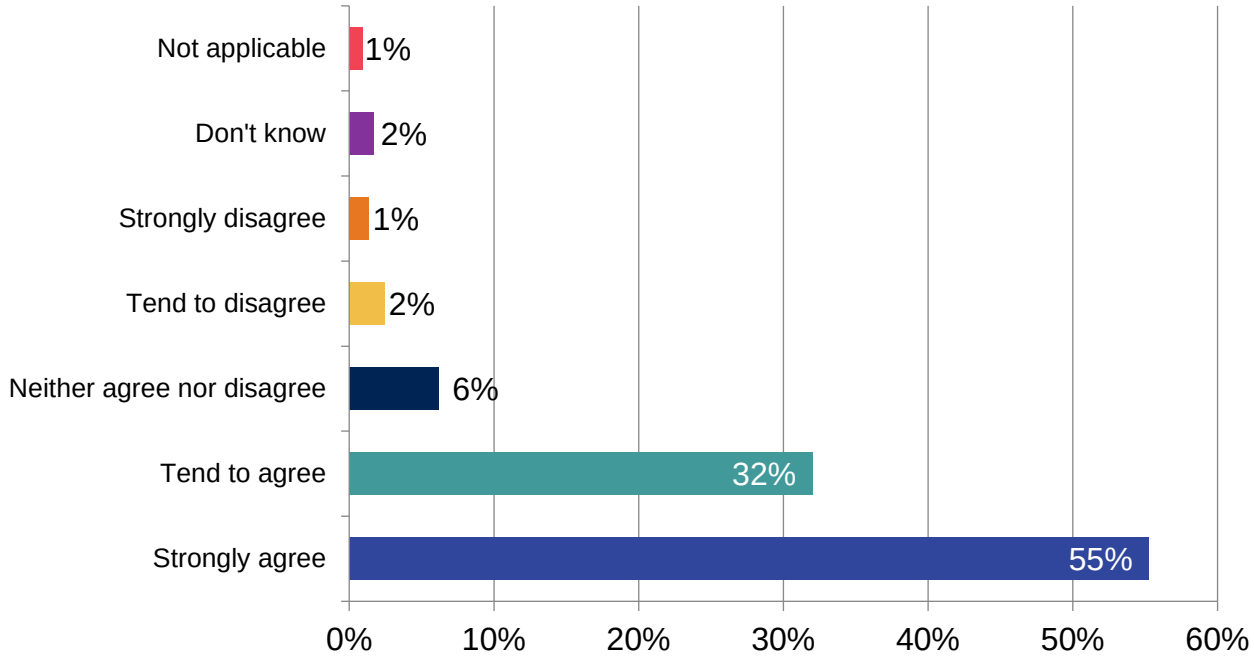
Indeed, concerns were expressed in the interviews that care providers did not always take ownership of their own cyber security for aspects that would not be the responsibility of a SaaS technology provider (such as care provider practices, staff behaviours, ICT setup and end user device configuration). In the example below, this was due to a lack of cyber expertise within the care provider organisation.

"We have had instances of detecting for example a distributed denial of service (DDoS) attack from the customer's IP address. The customer had not been aware of malware being on their computers and this resulted in our blocking the customer's IP addresses and so no carers could log onto the system. We had to explain that the lack of access to the system was an issue at their side rather than ours and then provided the care provider with advice and guidance on how to respond to and recover from the situation." – Technology Supplier

9.2 Confidence in the cyber security of the technology used

Care providers' confidence that technology suppliers have appropriate cyber security measures in place is very high: in the survey, 87% of care providers agreed with the statement 'I am confident that the technology we use has appropriate cyber security measures in place'. Asked the same statement, 8 out of the 9 technology suppliers who completed the survey also agreed.

Figure 47: Confidence of care providers that the technology used have appropriate cyber security measures in place



Base: Care providers (575)

This level of agreement was similar across care providers' service type and organisation size. Agreement with the statement was higher than average among care provider with 11 rules or controls (94%), those with a complete cyber incident response plan (96%), those with a specific cyber insurance policy (97%) and those accessing cyber expertise from BSBC at the Digital Care Hub (95%).

This confidence was also shared by care providers in the qualitative interviews.

"I can't imagine there's anybody safer than Microsoft, I just can't, and (our technology supplier), I can't imagine there's anyone safer than them, because they have to protect our information as well." – Care Provider

9.3 Selecting a supplier or a technology product or service

Knowing what to look out for when selecting a supplier

There was high confidence among care providers in their commissioning staff's ability to purchase safe and secure technology: 4 in 5 either tended to agree (37%) or strongly agree (44%) with the statement 'when purchasing digital technology, commissioning staff in my organisation know what to look out for to ensure the technology is safe and secure'. Only 6% of care providers disagreed.

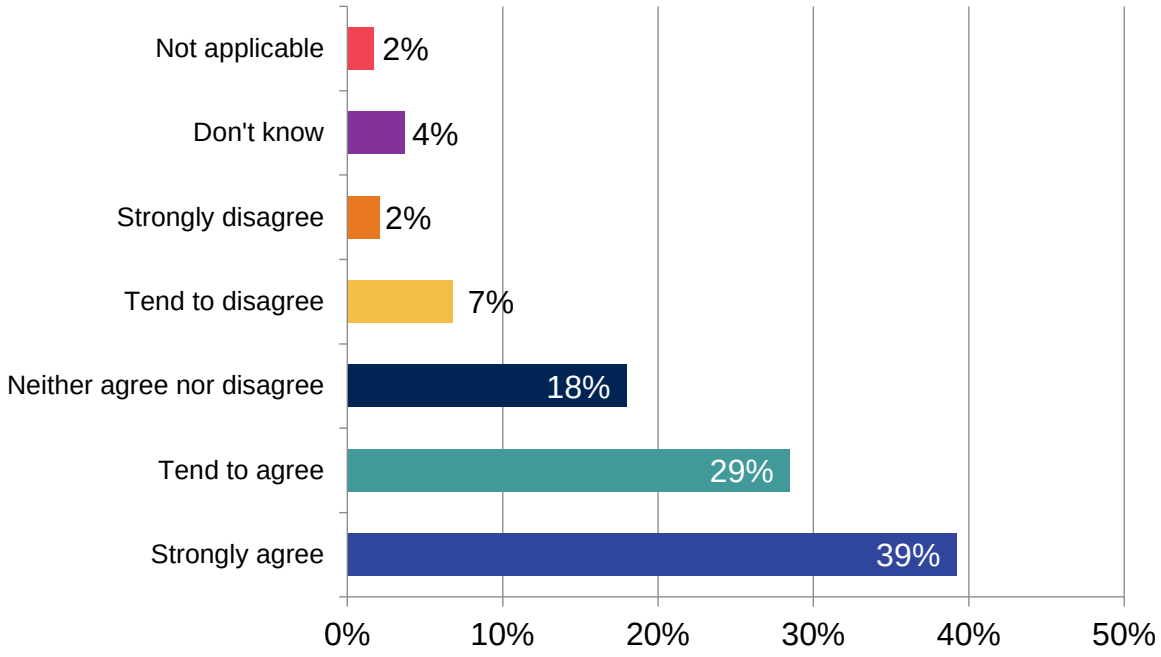
Agreement was slightly lower for care providers with only 1 to 5 rules or controls in place (67%); no business continuity plan covering cyber security (70%); and no formal policies covering cyber security (69%).

When considering the same statement, 7 of 8 technology suppliers agreed with it in relation to their own procurement.

Functionality and price versus cyber security

In response to the survey statement ‘when we purchase digital products or services, we would be prepared to trade functionality, or to pay more, to receive high quality cyber security’: 2 in 3 (68%) agreed, including almost 2 in 5 (39%) who strongly agreed. 9% of care providers disagreed.

Figure 48: Whether care providers would be prepared to trade functionality, or to pay more, to receive high quality cyber security



Base: Care providers (575)

Care providers who were most likely to agree with the statement were those who had: accessed expertise from BSBC at the Digital Care Hub (80%); a specific cyber security insurance policy (83%); and those who had 11 to 15 rules or controls in place (75%).

This is consistent with the findings from technology suppliers, who were asked to consider a similar statement: ‘When customers purchase digital technology, functionality and price are more important considerations for them than cyber security’. Seven out of the 9 technology suppliers who completed the survey agreed with this.

However, while technology suppliers reported more care providers seeking assurance on cyber security, they also thought that buying decision still commonly focused on functionality and cost. Care providers who took part in the depth interviews also supported this view. Still, they noted that procuring a technology supplier was an infrequent activity as usually the selected application will be used for several years to realise the return on investment, with there often being barriers (in terms of costs and interoperability) to changing applications.

9.4 Contracting with technology suppliers

Due diligence

The qualitative interviews showed that cyber security is increasingly considered when technology is purchased. Technology suppliers interviewed as part of the qualitative interviews explained there had been an increase over the last 2 to 3 years in care providers asking for information on the technology

supplier's cyber security arrangements. This was felt to be driven by both DSPT registration and in response to commissioner framework qualification questionnaires. Technology suppliers' and sector representatives and leaders' perception was that care providers' cyber security exploration was biased towards care planning, management and rostering applications rather than areas such as Human Resources and Finance systems, or their ICT setup and support.

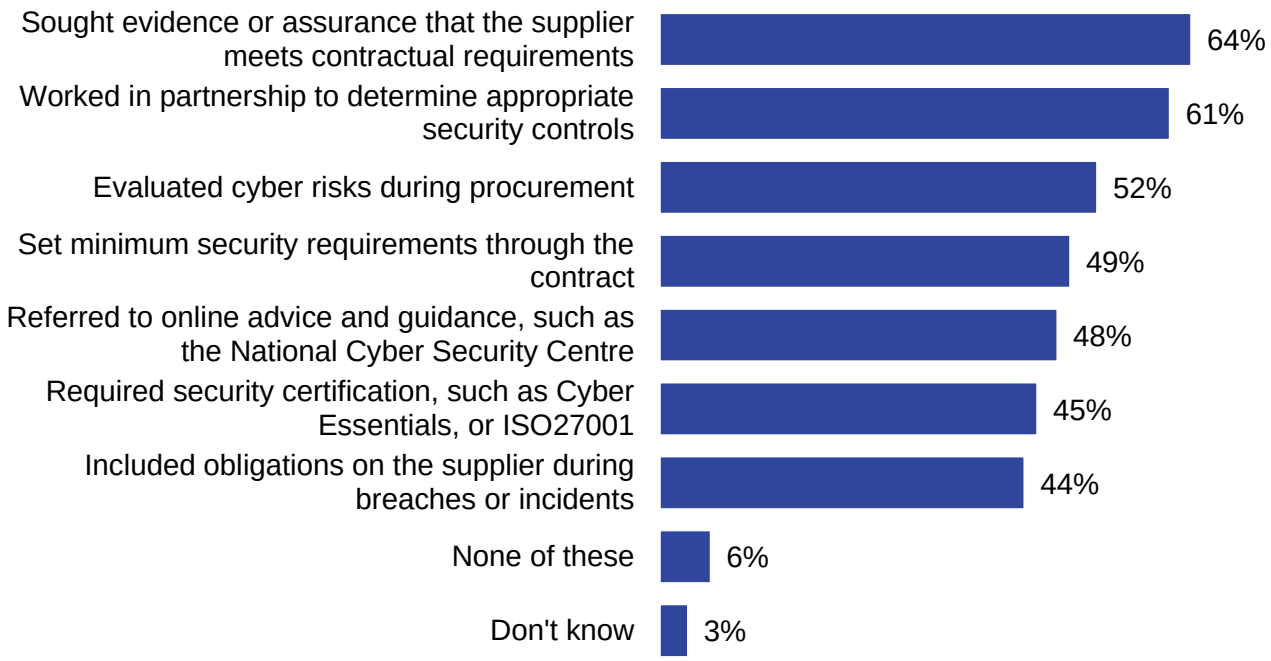
"Five years back, I would say that I would get maybe one or 2 requests a year to fill out some kind of assessment or an attestation to our security practices. I'd say now it's more like 2 or 3 a week." – Technology Supplier

This perception was reflected in the survey findings. Asked to consider the statement 'when purchasing digital technology, products and services, data security considerations are built into the contracting process', 3 in 4 (73%) care providers tended to agree (31%) or strongly agreed (42%) with it. 6% of care providers disagreed.

Agreement was higher than average among care providers who accessed expertise from BSBC at the Digital Care Hub (83%); and those who had 11 to 15 rules or controls in place (81%). Care providers who were more likely to disagree were those with no cyber incident response plan (11%) and those who had 1 to 5 rules or controls in place (15%). When considering the same statement, 7 of 8 technology supplier survey participants agreed with it for their own procurement.

Care providers who said their organisation builds data security in the contracting process were asked a follow up question asking them how this was done, from a list of possible measures. All the measures listed were selected by at least 2 in 5 care providers. A minority of care providers said they had not done any of these things when contracting technology suppliers (6%) (this is in addition to the 6% of care providers who were not eligible for this question).

Figure 49: Measures taken by care providers when contracting digital or technology suppliers



Base: Care providers who build data security into contracting process when purchasing tech, products and services (538)

Sub-group differences across these contracting measures were in line with those previously observed:

- care providers with 11 or more rules and controls, those with formal policies covering cyber security, those who back up their data, or have a complete cyber incident response plan, were more likely than average to select each of the measures listed
- for most of the measures listed, this was also the case among those with cyber security insurance and/or a business continuity plan covering cyber security, and those with an internal cyber security expert team or individual or a cyber security contract with an external organisation
- in contrast, those who do not back up their data (17%), do not have formal policies covering cyber security (12%), do not have cyber security insurance (13%) or have only 1 to 5 rules or controls in place (14%), were more likely than average (6%) to say they had not done any of these measures listed when contracting digital or technology suppliers

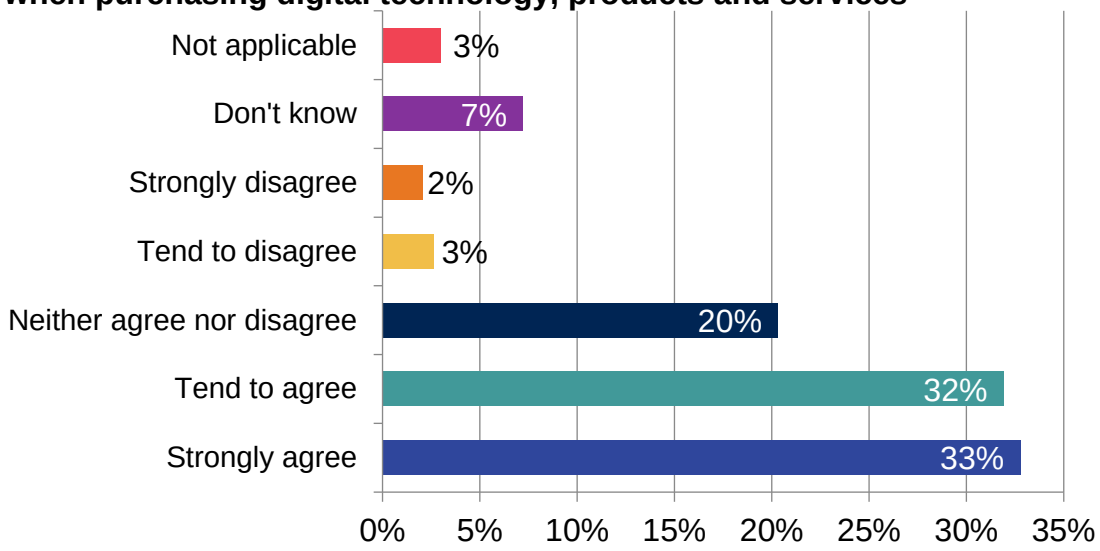
In addition to the above measures, technology suppliers explained that around half of their customers required them to have cyber insurance cover. Technology suppliers also shared that larger care providers were also more likely to undertake due diligence and more specifically consider cyber security in their procurement process.

"Larger care providers tend to have a very high expectation of what information security and cyber security measures we have in place, and conduct due diligence to ensure we have certain accreditations and appropriate policies and procedures. This can sometimes be a requirement that has to be met before price and functionality are considered. But the degree to which cyber security is considered and influences the sourcing decision is very varied." – Technology Supplier

Interoperability

Turning to interoperability, 2 in 3 (65%) care providers tended to agree (32%) or strongly agreed (33%) with the statement 'when purchasing digital technology, products and services, interoperability considerations are built into the contracting process'. 5% of care providers disagreed. When considering the same statement, 8 of the 9 technology suppliers who were asked this question in the survey agreed with it for their own procurement, and one disagreed.

Figure 50: Whether interoperability considerations are built into the contracting process when purchasing digital technology, products and services



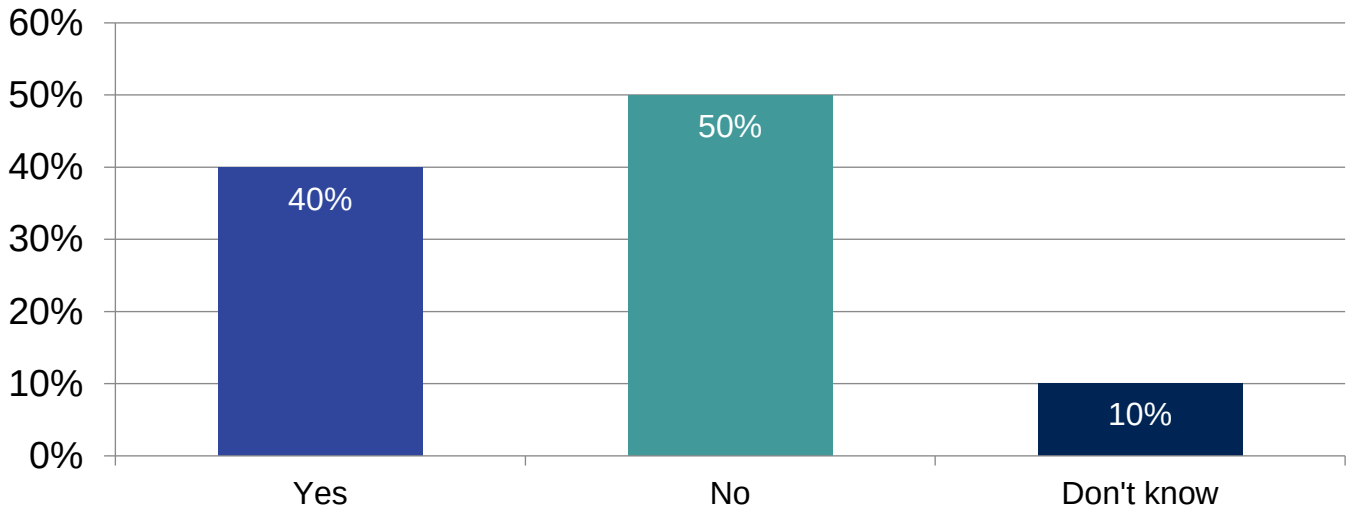
Base: Care providers (575)

Care providers who were most likely to build interoperability considerations into the contracting process included those who accessed expertise from BSBC at the Digital Care Hub (77% agree); and those who had a specific cyber security policy (81%); 11 to 15 rules or controls in place (75%), a complete cyber incident response plan (82%), or Cyber Essentials or other nationally recognised certification (80%).

9.5 Managing and monitoring risks arising from the digital supply chains

There appears to be limited ongoing monitoring of cyber security risks by care providers after the contracting process. Technology suppliers mentioned that generally care provider cyber security requirements at procurement stage tended not to be monitored and reviewed on an ongoing basis once systems had been implemented. This was also reflected in the survey with care providers: half of care providers said their organisation had not carried out any work to review the potential cyber security risks presented by their supply chain (50%). Two in 5 (40%) care provider survey participants had carried out such work and 10% of survey participants did not know if a review had been undertaken.

Figure 51: Whether care provider has carried out work to review the potential cyber security risks within their supply chain



Base: Care providers (575)

Care providers with fewer than 10 staff were more likely to say no review had been carried out (62%), and so were those with 1 to 5 controls and rules in place (73%) and those with no cyber incident response plan (64%).

Care providers with the following characteristics were more likely than the average (40%) to have undertaken a review of the potential cyber security risks presented by their digital supply chain: those with an internal expert team (54%); a specific cyber security insurance policy (56%); or 11 to 15 rules or controls in place (52%).

In the survey, care providers were asked what the 3 biggest challenges were that have made it difficult to manage cyber security risks in their supply chain. This was also discussed in the qualitative interviews. The main challenges and barriers identified by the research were:

- lack of time or money to dedicate to this (41% of care providers). This was a more frequently held concern among supported living (51%) and day care (53%) providers and those with no cyber insurance (58%). In the qualitative interviews, both care providers and technology suppliers stated that this meant cost and functionality took precedence over cyber security considerations during

the procurement process (see section 9.3). However, technology suppliers' experience was that larger care providers tended to have high expectations regarding their technology suppliers' cyber security and would be more inclined to undertake due diligence on this

- too small to have enough bargaining power on cyber security (selected by 41% of care providers). Concerns were raised by sector representatives and leaders about the large market share of a small number of technology suppliers in relation to Digital Social Care Records (DSCR) solutions, which could potentially be aggravated with further consolidation in the market. They thought this resulted in care providers having very little negotiation leverage and the potential for a significant numbers of care providers to be affected if one of the larger technology suppliers had a cyber incident

- not knowing what kinds of checks to carry out (27%). Sector representatives and leaders felt this could result in the adoption of systems with potential vulnerabilities, as providers may be unable to check or challenge the technology supplier's offer and would prioritise affordability and functionality features over cyber security. It was noted that cyber insurers provide support and guidance on this issue but few care providers access it

- lack of skills to be able to check technology suppliers (25%). Participants in the qualitative interviews viewed the DSCR Assured Solutions List as a valuable means of addressing many care providers' lack of skills and expertise necessary to undertake robust due diligence, as well as providing an efficient due diligence route for technology suppliers and care providers. The roadmap to be on the DSCR Assured Solutions List and related standards were viewed as a useful basis for discussion between care providers and technology suppliers

Figure 52: Three biggest challenges that make it difficult for their organisation to manage cyber security risks within their supply chain

Base: Care providers (575)

Around one in 5 (18%) care providers stated they did not face any challenges managing cyber security risks from their digital supply chain. Care providers were more likely than average to say they did not

face any challenge if they accessed cyber expertise from BSBC at the Digital Care Hub (28%), if they exceeded DSPT standards (24%), or if they had not had a cyber incident in the last 3 years (23%).

The mean number of challenges mentioned was higher than average (1.83) among care providers who had ad hoc access to an external cyber security specialist (2.02), those who had no cyber incident response plan (2.08) and those who had experienced at least one type of incident in the last 3 years (2.01).

9.6 Support from technology suppliers around cyber security

According to the technology suppliers, most offered online training as standard (7 mentions, out of 9 technology suppliers) during implementation, and/or remote technical implementation (6 mentions). Fewer selected on-site or online training for an additional charge (5 and 3 respectively).

After implementation, support offered by technology suppliers as standard was more limited: 7 still offered remote technical support, but only 2 provided on-site technical support and one offered on site refresher and/or new staff training. Other forms of support were offered but incurred an additional charge.

The most requested form of support from technology suppliers related to employees who may act maliciously and involved responding to requests to reduce individual's access rights or helping support investigations by providing logs of access, and the like.

Care providers described good, long-term relationships with their technology suppliers in the qualitative interviews. They talked about having single point of contact – via a 24-hour helpline for example, or regular email exchanges, and knowing who to get in touch with when things go wrong. This tended to focus on functionality – and the extent to which this relationship encompasses cyber security seems to be variable.

There were some mentions of provision of training, practical support, updating software and apps from technology suppliers to improve cyber resilience. This was not consistent and other care providers reported that this kind of support was lacking, or that this support could be too technical for their staff.

There was again some degree of faith expressed by care providers that their technology supplier would be keeping up to date with cyber security, and therefore will provide updates and support when needed. Other participants could not recall discussing cyber security with their technology suppliers, and their relationship was more focussed on troubleshooting problems or ensuring the digital technology meets the organisation's needs.

"I know that our suppliers keep up to date with what we should be doing. So, to my knowledge, we're not lacking anything." – Care Provider

Observations from the representatives and leaders also suggest that relationships between care providers and their technology suppliers tend to focus on functionality rather than cyber security. Representatives and leaders also said that support can be variable, or they were not aware of support from technology suppliers extending to cyber security. The issues they identified included:

- support being focussed on the solution, software or platform rather than the devices upon which with solution is being used, or on good practice (which is where a lot of cyber security risk lies)
- support being offered in complex technical language or being prohibitively expensive

- technology suppliers lacking the technical expertise to provide the kind of cyber security support that care providers need
- support from technology suppliers being better suited to larger organisations (where they can have a single point of contact in the care provider organisation across multiple settings) rather than SMEs (where greater capacity is needed to support multiple SME customers)

"They're not cyber-specialists and they don't understand enough about the kind of data held and the CQC regulation aspect, they don't understand the sector well enough to be able to give them appropriate cyber advice." – Representative and Leader

Support in response to a cyber incident

Care providers and technology suppliers expressed confidence that their digital suppliers would act responsibly towards them in the event of a catastrophic cyber incident: 6 in 7 (86%) care providers either agreed or strongly agreed with the statement, and 8 of 9 technology suppliers also did when asked to consider their digital products and services suppliers.

In the qualitative interviews, technology suppliers reported that the support they offered to care providers would be mainly in the event of them experiencing an incident. They typically did not offer any formal support if care providers experienced an incident. For example:

- support offered in the event of an incident on the supplier side: this took the form of providing back-up data, electronic forms, and the like so care providers could operate 'offline' for a period using soft and hard copy documents and manual recording. Sector representatives and leaders noted that where the technology supplier had experienced an incident, the anticipated support to allow care providers to access their data and restore application availability within a few days did not always materialise
- support when the care provider is the victim of a cyber incident: this was viewed as being the responsibility of the care provider's ICT supplier and/or cyber insurance provider. Where guidance and support had been provided, this was on a case by case and goodwill basis, often related to guidance on basic cyber hygiene practices, and usually with smaller care providers. Four of 9 of the technology suppliers who took part in the survey stated they offer advice on incident response to their customers if they are victim of a cyber incident

"Some customers have also reached out for advice when they have had cyber incidents. For example, one instance was around a malware attack and another was around a spear-phishing attack, which caused them to transfer some funds when they shouldn't have done so." – Technology Supplier

However, where the technology supplier provided a SaaS solution, examples were given of the technology supplier's cyber defences identifying care provider cyber incidents. Where a technology supplier did provide a commercial offer that included supply and configuration of End User Devices (EUDs) and establishment of a Virtual Private Network (VPN), they had little take-up from care providers.

The important role that insurers play in the event of an incident was also raised in the interviews with representatives and leaders. It was explained that when a care provider has cyber insurance, the insurer will usually liaise with the care provider, the relevant technology suppliers, and specialist ICT and/or cyber expertise in the event of a cyber incident to respond to and recover from the incident. The insurer

will also guide the care provider through all the legal aspects they need to think about, including reporting of the incident to appropriate bodies for example ICO or CQC.

The ways in which support to care providers could be improved is further discussed in chapter 10.

10

Improving cyber resilience

10 Improving cyber resilience

This chapter provides the research analysis and findings on how cyber resilience could be developed in the adult social care sector. The analysis explores the range of participants' experiences and views on the DSPT (DSPT) and how this could evolve; improvements required in cyber security; barriers to improving cyber security; and support for care providers to manage cyber security.

Summary

Research participants viewed the DSPT as useful for raising awareness of cyber security and driving up implementation of basic controls. However, DSPT compliance was not viewed as an accurate measure of cyber resilience in the sector. It was thought that some care providers treated DSPT completion as a 'tick-box', and that meeting DSPT standards did not necessarily equate with depth of knowledge and engagement with cyber security issues. Mixed and conflicting suggestions were made for the future of the DSPT, ranging from simplification (to make it more proportionate to the mix of care providers in the sector) to greater inclusion of Cyber Essentials requirements and external verification of the self-assessment.

Barriers to improving cyber security focussed around 2 broad themes, with costs being the main one (mentioned by 49%) followed by time and capacity to dedicate to this (34%):

- Cost, time and capacity: this included the cost of updating out of date and legacy digital systems, the time for staff to invest in training and learning about cyber security, and the cost of working with a cyber security supplier providing the level of expertise needed.

- The limited knowledge and expertise around cyber security within the workforce at all levels.

Suggestions for improving cyber resilience varied, and focussed on:

- Ensuring all care providers are aware of the range of support options available to them (for example from LSOs);

- Education and awareness raising across all staff;

- Supporting care providers financially;

- Strengthening requirements and assurances for care providers and technology suppliers to promote safer cyber practices;

- Central coordination of cyber resilience testing and incident response; and

- The role of technology suppliers in supporting and upskilling their customers.

All audiences generally supported a national reporting function for cyber security incidents in adult social care where the incident could potentially impact care delivery, on the grounds that the function should facilitate sector learning and that providers would not be identifiable in any publicly shared information. Linking the reporting of incidents to a cyber incident response coordination offer would encourage the reporting of incidents.

10.1 The DSPT

Sector representatives and leaders and technology suppliers who took part in the research viewed the DSPT as useful because it raised awareness of data and cyber security issues and set minimum requirements for basic controls implementation. They felt that the proportion of care providers not

meeting DSPT standards (currently around 29%) showed that cyber maturity and resilience in the sector was patchy. Participating technology suppliers knew of care providers who had not completed the DSPT and stated this was due to a mixture of not being aware of the DSPT or not feeling it applied to them.

However, sector representatives and leaders and technology suppliers did not consider that the level of DSPT registration by care providers and the proportion assessed as 'standards met' were an accurate measure of cyber resilience in the sector. They cited the following reasons:

- DSPT completion can be treated as a process rather than care providers fully taking on board the principles behind it. For example, a care provider explained that their ICT sub-contractor completed the DSPT on their behalf without involving them in the process
- it does not give assurance on the degree of engagement with cyber security within the care provider
- it only measures one moment in time, with annual updates not necessarily evidencing progressive maturity and resilience
- 'Standards met' is a self-assessment without external validation of the assessment

"Even though many care providers have completed the DSPT, it appears to have been a process for some rather than fully taking on board the principles behind it. So not that strong an indicator of cyber maturity in the sector." – Technology Supplier

This view was evidenced by the sub-group analysis of the care provider survey data: there are very few significant differences by DSPT status. Instead, variables that consistently show differences in care providers' views and responses relate to the type of cyber expertise accessed (for example from internal experts, BSBC programme), the number of rules and controls in place, the availability of a cyber incident response plan, formal policies and/or business continuity plan covering cyber security.

Sector representatives and leaders, technology suppliers and care providers shared a variety of views on how the DSPT could be developed to increase care providers' engagement with cyber security and become a stronger indicator of the sector's cyber resilience. They are listed below, but it is worth pointing out that some of the views expressed contradict each other for example requiring Cyber Essentials and/or external verification would increase the burden on the sector rather than simplify the DSPT.

- DSPT was over-engineered for the adult social care sector and could be simplified to be proportionate without compromising the materiality
- increased use of links to further examples and template documents that providers can use to address the particular standards requirements
- maintaining a stepped approach to the level of DSPT requirements that ensures it is proportionate to the care provider, for example in terms of organisation size, the services it provides and whether it shares data with the NHS
- other stakeholders, such as local authorities or CQC, consistently requiring care providers to complete the DSPT
- inclusion of Cyber Essentials certification as a DSPT requirement

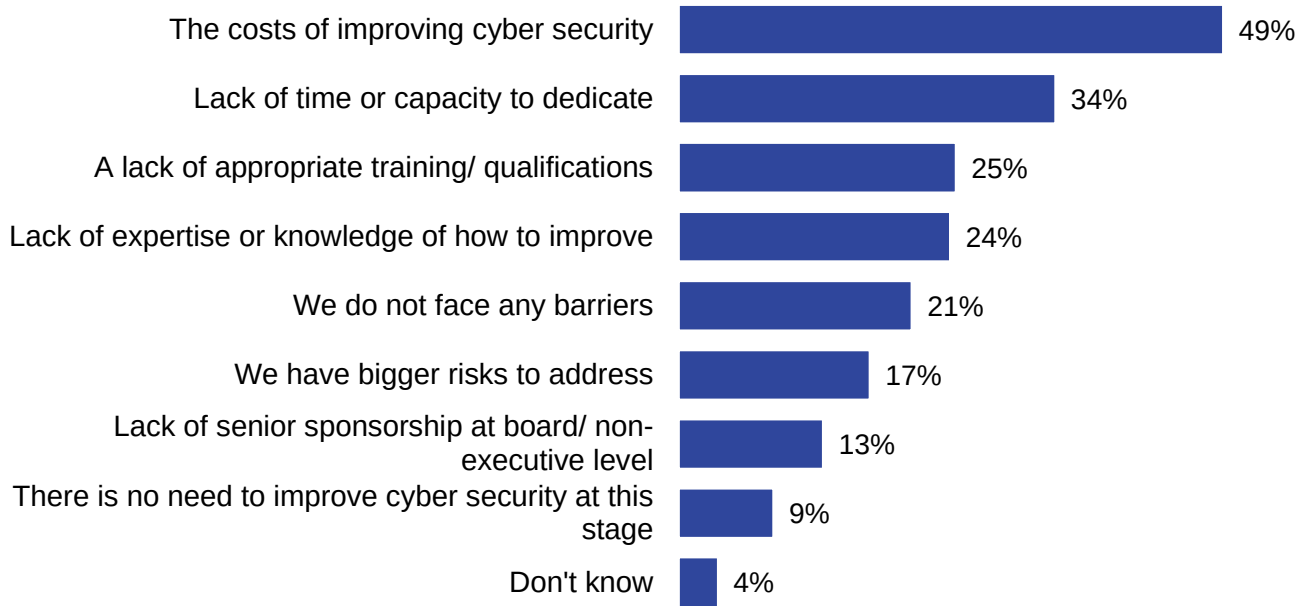
- external verification of the assessment becoming a requirement

Seven out of the 9 participating technology suppliers were at either DSPT ‘Standards Met’ or ‘Standards Exceeded’. Completion of the DSPT was considered useful in providing basic reassurance to the care providers they worked with regarding data and cyber security.

10.2 Barriers to improving cyber security

In the survey, care providers were asked what prevented their organisation from improving or further improving its cyber security over the last 3 years. The main barrier is costs, reported by nearly half (49%) of care providers. A third (34%) cited a lack of time or capacity to dedicate to improving cybersecurity, a quarter (25%) mentioned a lack of appropriate training and/or qualifications in the subject areas they need and a lack of expertise or knowledge of how to improve cybersecurity (24%). A fifth (21%) reported not facing any barriers to improving cybersecurity and one in 10 (9%) said there was no need to improve cyber security in their organisation at this stage.

Figure 53: Barriers to improving cyber security



Base: Care providers (575)

Not facing any barriers was more common among care providers that have Cyber Essentials or other nationally recognised certification (27%), those that exceeded DSPT standards (29%), those that have a complete cyber incident response plan (32%), and those with an internal team or individual with cyber security expertise (33% and 28% respectively).

Care providers with ad hoc access to cyber expertise from an external organisation, those with no cyber security insurance, those with 2 locations or settings were more likely than average to mention many of these barriers, in particular costs (57%, 60% and 65% respectively versus 49% on average) and lack of time or capacity (43%, 50% and 49% versus 34% on average).

Care providers who employed 50 or more people were more likely to report a lack of time or capacity to dedicate to improving cyber security (38% versus 18%) and bigger risks in the organisation to address (18% versus 7%), than the organisations that employed less than 10 members of staff.

In the qualitative interviews, the barriers discussed also related to these 2 broad areas: barriers associated with costs, time and capacity; and barriers associated with training, knowledge and expertise. These are explored below.

Cost, time and capacity

The cost of cyber security was identified as a major barrier to improving cyber security. Aspects of costs that were discussed included the cost of updating legacy and out-of-date digital technology and systems – including hardware, software and things like implementing secure internet connections. It was noted that financial constraints were preventing organisations from investing in technology that could reduce their risk of a cyber security incident. For example, a technology supplier explained that the workforce could be provided with locked down, individual devices, but this was not something care providers could afford to invest in.

“In my view, any carer should have a locked-down phone, and they should only be able to use that phone. But, you can't say that to a dom[iciliary] care company with 300 carers…they're not going to say, 'We're going to buy 300 locked-down phones'” – Technology Supplier

Financial constraints were also discussed in relation to a lack of staff time and capacity to look at cyber security in detail or pay consultants to do this.

“The issue isn't hardware or software, it's staff time to have someone who can really take a good hard look at this. Or potentially pay for consultants to come in." – Care Provider

One care provider gave an indication of how much they spent on cyber security management. Taking into account the external cyber security provider they had appointed, and the additional monitoring systems and procedures they put in place, the participant estimated that they were spending £20,000 a year on cyber security.

"If you're looking at time spent and putting extra systems in place…It's probably cost us at least £20,000 so far in additional costs that we can't make savings on. They're additional costs per year, every year." – Care Provider

Training, knowledge and expertise

One of the barriers to improving cyber security, discussed in the qualitative interviews, was the limited digital skills and knowledge of cyber security among the workforce at all levels (this is discussed in chapter 5). The lack of expertise was linked to issues affecting the adult social care workforce, for example high staff turnover, a proportion of staff with basic English speaking skills, and older staff who were educated before the wide-spread use of digital technology. These were thought to make it difficult to instil cyber security into organisational practices, making the sector vulnerable to cyber attacks.

“[In care there are] some really good people who are motivated by something other than what they earn. But what they don't do is retain enough people with the level of career building skills that you need for things like having really good data information management systems.” – Representative and Leader

In relation to training specifically, the barriers discussed in the qualitative interviews included:

- lack of time and expertise to deliver the training that is required
- mandatory training being prioritised over cyber security training, particularly in the context of high staff turnover
- perception that cyber security training is for frontline and back-office staff, and not necessarily for senior leaders or management

"I think there's already really limited time within the sector to teach training. So, where this is not something which is a mandatory training or requirement for frontline staff I don't know if that's something that normally picked up. Generally, as a population, there is a lack of digital skills and awareness around cyber security." – Representative and Leader

10.3 Support for care providers to manage cyber security

Current awareness of support and accessing support

The analysis of the care providers survey data showed that accessing cyber expertise from BSBC was consistently associated with more positive responses throughout the survey. Compared with the average, care providers who said they accessed this source of expertise had higher awareness of the risks associated with ECDs and of the potential impact of a cyber incident on service users. They also used a larger number of approaches to identify security risks, were more likely to have a number of policies, procedures or accreditation in place related to cyber security, to have a range of measures in place to respond to a cyber security incident and more complete cyber incident response plan. They were also more likely to strongly agree with various statements on cyber security training and awareness for staff.

Sector representatives and leaders also noted the importance of the support offered to care providers through the Digital Care Hub's BSBC programme, particularly through the local support organisations (LSOs).They were concerned at the proportion of care providers who did not know about or access the support, despite the availability of this support to improve data and cyber security and complete the DSPT. Further, it was also reported that LSO support offers, such as a soft-audit service, were not always being taken up by care providers due to capacity and cost pressures.

In the qualitative interviews, an example of some care providers' lack of awareness of the support options available was given. A care provider participant who worked solely with self-funding clients made the point that care providers which do not get commissioned by local authorities can often be 'out of the loop' on much of the awareness raising and support on cyber security. Care providers who were aware of the support available were accessing them in some form, including that provided by their local authority commissioners.

"[We are] currently working outside of local authority commissioning, so outside the loop on communication." – Care Provider

A sector representative and leader explained that care providers were half as likely than other sectors to have cyber insurance cover, and when they did they were not always aware of the support available from their insurance provider. For example, the information produced by insurers identifying emerging cyber threats and their mitigations was not always accessed and acted upon by care providers.

Support needed to improve cyber resilience

Education and awareness raising: All groups in the qualitative interviews expressed the view that education and awareness raising with care providers on their cyber security vulnerabilities and responsibilities was still required. This was needed across care provider leadership, management and staff to ensure a robust and consistent basic level of good cyber control and practice across the sector. The suggested ways information and training could be shared to make it most effective included:

- making it mainstream, rather than treating it as a technology issue – for example, including cyber security in sector conferences
- making the issue specific to care providers and avoiding an NHS bias
- pulling together the range of information to address cyber security – for example a summary or central resource

"Attaching a cyber strand to one of the big Social Care or Housing Conferences, would help." – Care Provider

Supporting care providers financially: Costs were the main barrier faced by care providers to (further) improve cyber security. In the qualitative interviews care providers suggested that grant funding, particularly for smaller care providers, would be beneficial to overcome some of the identified barriers to cyber maturity and resilience. Such grants would need to be flexible to reflect the specific needs of care providers. For some this could relate to implementation of digital applications or ICT infrastructure, and others could be funding staff time for system implementation and training.

Developing a more robust infrastructure around cyber security, this included strengthening the requirements and assurances that care providers and technology suppliers should meet. For example:

- representatives and leaders viewed the Care Quality Commission's (CQC) focus on cyber security through it's 'Well-Led' theme as likely to provide greater impetus for care providers to understand and act upon their cyber responsibilities and accountabilities. It was suggested that further leverage could be applied by all local authority commissioners having explicit requirements, such care providers meeting DSPT standards. This was also reflected in an interview with a care provider – who said until cyber requirements were statutory there was limited incentive to meet any requirements

"If there was a statutory requirement for us to move to cyber, there's lots of talk about it, but so far it's not a statutory requirement. If there was, I would expect a statutory body to be responsible for sorting it out. CQC or some government agency." – Care Provider

- representatives and leaders also felt that increasing the scope of the Assured Solutions List (ASL) approach was needed. Central assurance of a broader range of adult social care digital solutions would reduce the level of technical knowledge and due diligence required by care providers to safely and successfully continue a digital adoption and innovation journey. It was proposed that other high impact applications were considered, for example payroll systems and ICT system services, with care providers also suggesting support to ensure favourable pricing on such systems and their implementation

More central coordination of cyber resilience testing and incident response: Sector representatives and leaders and technology suppliers suggested that a greater awareness of cyber vulnerability in the adult

social care sector could be achieved by encouraging and supporting greater testing of care providers cyber defences. This could take the form of encouraging use of the National Cyber Security Centre's (NCSC) Exercise in a Box resources or centrally funding a degree of penetration testing and mock phishing exercises, which could be linked to DSPT assessment.

A cross section of participants also proposed that it would benefit care providers, technology suppliers and other stakeholders if there was some form of central coordination of cyber incident response and recovery. Not only do many care providers not have the capability, or cyber insurance, to effectively respond and recover, but when there is an incident at technology supplier level then a significant degree of coordination is likely to be required across the system.

"There would be benefit for both care providers and technology suppliers if there was some form of central coordination of cyber incident response and recovery." – Technology Supplier

Support from technology suppliers: As discussed in chapter 9, participants in the qualitative interviews (both representative and leaders, and care providers) demonstrated that support to care providers from their technology suppliers is variable and can lack a focus on cyber security. Sector representatives and leaders suggested ways technology suppliers could do more to support their customers – for example, by providing templates and data download options to mitigate risks of data loss, or emergency systems to allow care providers to continue working in the event of an incident. A care provider also suggested that they would like to learn more from their technology supplier about cyber security and risk.

"[I'd like to know] what the latest attacks are. What to look out for, what the new threats are. Because there's always new and evolving threats. And it's just interesting to find how unscrupulous people are trying to break down your barriers." – Care Provider

Participants were unclear on what cyber support was available for unregulated parts of the sector, for example technology enabled care services.

Views of the role of central government and other organisations to coordinate support

As discussed above, there was agreement in the qualitative interviews that more central coordination of cyber resilience testing, and coordination of cyber incident responses would be welcomed. Furthermore, there was general agreement across all 3 audiences that there should be a system-wide approach to cyber security in the sector.

For example, technology suppliers and representatives and leaders agreed that government bodies should be involved in supporting cyber incident response in adult social care and that this could be through existing entities such as the NHS Cyber Security Operations Centre or be capacity built into the BSBC programme. The role of local support organisations (LSOs) was also emphasised as an important one; these organisations were seen as important vehicles for disseminating awareness raising activities and training, and as a central resource for response and recovery from an incident. This could be through a cyber advisor for every LSO, for example.

"I think there's an opportunity there for [LSOs] to have an advanced offer, but also enhanced recognition by the whole supply chain of their validity and their role in this." – Representative and Leader

Care providers supported central coordination of cyber incident response and recovery, whether at local authority level or more broadly. This was felt to be particularly valuable as they expected that the challenges their sector faced were unique – so an opportunity to share learnings would be welcomed.

However, they expressed mixed views regarding sector collaboration on cyber security: while there was interest in sharing learnings from incidents, emerging threats and good practice, there was also an acknowledgement that collaboration between providers could be inhibited by care providers competing for clients and staff.

"Owners of companies: they don't want you sharing things with other companies. They don't want you giving out your secrets that will improve that other company above you." – Care Provider

Views on a reporting scheme in future

Across all 3 audiences, there was broad support for a national reporting function for cyber security incidents in adult social care where the incident could potentially impact care delivery. This support was based on the assumption that such function would facilitate sector learning. It was suggested that reporting could build on existing routes such as the DSPT helpline and/or incident reporting system, NCSC, ICO or CQC reporting. This would complement reporting to insurers where there is cyber insurance cover. The function could also consider automatic notification to other stakeholders such as Action Fraud.

While support for this was broad, concerns were expressed about the details, in particular:

- placing a further reporting requirement on care providers
- the level of information required to be reported. It was suggested that this should avoid commercially sensitive information and that the information should be anonymised before being shared publicly to avoid reputational risk for the technology supplier or care provider concerned
- that the reporting scheme could add to the uncertainty or confusion over existing reporting requirements for data breach. Technology suppliers shared their experience that SME care providers can be uncertain and confused on current data incident reporting and so the reporting of cyber incidents needs to be handled in a way that is simple and facilitates compliance

Participants suggested that the reporting would be more effective and complete if this was linked to a cyber incident response coordination offer.

“If the organisation thinks they're going to get some help and support out of reporting it (cyber incident), they're more likely to report it than if they're just reporting it for regulatory purposes.” – Representative and Leader

11

Conclusions

11 Conclusions

This chapter provides conclusions from this research. It first outlines the strengths and limitations of the findings, and then identifies implications and possible next steps.

11.1 Strengths of the findings

The findings provide a clear and coherent picture of cyber security in the adult social care sector in England. They are based on a representative survey of 575 care providers, 41 depth interviews with 3 different audiences (care providers, technology suppliers, and sector representatives and leaders), and a small survey with 9 technology suppliers. The project was informed by a rapid evidence review and a scoping phase, a workshop with stakeholders, and benefited from the input of a Data End User Group – all these steps helped ensure the research focused on issues, and used terminology that was appropriate and relevant to participants.

The sample for the survey with care providers was drawn from the BSBC sampling frame of regulated care providers, at parent organisation level. The 2 routes used to disseminate the survey invitations, using contact details held by the DSPT team and CQC, mean that the achieved sample includes organisations that have completed the DSPT as well as some that have not. The mixed mode approach (online and telephone) enabled telephone interviewers to reach out to care providers who did not respond to the online survey invitation, in particular care providers who may not typically engage with cyber security issues.

At the data processing stage, survey data were weighted to the known population profile of regulated care providers. Responses to the questions asked at the start of the care provider survey show that the views captured are those from people in charge of cyber security (in companies where such role exists), of commissioning digital technology products or services, or of liaising with a third-party in charge of the provider's cyber security. They were the people best placed to answer the questions, and the intended audience for the survey.

There is a possibility that the survey over represents care providers which are interested in or prioritise cyber security. However, the inclusion of some care providers with limited cyber security measures in place suggests that the survey did reach at least some care providers with limited knowledge or understanding of cyber security. The telephone mode enabled us to reach care providers who would not have been interested enough in the topic to respond to the online survey invitation.

These steps mean we can be confident that the survey findings are robust and representative of the population of regulated adult social care providers in England.

11.2 Limitations of the research

Despite numerous attempts to engage with technology suppliers, the project was not able to achieve as many survey responses from this audience as it was originally hoped. Only 9 technology suppliers completed the survey which was aimed at this audience, with many more stopping half-way through because they found the survey too long. The lack of engagement partly stems from the difficulties involved in conducting research with this audience: as there is no register of technology suppliers in adult social care, and no sampling frame, the survey had to use an open link approach. This open link was disseminated to the sector by umbrella organisations through their mailshot and newsletters. In practice, this means that with the exception of suppliers on the Assured Solutions List, the research team could not send out survey invitations and reminders to technology suppliers directly, nor call them to

follow up non-respondents - unlike the survey with care providers. The lack of a sample frame and the small achieved sample size means it was not possible to weight the technology supplier data.

The lack of sampling frame also affected the recruitment of technology suppliers for the qualitative interviews: they were recruited through IPC networks, from those who took part in the survey, and from those who expressed an interest in taking part after receiving communications about the research sent by umbrella organisations.

Overall, the limited engagement from technology suppliers means the findings from this audience are more limited and may not reflect the full range of views and experiences of the technology suppliers sector. Significant engagement with umbrella organisations representing technology suppliers aimed to compensate for this.

A second limitation relates to the reporting of cyber incidents and unsuccessful attacks by care providers and technology suppliers. The rate of cyber incidents or unsuccessful attacks reported by care providers is lower than the rate reported by businesses in the Cyber Breaches Survey 2024. Although the introduction and privacy notice for the 2 surveys clearly explained that nobody outside Ipsos and IPC would know who took part, and that the findings would be used for research purposes only, it is possible that care providers and technology suppliers preferred not to disclose cyber incidents and unsuccessful attacks experienced over the last 3 years, due to commercial considerations and fear of reputational damage. It is also possible, especially among care providers, that some did not realise they had been victim of an incident or attack. Whatever the reason, the small number of incidents reported impacted on the economic analysis that could be conducted regarding the cost of cyber incidents faced by care providers.

To minimise burden on participants, it was not possible to ask full details of all incidents experienced in the last 3 years. The survey asked about costs and impacts for up to 3 most costly types of incidents and then the most costly incidents of each type. For providers with more than 3 types a catch all question was asked about all other costs of incidents, but this was not asked for organisations with 3 or fewer types but potentially more than one incident of each type which means we did not capture the overall costs for all incidents experienced by the care providers surveyed. At the same time, the focus on the most costly incidents could overstate average costs of each type of incident. There was also a need to impute costs (based on median values within a range) where providers only gave a range rather than a specific cost for each type. The incidence of incidents may have been under-reported leading potentially to lower overall costs than actually experienced. The limitations in the levels of detail that could be asked and the assumptions needed for the economic analysis mean estimated costs should be taken as indicative.

11.3 Implications

Awareness is high but not fully embedded: The research found that awareness of cyber security issues among care providers and commissioners is high, and has risen significantly over the last few years. However, suggestions from the qualitative research is that this awareness is not yet embedded in care providers' working practices, and good practices are inconsistently applied.

A minority of care providers are further behind: A small but non negligible number of care providers do not appear to engage with cyber security. They have few rules and controls in place, do not have a team or person dedicated to cyber security, do not complete the DSPT, have few of the policies they should have in place and do not necessarily have compulsory training on cyber security for new joiners. They are ill-equipped to deal with a cyber incident, if they were victim of one. Providers who do not have

access to cyber expertise, or only have ad hoc access to it, and those who lack leadership on cyber security, tend to be in this situation. Their awareness of cyber security needs to be raised, and they are likely to need significant hands-on and tailored support to catch up with the rest of the sector, for example from LSOs and the BSBC programme.

The scale of cyber threats is underestimated or misunderstood: Even among care providers who engage with cyber security issues, the research showed a degree of naivety around the likely impact of an incident, and what it would mean for providers' ability to deliver care, for the people they support, and for their staff. There was a significant gap between what care providers believed would happen if they were victim of a severe incident, and the likely reality. Many providers failed to realise that a cyber incident could impact their access to HR records and their ability to pay staff wages, and that recovering from an incident could take months rather than days. There is a need to continue to raise awareness of the potentially catastrophic, wide-ranging, and sustained impact of a cyber incident.

Cyber attacks were under-reported in the survey, possibly linked to poor monitoring: It is not possible to say with certainty why the reporting of cyber incidents and attacks (whether successful or not) among care providers was lower than that reported by businesses in the Cyber Breaches Survey 2024. However, one hypothesis is that there could be a lack of cyber security monitoring among providers, leading to them not realising when they are victims of incidents or attacks. This lack of monitoring could be related to care providers not realising the importance of monitoring their cyber security, and/or to a lack of resources to invest in monitoring their own cyber security in light of competing priorities.

Training and risky behaviours are an area of weakness: While most care providers train their staff on cyber security, fewer appear to provide refresher training or information. There were also some concerns that training is 'tick-box', rather than providing comprehensive information on cyber security and risk and driving safer practices. The prevalence of persistent risky cyber practices shown by the research suggests that training does not always translate into cyber secure practices, and that policies, where they exist, may not be known, understood and consistently applied by all staff. Staff clicking on phishing emails and human errors are still the main risks care providers are concerned with. This clearly points out to the importance of staff when it comes to cyber security, with leaders prioritising it and front line staff adopting good cyber practices in their everyday work. Regardless of training, the prevalence of some of these risky practices is also caused by resource and financial constraints, with care providers not being able to afford to move away from them despite knowing they involve cyber security risks (for example staff using their own devices for work purposes, providers not being able to afford enough licences).

The DSPT has raised awareness, without necessarily changing behaviours: The research found very few significant differences between the survey responses of care providers who exceeded, met or did not meet DSPT standards. This means that in the survey, completion of DSPT is not associated or correlated with better cyber practices. This finding supports the views expressed by representatives and leaders that while DSPT has helped raise awareness of cyber security issues, it is not enough in itself to ensure the consistent implementation of the policies, procedures, rules and controls that it requires care providers to have in place. However, in the survey accessing cyber security expertise from the BSBC programme was consistently associated with better outcomes, indicating that the support received from BSBC to help care providers complete the DSPT makes more difference than the completion of the DSPT itself.

The supply chain has a number of weaknesses**:** Care providers' relationships with their technology suppliers tend to rely on trust as care providers do not always have the skill set, resources or capacity to

check their technology suppliers, or conduct due diligence. There are indications that due diligence at commissioning stage is increasing among medium and large providers, but not necessarily among small providers who make up the majority of the sector (and do not feel they have any bargaining power). A possible way forward could be to widen the Assured Solutions List beyond software for Digital Social Care Records (DSCR), so it includes a larger range of digital products and services including critical systems such as care rostering systems. This would make it easier for providers to choose and procure digital technology, by reducing the amount of due diligence they need to conduct. As being on the Assured Solutions List involves meeting requirements regarding inter-operability and functionality, choosing from companies offering consistent standards on these issues would also make it somewhat easier for care providers to change suppliers if they need to, for example to choose a more cyber secure solution. Indeed, the time and costs involved in changing suppliers tend to be prohibitive for care providers.

Expansion of Software as a Service (SaaS) has improved cyber resilience but also increased the potential scale of a cyber incident: The expansion of SaaS has increased the cyber resilience of the sector, with technology suppliers requiring for example 2-factor authentication or setting up cloud back-up as part of their SaaS solution. While this is undeniably safer, it also means that if a technology supplier is victim of a cyber incident, a large number of care providers would be impacted. This risk is compounded by the size of the technology suppliers' sector, with a small number of suppliers dominating the market. In this context, checking, monitoring and auditing the cyber security of technology suppliers is crucial. As technology suppliers' engagement with the research was limited, it will be important to engage with them when decisions are made that affect them.

Backing for more national support: Finally, the research showed there is appetite and broad support for a national system to coordinate response to and recovery from incidents in the sector. Support in case of incidents could be linked to the supply or use of a product or service on the Assured Solutions List, with the Assured Solutions List setting out clear requirements in terms of cyber security and requiring mandatory reporting of incidents. There was also support for a national reporting function for cyber security incidents in adult social care, where the incident could potentially impact care delivery. Access to support in case of incidents could be conditional on the reporting of the incident.

11.4 Next steps

Many of the findings are relevant to relevant to a range of organisations working in the sector, whether care providers, technology suppliers, commissioners and local authorities, people drawing on care and support and their families, umbrella organisations (for example TSA, CASPA, techUK, LGA, ADASS), and regulators, as well as the BSBC programme and the DSPT team. However, some of the findings are sensitive and publishing them could potentially increase cyber security threats in the sector. It is therefore very important to carefully consider which findings can be disseminated to those who need to see them, and how this can be done, without putting the sector at risk.

Our standards and accreditations

Ipsos' standards and accreditations provide our clients with the peace of mind that they can always depend on us to deliver reliable, sustainable findings. Our focus on quality and continuous improvement means we have embedded a "right first time" approach throughout our organisation.

ISO 20252

This is the international specific standard for market, opinion and social research, including insights and data analytics. Ipsos UK was the first company in the world to gain this accreditation.

Market Research Society (MRS) Company Partnership

By being an MRS Company Partner, Ipsos UK endorse and support the core MRS brand values of professionalism, research excellence and business effectiveness, and commit to comply with the MRS Code of Conduct throughout the organisation and we were the first company to sign our organisation up to the requirements and self-regulation of the MRS Code; more than 350 companies have followed our lead.

ISO 9001

International general company standard with a focus on continual improvement through quality management systems. In 1994 we became one of the early adopters of the ISO 9001 business standard.

ISO 27001

International standard for information security designed to ensure the selection of adequate and proportionate security controls. Ipsos UK was the first research company in the UK to be awarded this in August 2008.

The UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018 (DPA)

Ipsos UK is required to comply with the UK General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA). These cover the processing of personal data and the protection of privacy.

HMG Cyber Essentials

Cyber Essentials defines a set of controls which, when properly implemented, provide organisations with basic protection from the most prevalent forms of threat coming from the internet. This is a government-backed, deliverable of the UK's National Cyber Security Programme. Ipsos UK was assessed and validated for certification in 2016.

Fair Data

Ipsos UK is signed up as a "Fair Data" company by agreeing to adhere to 12 core principles. The principles support and complement other standards such as ISOs, and the requirements of data protection legislation. .

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

www.ipsos.com/en-uk
http://twitter.com/IpsosUK

About Ipsos Public Affairs

Ipsos Public Affairs works closely with national governments, local public services and the not-for-profit sector. Its c.200 research staff focus on public service and policy issues. Each has expertise in a particular part of the public sector, ensuring we have a detailed understanding of specific sectors and policy challenges. Combined with our methods and communications expertise, this helps ensure that our research makes a difference for decision makers and communities.