Protecting care providers from cyber attack

Findings of a research project: Identifying cyber risk in the adult care sector and identifying and testing solutions to help protect providers, staff, and service users.

October 2024

Contents

1 Forward

This paper, produced by Care England, marks the culmination of a year-long research project undertaken with the Cyber Centre of Excellence (CCoE), an organisation led by experienced cyber security experts and overseen by an Advisory Board of some of the UK's leading cyber security professionals.

Care England and the CCoE's joint aim was first to understand the cyber threats facing the care industry and, secondly, to road-test a package of affordable and effective cyber security solutions with a sub-section of Care England members to develop an off-the-shelf all-round cyber security offering designed by the sector for the sector to give time-pressured care provider leaders reassurance that they are adequately protected against the ever-growing cyber threat.

Traditionally care providers, like many other businesses, have relied on standard anti-virus solutions for cyber protection. While these products still have their place, the focus is now on what is known as defence-in-depth or layered solutions.

Cyber threat has become more complex, with cyber criminals finding ways around standard anti-virus solutions with zero-day attacks – those never seen before and therefore unable to be recognised and stopped – and other methods of infiltration, such as through third-party supply chains and sophisticated phishing attacks.

While a care provider may not be the intended or original target of a cyber-attack, having cyber protections that are not up-to-date or adequate in today's environment increases the likelihood of being exposed to potentially devasting consequences – financially, legally and reputationally.

The Care Protect package developed by Care England and the CCoE through its research and testing with the sector is made up of five elements to help providers build defence in depth. This includes a vulnerability scan to identify cyber vulnerabilities and take steps to fix them, and a session with a qualified cyber expert which looks at risks and solutions in depth at a company level. Also included is licences for a sophisticated product developed in the US defence environment which can be installed on computers and servers (endpoints) to stop threats in their tracks, including zero-day threats. Additionally, because employees are understood to be a large part of any organisation's cyber risk, a NCSC-assured cyber board course is included for senior staff, while other employees can access a range of online training modules to build essential knowledge.

The multi-layered approach provided by Care Protect gives the high-level of protection needed as cyber threat continues to grow.

This paper outlines our research findings and breaks down the elements of Care Protect to give readers an overview of the risks posed by cyber to the care industry and an outline of the potential solutions.

Statement from Care England

In the last year we've seen a huge increase in cyber-attacks on health and social care organisations. As a sector we have so far avoided any major attacks, but we have seen other organisations in health and social care, including the NHS, badly hit. Whilst care providers are becoming more aware of the risk, there is still some way to go in raising awareness and implementing effective cyber security measures.

Professor Martin Green OBE, Chief Executive of Care England.

The adult care industry continues to face a great deal of pressure. Regulation, staff shortages, high staff turnover and underfunding are major daily issues. Cyber security is a more hidden threat and therefore often takes lesser priority, but this is a dangerous position. A successful cyber-attack could leave care sector businesses open to financial repercussions, reputational damage and, worst of all, potential harm to service users through loss or corruption of data. Health data is recognised as a valuable commodity, with a report by EY highlighting that NHS data holds 'immense value'[1].

Our members' position in the supply chain with links to local authorities and other care organisations, such as the NHS, makes them an attractive target. While this hasn't yet been exploited, it is only a matter of time.

As an industry body, Care England already provides access to a self-assessment data security protection toolkit. We have now joined forces with the CCoE, an organisation led and backed by some of the UK's leading cyber security experts to understand the likely and potential cyber risks and issues faced by care providers. After a year-long research project we are proud to jointly bring Care Protect to the market, a complete off-the-shelf package of cyber solutions and protections designed to meet the unique needs of care providers and help give our members peace of mind. We also continue to work with the CCoE to find solutions to other issues our members face, such as obtaining cyber insurance.

As an industry we cannot ignore cyber threat. It's time to start thinking seriously about the risk of cyber-attack, because unfortunately it is not a case of 'if', it is a case of 'when'.

Professor Martin Green OBE, Chief Executive of Care England

Statement from the CCoE

The CCoE was created in response to the growing threat organisations in the UK and beyond face daily from cyber-attack. It has brought together an Advisory Board of some of the UK's leading experts in cyber security with the aim of making the UK the safest place to live, work and play online.

Kurtis Toy, CEO of the Cyber Centre of Excellence (CCoE).

The CCoE has been delighted to work with Care England over the last year to assess the cyber security needs of the adult care sector. We are pleased that the research project and testing undertaken with the organisation and five of its members has resulted in the launch of a complete package of cyber support and protection – a solution designed in conjunction with the sector for the sector which is now available to procure through Care England or from the CCoE.

Through our research activities and projects across many sectors to date we have consistently found worrying gaps in cyber security which the businesses and organisations we work with were unaware of. Often these organisations believed they were adequately protected but a step change in cyber threat requires a step change in response.

Frequently seen vulnerabilities we have found include badly configured services and out of data software, forgotten servers and neglected websites affected by mergers or organisational changes. Often configuration changes can be made which accidently make information available online without an organisation's knowledge. These are effectively open back doors which could be easily exploited by those with malicious intent.

Unfortunately, the common-place tactic of many businesses of setting and forgetting anti-virus software is no longer adequate – the risks are now manifold, and the solutions therefore need to be more complex. This can be daunting, especially if an organisation lacks the resources for in-house expertise and we are aware that it can be difficult to assess vendors' claims in a crowded marketplace. The CCoE, backed by parent company not-for-profit consultancy iESE, aims to remove the confusion by staying abreast of new threats and emerging technologies, while our collective buying power helps us meet our aim of offering military-grade cyber protect at high-street prices.

Kurtis Toy, CEO of the Cyber Centre of Excellence (CCoE)

2 Executive summary

Adult social care providers are already under pressure, but one challenge often not acknowledged is the ever-increasing cyber threat. While the adult care industry may not be as attractive to hackers as other organisations, such as local authorities or the NHS, the care sector is intrinsically linked through the supply chain to these organisations.

Unfortunately, as local authorities and the NHS become more cyber savvy, it is more likely attackers will look for other routes in through third parties such as care providers.

It is recognised that cybercrime is now the third largest economy after the US and China[2] and while NHS health data has been recognised as a valuable commodity[1], Check Point's *2022 Mid-Year Security Report*[3] cited healthcare as the fifth most targeted industry globally by cyber attackers.

In addition, the cyber risk continues to build. The introduction of Artificial Intelligence (AI) will lead to more sophisticated attacks which are quicker for hackers to develop and deploy. As an industry we also continue to advance digitally. While this will boost productivity, enhance the quality of care, and enable data-driven decisions, it also brings a greater need for cyber awareness and protections.

Organisations which store personal data have **legal obligations** to ensure this data is stored safely and protected from being stolen or intercepted through a breach, including a cyber-attack. Under UK law, health data is treated as 'special category data' due to its sensitive nature, meaning greater efforts need to be made to protect it.

With the social care sector digitising its care records and data at pace, and with many providers already facing funding issues and at risk of closing services, becoming the victim of a cyber-attack would bring additional financial burden, both in terms of recovery costs and possible fines incurred from the Information Commissioner's Office (ICO), the organisation which oversees data protection compliance in the UK. A serious attack could also leave adult care providers exposed to reputational damage and potentially have devastating consequences for service users.

Whilst at the time of publication, the adult care sector has managed to remain unscathed by any major cyber-attacks, as an industry it is time to face this threat before it is too late.

Care providers are often time and resource poor and need access to support and guidance along with ready-made solutions to the ever-growing cyber threat. To achieve this, Care England has been working with the CCoE, a body led and advised by some of the UK's best cyber security experts to establish an affordable package of cyber protection and support tailormade for the sector with the sector to ensure care providers can continue to operate knowing they are as cyber safe as possible.

3 The problem

Adult social care providers are already struggling and under pressure. A recent report found that more than a quarter of providers had considered exiting the market in the twelve months previous[4]. Challenges include the cost-of-living crisis, staff shortages, and increasing wage bills. According to the *2023 Sector Pulse Check Report*[5], these pressures have already led to 43 per cent of providers handing back contracts or closing some services.

As highlighted by the Care Quality Commission *State of Care 2022/23 report*[4], it is also an industry with an "overworked, exhausted, and stressed workforce". According to Skills for Care[6] there were approximately 131,000 vacancies in the industry in 2023/24, equating to 8.3 per cent of adult social care roles.

One lesser acknowledged challenge is the risk of cyber-attack, but this is a persistent and increasing threat. According to the *Cyber Security Breaches Survey 2024*[7], in the previous twelve months half of all business and a third of charities had experienced a cyber breach.

In the UK care sector, there have been multiple instances where organisations believed they had adequate cybersecurity protections but were later found vulnerable to cyberattacks. These breaches often expose sensitive data of patients and care recipients, making the care sector an attractive target for cybercriminals. In addition, personal data from social care providers have been found on the dark web, likely from multiple sources including ransomware attacks and breaches in third-party systems.

In January 2023, Cambian Group, a large provider of children's care services owned by CareTech, suffered an unauthorised breach which impacted its operations[8]. There have already been a string of significant NHS attacks this year. In June 2024 ransomware hackers infiltrated the computer systems of a company used by two NHS Trusts, leading to major disruption with hundreds of patient appointments cancelled[10]. A study carried out by Obrela Security Industries found two-thirds of UK healthcare organisations had cancelled patient appointments due to a cyber-attack, while 65 per cent said they were concerned that an attack on their systems could lead to a loss of life[11].

Below are some notable examples of cybersecurity incidents in the UK care and social care sector, listed in order of impact rather than by date, where protections believed to be sufficient turned out to be inadequate:

1. NHS WannaCry Attack (2017)

- **Incident:** The WannaCry ransomware attack[9] crippled large parts of the National Health Service (NHS) in May 2017, impacting around 80 out of 236 NHS trusts.
- **Vulnerability:** The NHS was relying on outdated Windows XP operating systems and had not applied the available security patch to protect against the known vulnerability (EternalBlue). Despite having firewalls and antivirus systems, the patch management process was not adequate. Many trusts believed their systems were adequately protected but had overlooked crucial updates.

- **Impact:** Hospitals were unable to access patient records or critical systems, resulting in the cancellation of 19,000 appointments and a diversion of emergency patients. The financial cost was estimated at £92 million.
- **Key Lesson:** Despite basic cybersecurity measures in place, the NHS's reliance on legacy systems and delayed patching exposed significant vulnerabilities. This highlighted the need for constant system updates, even for seemingly "adequately" protected environments.

2. Hackney Council Cyberattack (2020)

- **Incident:** In October 2020, Hackney Council, which provides numerous social care services, was hit by a significant ransomware attack that disrupted services for months.
- **Vulnerability:** Hackney Council had cybersecurity measures in place but was not fully prepared for a sophisticated ransomware attack that targeted vulnerabilities in their system. It was later revealed that certain data, including personal information related to social care services, had been stolen and was leaked on the dark web.
- **Impact:** Essential social care services, including housing benefits and local welfare support, were severely disrupted. Personal information, including care details, was found circulating on the dark web.
- **Key Lesson:** The council's perception of its cybersecurity readiness was flawed, particularly in the area of data protection and ransomware defences. This incident demonstrated that local authorities and care providers must strengthen both detection and response capabilities.

3. Blackbaud Data Breach (2020)

- **Incident:** Blackbaud, a third-party service provider for numerous charities and care organisations in the UK, including mental health and social care services, suffered a ransomware attack in 2020.
- **Vulnerability:** Although Blackbaud had what they considered robust cybersecurity systems, the attackers managed to infiltrate their systems for months without being detected. The breach affected the personal data of donors, patients, and service users, including those from social care organisations. Sensitive information, such as patient treatment data, was compromised.
- **Impact:** Several UK-based care organisations, including hospices and care centres, were impacted, with personal information and healthcare details potentially exposed. The attackers reportedly demanded a ransom to prevent the public release of stolen data, which included sensitive personal information related to care services.
- **Key Lesson:** Many social care organisations using Blackbaud's services assumed their data was secure under third-party management, only to find that it had been compromised. This breach highlighted the risks of outsourcing data management without thorough due diligence and ongoing assessments of vendor security protocols.

4. COVID-19 Vaccine Rollout Phishing and Ransomware (2021)

- **Incident:** During the COVID-19 vaccine rollout, several social care providers and NHS-affiliated bodies were targeted by phishing and ransomware attacks, as cybercriminals sought to exploit the chaos around vaccine distribution.
- **Vulnerability:** Many social care organisations, under pressure during the pandemic, believed their existing protections (basic firewalls, antivirus software) were enough to handle external threats. However, they were not equipped to handle advanced phishing campaigns or targeted ransomware attacks that exploited unpatched systems or used social engineering tactics.
- **Impact:** Though not as catastrophic as WannaCry, these attacks resulted in disruptions to care services, delays in vaccine distribution, and the exposure of sensitive patient data. The increase in remote work also created vulnerabilities in Virtual Private Networks (VPNs) and access points that were previously thought secure.
- **Key Lesson:** Social care organisations underestimated the scale of attacks they could face, revealing vulnerabilities in endpoint security, staff awareness, and rapid response capabilities during a high-stakes public health crisis.

5. Social Care Data Found on the Dark Web

- **Incident:** Reports emerged in 2020 and 2021 of personal data from social care providers being found on the dark web, likely from multiple sources including ransomware attacks and breaches in third-party systems.
- **Vulnerability:** Social care providers, particularly smaller organisations or charities, had limited cybersecurity budgets and outdated technology, leading to weak data protection practices. Even organisations that believed they had adequate protection often failed to account for vulnerabilities in their supply chains or third-party systems.
- **Impact:** Personal and medical data of vulnerable individuals, including information about their care, disabilities, and medical treatments, was discovered being sold or leaked on the dark web. The exposure of such sensitive data poses a significant risk for identity theft, fraud, and targeted exploitation of individuals in care.
- **Key Lesson:** Many organisations in the care sector underestimated the threat of cyberattacks and how data, once compromised, could be exploited on the dark web. This highlights the need for more robust encryption practices, even in seemingly "protected" systems, and greater monitoring of dark web activity for stolen data.

The vulnerabilities exposed in the cases highlighted above suggest that organisations in the care sector must be more proactive, not just reactive, in addressing cybersecurity concerns, particularly given the sensitivity of the data they handle.

Based on previously seen attacks on the health and social care sector, there are some **key takeaways** for the UK Care Sector:

- **Underinvestment in Cybersecurity:** Social care organisations, particularly smaller ones, often underinvest in cybersecurity, mistakenly believing that basic firewalls and antivirus software are sufficient.

- **Outdated Systems:** Legacy IT systems in the care sector are often not updated regularly, making them vulnerable to known exploits like WannaCry.
- **Third-Party Vulnerabilities:** Many organisations depend on third-party vendors for data management and other services, but do not sufficiently assess these vendors' cybersecurity practices.
- **Exploitable Data on the Dark Web:** Personal data from social care systems, once breached, often ends up on the dark web, exposing vulnerable populations to fraud and identity theft.
- **Need for Ongoing Threat Awareness:** Cybersecurity threats evolve, and the care sector must continuously update its defences and train its staff in identifying phishing attempts and other cyber threats.

What is the cyber threat?

There are many types of cyber-attack organisations could fall victim to. These include malware, phishing, ransomware, zero-day attacks, Advanced Persistent Threats (APTs), supply chain attacks and extortionware (see the glossary on page 21 for more detail).

The risk comes from multiple 'threat actors' with various motivations, methods, and skill levels. While the term 'hacker' might suggest the idea of a lone teenager operating from a dark bedroom, cybercrime is a big business, which according to the *Boardroom Cybersecurity Report on Cybercrime*, is now the third largest economy after the US and China1. Nation-state attacks are also a growing threat – a type of attack where state-sponsored hackers act on behalf of their government to attack critical infrastructure, gather intelligence, or cause disruption[12].

Care providers might find it hard to believe that their business would be of any interest to cyber attackers, but even non-targeted attacks can be damaging, such as those which reach an organisation's systems through the supply chain. **There is an additional risk that as larger organisations such as local government and the NHS strengthen their defences, care providers could be seen as a weak link into the supply chain to reach these attractive and proven targets.**

Currently, phishing attacks (also known as social engineering attacks) are the most common type of attack. This is where messages (texts, emails, phone calls) trick receivers into action such as clicking on a link or handing over security credentials. *The Cyber Security Breaches Survey 2024*[7] found that of those businesses which reported being attacked, phishing was the most common (84 per cent of businesses), followed by others impersonating organisations in emails or online (35 per cent of businesses) and then viruses or other malware (17 per cent of businesses).

Phishing can be used as a tactic for hackers to instal malware (malicious code), which could also take the form of ransomware (malware which prevents system access until a ransom is paid) or extortionware (data is exfiltrated and a sample is published online, followed by a demand, usually for money). Even if a demand is met, which is not a recommended action to take, there is no guarantee that what is known as an Advanced Persistent Threat (ATP) will not have been left behind.

It is also recognised that the ability to spot phishing is getting more difficult. The spelling errors and other inconsistencies which may have once featured in these communications are vanishing. As cyber attackers become more professional, so does their output. The National Cyber Security Centre's (NCSC) *2023 Annual Review*[12] reported that the organisation received an all-time high of incident reports in 2023, with 2,005 reported incidents, up from 1,226 in the previous year (a 64 per cent increase). Of these, 327 incidents involved the exfiltration/extortion of data, which was up 18.5 per cent on the previous year.

Previous CCoE research has found that organisations often have ways into their systems which are freely available to exploit online that they are completely unaware of. Working with a partner company, the CCoE can perform a scan of the Internet to look for misconfigurations, security vulnerabilities and exposed data. Any Open Source information the tool finds could be seen by anyone online, including amateur hackers.

The CCoE has found that vulnerabilities frequently found included badly configured services or out of data software. They might also include forgotten servers and neglected websites affected by mergers or organisational changes. Often configuration changes are made which accidently make information available online without an organisation's knowledge. Carrying out a scan, which is part of Care England and the CCoE's newly-developed Care Protect offering, can help bring unknown vulnerabilities to light and shut the open back doors to an organisation's infrastructure.

While the remedy to these vulnerabilities can be fairly simple, with remediations for many identified vulnerabilities typically requiring updating software or hardware, commonly servers, to a version which is not vulnerable, these risks need to be highlighted and addressed before they are exploited.

An ever-growing threat

Hackers having access to Artificial Intelligence (AI) has been highlighted as a threat by the National Cyber Security Centre's (NCSC) *2023 Annual Review*[12]. **AI will increase the speed at which cyber-attacks can be developed and deployed by lower-skilled hackers, making it increasingly likely that care providers will be targeted directly or caught up in a supply chain attack.**

A recent survey by ClubCISO[14] highlighted that the majority (63 per cent) of CISOs (Chief Information Security Officers) rate the threat of AI cyber-attacks as critical or high and with the potential to be extremely damaging to businesses. In addition, 62 per cent felt the cybersecurity industry was not equipped to deal with the threat.

A deeply concerning development is the emergence of 'deepfakes' – videos, audio clips or pictures which have been doctored using AI to mimic a person's voice and facial features to look real.

Supply chain cyber-attacks are also becoming more commonplace, when an attack spreads from one organisation to another or uses one to access the other, such as provider to customer. The *2021 CrowdStrike Global Security Attitude Survey*[15] found 84 per cent of IT personnel believed software supply chain attacks could become the biggest cyber threat to organisations by 2024.

Supply chain attacks are an increasing risk, including through the infiltration of software, as seen with the SolarWinds attack[16] where attackers compromised a software update process affecting many companies, but there are other potential routes into organisations through their supply chain, including through hardware.

Increasingly, attacks are coming from hackers gaining access to a third party and then monitoring traffic between the third party and the target organisation before intervening and sending what looks like a legitimate email in a phishing attack.

The most recent data from Verizon's *2023 Data Breach Investigations Report*[17] highlighted that 74 per cent of breaches involve a human element. This means understanding the risk posed by staff and deploying staff training to help them understand cyber security is essential.

The risks of staff accidently facilitating a cyber-attack could be higher in the care industry than some other sectors. Staff using their own devices is common in the care industry, which can cause potential problems when linking to company databases through insecure networks. Time-poor employees may also be more likely to click a nefarious link. However, while employees are a risk factor in attacks, they are also a key part of cyber defence.

While there can be a financial impact of a cyber breach in terms of recovery costs, loss of business and potential fines from the Information Commissioner's Office (ICO), the health and social care industry is also an attractive target due to potential disruption an attack could cause and the interlinking between organisations.

There could be legal repercussions of not being cyber secure, including the potential of being issued with a fine or given a potentially reputationally damaging reprimand by the Information Commissioner's Office (ICO), the organisation responsible for overseeing compliance with data protection in the UK. Organisations which collect personal data have a legal obligation under the Data Protection Act 2018, the UK's implementation of the General Data Protection Regulation (GDPR), to ensure that this data is stored and handled securely. This includes ensuring that it is protected against being accessed unlawfully, lost, destroyed or damaged. There are stronger rules around the processing of what is known as 'special category data' which includes health data. (See the section below: What legal obligations do care providers have?).

What legal obligations do care providers have?

All care providers collect and store personal data belonging to their staff and their clients. Organisations which process personal data generally need to register with the Information Commissioner's Office (ICO) and pay a fee annually. Failing to do so could incur a fine of up to £4,000 in addition to the annual fee due.

Additionally, under the General Data Protection Regulation (GDPR), which is implemented in UK law by the Data Protection Act (2018), personal data must be protected from potential misuse and security breaches and only stored for as long as needed to fulfil a purpose. Health data is regarded as 'special category data' which requires additional protections due to its sensitive nature.

If an organisation suffers a data breach, for example through a cyber-attack, an organisation has a duty to report it within 72 hours to the Information Commissioner's Office (ICO). Any individuals likely to be adversely affected by a breach of their personal data also need to be informed.

There are several steps organisations can take to help them comply with the regulations and show that they understand their obligations under the Data Protection Act (2018). These include:

- Providing data protection training for staff who deal with client information.
- Putting strong data security measures in place which are regularly reviewed and audited.
- Writing data protection policies which are regularly reviewed and updated, including data breach response plans and data retention schedules.
- Being transparent with clients about how their data is used.

Public authorities and bodies and some other organisations carrying out certain activities are legally required to appoint a Data Protection Officer (DPO). Organisations which process large volumes of special category data, including health data, could fall into this category. Even if a care provider is not currently required to appoint a DPO they can decide to do so voluntarily. This person must be suitably knowledgeable and can be an internal employee or externally appointed. A DPO can help ensure that a company is meeting its data protection obligations, can help carry out audits and assessments and can act as a contact with the ICO if required.

Sometimes companies also choose to appoint a Chief Information Security Officer (CISO) to oversee cyber security risk. In cases where this is not a full-time position, a Virtual Chief Information Security Officer (vCISO) could be considered on a part-time basis.

However, even where a DPO, CISO or vCISO is appointed, this person does not have personal responsibility for data protection. Under the law, organisations or individuals processing data are either known as 'data controllers' or 'data processors'. A controller, which could be the owner of a business, for example, has greater responsibility for compliance with the DPA but processors, such as staff members, also have obligations too, which is why staff training is key. The ICO can act against both controllers and processors.

Organisations which fail to take adequate security measures to prevent or contain a data breach could be fined by the ICO. There are two tiers of penalties – the higher maximum amount (£17.5 million or four per cent of total annual worldwide turnover in the previous financial year if higher) and the standard maximum (£8.7m or two per cent of total annual worldwide turnover in the previous financial year if higher). In practice the fines are often less. In February 2024, for example, the Ministry of Defence was fined £350,000 for using the 'To' field in an email rather than the 'BCC' field, while in April 2024, the Central Young Men's Christian Association (YMCA) was fined £7,500 for using the 'CC' field rather than the 'BCC' field in a bulk email sent to individuals participating in a programme for people living with HIV.

The ICO can also issue a 'reprimand' – a written notification given where the ICO believes an organisation has not complied with GDPR but does not think a fine is a useful action. It may include recommendations that the organisation should take to rectify an identified issue. While a reprimand does not include a financial penalty, there can be a reputational impact on a company if it is issued with an ICO reprimand and it will often be required to report it in tenders and contracts it has secured or is bidding for which could impact future business.

4 The Solution

Reading the plethora of tactics and types of attack outlined in section 3 of this report would be scary for any organisation, large or small. Sadly, this is not scaremongering, and as the attack potential increases, so should the strength of an organisation's defences.

To understand the risks faced by the adult care sector and find affordable solutions for providers, Care England carried out a year-long research pilot programme with the CCoE which aimed to understand what the care industry would need in an off-the-shelf cyber protection package to sufficiently protect care providers and their data.

The cyber security industry is one in which many experts claim to have the one overriding solution, but no single solution exists which can meet an organisation's cyber needs and risks. What is needed for optimal protection, and what we have aimed to provide through Care Protect, is a layered approach to security.

Through its networking capabilities, the CCoE has relationships with providers offering state-of-the-art technologies and solutions, which due to its bulk-purchasing power it can access at preferential rates. The CCoE is led and advised by some of the UK's leading experts in cyber security. These experts include:

- **Kurtis Toy,** CEO of the CCoE and a Virtual Chief Information Security Officer (vCISO).
- **Major General Martin Smith CB MBE,** Managing Director of CyberPrism, a cyber security company which protects Operational Technology (OT) and IT in the UK and internationally.
- **Irene Coyle,** Chief Operating Officer at OSP Cyber Academy, a managed service provider of cyber, information security, data protection training and education programmes.
- **Thomas McCarthy,** founder and Managing Director of OSP Cyber Academy and a CCoE Director.
- **Sandip Patel KC,** a Barrister for more than 30 years who was appointed Queen's Counsel (QC), now King's Counsel (KC), more than ten years ago.
- **Colin Jupe,** CEO of Assurity Systems, a company which provides advanced cyber security solutions to a variety of sectors including local government.
- **David Woodfine,** Managing Director of Cyber Security Associates (CSA).
- **Dougie Grant,** Managing Director Europe & Global Head Incident Management at Nihon Cyber Defence.

(See here for full biographies of the CCoE Advisory Board).

Some of the CCoE providers include:

- **OSP Cyber Academy,** a UK Government-assured cyber security and awareness training provider which can help demonstrate compliance with legal requirements.
- **AppGuard,** an endpoint cyber security solution which can protect systems from all threats – even the never-seen-before attack known as 'zero-day'.
- **FractalScan Surface,** an attack surface management tool which scans the Internet to look for misconfigurations, security vulnerabilities and exposed data.

(See here for more information about the CCoE provider partners).

While at the time of publication there had not been any high-profile cases of a cyber incident in the adult care sector, we know that unfortunately it is a case of when, not if. As the sector continues to move towards digitisation its risk levels increase and as local authority and other public sector services start to become more secure, hackers are likely to look for weaker points in the supply chain to reach these higher-profile targets. It is also increasingly likely that our health partners will start to undertake more detailed due diligence on our cyber protections as a requirement prior to commissioning.

The adult care industry is time and resource poor and struggling with years of underfunding. Cyber security may not be a top priority as organisations face issues such as staffing, regulation, and an increasing cost base along with two consecutive large increases in the National Living Wage. However, in an industry where staff changes are common, where employees use their own devices to access company networks possibly through unsecure connections, and where staff are time poor and under pressure, having a good level of cyber protection is vital.

We know falling victim to a cyber-attack can be costly and time-consuming, but it can also be dangerous to clients if their data becomes inaccessible. It is understandable that our members want solutions, not just to be told about the problems, which is why Care England set out to develop a complete cyber protection package with the sector for the sector to help give members peace of mind.

We carried out a year-long pilot with the CCoE which took place from April 2023 until May 2024 which aimed to understand what the care industry would need in an off-the-shelf cyber protection package.

The pilot

The CCoE and Care England ran a pilot study from April 2023 until May 2024 which aimed to understand what the care industry would need in an off-the-shelf cyber protection package.

Six organisations took part in the pilot – two large national providers, one learning disability provider, two small providers and Care England. These were all given access to a range of practical support and solutions and then asked to feedback their experiences.

We asked the participants what their key areas of cyber concern were. Budget was a commonly raised issue. Other frequently mentioned concerns included: clicking a link that affects the company, data breach, phishing emails, ransomware, insider threat, malware, management support, security strategy and state sponsored attacks. The average rating participants gave as to whether cyber security was a concern for their organisation was 4.5 out of a possible 5, highlighting that cyber is a key worry for care providers.

As part of the pilot, participants were able to take advantage of a range of cyber security support and measures. All elements of the pilot were offered by CCoE partner organisations which have been carefully assessed and rigorously tested by the CCoE, its Advisory Board and CCoE parent company iESE to ensure that they are best of breed.

The seven elements of the pilot which the participants tested were:

- Half-day NCSC-assured board member course
- Installation of an end-point security solution (AppGuard)
- Session with a virtual Chief Information Security Officer (vCISO)
- Access to a suite of NCSC-assured online cyber training sessions
- Access to a mobile device security application
- Passive scan on each company's security vulnerabilities
- Tailored advice on how to fix areas of concern.

At the end of the pilot, participants rated each element of the trialed package as helpful and rated the pilot overall as helpful (see table below):

Pilot element	Rating out of 5
Half Day Board Course Training Value	4.3
AppGuard Installation & Usage	3.0
AppGuard Value	4.0
vCISO Session / Support Value	4.7
Online Training Value	4.3
Passive Scan Value	4.7
Pilot Project Overall Value	4.0

Pilot feedback

Kurtis Toy, CEO of the CCoE, said he was impressed with the willingness of the pilot's participants to engage with the trial. **"What we understand is that we need to remove as many barriers as possible to cyber security because this is an industry that is already under-resourced and time poor. We are confident from running the trial that the solution we are now able to offer offers the right level of ready-to-go support and solutions for the care industry."**

In the closing meeting for the pilot project, one of the care providers involved in the trial said the most valuable part of the pilot was the reassurance the CCoE expertise gave them around who to trust. "We get offered a lot of cyber security solutions, but it is hard to know how much of what is recommended is good and whether it will enhance the security of the organisation, or whether it is being offered to meet sales targets," said Manlio Mannisi, Head of IT at SeeAbility. His colleague, Mandy Kendrick, Fundraising Coordinator at SeeAbility, added: "I undertook the online training courses as part of the pilot. The short modules were designed in a way that made them easy to complete. They were simple to follow and, even if you already know a lot about cyber security, they are still excellent reminders and refreshers."

Staff training is a vital part of the package. Data from Verizon's *2023 Data Breach Investigations Report*[17] highlighted that 74 per cent of breaches involve a human element. Additionally, Skills for Care research 3 has found that care workers who receive regular training are less likely to leave (20.6 per cent turnover rate compared with 31.6 per cent).

Care England was one of the six organisations which took part in the pilot programme. Louis Holmes, Digital and System Transformation Projects Manager at Care England, said the organisation had welcomed the chance to be involved with the pilot and to recruit the other five organisations involved through its membership body. "The pilot gave us a lot of takeaways to take forward as an organisation and is a great starting block to build on. I know that the other organisations we brought into the process found it useful as well."

Holmes was the person at Care England who attended Cyber Risk & Resilience Board & Executive course provided as part of the pilot: "It was really interesting and found it very useful as a starting point for the project," he explained, "The package of online courses acted as a bit more of a reminder for me but my colleagues who did them found those useful. They were very helpful bite-sized interactive sessions."

He said that the vulnerability scan and vCISO session were particularly useful elements of the trial too. "The vulnerability scan indicated that there was a potential vulnerability in one of our membership items. While it does not have any personal data on it, if it went down it would take time and money to fix. Having the potential issue alerted has helped us secure it. The vCISO session was also useful as it identified some things to address and how we can work with our Managed Service Provider better."

Holmes said he would encourage all care providers to consider engaging with the Care Protect offering. "Care providers should be completing the data security protection toolkit which we promote as a starting point for any cyber security practice. However, that is a self-assessment kit, so it doesn't provide any cyber security practicalities. Care Protect is a next step and gives you things to implement with the senior staff training, staff training and software. It is all about risk management and it is designed to help support and mitigate the impacts of a cyber-attack on your organisation."

He highlighted that the increasing push towards digitisation in the care provider market is making cyber an increasingly prevalent issue. **"The last year has seen a huge increase in cyber security attacks on health and social care organisations, so I think care providers are becoming more aware of the risk but there is still a lack of awareness across the board. The Local Government Association is increasingly interested in what care providers contingency plans are but there is still some way to go in raising awareness and implementing effective cyber security measures – not just having a standard anti-virus solution installed on devices."**

There is also a possibility that being able to demonstrate that there are adequate protections in place in an organisation, through schemes such as Care Protect, will allow care organisations to apply for and obtain cyber insurance.

The Care Protect package

Following the success of the pilot programme, Care Protect has been designed as a complete off-the-shelf package of support and protection to meet the cyber needs of the adult care sector. It is suitable for organisations of any size and can be tailored and adapted if required. Importantly, the care industry can be assured that Care Protect has been developed in accordance with care industry providers' concerns, with the backing of some of the UK's leading cyber security experts and high-quality partner organisations of the CCoE.

The five elements of the package are:

1) **National Cyber Security Centre (NCSC) assured Board Course**

   Access to a half-day National Cyber Security Centre (NCSC) assured online Cyber Risk & Resilience Board & Executive course from CCoE training partner OSP Cyber Academy for one senior management member.

2) **Passive scan of vulnerabilities**

   A passive scan using attack surface management tool FractalScan Surface. The technology scans the Internet using a domain name or IP address to look for misconfigurations, security vulnerabilities and exposed data. The vulnerabilities identified by the tool could be seen by anyone online, including hackers, revealing potential routes – or open back doors – into organisational systems. A report is generated on any vulnerabilities found and advice given on how to resolve them.

3) **Online staff cyber training**

   Access to online bite-sized NCSC-assured courses from CCoE partner OSP Cyber Academy. These are Ransomware and Malware, Password and Access Management, Phishing and Social Engineering, Cyber Security at Home, Mobile Device Security and Data Breach.

4) **vCISO support session**

   The Care Protect package includes access to a virtual Chief Information Security Officer (vCISO), including an individual vCISO session where tailored advice is given on improving cyber security. This could include advice on how to manage risk from the use of personal devices such as mobile phones.

5) **AppGuard licences**

   Under Care Protect licenses are included for the zero-trust cyber security solution AppGuard which can be installed on individual devices. Find out more about AppGuard below.

To speak to someone about procuring Care Protect for your organisation, contact Care England at info@careengland.org.uk or the CCoE at enquiries@ccoe.org.uk

5 About the CCoE and its provider partners

The Cyber Centre of Excellence (CCoE)

The Cyber Centre of Excellence (CCoE) was created in response to the growing threat from cyber-attacks. It has brought together an Advisory Forum of some of the UK's leading experts in cyber security with an aim of making the UK the safest place to live, work and play online. Backed by parent company iESE, a not-for-profit consultancy which works with local authorities and public bodies to help them improve and deliver services, the CCoE uses its bulk purchasing power to access military-grade cyber protection at high street prices. The CCoE keeps abreast of emerging threats and new innovations and is working across multiple sectors, including the care industry, to provide packages of support which meet needs and give them peace of mind at reasonable prices.

Cyber Centre of Excellence for Local Public Services

iESE Ltd

iESE is the parent company of CCoE Ltd. iESE was created by local authorities in 2004 as a shared resource to transform public services and retain experience in the sector. It is a not-for-profit enterprise where any surplus generated is invested in research on behalf of the sector. It has delivered real savings of more than £1bn for its members and clients. iESE is also the parent company of iESE Innovation Ltd which supplies and develops systems to support a fair and equitable health and social care market.

The public sector transformation partner

OSP Cyber Academy

The Cyber Centre of Excellence (CCoE) has teamed up with UK Government-assured cyber security and awareness training provider OSP Cyber Academy to provide access to a wide range of cyber security and data protection training programmes which reduce risk, improve cyber resilience, and demonstrate compliance with legal requirements.

Training days, such as the Cyber Risk & Resilience Board & Executive Awareness Course can be offered in person, while an online system allows an organisation's wider employee population to access various online courses. These include: GDPR Staff Awareness, Cyber Security Staff Awareness, Phishing and Social Engineering, Mobile Device Security and Supply Chain Cyber Awareness.

AppGuard

AppGuard is an endpoint cyber security solution which can protect systems from all threats – even the never-seen-before attack known as 'zero-day'. Developed in the US defence environment, it has recently become commercially available in the UK and is being offered by the CCoE in partnership with its European distributors, Assurity Systems Ltd.

Traditional endpoint defences incorporate anti-virus and anti-malware solutions, however even with the latest Endpoint Detection and Response (EDR), Machine Learning and Artificial Intelligence, this combination of defences still relies on recognising the signature of the threat or recognising it as being like one seen before. The problem with the new sophisticated wave of targeted cyber-attacks, is that if malware has never been encountered by a defence system before, there is a high probability it will be able to penetrate endpoints and activate. AppGuard offers the required step-change in endpoint and server defences because it operates in an entirely different way to traditional solutions.

- Find out more: www.iese.org.uk/project/appguard

FractalScan Surface

FractalScan Surface is an attack surface management tool which scans the Internet accessing Open-Source information visible to anyone online to look for misconfigurations, security vulnerabilities and exposed data to give organisations a real-time report of their security risks and likelihood of being attacked. Knowing where these vulnerabilities are allows these potential gateways into the organisation to be fixed before they are found by cyber criminals. Besides scanning for an organisation's own risks, FractalScan Surface can also be used to check a vendor's security posture to assess potential supply chain vulnerabilities.

- Visit www.ccoe.org.uk to find out more about the CCoE and its provider partners.

6 Glossary

Advanced Persistent Threat (ATP)

An ATP uses continuous and sophisticated hacking techniques to gain access to a system and remain inside unknown. This method of attack is usually levelled at high-level targets with the goal of stealing valuable information. It is also possible that an ATP attacker could target smaller companies in the supply chain as a way of gaining access to larger organisations through these often less-well defended routes. Even when an ATP attack is discovered and dealt with, the hacker could leave routes open to return.

Breach

A cyber security breach is an incident resulting in the unauthorised access of computer data, applications, networks, or devices which results in information being accessed without authorisation. A breach can cost a company a large amount of money, not just in shoring up defences to prevent further breaches but also for potentially stolen intellectual property or critical company data. If the breach also includes personal data, the ICO (Information Commissioner's Office) **must** be informed within 72 hours of the organisation becoming aware of the breach. Fines may be issued under the GDPR if adequate protections for personal data were not in place.

Dark Web

The dark web refers to websites which cannot be found using traditional search engines or visited using traditional web browsers. It is different from the Deep Web, which is where information may sit not intended for public view (such as a test webpage). In the event of an extortionware attack this is where the hackers will auction stolen information.

Extortionware

With this type of attack, the cybercriminal gains access to and exfiltrates your data which they may publish a sample of online so you know they have it. This will be followed by a demand, usually for money. Your data may be auctioned on the dark web to the highest bidder. Even if you pay, which is not recommended, the hackers could leave coding (an ATP) to activate later.

Immutable Backups

An immutable backup is a copy of data that cannot be altered, deleted or changed in any way once the back-up has completed, not even by system administrators. This type of back up can be critical when a company needs to recover or restore data after it has been lost or damaged, whether through a cyberattack or a natural disaster.

Layered Approach

A 'Layered Approach' is a term often used within information security. Whilst it sounds like this means one tier of security being layered on top of another, it really means multiple solutions should be put into effect to defend against the same or similar issues. The idea is to build a suite of defences to act as contingency plans for one another and should include security tactics for people, processes, and technology. The best approach is to have a failover for every avenue possible and review your security controls on an ongoing and regular basis.

Malware

Any type of malicious code designed to infiltrate a device, including a mobile device, without the user's knowledge. Malware gets activated by the user unwittingly downloading or installing the malware, such as by clicking on a link or visiting a malicious website. Malware includes ransomware and extortionware (see below).

Multi Factor Authentication (MFA)

When logging in, we use at least one factor to identify ourselves, such as a password or PIN, through a smartphone or a secure USB key, or via a fingerprint or facial recognition. Multi-factor Authentication uses at least two of these methods to log in, helping prevent password compromise.

Nation State Threats

Cyberattacks of this nature are initiated and sponsored by countries or geopolitical groups and are referred to as Nation State Threats, which aim to disrupt infrastructure, business, government and military. These types of attack can be particularly difficult to identify as the attackers often shift blame to cyber gangs, other foreign entities or hacktivist groups.

Phishing

'Phishing' describes an unwanted communication that might contain dangerous content or have a hidden agenda. This could be in the form of a hyperlink or URL that redirects to a malicious site or download an attachment with hidden malicious content.

Ransomware

Malware which typically locks or denies access to files until you pay a ransom to the hacker. Any organisation storing sensitive information is at risk. Even if you pay the ransom the hackers could leave coding (an ATP) set to activate later.

Zero Day

A 'Zero Day' vulnerability is a security flaw that has been discovered but there is no security patch for it yet. Once discovered, Zero Day flaws are often exploited very quickly so it becomes a race against time for the software provider to develop and distribute a security patch.

Zero Trust

'Zero Trust' is a term a used for both security models and network architectures. In both cases, the main concept is "never trust, always verify". This means all devices, access or identities should not be trusted by default, even if they were previously trusted or are connecting through a known network or location. Zero Trust is often implemented to promote strong verification processes that are continually re-examined and re-established and provide minimum access privileges.

7 Contributors

The Cyber Centre of Excellence (CCoE)

The Cyber Centre of Excellence (CCoE) is an initiative aimed at making the UK the safest place to live, work and play online. The CCoE has an Advisory Board of some of the UK's leading experts in cyber security.

The CCoE Advisory Board:

Kurtis Toy

Kurtis Toy is the CEO of the CCoE and a Virtual Chief Information Security Officer (vCISO). He is a GDPR Foundation and practitioner (Data Protection Officer), ISO 9001 internal auditor training and ISO 27001 lead implementor. He is also a CISSP (Certified Information Systems Security Professional).

Major General Martin Smith

Major General Martin Smith CB MBE is the Managing Director of CyberPrism, a cyber security company which protects Operational Technology (OT) and IT in the UK and internationally.

Major General Smith had a 33-year career in the Royal Marines, becoming Commandant General of the Royal Marines. He commanded the UK's Amphibious Force and led the UK's maritime counter terrorism force. He also founded the unit known as 30 Commando Information Exploitation Group.

Irene Coyle

Irene Coyle is Chief Operating Officer at OSP Cyber Academy, a managed service provider of cyber, information security, data protection training and education programmes. She joined OSP Cyber Academy after a 30-year career in the police force in a variety of roles, including that of Chief Inspector for recruitment within Police Scotland. Coyle is also a Data Protection Officer, a National Cyber Security Council (NCSC) Certified trainer and holds a teaching degree. OSP Cyber Academy has joined with the CCOE to provide member access to its suite of training tools.

Thomas McCarthy

Thomas McCarthy is the founder and Managing Director of OSP Cyber Academy and is also a CCoE Director. He has previously held various roles in training auditing and safety, including several positions in the energy sector. As someone with a wide range of industry contacts and knowledge, McCarthy was instrumental in helping to establish the CCoE's Advisory Forum.

Sandip Patel KC

Sandip Patel has been a Barrister for more than 30 years and was appointed Queen's Counsel (QC), now King's Counsel (KC), more than ten years ago. He became involved in cyber security law after being asked to prosecute several cases for the Crown Prosecution Service. Patel is also Director of cyber security consultancy Quantum Resilience International and Chief Legal Advisor at OSP Cyber Academy.

Colin Jupe

Colin Jupe is CEO of Assurity Systems, a company which provides advanced cyber security solutions to a variety of sectors including local government. He is also a qualified General Data Protection (GDPR) practitioner and the Managing Director of VXPartners, a company which helps organisations become and remain compliant with UK Data Protection law. Prior to launching Assurity Systems, Jupe held a management consulting role where he predominantly assisted technology companies with marketing and finance strategy and was also formerly Director of a marketing database and data processing company.

David Woodfine

David Woodfine is the Managing Director of Cyber Security Associates (CSA), a company he started with former colleague James Griffiths in 2013. CSA began as a consultancy practice and still offers this trusted advisor service helping clients with aspects of cyber security such as assessments, help gaining certifications, incident response and general cyber road maps and development. CSA also provides 24/7 managed Security Operations Centre (SOC) services to help monitor, prevent, detect, investigate, and respond to cyber threats.

Dougie Grant

Dougie Grant is Managing Director Europe & Global Head Incident Management at Nihon Cyber Defence. He started his career in the military and from there moved to the private sector working in IT where he became interested in cyber security. From here, he progressed into law enforcement, spending eight years as the Cyber Lead for the Police Service of Northern Ireland where he started building online investigative capability looking at the online components of crimes. He finished his public sector career in the City of London Police seconded to GCHQ and NCSC where he spent five years as a Senior Coordinator at the National Cyber Security Centre (NCSC). He remains associated to the NCSC as part of its Industry 100 (i100) initiative.

Care England contributors:

Professor Martin Green OBE, Chief Executive of Care England

Martin Green has had an extensive career in NGO development, both in the UK and internationally. He is a Trustee of the National Centre for Creative Health (NCCH), Vice President of The Care Workers Charity, Champion of The National Aids Trust and Commissioner of the Royal Hospital Chelsea. In 2013 he was appointed Visiting Professor of Social Care to Buckinghamshire New University.

In 2012, in his role as Department of Health and Social Care Independent Sector Dementia Champion, he led the development of the Dementia Care and Support Compact for The Prime Minister's Challenge on Dementia.

In 2008 he was named care personality of the year and was awarded an OBE for Services to Social Care in the 2012 Queen's Birthday Honours List. In 2019 he was presented with the Health Investor Outstanding Contribution award. He writes and broadcasts extensively on social care issues and is on the Editorial Board of Community Care Market News and Care Talk magazine.

Richard Ayres, Social Care Advisor, Care England

Richard Ayres joined Care England in March 2021 as a Social Care Advisor although has worked collaboratively with Care England since 2014 having formerly worked within the care sector in a commercial capacity addressing health and social care commissioning challenges experienced by care providers since the austerity period.

He previously held a 25-year career history in procurement spanning Utilities, Banking, Travel and Care Sectors. His current role is to provide technical and commercial support to the team in areas such as funding, workforce, VAT, and social care reform.

Pilot participants:

Care England

Care England is a registered charity which is the largest and most diverse representative body for independent providers of adult social care in England. It works on behalf of small, medium, and large providers to speak with a unified voice for the whole care sector. Its aim is to create an environment in which care providers can continue to deliver and develop the high-quality care that communities require and deserve.

Care UK

Care UK has more than 150 care homes across England, Wales and Scotland providing a range of services, from residential and nursing care through to dementia care and end of life care.

Serene Care

Serene Care is a 'Boutique' care provider with three care homes in the UK.

SeeAbility

SeeAbility provides specialist accommodation and support services in the South of England for people with learning difficulties or Autism who may also have sight loss.

8 References

1. EY, Realising the value of healthcare data: a framework for the future, 2019: ey-value-of-health-care-data-v20-final.pdf
2. Secureworks, Secureworks Boardroom Cybersecurity 2023 report: Cyber Ventures Boardroom Cybersecurity Report 2023 | Secureworks
3. Check Point, Cyber Attack Trends 2022 Mid-Year report: 2022 Cyber Attack Trends: Mid-Year Report (checkpoint.com)
4. Care Quality Commission, State of Care 2022/23 report: State of Care 2022/23 - Care Quality Commission (cqc.org.uk)
5. Care England, 2023 Sector Pulse Check Report: (Hft-Sector-Pulse-Check-2022-Single-Pages-Digital.pdf (careengland.org.uk)).
6. Skills for Care: www.skillsforcare.org.uk/adult-social-care-workforce-data/Workforce-intelligence/publications/Workforce-estimates.aspx
7. Department for Science, Innovation & Technology, Cyber Security Breaches Survey 2024: Cyber security breaches survey 2024 - GOV.UK (www.gov.uk)
8. Children and Young People Now article: https://www.cypnow.co.uk/news/article/children-s-home-provider-targeted-by-hackers
9. Acronis news piece: The NHS cyber attack: how and why it happened, and who did it (acronis.com)
10. NHS England news update: NHS England — London » Update on cyber incident: Clinical impact in south east London – Thursday 27 June
11. Obrela Security Industries study: (81% of UK Healthcare Organizations Hit by Ransomware in Last Year - Infosecurity Magazine (infosecurity-magazine.com))
12. NCSC, NCSC Annual Review 2023: Threats and risks - NCSC.GOV.UK
13. Splunk, State of Security 2024: The Race to Harness AI report: State of Security 2024: The Race to Harness AI | Splunk
14. ClubCISO survey: AI cyber-attacks a critical threat, but CISO priorities are not changing yet, according to the latest ClubCISO research - ClubCISO
15. CrowdStrike, CrowdStrike Global Security Attitude Survey: 2021 CrowdStrike Global Security Attitude Survey | Report | CrowdStrike
16. TechTarget news: SolarWinds hack explained: Everything you need to know (techtarget.com)
17. Verizon, Verizon 2023 Data Breach Investigations report: 2023 Data Breach Investigations Report: frequency and cost of social engineering attacks skyrocket | News Release | Verizon

CARE ENGLAND
Representing independent care providers

Care England
info@careengland.org.uk
www.careengland.org.uk

CCoE
Cyber Centre of Excellence
for Local Public Services

Cyber Centre of Excellence
enquiries@ccoe.org.uk
www.ccoe.org.uk