Cyber Attacks on Social Care: A case of ‘when, not if’

DSPT
Better security.
Better care.

17th October 2023

Digital Care Hub

The technical issues

DSPT
Better security.
Better care.

- This webinar is being recorded
- This is for care providers who want to learn how to reduce the risk and impact of a cyber attack.
- Attendees are on mute and can't be seen
- Please use the Q&A function to ask questions.
- On a phone, tap the screen to see the controls – choose More and then Q&A
- Questions that we can't answer: we will come back to you. Add your email to Q&A
- This webinar is 1 hour 30 minutes.
- You will get access to the recording and the presentation (inc links)

Digital
Care Hub

Agenda for today

- **Why cyber security matters for social care** – Michelle Corrigan, Better Security, Better Care Programme Director
- **The Cyber Security strategy for health & social care –** Ethan Gray, Department of Health and Social Care
- **The Impact of a cyber attack on a care service** – David Glover, Caremark Ltd
- **Top tips for reducing risk and impact of an attack –** Michelle Corrigan, Better Security, Better Care

- Please use Q&A (not Chat) for your questions

Digital Care Hub

Poll

DSPT
Better security.
Better care.

Care providers:

- Are you a single or multi site organisation?
- Has your service completed the Data Security & Protection Toolkit (DSPT)?
- Are you planning to complete the DSPT by the 30 June deadline?

Digital Care Hub

Why Data Protection & Cyber Security Matters for care

Michelle Corrigan - Programme Director Better Security, Better Care

DSPT

Better security.
Better care.

Digital Care Hub

Why data and cyber security matters for all care services

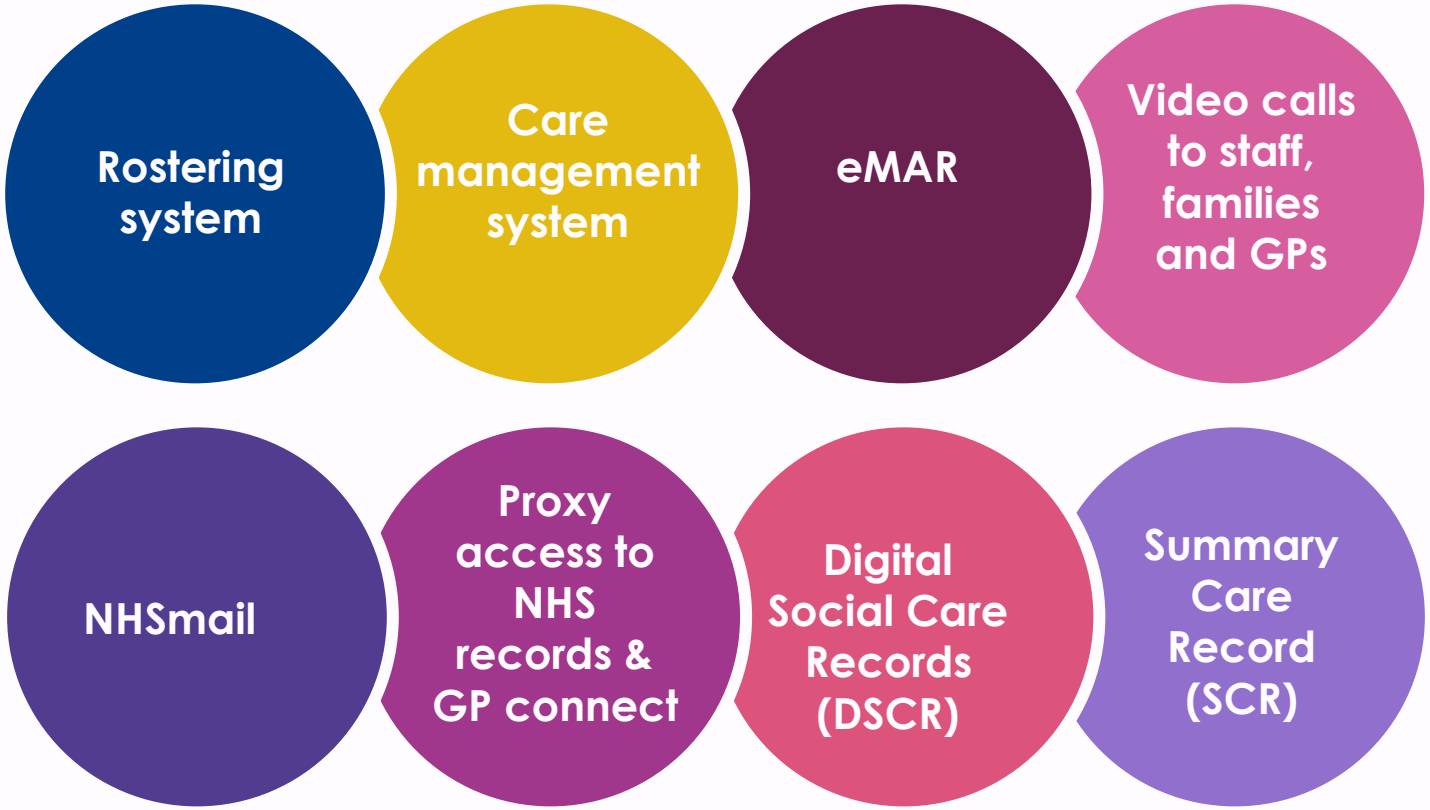
DSPT
Better security.
Better care.

- Data safety is client safety
- Legal responsibility to protect data
- Increased data sharing: real benefits, but also new risks such as cyber attacks
- The present – never mind the future – is digital
- Indicator of good quality
- Regulatory requirement
- Increased loss of data risk with some service types i.e. homecare
- Staff using their own devices for work purposes

Digital Care Hub

The future is about sharing information securely

DSPT
Better security.
Better care.



Digital Care Hub

A Cyber Security Strategy for Health & Social Care

Ethan Gray – Cyber Security Policy Manager, Department of Health & Social Care

DSPT
Better security.
Better care.

Digital Care Hub

The challenges

The Cyber Strategy spans across Health and Social Care, and is important in showing the our vision to secure the system. It is important that we do not approach Care in the same way that we approach the NHS.

The challenges we face across the sectors are often very similar:

- High operational pressures
- Complex sector
- Vulnerable supply chain
- Limited cyber workforce
- New digital technology and data

But our approach must be tailored to the Social Care, if we want to ensure the Health and Care system is as resilient as possible to cyber threats.

Digital Care Hub

The 5 pillars

DSPT
Better security.
Better care.

Focus on the greatest risk and harms

Defend as one

People and culture

Build secure for the future

Exemplary response and recovery

Digital Care Hub

Our Commitments for Adult Social Care

DSPT
Better security.
Better care.

Publish an implementation plan setting out planned activity for the next 2 to 3 years to support the strategy

Develop a product to map our most critical suppliers, and ensure consistent engagement

Provide funding for local cyber resource with national training support

Publish a comprehensive and data-led landscape review on the status of cyber security in adult social care

Digital Care Hub

The impact of a cyber attack on a care service

David Glover – Joint CEO of Caremark Limited

DSPT
Better security.
Better care.

Digital Care Hub

A BIT ABOUT US

Founded in 2005

140 Franchised Offices in UK and Internationally

2023 UK Network Turnover £125m est.

Support 8,000 customers per week

SOFTWARE

Franchisees have to comply with Caremark model

Caremark mandates 2 different rostering systems

Care Planning Software currently optional

Review of Software provision was scheduled for Q1

ISSUES

- 4th August 2022, Cyber Attack of one of the mandated software
- System shut down immediately without warning
- Providers back up system failed
- Affected 50% of Caremark network
- Largest office has up to 30,000 calls per week

SOLUTIONS

Quickly became apparent that restoration of software not imminent

Immediate consideration of how to support Franchisees

Support needed with rostering, payroll and invoicing

Specialist In House team created with experts from different areas

At height of outage Caremark had five full time staff seconded

SOLUTIONS

In House built manual workarounds in Excel for invoicing and payroll
Liaising with 3rd Party care planning software providers
Use of existing 3rd party software or manual workarounds for rostering
£15m of manual workarounds processed by in house team
Ongoing regular dialogue at director level with software provider
Minimum weekly franchisee updates/webinars
Working with alternative mandated rostering software provider

CHALLENGES

- Local Authorities
- Franchisee Cashflow
- Loss of staff at Franchisee level
- Inability to take on new customers
- Potential data breaches / informing customers
- Alternative software systems
- Moving Franchisees to alternative software provider

LESSONS LEARNT

- Ensure robust business continuity plan
- Communication is imperative
- Consideration of internal data back up systems
- Standardisation of operating systems across the network
- Don’t deviate from your fundamental business model
- Reliance on third party suppliers – good or bad?

Top tips for reducing the risk and impact of a cyber attack

Michelle Corrigan – Better Security, Better Care

DSPT
Better security.
Better care.

Digital Care Hub

Complexity of a modern small organisation

DSPT
Better security.
Better care.

- Emails
- Mobile devices
- Websites
- Social media
- Ecommerce systems
- Online banking
- BYOD and office policy
- Network management
- Backup and remote access

Digital
Care Hub

Small Organisations, Big Impact

DSPT
Better security.
Better care.

Why put your already limited resources into preparing for and protecting against cybersecurity attacks?

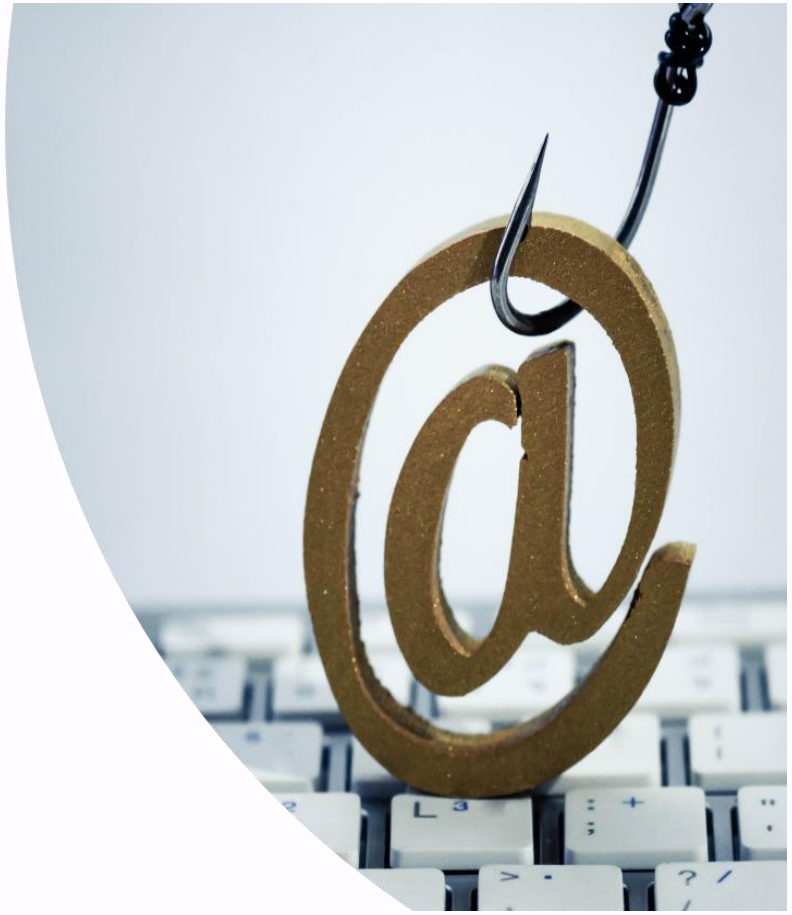
Vulnerability	Cost	Reputation
Attackers can see small organisations as easy targets	Attacks can be extremely costly and threaten the viability of an organisation	Users, the general public and employees expect and trust you to keep their information secure

Digital Care Hub

Cybersecurity Threats

DSPT
Better security.
Better care.

- Phishing Attacks
- Ransomware
- Hacking
- Social Engineering

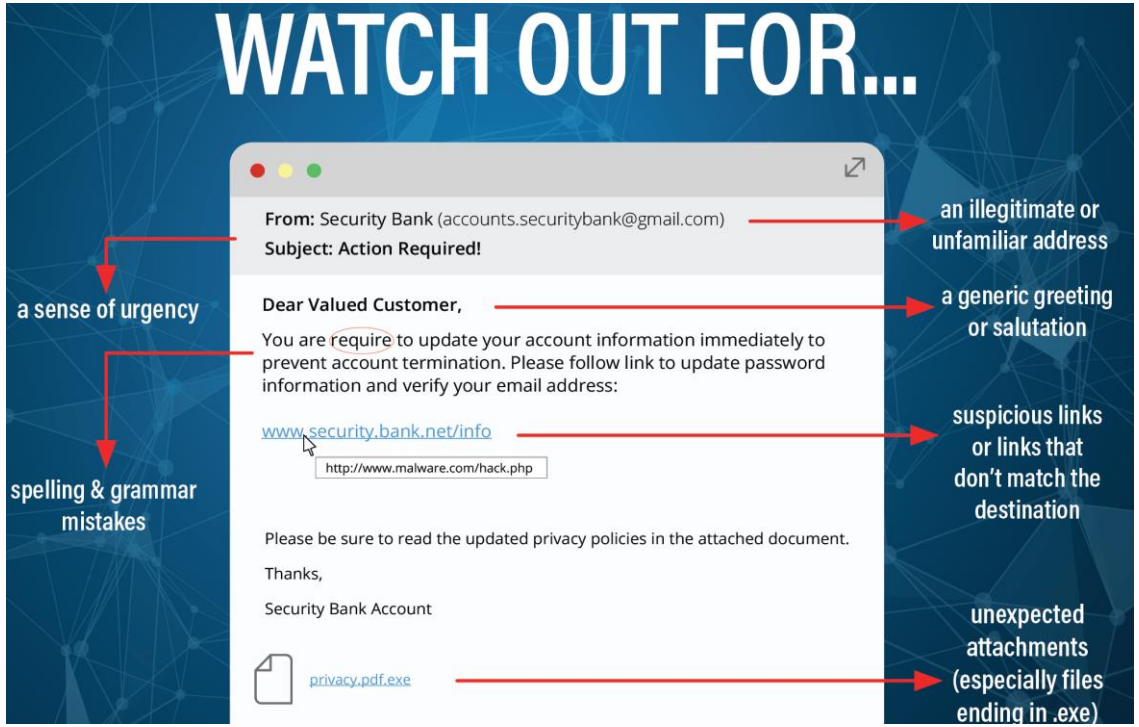


Digital
Care Hub

Phishing Attacks

DSPT
Better security.
Better care.

- Attack involving trickery, often confidence manipulation.
- Designed to gain access to systems or steal data.
- Targeted phishing is “spear phishing”.
- Variants include:
  - Vishing - attacks by telephone
  - Smishing - those using SMS or text
  - Whaling - targeting high profile people
  - Pharming - Fake website to trick into entering credentials to attacker



Digital Care Hub

Ransomware

DSPT
Better security.
Better care.

- Type of software with malicious intent and a threat to harm your data
- The author or distributor requires a ransom to undo the damage
- No guarantee the ransom payment will work
- Ransom often needs to be paid in cryptocurrency

Example:

WannaCry was one of the most devastating ransomware attacks in history, affecting several hundred thousand machines and crippling banks, law enforcement agencies, and other infrastructure.

Digital Care Hub

Hacking

DSPT
Better security.
Better care.

- Unauthorised access to systems and information
- Website attack such as DDoS (distributed denial-of-service)
- Access denied to authorised users
- Stolen funds or intellectual property

Example:

Shops point-of-sale system was hacked; malware installed. Every customer's credit card information was sent to criminals.

Digital Care Hub

Social Engineering

DSPT
Better security.
Better care.

- Someone “official” calls or emails to report a crisis situation.
- They represent HMRC, a bank, the lottery or “Microsoft” technical support.
- There will be a sense of urgency and a dire penalty or loss if you don’t act now.

Example:

HMRC scams – You receive a phone call claiming to be HMRC, reporting you owe money and need to pay or else get hit with a fine.

Digital Care Hub

Smartphones – BYOD or Provide?

DSPT
Better security.
Better care.

Bring your own device	Corporate Owned
Pros: ✓More cost effective ✓Staff already comfortable using the device	Pros: ✓Easier to ensure they are managed securely ✓Better oversight
Cons: ✘Need to enforce BYOD policy ✘Less oversight	Cons: ✘Cost ✘May require technical expertise

Digital Care Hub

BYOD – The law and what you need to know

DSPT
Better security.
Better care.

- The legal responsibility for protecting personal information is with the data controller, not the device owner.

- the Data Protection Act (DPA), states employees must take measures against unauthorised or unlawful processing of personal data

- the Employment Practices Code, which states that employees are entitled to a degree of privacy in the work environment

- https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

Digital Care Hub

BYOD – what to do

DSPT
Better security.
Better care.

- Consider what information your staff might share
- Social media
- Apps automatically saving photos
- https://www.ncsc.gov.uk/guidance/byod-executive-summary

Digital Care Hub

BYOD – what to do

DSPT
Better security.
Better care.

- Which devices and operating systems?
- What are the potential impacts on your organisation?
- Who is responsible for ensuring compliance with licensing requirements?
- How to ensure security management and application control software is installed.
- Managing staff changes- e.g what happens when staff leave?
- Security incident management plans – users must be able to report the loss of devices and you need a plan for if this happens.
- Will work-related data be segregated from the owner's private data?
- What are the training requirements for staff?

Digital Care Hub

https://www.digitalcarehub.co.uk/resource/smart-phone-policy-template-byod/

BYOD – what to do

DSPT
Better security.
Better care.

- Mobile Device Management (MDM) can help you remotely secure, manage and support personally owned devices.

BUT

- It is important to balance technical controls with usability

Digital Care Hub

BYOD – what to do

DSPT
Better security.
Better care.

- Staff may use a personal device differently to a corporate device
- Staff buy-in reduces workarounds and unsafe practice

Digital Care Hub

Things to consider if providing staff with phones

DSPT
Better security.
Better care.

- Does the software you want to use work on all operating systems?
- Will there be one user per device or multiple?
- Who is responsible for auditing devices?
- Who is responsible for managing users and updating devices?
- Do you allow staff to use the device for personal use?

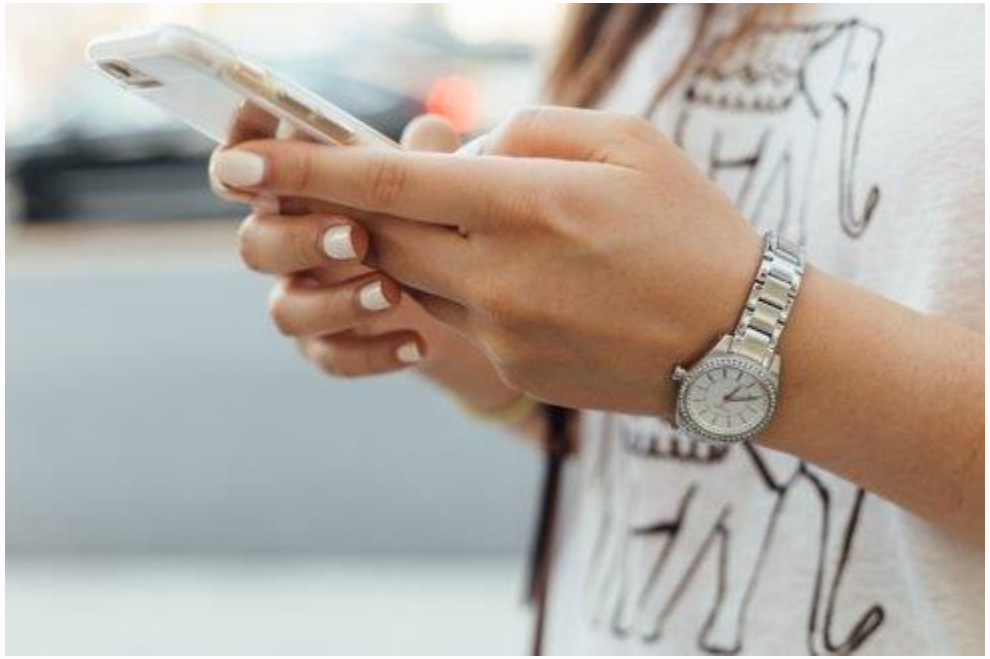
Digital Care Hub

Text messaging – is it safe?

DSPT
Better security.
Better care.

There are several vulnerabilities to consider when using SMS to communicate sensitive information with staff

- Who can see that message?
- What happens when someone leaves?
- SIM swaps
- Malware



Digital Care Hub

Text messaging – secure alternatives

DSPT
Better security.
Better care.

- **Encryption** – does the app have End to End Encryption (E2EE)
- **End-user verification** – can the app verify that the people using the app are indeed who they say they are?
- **Passcode protection** – can a secondary PIN be used to protect the app, and can it be time-out enabled?
- **Remote-wipe** – can the messages be removed if the device is lost, stolen or redeployed to another staff member?
- **Message retention** – does the app allow automatic deletion of messages after a set period of time?

Digital Care Hub

Strong passwords

DSPT
Better security.
Better care.

Digital Care Hub

- Passwords should be easy to remember and difficult to guess.
- Use strong, separate passwords for important accounts.
- National guidance recommends using three random words to create a strong password.
- For important accounts – use two factor authentication. This means adding a second layer security measure i.e. entering a code sent to your device, answering a security question.

Have a business continuity plan that includes data and cyber security

DSPT
Better security.
Better care.

A business continuity plan that includes data and cyber security will help you to manage risks such as:

- If you lost data records
- If you were hacked
- If phone operating systems were down
- If your supplier's system failed

Don't forget to test your plan!

Digital Care Hub has a template plan you can download and adapt for your service.

Digital Care Hub

Staff training

DSPT
Better security.
Better care.

Don’t underestimate human error.

Cyber awareness training will educate staff on important issues such as how to spot a cyber attack.

Better Security, Better Care are launching a **free** online training platform for frontline care staff in December.

Free cyber awareness training and e-materials available through the National Cyber Security Centre (NCSC).

Digital Care Hub

Managers' Discussion Tool & Quiz for Staff

DSPT
Better security.
Better care.

Data Protection Discussion Tool
Cyber Security Training Resources for Staff

Better Security, Better Care
Managers' discussion tool

Version 2 – July 2022

This discussion tool is designed to help you have discussions with your frontline staff to check their knowledge and provide evidence of their competence in data security and protection to meet requirement 3.2.1 of the Data Security and Protection Toolkit.

The tool is broken down into four colour coded sections covering the four learning outcomes for frontline social care staff:

1. Understand the importance of data security and protection in the care system and your personal responsibility to handle data safely
2. Be able to apply relevant data security and protection legislation and principles
3. Be aware of physical and digital threats to data security and know how to avoid them, including:
   i. being alert to social engineering
   ii. safe use of digital devices
   iii. safe keeping of physical records
4. Be able to identify data breaches and incidents and know what to do if one happens

Digital
Care Hub

Better Security, Better Care
Multiple choice quiz for frontline staff

Version 2 – July 2022

This quiz will provide evidence that you have completed data security and protection training that meets requirement 3.2.1 of the Data Security and Protection Toolkit. Circle or tick the correct answers.

Name: _____ Date: _____ Score: _____

1. Understand the importance of data security and protection in the care system and your personal responsibility to handle personal data safely

Question		Answer options
1a	True or False: We have a legal duty to respect the privacy of the people who use our care services?	True False
1b	True or False: Sharing information with the right people can be just as important as not disclosing to the wrong person?	True False
1c	Can someone you support ask to see and have a copy of the personal data that is held about them?	Yes No
1d	When should information be recorded? Choose the correct answer.	As soon as possible, whilst the event is still fresh in your mind Within a couple of weeks When there is time to do it

Manage your supply chain

DSPT
Better security.
Better care.

You're only as strong as the weakest link in your supply chain.

Check what security controls your suppliers have in place & consider asking them to seek out Cyber Essentials Plus certification.

Use Digital Care Hub's supplier list template to keep track of what suppliers process personal information.

Digital
Care Hub

Back ups

DSPT
Better security.
Better care.

If your device is infected by a virus or accessed by a criminal, your data may be damaged, stolen or held to ransom.

Back up your most important data to somewhere **separate from your computer.** This could be an external hard drive or storage system based in the Cloud.

Digital
Care Hub

Use the Data Security & Protection Toolkit

DSPT
Better security.
Better care.

It will help you reassure people who use your services and their families, and your staff that you keep data safe, and share it appropriate and securely

It will help protect your business from the risk of being fined for a data breach and from the disruption of a cyber attack

It gives guidance so that you can practice good data security and be sure that personal information is handled and processed correctly

Data and cyber security arrangements, DSPT and insurance claims

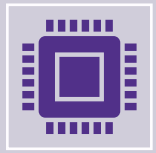
DSPT
Better security.
Better care.

£ According to the Cyber Claims report 2022, the average cost of a claim for a small business owner was £115,000

Insurance companies are demanding that before an insurance policy is issued or renewed, the enterprise must show they have the tools in place to protect against ransomware.

DSPT and insurance claims

DSPT
Better security.
Better care.



The DSPT is an excellent tool to show insurance companies that you are serious about data breach prevention (and cyber in general).

It can lower premiums and speed up pay-outs if the worse does happen as you have a to-hand report of “here’s how seriously we protect our systems and train our staff”.

You can allow the insurer a temporary “viewer” account or print-out and they have read-only access to your DSPT.

National Data Guardian Standards

DSPT
Better security.
Better care.

Personal confidential data	**Staff responsibilities**	**Training**	**Managing data access**	**Process reviews**
Responding to incidents	**Continuity planning**	**Unsupported systems**	**IT protection**	**Accountable suppliers**

- All DSPT sections are aligned with the National Data Guardian Standards
- Completing these sections demonstrates compliance with NDG and other data laws

Data Security & Protection Toolkit: Local Support Organisations to assist you

- There is free support offered to social care to assist you in building up operational resilience
- Free template policies and procedures to use in your organisation.
- 1:1, direct support to help you use the DSPT
- Bespoke workshops and webinars to assist you with delivery.
- Demonstration of the DSPT and what good looks like with regards to evidencing your DSPT self-assessment
- Free national helpline 0808 196 4848

www.digitalcarehub.co.uk/bettersecuritybettercare

Resources | Digital Care Hub

Any questions?

DSPT
Better security.
Better care.

Digital Care Hub

Poll

DSPT
Better security.
Better care.

Care providers:

- How likely are you to use the DSPT after watching this webinar?
- Would you recommend this webinar to a friend?
- How did you hear about this webinar?

Digital Care Hub

THANK YOU

DSPT
Better security.
Better care.

Digital
Care Hub