DSPT
Better Security.
Better Care.

Digital
Care Hub

hcpa

Future Proofing Your Business in Cybersecurity

Welcome

Your session will start soon

Today's Presentations

Deb Parker – HCPA
Data Security and Protection

Paul Davis – Virtual IT
DPST to CSAF: Are You Prepared for the Security Shake-up?

Ed Farthing – Howden
Are You Prepared for a Cyber Incident?
Exploring Real-Life Incidents, Responses, and Means of Protection.

DSPT
Better Security.
Better Care.

Digital
Care Hub

hcpa

DATA SECURITY & PROTECTION

Deb Parker

Information Governance Training & Support Lead

dspt.dparker@hcpa.co.uk

THE NATIONAL PROGRAMME - BSBC

BETTER SECURITY, BETTER CARE

A fully funded programme, through NHS England & Department of Health & Social Care, to help Adult Social Care Providers to store and share information safely, securely and meet GDPR principles.

It covers paper and digital records, and supports Providers with the completion of their annual Data Security & Protection Toolkit (DSPT)

DSPT
Better Security.
Better Care.

Digital
Care Hub

hcpa

DATA SECURITY & PROTECTION TOOLKIT

An annual, on-line self assessment, 42 questions covering Staffing & Roles, Data Security, IT Systems & Devices and Policies & Procedures.

CQC will ask for evidence of a current DSPT when inspecting Governance, within Well-Led, as part of their Assessment Framework.

Both Residential & Homecare should complete a DSPT annually.

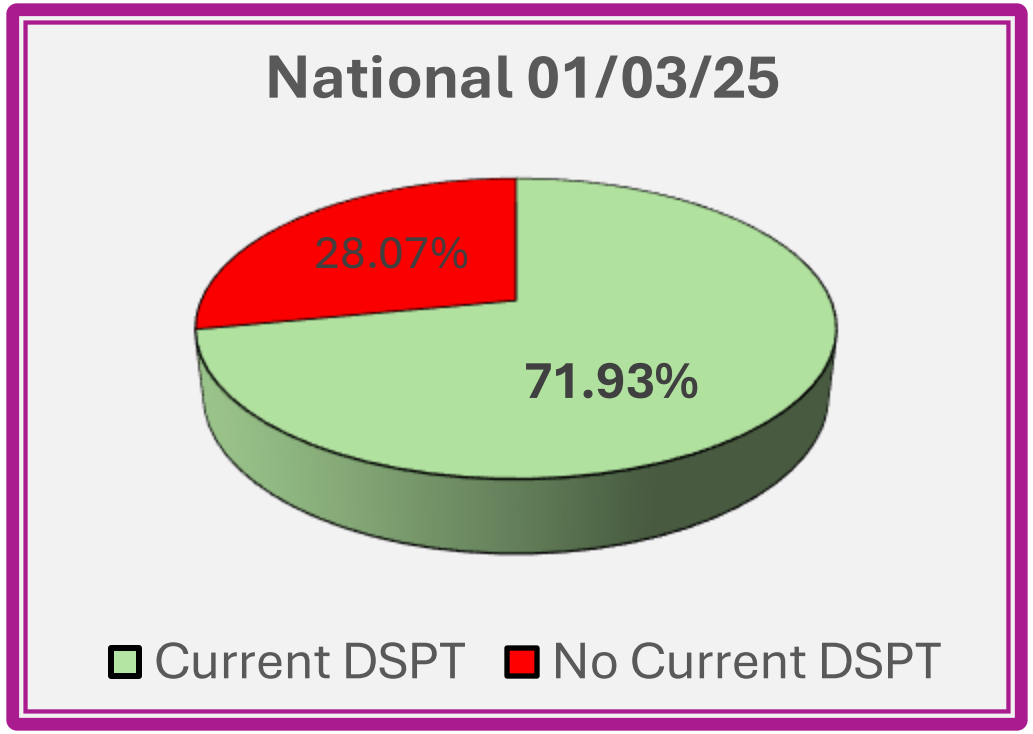
DSPT
Better Security.
Better Care.

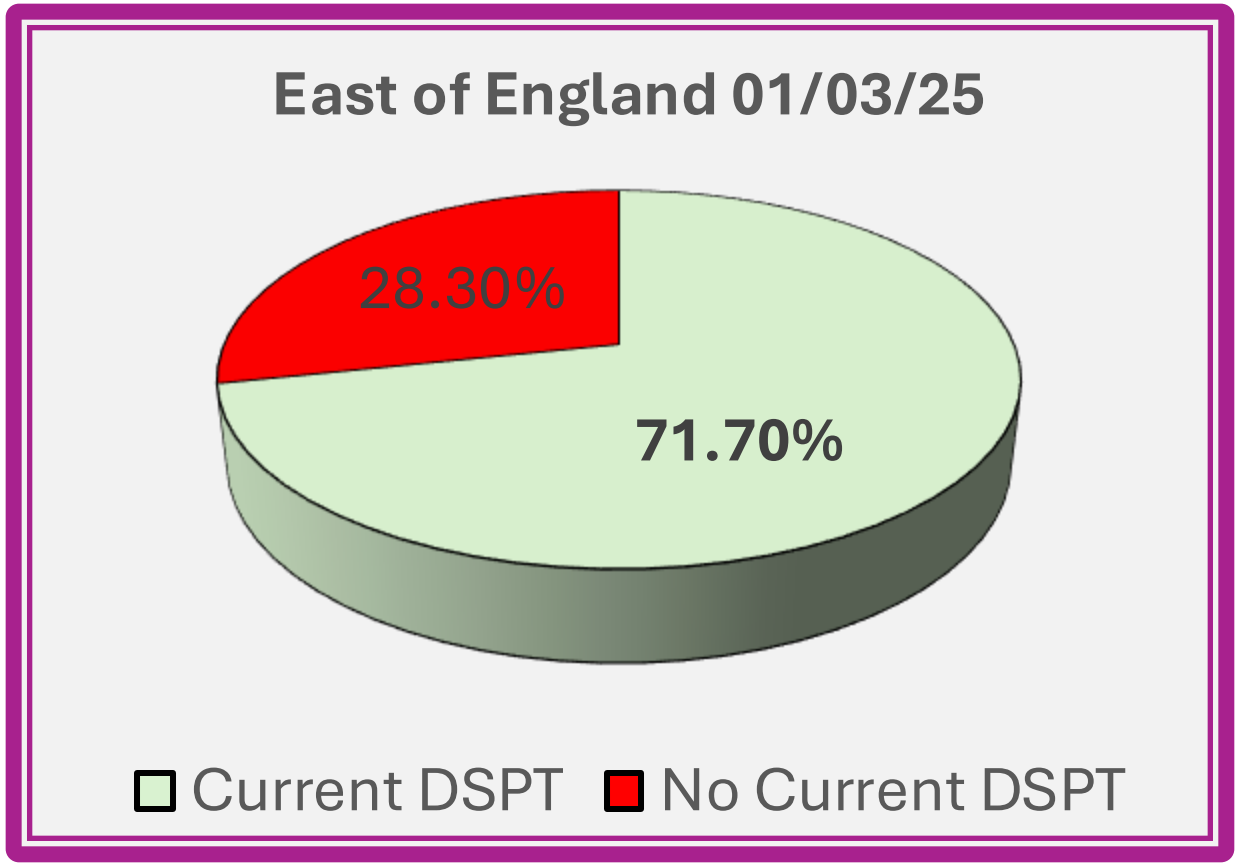
Digital
Care Hub

hcpa

BSBC PROGRAMME – Where are we now?

DSPT compliance 2020 - <11%





DSPT
Better Security.
Better Care.

Digital
Care Hub

hcpa

WORKING WITH DATA

Your Data

- Know what you have.
- Know where it's held.
- Know who you are sharing with (outside the organisation).
- Know why you are sharing.
- Ensure ALL of these are mapped.

How to Document Your Data Processing - Digital Care Hub

WORKING WITH DATA – Staff Contracts

Data Security & Protection clause in contracts must include responsibility for the Confidentiality, Integrity and Availability of all data in the workplace.

[Staff Data Security Contract Clause - Template - Digital Care Hub]

> It is the responsibility of all staff to ensure data security. You will be responsible for the confidentiality, integrity and availability of all data which you have access to in the course of your work.

DSPT Better Security. Better Care. | Digital Care Hub

DATA BREACHES – Think CIA

- **Confidentiality**

Personal Information must not be shared (paper, digital or verbal) unless there is a **Lawful Basis** for doing so.

Breach example - Talking about a resident's health diagnosis in a communal area or leaving a care plan on a table in a communal lounge.

- **Integrity**

Personal Information must be fit for purpose, accurate, complete and up to date, so that errors are minimised.

Breach example - Changes or incidents not logged correctly. Updates to medication or care needs not recorded.

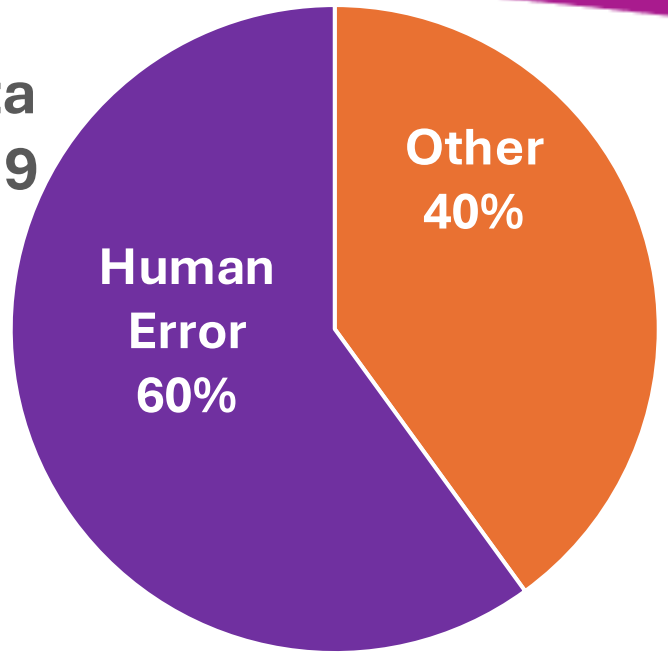
- **Availability**

Personal Information must be available. Whilst personal information must be held securely, it must also be available when required by authorised persons.

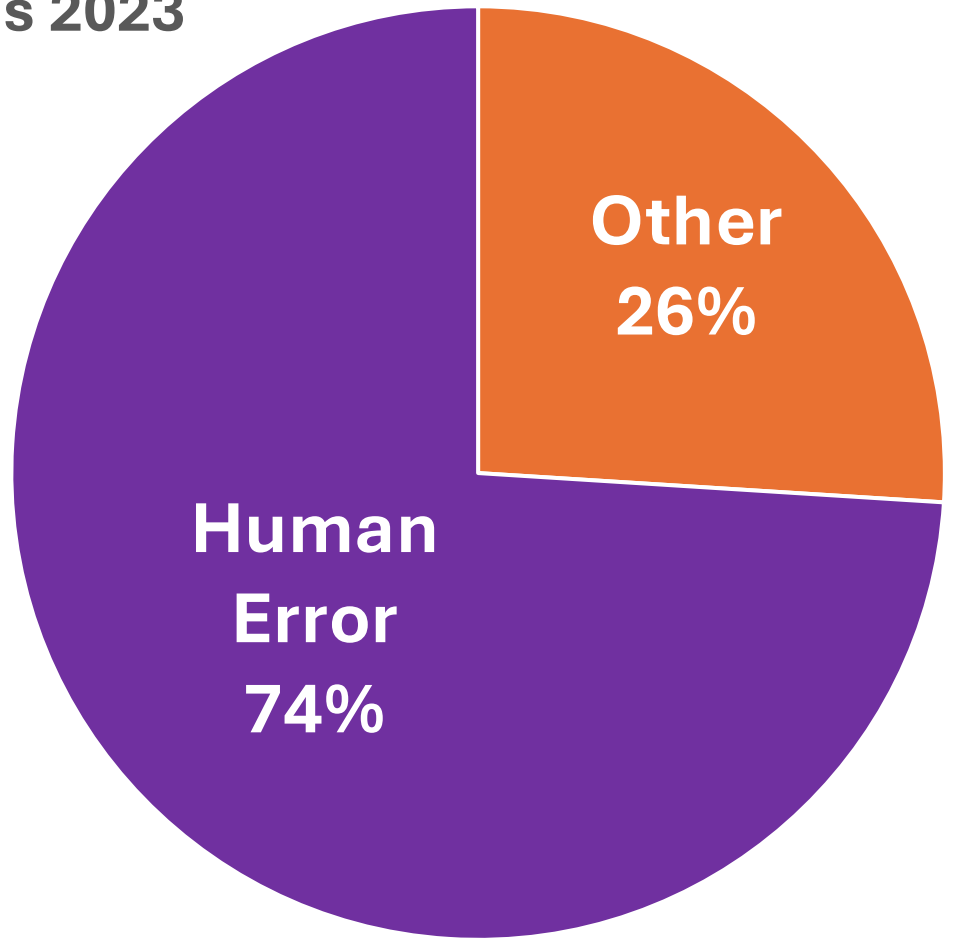
Breach example - Lost key to care plan cabinet or Phishing email locks systems

DATA BREACHES

Reported Data Breaches 2019



Reported Data Breaches 2023



Training is key to reducing Data Breaches and Cyber Attacks

DSPT
Better Security.
Better Care.

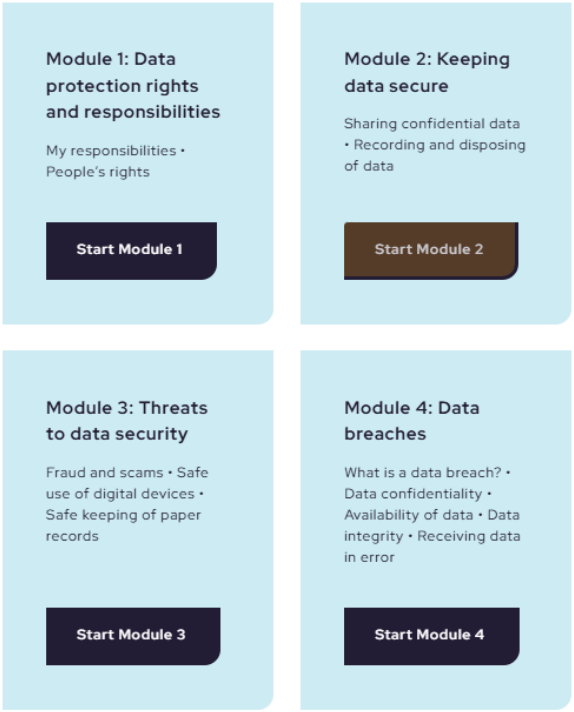
Digital
Care Hub

hcpa

WORKING WITH DATA – Well Trained Staff

Everyone in your organisation must complete their Data Security & Protection eLearning annually. This is **specifically designed Care Sector training.**

Data Security And Protection In Social Care Course



DSPT
Better Security.
Better Care.

Digital
Care Hub

SYSTEMS, DEVICES & TECHNOLOGY

- Must still be supported by the supplier.
- Must have the current software, operating platforms etc.
- Map your devices and regularly monitor that they are up to date (both business & own use if applicable).
- Ensure you have a robust and tested Business Continuity Plan.
- Map everything you are using.

WORKING WITH DATA - Supply Chain

Map your supply chain.

Could you continue to provide care if a supplier is affected by a Cyber Attack?

- Do they supply essential services?
- Do they own/hold your data?
- Would you still have access to what you need?
- What does **their** Business Continuity Plan look like?
- What is the impact to you and your services?

SO MUCH TECH OUT THERE ALREADY

What are you already using?

Falls prevention & detection tools

Digital Social Care Records

Wearable health monitoring & diagnostic devices

Smarthome Apps & devices

Medication Dispensing

Voice Activated controls

Devices & apps for connecting with people

Video calls with healthcare professionals

Text to Speech apps

Pain assessment

Shared visibility of medical information

DSPT Better Security. Better Care.

Digital Care Hub

hcpa

WHAT DOES THE FUTURE LOOK LIKE?

- The Sector must understand how to **manage data securely**, completing your DSPT will demonstrate that you do.
- **CQC** will ask whether you have a current **DSPT.**
- Many **Local Authorities** are writing **DSPT** into their contracts.
- Many **funding opportunities** are dependant on a current **DSPT.**
- Correct and appropriate care provision is reliant on having access to Accurate, Complete, Up to Date & Fit for Purpose records and preventing unauthorised access.
- **Technology** increases to be an integral part of our daily lives, we need to adapt and understand how technology and data fit together to **provide Person Centred Care**.

WHERE TO GET HELP

Central Bedfordshire and Bedford
Central Bedfordshire Council
Websites https://dspt.bedscaregroupltd.co.uk/
Email SCHHServiceDevelopment@centralbedfordshire.gov.uk

Norfolk
Norfolk & Suffolk Care Support Ltd
Website https://norfolkandsuffolkcaresupport.co.uk/bsbc
Email bsbc@norfolkandsuffolkcaresupport.co.uk
Tel 01603 629211

Cambridgeshire and Peterborough
The Care Alliance
Visit: www.thecarealliancecnp.co.uk
Email: admin@thecarealliancecnp.co.uk
Tel: 07831597711

Suffolk
SCA Ltd Suffolk Care Associaion
Website scaservices.org.uk
Email admin@scaservices.org.uk
Tel 01449 490750

Hertfordshire, Essex, Thurrock and Southend
Hertfordshire Care Providers Association
Website https://www.hcpa.info/data-protection/
Email DataProtection@HCPA.co.uk
Tel 01707 708 018

DSPT Better Security. Better Care. | Digital Care Hub | hcpa

DSPT
Better Security.
Better Care.

Digital
Care Hub

hcpa

THANK YOU

QUESTIONS?

Deb Parker

Information Governance Training & Support Lead

dspt.dparker@hcpa.co.uk

THE HERTFORDSHIRE CARE PROVIDERS ASSOCIATION

DPST to CAF: Are You Prepared for the Security Shake-up?

VIRTUALIT

PRESENTED BY
PAUL DAVIS

INTRODUCTION

PAUL DAVIS

Virtual IT

VIRTUALIT

VIRTUALIT

CyberSecurity in the Care Sector:

From DPST to CAF

DPST to CAF: Are You Prepared for the Security Shake-up?

What is CAF?

DATA PROTECTION AND SECURITY TOOLKIT (DPST):	CYBER ASSESSMENT FRAMEWORK (CAF):
Scope and Application: Focused on healthcare organisations.	**Scope and Application:** Broad application across multiple sectors.
Framework Structure: Comprehensive for data security and regulatory compliance.	**Framework Structure:** Structured approach to evaluating and improving security protocols.
Risk Management: Evaluates existing security measures.	**Risk Management:** Provides a more structured and comprehensive approach to managing risks.
Regulatory Compliance: Ensures compliance with healthcare regulations.	**Regulatory Compliance:** Aligns with the latest cybersecurity standards and regulations.

Why is Compliance Important?

Who’s my Neighbour?

The Medusa Ransomware Attack on HCRG Care Group

- Cyber criminal gang infiltrates healthcare provider
- Stole 2.275 TB of data
- Demanded a ransom of $2 million (£1.6 million)
- Threatening to leak the information online
- Charge £8,000 per 24 hrs to delay leaks

February 2025

VIRTUALIT

The Potential effect of a Cyber Attack?

- Business folds!
- Service Disruptions
- Patient Data Compromised
- Privacy concerns and fines
- Damaged Reputation
- Potentially dire consequences to patient's health
- Loss of contracts
- Lost revenue
- Supply chain disruptions
- Invoice fraud

VIRTUALIT

Just How at Risk is the Care Sector?

- 2.39 million instances of cybercrime in 2023.
- 52% of these targeted health and social care businesses.
- Average cost of a data breach in the health and social care sector is up to £3 million per incident.

VIRTUALIT

Is My Organisation at Risk?

If so, from what?

- Ransomware Attacks
- Phishing & Social Engineering
- Insider Threats & Human Error
- Unsecured IoT Devices
- Weak Data Protection & Compliance Issues

VIRTUALIT

Practical Steps We Can All Take

Regular Cybersecurity Training

Upgrade Legacy Systems

Strict Access Controls

Routine Backups

Strong Endpoint Protection

Password Hygiene

VIRTUALIT

Embrace Compliance...

Get the ***fundamentals*** in place and partner with the right **technology provider**

Focus on delivering ***exceptional*** care while **compliance** is taken care of in the background.

...and Win Coveted Tenders

VIRTUALIT

Smooth Sailing in Healthcare Compliance

Ensure compliance is met **by partnering with the right provider**

Continue to provide excellent patient care

VIRTUALIT

THANK YOU

Please get in touch to receive your free **Cyber Health Assessment**

Data Security and Protection Toolkit (DSPT) to the Cyber Assessment Framework (CAF)

PRESENTED BY PAUL DAVIS

VIRTUALIT

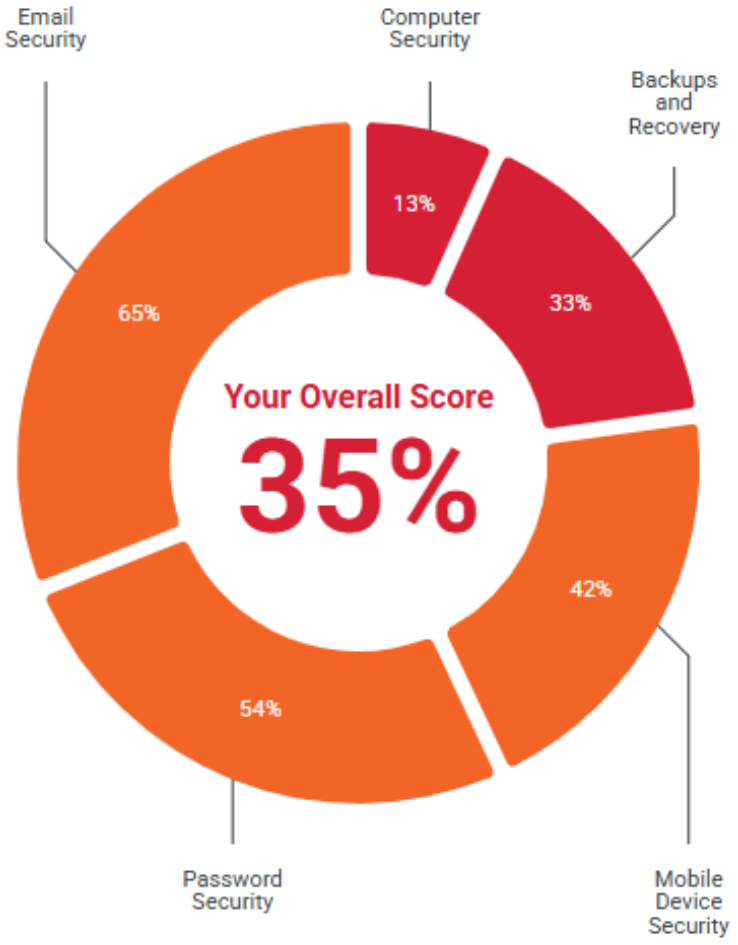
Please get in touch to receive your free **Cyber Health Assessment**

SCAN ME

and receive **20% off any security products** we help you with.

VIRTUALIT

Discover your Cyber Health Scorecard



EMAIL CYBERSECURITY@VIRTUALIT.CLOUD

WEB

WWW.VIRTUALIT.CLOUD

INSTAGRAM

@virtual_it.cloud

LinkedIn

Virtual IT Ltd

Please get in touch: cybersecurity@virtualit.cloud

VIRTUALIT

THANK YOU

DPST to CAF: Are You Prepared for the Security Shake-up?

PRESENTED BY PAUL DAVIS

VIRTUALIT

Howden Health & Care

Are You Prepared For A Cyber Incident?

Exploring real life incidents and responses

Ed Farthing
Senior Account Executive, Howden

HOWDEN

Hospitals cancel operations as NHS declares 'critical incident' after cyber attack

Three hospitals have had to cancel urgent operations in London after a cyber attack on services run by NHS IT firm Synnovis.

By ISABELLA MARSANS, FIONA CALLINGHAM, Health Reporter specialising in medical studies, symptoms of diseases and conditions, real life stories and the latest public health issues.
13:01, Tue, Jun 4, 2024 | UPDATED: 13:26, Tue, Jun 4, 2024

Cambridge among universities hit by 'malicious' cyber attack

The attack meant internet access was intermittent and some services for staff and students were 'degraded'

NEWS By Cait Findlay Senior Reporter
11:20, 20 FEB 2024 | UPDATED 12:17, 20 FEB 2024

Bookmark

News | Cybercrime

UK Defence Ministry targeted in cyberattack: Minister

Third-party payroll system with names and bank details of armed forces staff hacked, reports say.

Leicester care home warning as cyber incident hits services

14 March

Ready meal distributor Apetito restores 'limited' deliveries in UK following cyber-attack

Adam Bannister 28 June 2022 at 14:30 UTC
Updated: 29 June 2022 at 07:34 UTC

Man charged over Network Rail terror message hack

Santander cyber hack puts 30m bank accounts at risk of dark web sale - should UK customers worry?

Redcar cyber-attack 'cost council £10.4m'

5 August 2020

Spy chiefs fear Britain is 'shockingly vulnerable' to cyber attacks

NHS and power grid can be hacked by foreign states through 'back door' private companies, says Technology Secretary

An incident IS going to occur

2.39 million instances of cyber crime and 49,000 instances of fraud relating to cyber crime in 2023.

52% of health and social care businesses were hit by a cyber attack.

The average cost of cyber crime for businesses is estimated at approximately £15,300 per victim.

A perfect storm of economic and sector specific challenges has led businesses to taking their eyes off the ball – the 2023 UK Cyber Security Breaches Survey stated that the number of micro businesses describing cyber security as a high priority fell from 80% in 2022 to 68% this year

Top 9 Common Cyber Risks

Phishing Attacks
Ransomware
Insider Threats
Malware and Viruses
Weak Passwords and Authentication
Social Engineering
Outdated Software and Systems
Data Breaches and Information Theft
Misconfigured Cloud Resources

According to the Beazley Cyber Buyer's Guide 2025

Case Study 1 – Social Engineering in a Care Setting

Route In: A Brute Force Attack on the CEO's email password

Causation: Weak Password or Use of Commonly Used Password & Human Error

Worsening Factors: No Multi-Factor Authentication, Lack of Due Process Being Followed

Route of Attack:

Brute Force Attack into CEO's Email Account – Access Gained to Calendar and Inbox – Calculated Schedule and How Transfers in the Business Take Place – Established Best Relationships with Finance Team Members – Waited Until CEO on Holiday – Email Spoofing Episode with Finance Team Member to Gain Trust (Not Using CEO's Account so Reply Wasn't Flagged) – Requested Settlement of an Invoice for £47,584 – Personal Touch Applied Throughout inc Nickname, Reference to Holiday, Personal Life **–** FUNDS PAID – Repeated the Next Day for £39,731 - Incident Flagged 1 Week Later When CEO Returned and Transfers Mentioned Verbally

Response:

Incident Reported to Police and Banks 1 week after funds transferred – Recovered just £600 via Banks

Incident Then Reported to CFC Cyber Team – Incident Response Team Activated – On Site/On Phone with Client within hours of notification and waiting period – Managed Incident Response including Reset of Passwords to Correct Standard - Searched Network to Identify Other 'Open' Entry Points – Liaised with Client to Manage Reputational Element – Recovered Funds for Client Under Policy Features

Impact:

With Cyber Insurance:
Funds recovered, full support recovering from the incident, vulnerabilities identified, discussed with management and rectifications made

Without Cyber Insurance:
Prospective Loss of £86,715 if Cyber Insurance wasn't purchased, no support in respect of incident recovery, no automatic vulnerability searches

Case Study 2 – Social Engineering in a Care Setting

Route In: Malware via Portal and Email Spoofing

Causation: Use of fraudulent portal allowing Malware infection

Worsening Factors: Lack of Due Process Being Followed in Respect of Checking Portal Links

Route of Attack:

Brute Force Attack to Gain Access to MD's Email Account - Spoof link sent via MD's Email Address to Finance Manager to set up a portal to make payments for third-party services – Finance Manager Fills in Credentials and Creates Account on Portal – Hacker Sends Out Email Asking for Donations to the Home as suffering with Increased Bills – Call from the 'Bank' – Finance Manager gives the Bank ALL of the details including Credentials, Secret Pin etc – Whole Bank Account Cleared for the Home

Response:

Police notified, attempt at funds recovery, mitigation of loss via Director's Loan to allow the business to continue running

Impact:

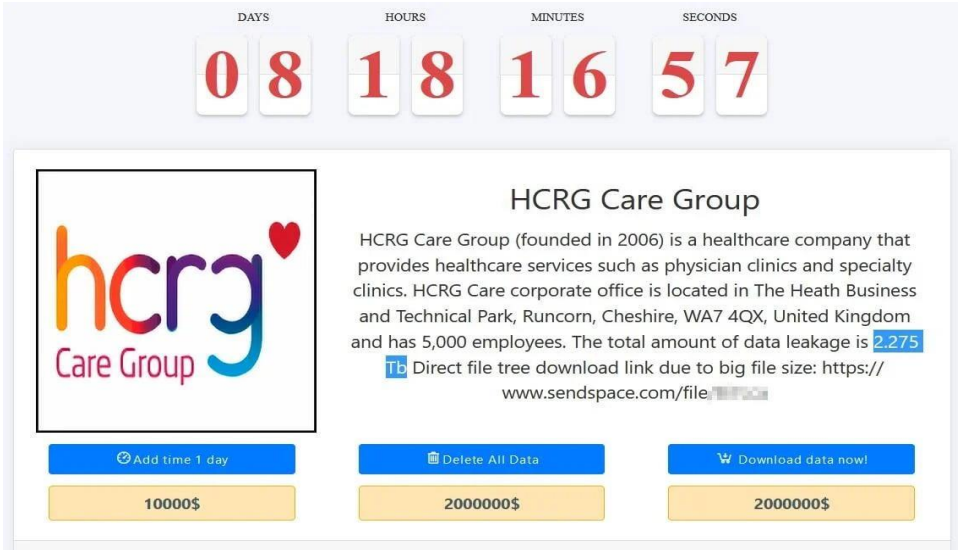
With Cyber Insurance:
Funds recovered, full support recovering from the incident, vulnerabilities identified, discussed with management and rectifications made

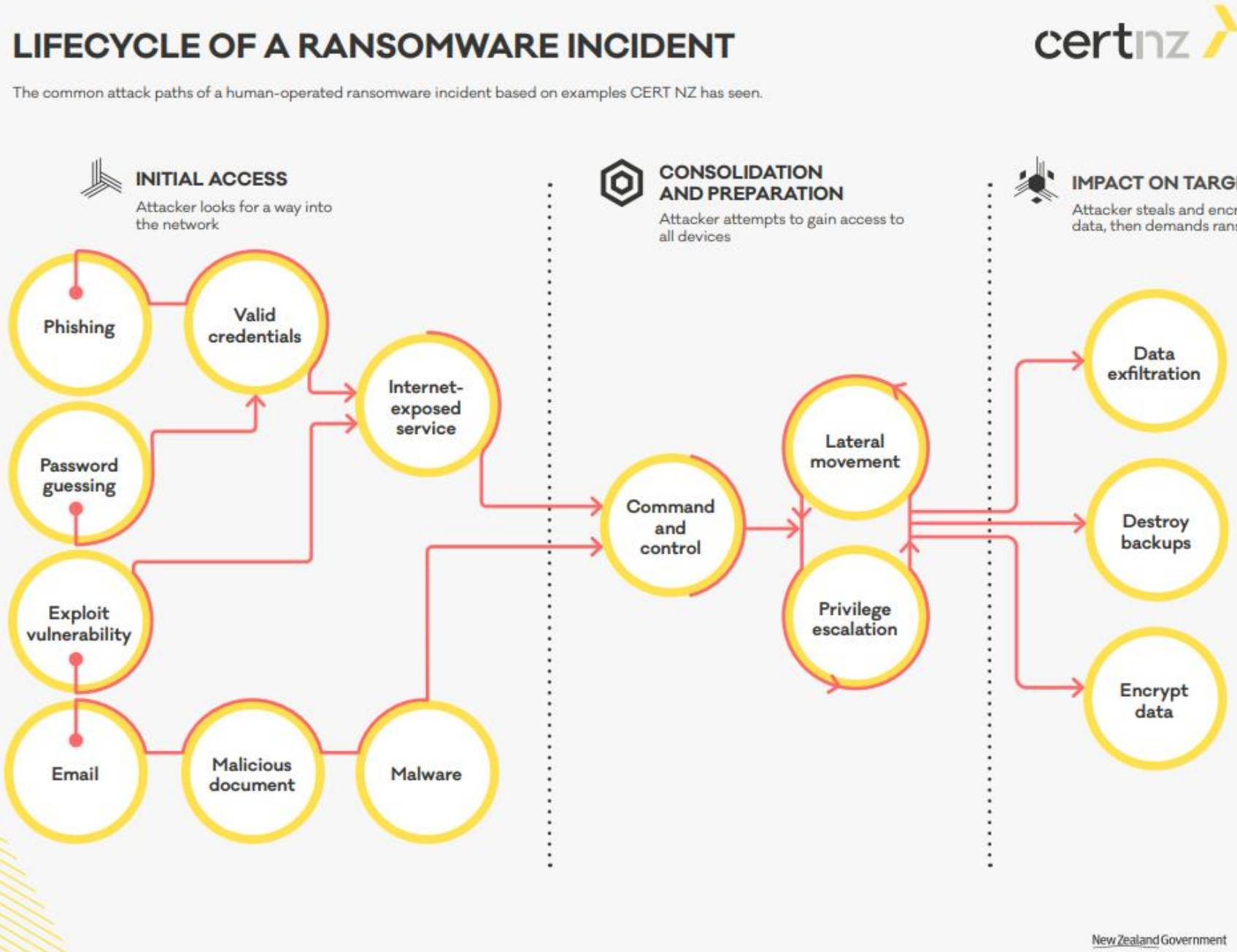
Without Cyber Insurance:
Loss of over £50,000 no support in respect of incident recovery, no automatic vulnerability searches

Ransomware


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
Send $300 worth of bitcoin to this address:
bitcoin ACCEPTED HERE
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personaly verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.
Click «Next» to select the method of payment.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
10/12/2013
3:15 AM
Time left
68 : 28 : 10
Next >>


DAYS
HOURS
MINUTES
SECONDS
0 8
1 8
1 6
5 7
hcrg Care Group
HCRG Care Group
HCRG Care Group (founded in 2006) is a healthcare company that provides healthcare services such as physician clinics and specialty clinics. HCRG Care corporate office is located in The Heath Business and Technical Park, Runcorn, Cheshire, WA7 4QX, United Kingdom and has 5,000 employees. The total amount of data leakage is 2.275 Tb Direct file tree download link due to big file size: https://www.sendspace.com/file
Add time 1 day
Delete All Data
Download data now!
10000$
2000000$
2000000$



Ransomware Attack:

The use of a type of malicious software designed to block access to systems until a sum of money (a ransom) is paid.

The totals required to gain access to the decryption key vary greatly with one of the highest payouts being CNA, ironically an insurance company, who paid $40million to regain control of their system after two weeks.

According to security shop Cybereason, last year 78 percent of organizations that paid a ransom were attacked again, with 63 percent facing demands for an even larger payout the second time around

How can you protect from an attack?

- Implement Cyber Essentials compliance, adherence to DSPT or equivalent where possible
- Ensure Third Party software providers are also compliant with this standards, adhere to the DSPT toolkit
- Introduce a formal cyber incident response plan
- Implement robust frontline firewalls for SME and medium sized businesses or EDR (Endpoint Detection and Response) tools
- Use multi-factor authentication where appropriate and available
- Back up your data at regular intervals and be cautious about cloud providers for sensitive data – what protections and guarantees can they offer?
- Train your staff regularly, not just via an online module at induction
- Ensure there is a connect between you and your IT Team whether this is internal or an external partner
  - Have you run a dummy event within your business?
  - What would you do first if ransomware popped up on your screen demanding cryptocurrency to unlock your files?
  - How would you manage the PR side of informing your service users their data was compromised?
  - How would you recover the data post event?
  - How would you trade without this data being available?
  - What is the direct impact on your service users?
- Purchase Cyber Insurance – some products will cover most of the above inclusive of the premium you pay

What's covered under a Cyber Insurance Policy?

- Incident response costs
- Legal and regulatory costs
- IT security and forensic costs
- Public communication costs
- Privacy breach management costs
- Extortion and cyber-crime
- System damage and rectification costs
- Loss of profits
- Consequential reputational harm
- Network security liability
- Privacy liability
- PCI fines
- Some Penalties
- Regulatory fines – via separate cover
- Defamation and breach of IP

beazley cfc  Coalition® cowbell®

Covers differ per policy and may be subject to additional premium depending on circumstances and availability

Services included under a Cyber Insurance Policy?

- Free Antivirus Licenses
- Free Access to Risk-Engineering Teams
- Free 1 hour session with cyber-resilience experts
- Free licenses for CPD accredited training courses for ALL staff
- Access to breach response app
- Access to training catalogue including downloadable best practice guides
- Free Port Scans pre-inception
- 5% premium reduction next year for completion of accredited training courses

beazley cfc  Coalition® cowbell®

Covers differ per policy and not all carriers offer all of the above options and additional services