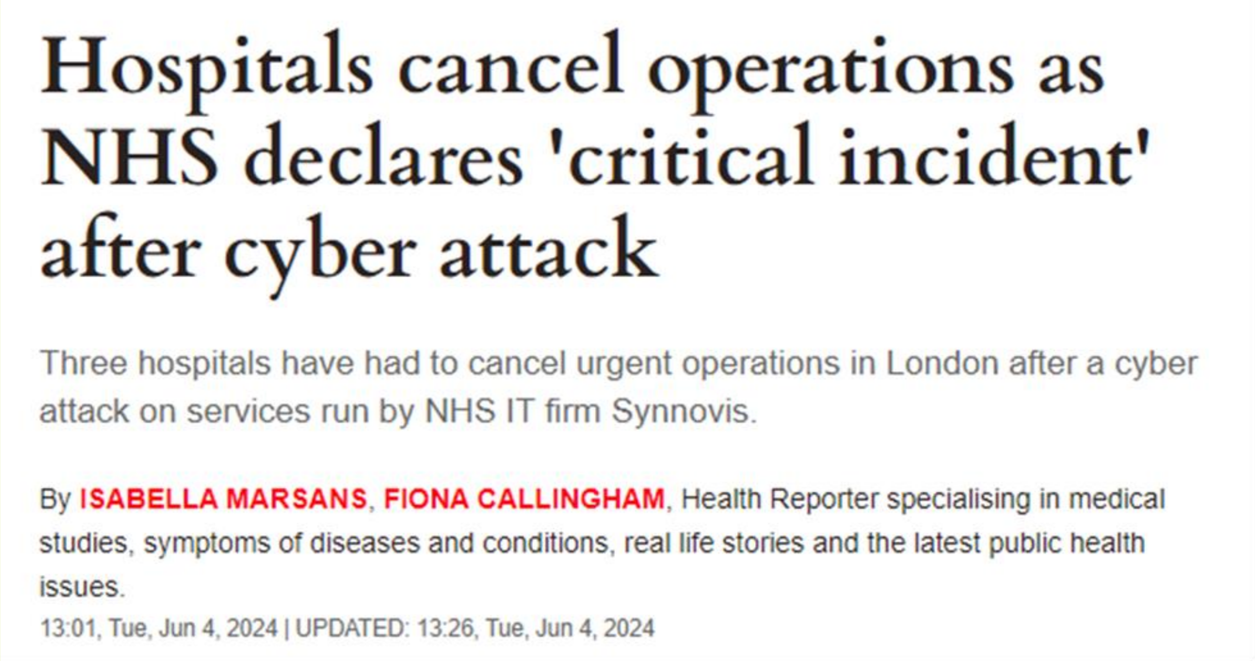
Howden Health & Care

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

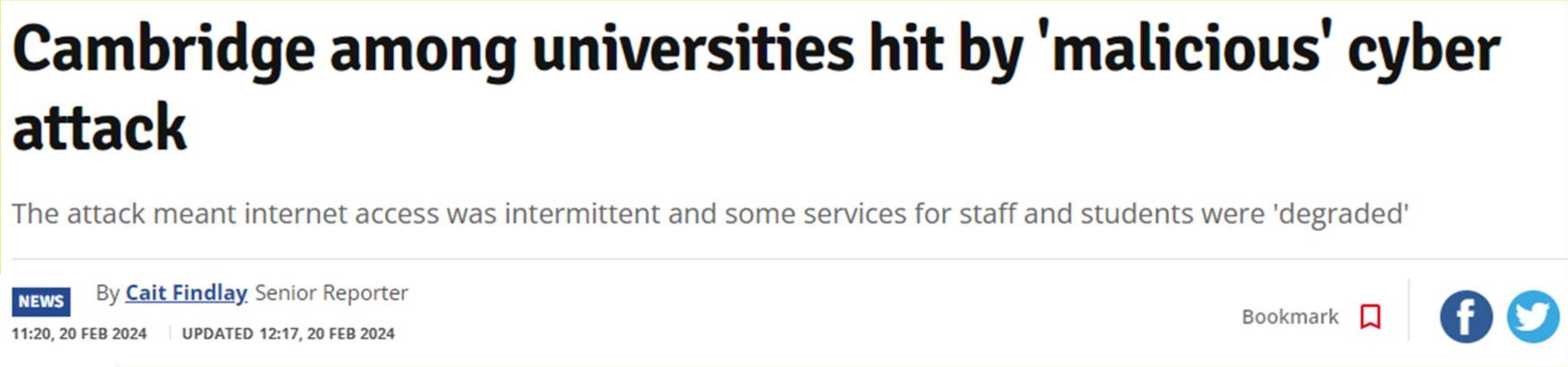
Three hospitals have had to cancel urgent operations in London after a cyber attack on services run by NHS IT firm Synnovis.

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

NEWS 3 JUN 2024

UK School Forced to Close Following Cyber-Attack

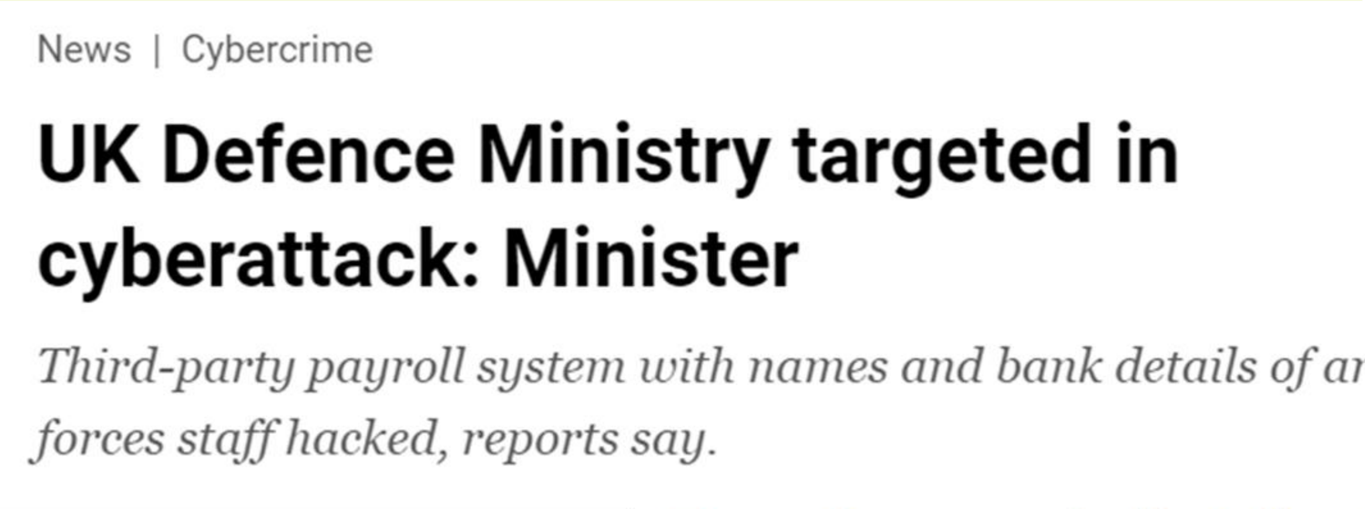


Cambridge among universities hit by 'malicious' cyber attack

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

NEWS By Cait Findlay Senior Reporter

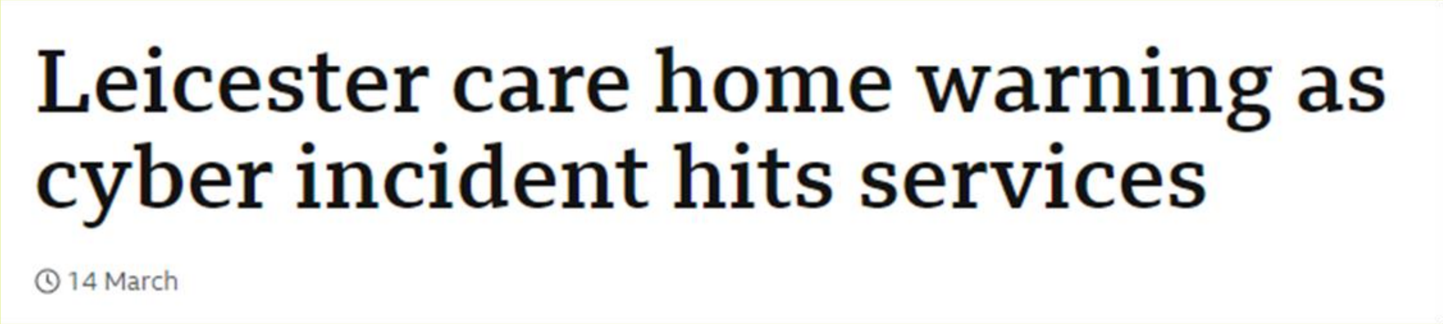
11:20, 20 FEB 2024 | UPDATED 12:17, 20 FEB 2024



News | Cybercrime

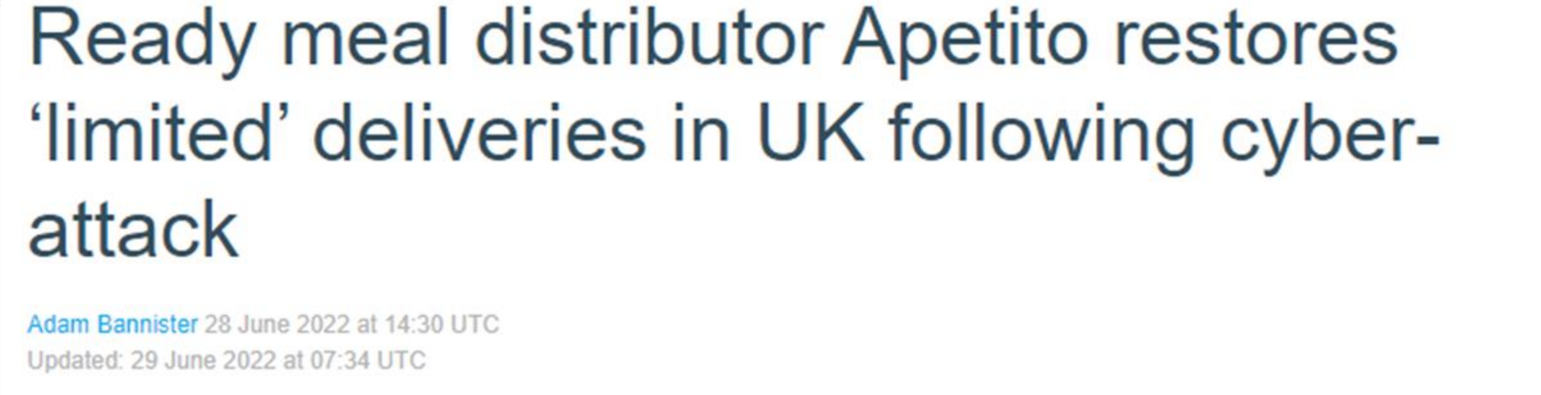
UK Defence Ministry targeted in cyberattack: Minister

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



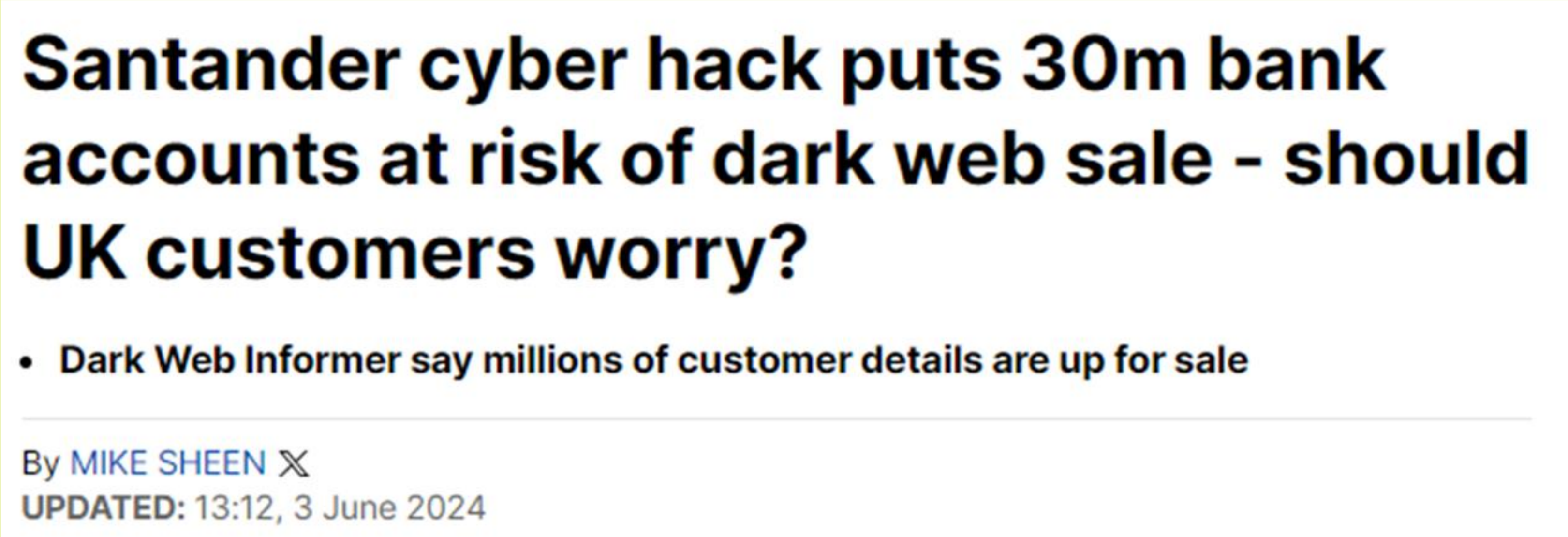
Leicester care home warning as cyber incident hits services

14 March



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

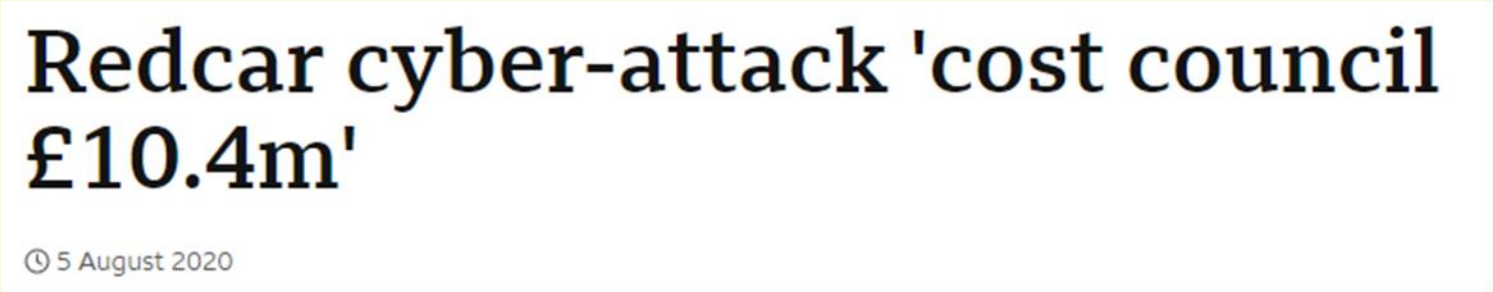
Adam Bannister 28 June 2022 at 14:30 UTC
Updated: 29 June 2022 at 07:34 UTC



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

- Dark Web Informer say millions of customer details are up for sale

By MIKE SHEEN
UPDATED: 13:12, 3 June 2024



Redcar cyber-attack 'cost council £10.4m'

5 August 2020

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:

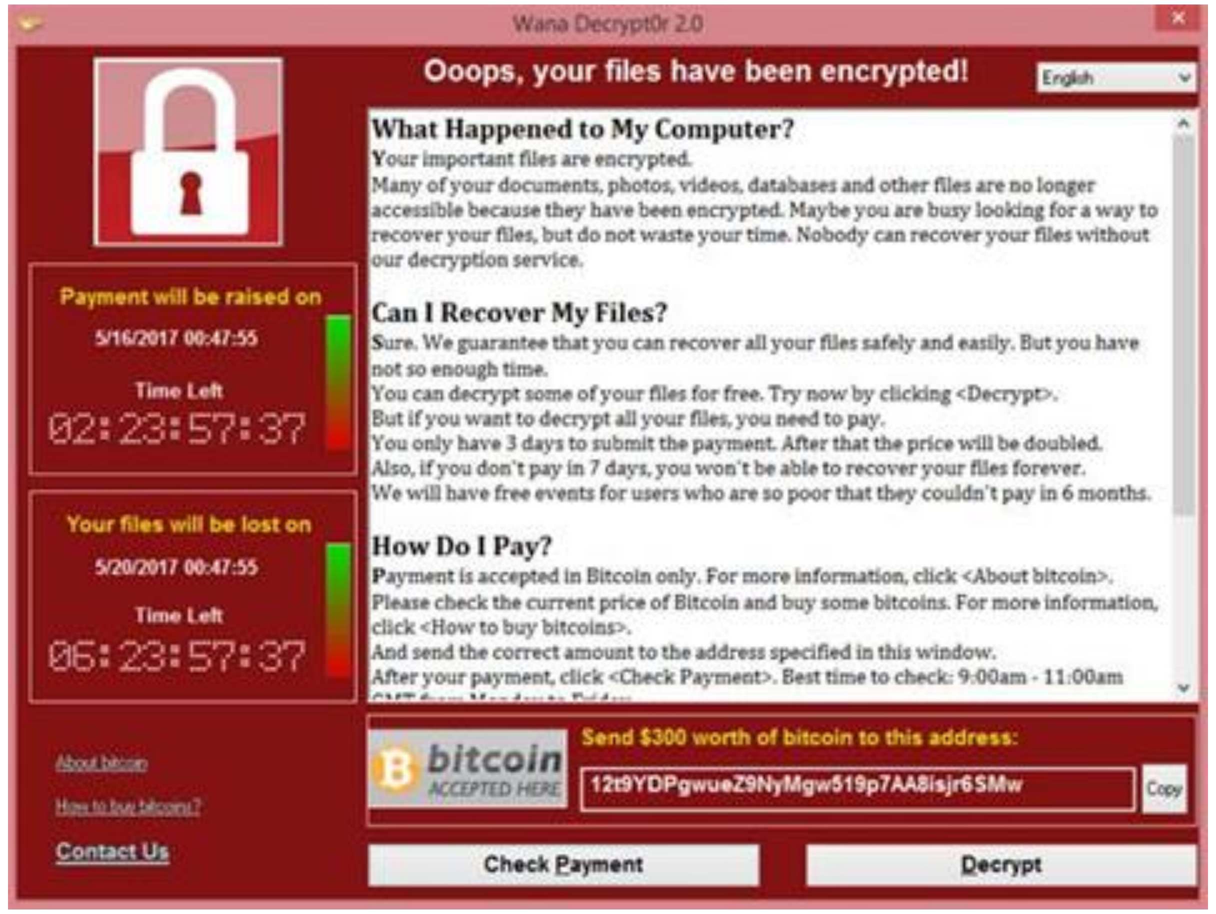
Police notified, attempt at funds recovery, mitigation of loss via Director’s Loan to allow the business to continue running

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



Ooops, your files have been encrypted!

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>.

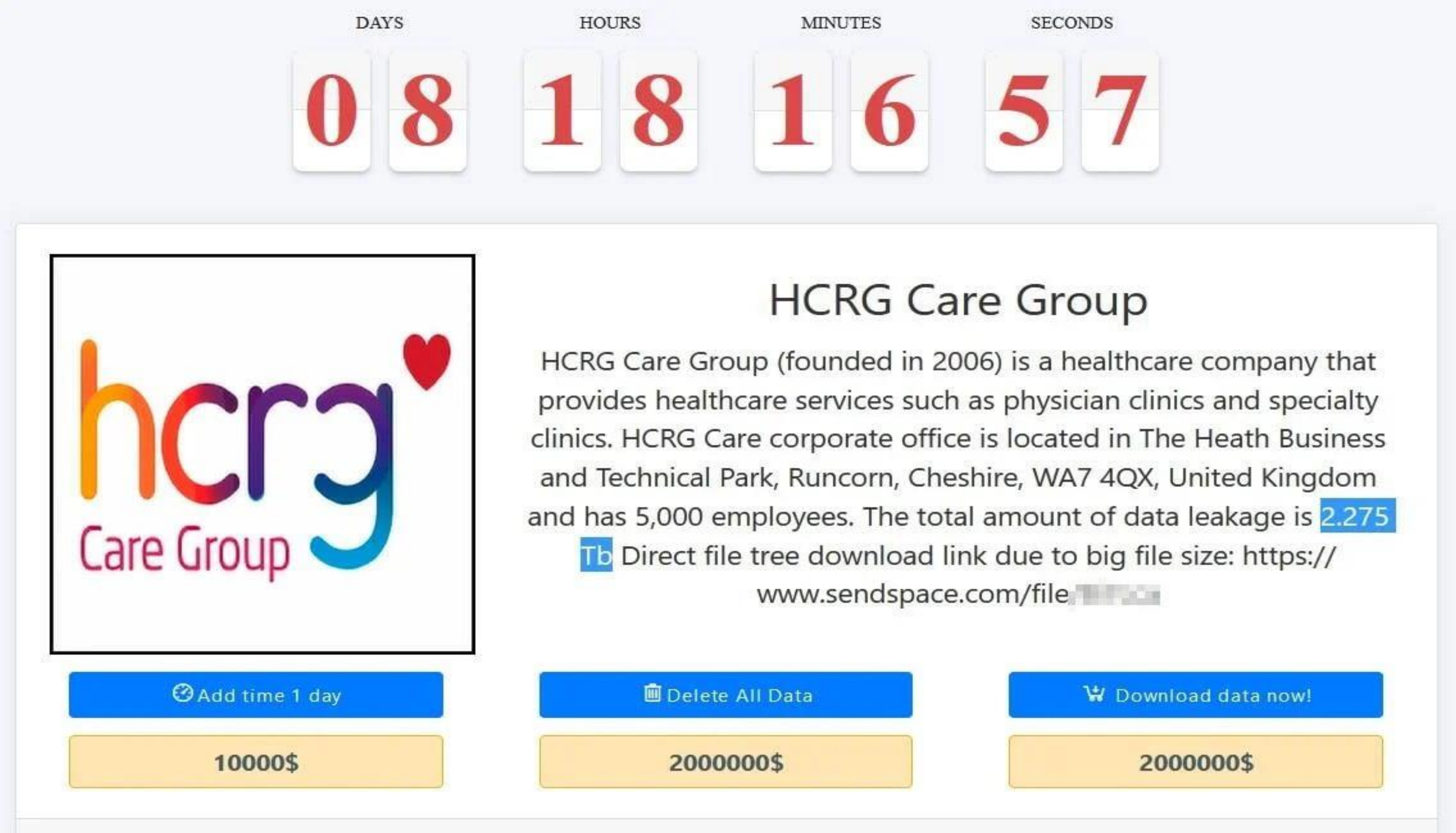
And send the correct amount to the address specified in this window.

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

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw



DAYS	HOURS	MINUTES	SECONDS
08	18	16	57

HCRG Care Group

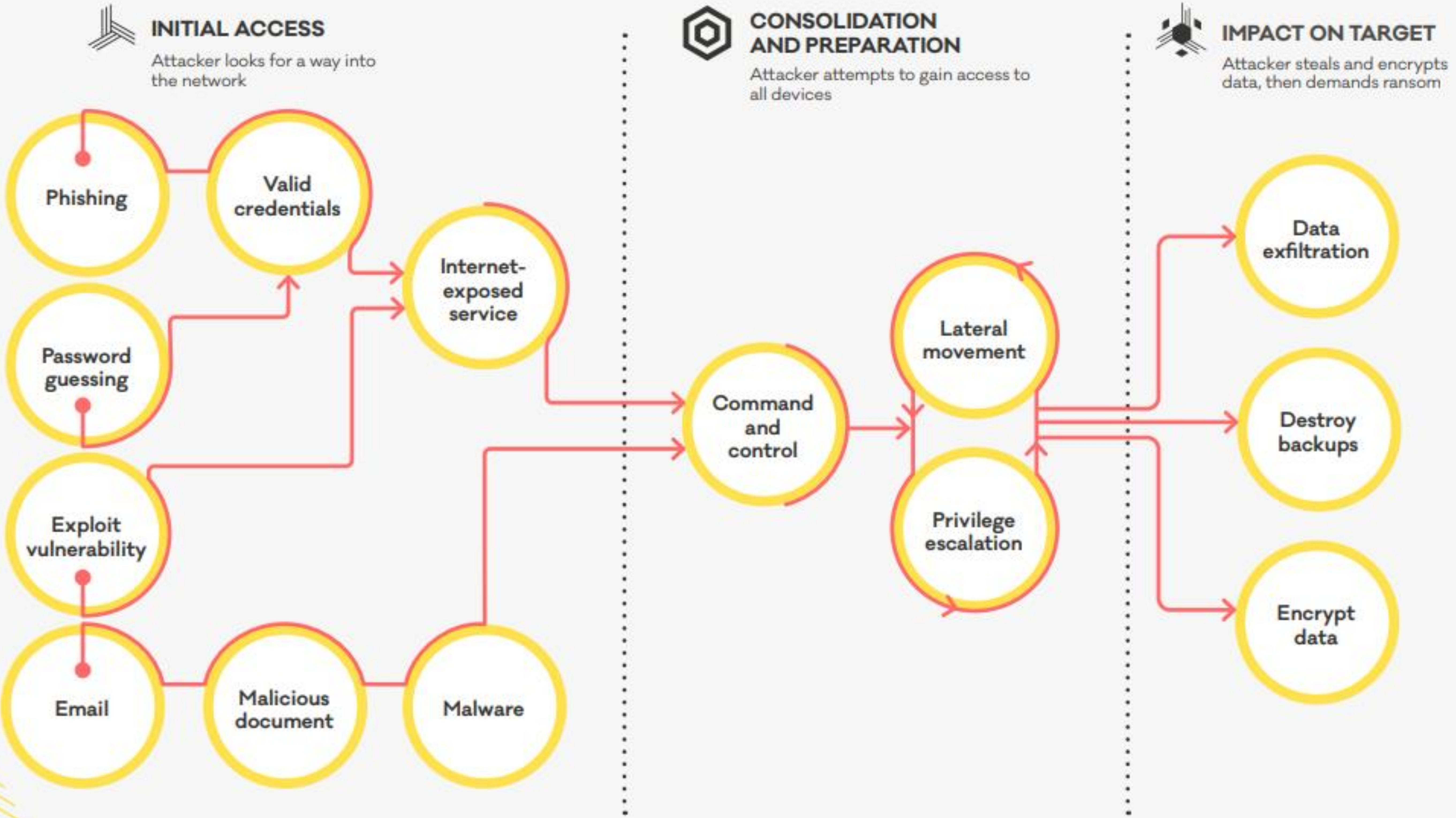
HCRG Care Group (founded in 2006) is a healthcare company that provides healthcare services such as physician clinics and specialty clinics. HCRG Care corporate office is located in The Heath Business and Technical Park, Runcorn, Cheshire, WA7 4QX, United Kingdom and has 5,000 employees. The total amount of data leakage is 2.275 Tb Direct file tree download link due to big file size: https://www.sendspace.com/file/[redacted]

Add time 1 day	Delete All Data	Download data now!
10000$	2000000$	2000000$

LIFECYCLE OF A RANSOMWARE INCIDENT

certnz

The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.



INITIAL ACCESS

Attacker looks for a way into the network

CONSOLIDATION AND PREPARATION

Attacker attempts to gain access to all devices

IMPACT ON TARGET

Attacker steals and encrypts data, then demands ransom

New Zealand Government

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 OSR 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 OSR Coalition® cowbell®

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

Q & A