Cyber Security

Defend as one


Jisc
Paul Barran
Cyber Security
Engagement Manager
Jisc


Jisc
Michael Pickett
Lead Cyber Security
Engagement Manager
Jisc

Reedham Ferry

Reedham Ferry

Reedham Ferry

Assured Service Provider
in association with
National Cyber Security Centre
Cyber Incident Response (Level 2)

CREST

CYBER ESSENTIALS

CIS SecureSuite Membership

Jisc

Your trusted cyber security partner

Assured Service Provider
in association with National Cyber Security Centre
Cyber Incident Response (Level 2)

CREST

CYBER ESSENTIALS

CIS SecureSuite Membership

Jisc

Threat Landscape 2023

Initial Access Vectors

- Phishing (still 90% of initial compromise)
- Access brokers (compromised credentials)
- Compromise of public facing vulnerabilities

Cloud Security

- Business Email Compromise (BEC)
- Security Misconfiguration
- Weak or no MFA

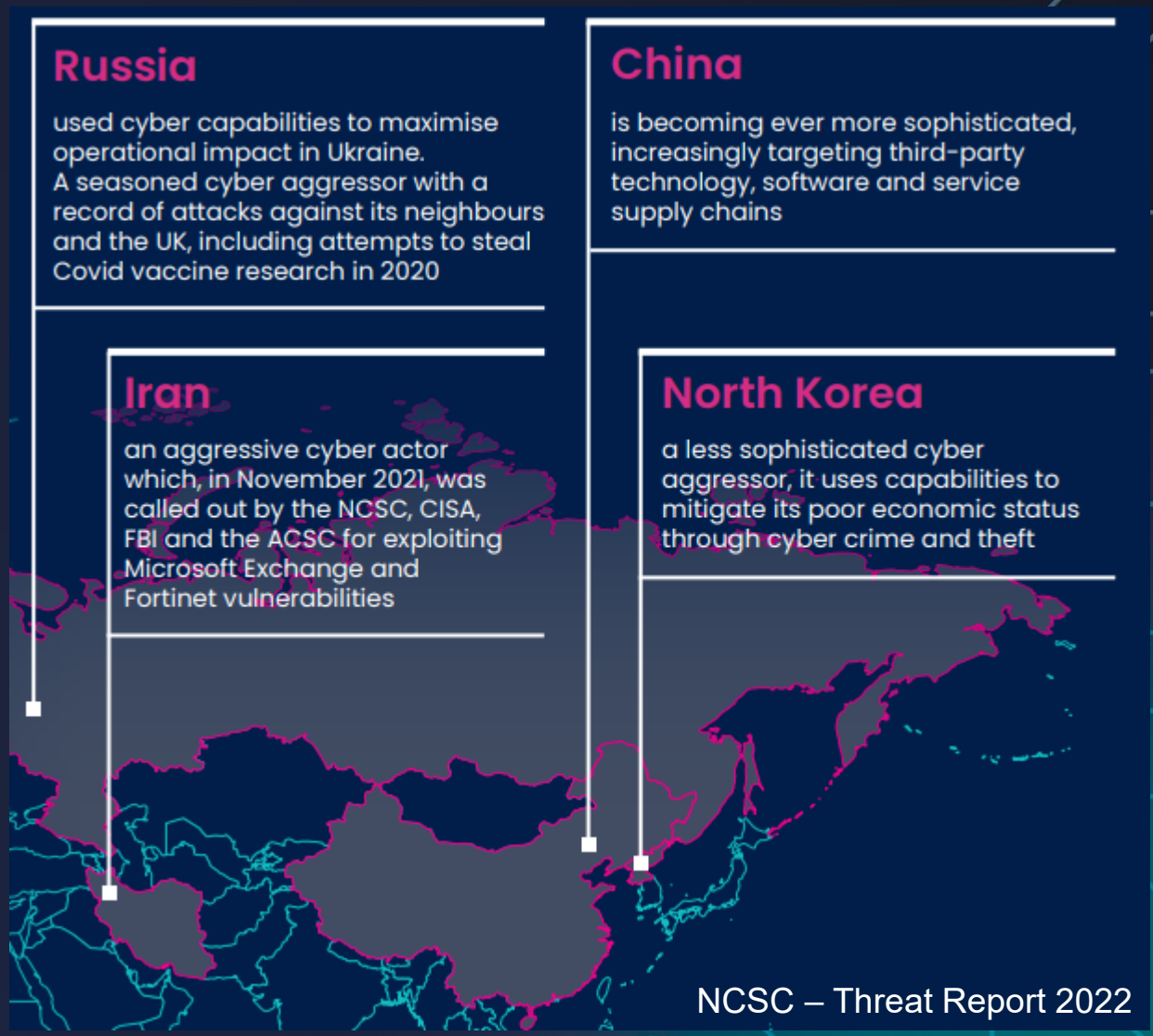
Server and Endpoint Protection

- Cloud console
- Weak or No MFA
- Lack of monitoring

Organisational risks

- Organised Cybercriminals
- Insider Threat
- Supply Chains
- State Actors

Ransomware (Still number 1!)



NCSC – Threat Report 2022

Who is targeting us?

- Education and research, are like all organisations, they are targets for ***high volume***, routine, speculative and opportunistic attacks by cyber criminals
- The ***data*** institutions hold and the work you do makes you an attractive target for specific attacks from more sophisticated threat actors
- Good ***situation awareness*** of cyber risk and threats is key to a strong security posture and facilitates good investment decisions (New joint guidance)
  - '75% of higher education institutions say they were negatively impacted regardless of whether there was a material outcome or not'
  - '48% stated that new measures were needed to prevent or protect against future breaches or attacks'

Department of science, innovation and technology – cyber breaches survey 2023

Assured Service Provider in association with National Cyber Security Centre Cyber Incident Response (Level 2) CREST CYBER ESSENTIALS CIS SecureSuite Membership Jisc

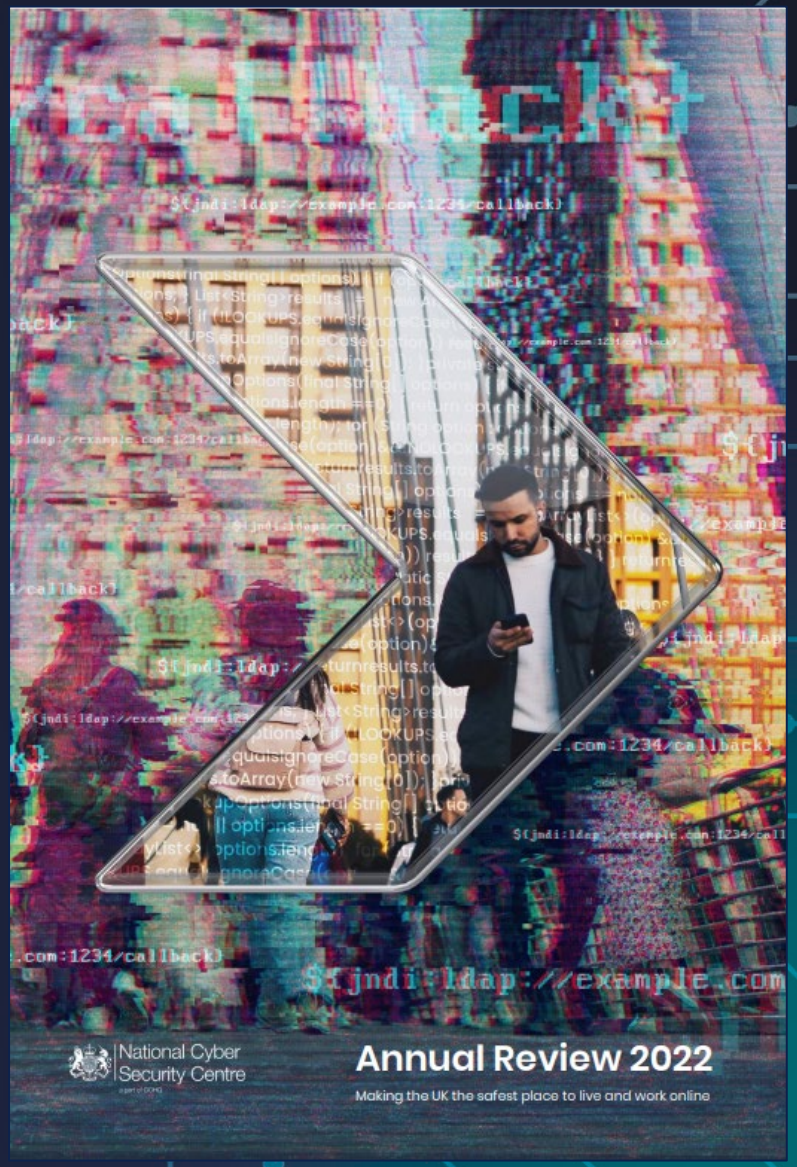
UK cyber security landscape

“Ransomware remains the most acute threat that businesses and organisations in the UK face.”

“This year, **18 ransomware incidents** required a nationally co-ordinated response...”

“… the true numbers of ransomware attacks in the UK each year **are far higher**, as organisations often do not report the compromises.”

https://www.ncsc.gov.uk/collection/annual-review-2022



Assured Service Provider
in association with National Cyber Security Centre
Cyber Incident Response (Level 2)

CREST

CYBER ESSENTIALS

CIS SecureSuite Membership

Jisc

Cyber security in the HE landscape

4100 incidents

Jisc's Security Operations Centre has dealt with more than 4100 incidents or cyber security related enquiries from HE institutions in the last year

£2.3m

Estimated cost of a single security incident

329 DDoS

attacks on HE colleges mitigated

2 minutes

DDoS mitigation launched within two minutes

Assured Service Provider in association with National Cyber Security Centre Cyber Incident Response (Level 2)

CREST

CYBER ESSENTIALS

CIS SecureSuite Membership

Jisc

Cyber security in the FE landscape

Only 3%
of FE organisations have a dedicated cybersecurity post

Only 10%
of FE organisations have 24/7 support around security incidents

835 incidents
Our security operations centre has dealt with more than 835 incidents or cyber security related enquiries from FE institutions in the last year

321 DDoS
attacks on FE colleges mitigated

2 minutes
DDoS mitigation launched within two minutes

£193k
Estimated cost of a single security incident

Assured Service Provider
in association with National Cyber Security Centre
Cyber Incident Response (Level 2)

CREST

CYBER ESSENTIALS

CIS SecureSuite Membership

Jisc

Summary of cyber security posture survey

58%
of Higher education institutions have a specific cyber budget

£797,000
Projected average budget f

Top threats

- Social engineering
- Phishing
- Human error
- Malware / Ransomware

5.8/10
Average perception of own cyber protection

87%
Engaged with Cyber essentials certificate

Top priorities

1. Protection / Prevention
2. Detection and response
3. User training and risk reduction

Assured Service Provider in association with National Cyber Security Centre Cyber Incident Response (Level 2)

CREST

CYBER ESSENTIALS

CIS SecureSuite Membership

Jisc

Q4 2022

- x5 Major Cyber incidents
- x0 Pre-Major incidents
- X86 DDoS attacks against 41 members

Q1 2023

- x3 Major Cyber incidents
- x1 Pre-Major incidents
- x282 DDoS attacks against 58 members

Q2 2023

- x1 Major Cyber incidents
- x2 Pre-Major incidents
- x254 DDoS attacks against 72 members

Q3 2023

- x3 Major incidents
- x12 Pre-Major incidents
- x148 DDoS attacks against 49 members
- 5 of the last 6 ransomware related incidents were detected by Jisc and encryption prevented

A deteriorating landscape

2020

- 15 Universities & Colleges

2021

- 18 Universities & Colleges

2022

- 21 Universities and Colleges

The “Lone Hacker” misconception

Impact of ransomware

“Ransomware is no longer just a financial crime; it is an urgent national security risk ”

- Exposure of sensitive information (Exfiltration)
- Encryption of data
- Direct impact costs - per institution - £2M
- Reputational damage
- Service disruption between 10 and 20 days




Risks and threats

- Security risks often appear hidden or abstract to users
- More widely understood risks, fire, road safety or health and safety security dangers are often immediate or obvious.

  - Reusing passwords
  - Not using strong passwords
  - Not using two-step verification (MFA)
  - Failing to apply a security update
  - Continuing to use software and hardware beyond the end of its service life

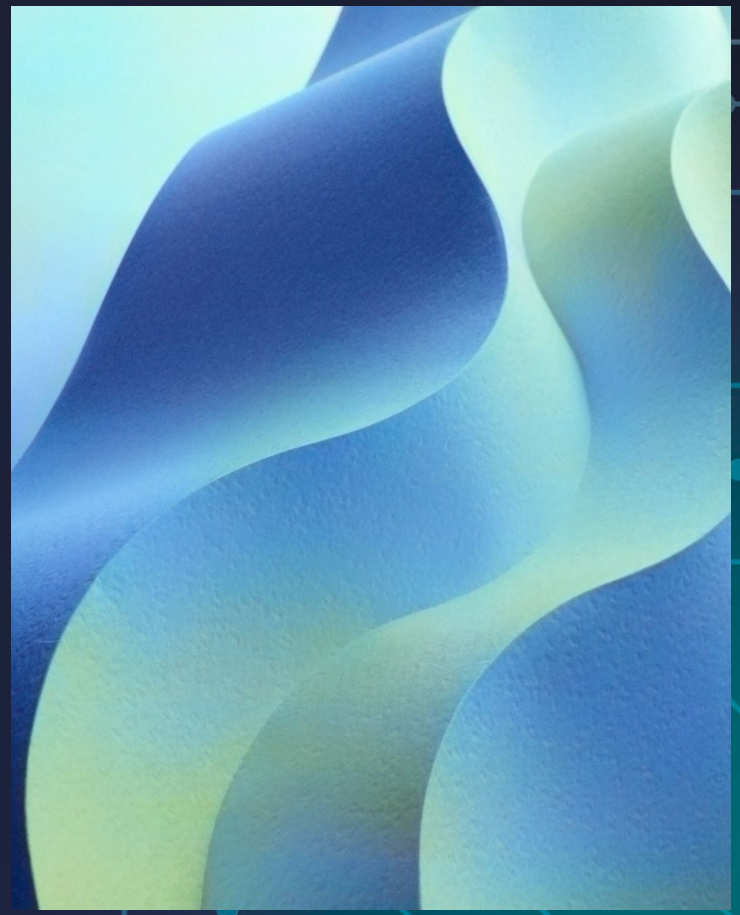
- Turning up to a ransomware incident feels like '***the fire service turning up to a house that has already burned down***'

https://www.ncsc.gov.uk/speech/rusi-lecture

Assured Service Provider in association with National Cyber Security Centre Cyber Incident Response (Level 2) CREST CYBER ESSENTIALS CIS SecureSuite Membership Jisc

How can we improve the Sector

Assets	Know your infrastructure – what are the critical assets
Backups	Ensure you have robust backup and recovery methods
Vulnerability	Ensure vulnerability and patch management Policies are in place
Monitoring	Ensure Logging and monitoring of key services are in place(early detection)
Defense in Depth	Multi-factor (staff and students) • Don't rely on a single technology (firewalls, Anti Virus etc) • Consistent Anti Virus across ALL servers and workstations
Awareness	Awareness training – staff and students (prevent phishing attacks) Training for your investment



Scan to read our full 16 point checklist

Assured Service Provider
in association with National Cyber Security Centre
Cyber Incident Response (Level 2)

CREST

CYBER ESSENTIALS

CIS SecureSuite Membership

Jisc

‘All hell was breaking loose’: How hackers forced a mega college to close

Fraser Whieldon

19 Mar 2021, 10:00

More from this author

See discussion

Exclusive

NEWS

Home | Brexit | Coronavirus | UK | World | Business | Politics | Tech | Science | Health | Family & Education

England | Local News | Regions | Lancashire

University of Central Lancashire among three hit by cyber-attacks

BirminghamLive NEWS IN YOUR AREA BLACK COUNTRY VILLA MORE

BUY A PAPER FUNERAL NOTICES JOBS ADVERTISE WITH US VOUCHER CODES DIRECTORY DATING BOOK AN AD BUY A PHOTO

News › Midlands News › South Birmingham College

Students told to stay at home all week after South and City College hacked

It was the target of a ransomware attack and now IT experts need a week to make repairs

SHARE COMMENTS

By James Cartledge
05:30, 15 MAR 2021 | UPDATED 08:42, 15 MAR 2021

NEWS

SOUTH & CITY COLLEGE BIRMINGHAM

The College has suffered a major ransomware attack on our IT system which has disabled many of our core IT systems. 15th March to allow our IT specialists to fix the problem.

On Monday 15th we will revert to online teaching for the rest of the week for all areas. We are therefore asking students to access their during this time and we ask that you bear with us and contact your tutor if there are any problems.

ilte

Jisc

NEWS

Home | Coronavirus | US Election | UK | World | Business | Politics | Tech | Science | Health | Family & Education

Technology

Greenwich University fined £120,000 for data breach

St Helens Star

Subscribe Puzzles

News Sport Saints What's On Events Announcements E-Edition Contact Us More

Video News

Police probe launches as Carmel College hit by 'cyber attack'

18th May

NEWS

Home | Coronavirus | US Election | UK | World | Business | Politics | Tech | Science | Health | Family & Education

England | Local News | Regions | Tyne & Wear

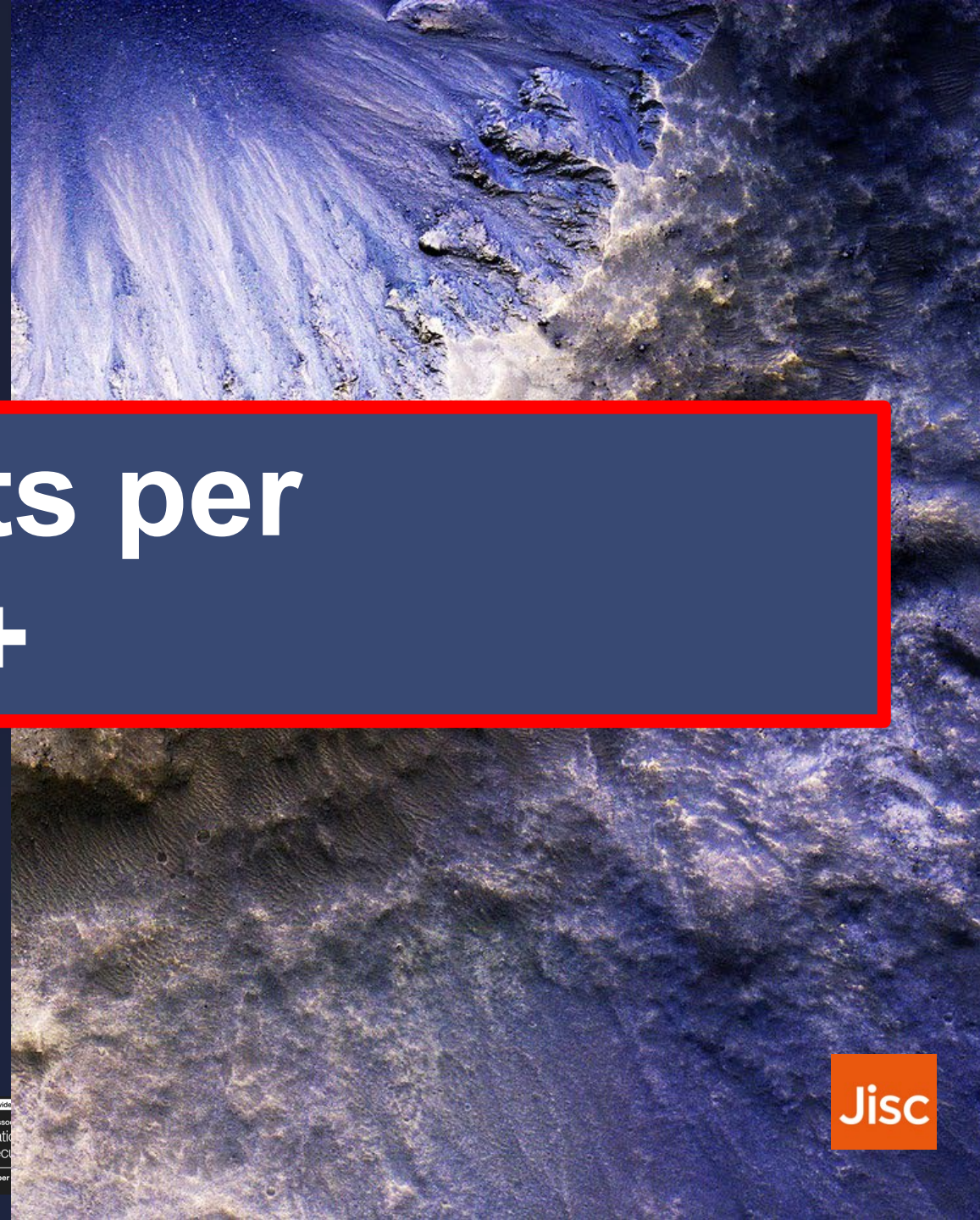
Northumbria University hit by cyber attack

CYBER ESSENTIALS

CIS SecureSuite Membership

Jisc

A deteriorating landscape



- **Direct impact costs per institution - c£2M+**


Incident in progress

It is the morning of Friday 1st December...

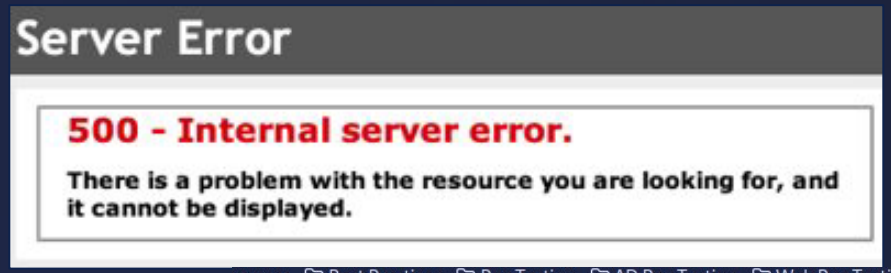
You notice that the door entry system doesn't appear to be functioning

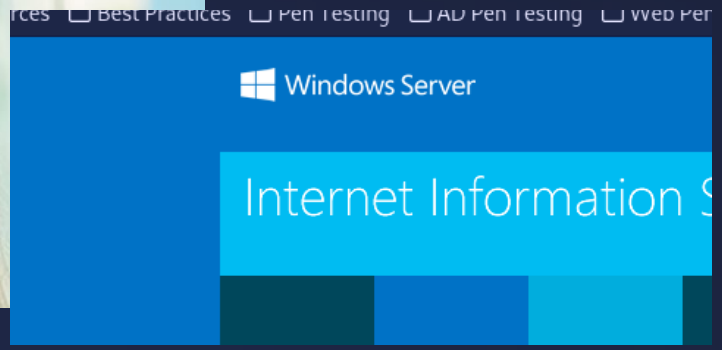
You start your computer but are unable to login

No systems are online

Midday – the Crisis Response SLT have met, IT have some information and it isn’t good...

Services not available





Friday 1st December

- **NO student records system**
- **NO finance system**
- **NO HR system**
- **NO Teams or email**

Discuss in your breakout groups…

How will my role be impacted?

How can you deliver your service in the short term?

What about the longer term?

Collate the responses to feedback to the main group

Cyber Incident Response
(Level 2)

Jisc

What you have just ‘experienced’ is the result of a cyber attack that we have seen several times against colleges and universities over the past few months.

Assured Service Provider
in association with National Cyber Security Centre
Cyber Incident Response (Level 2)

CREST

CYBER ESSENTIALS

CIS SecureSuite Membership

Jisc

Group feedback

Your questions

Key extra resources / free tools

- Cyber security and universities managing risk
- Web Check checks your websites for common web vulnerabilities and misconfigurations in an unobtrusive way and tells you what you should be concerned about and what you need to do about it.
- Mail Check It is a service that helps with email security configuration and reporting.
- Cyber impact report real costs

Assured Service Provider in association with National Cyber Security Centre Cyber Incident Response (Level 2) CREST CYBER ESSENTIALS CIS SecureSuite Membership Jisc