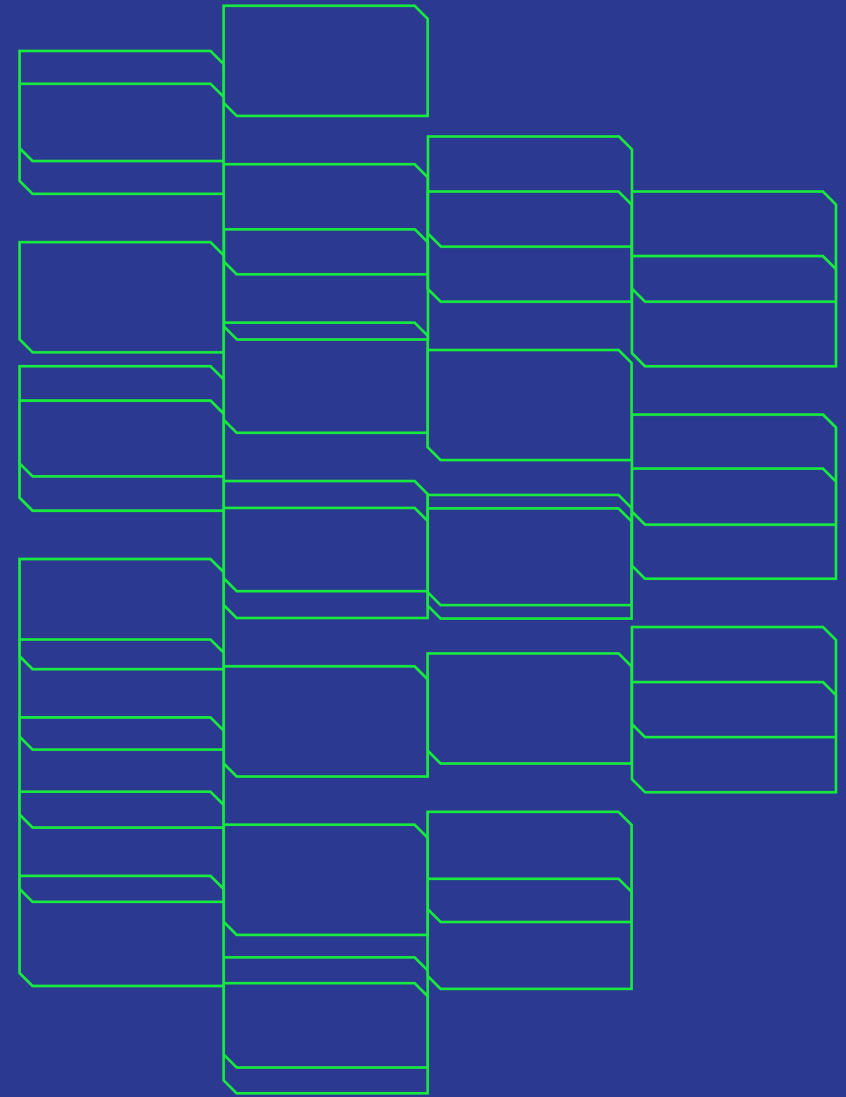


Delivering cyber security awareness and training to education and research

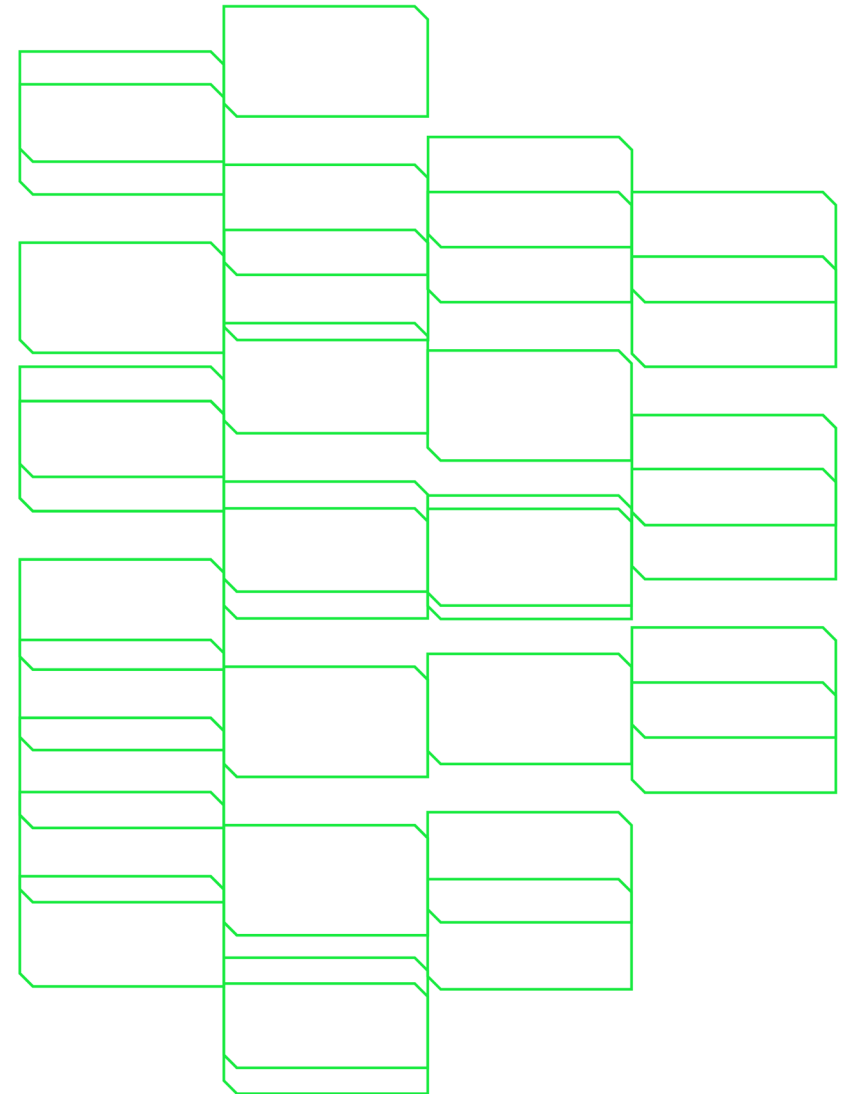
Mark Tysom



Co-funded by
the European Union

Threat landscape: UK Education sector

- *In 2023, 85% of Higher and Further Education institutions reported experiencing at least one cyber incident in the previous 12 months*
- *50% of universities experience weekly cyber attacks or data breaches*
- *Ransomware and phishing ranked as the top two cyber threats*



Numbers of serious incidents involving loss of critical systems

2020

- 15 Universities & Colleges

2021

- 18 Universities & Colleges

2022

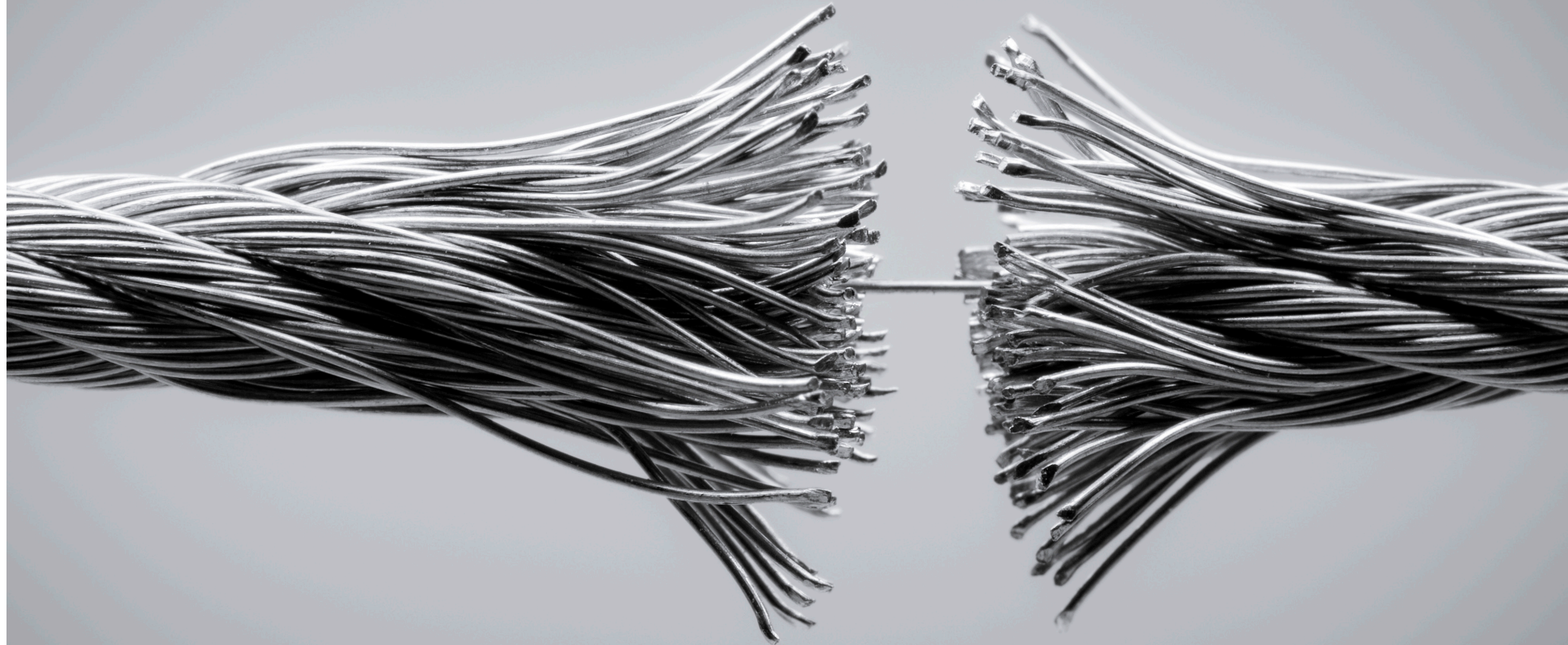
- 21 Universities and Colleges

2023

- 18 Universities & Colleges

**Average
downtime of
critical systems**

**10–20
days**



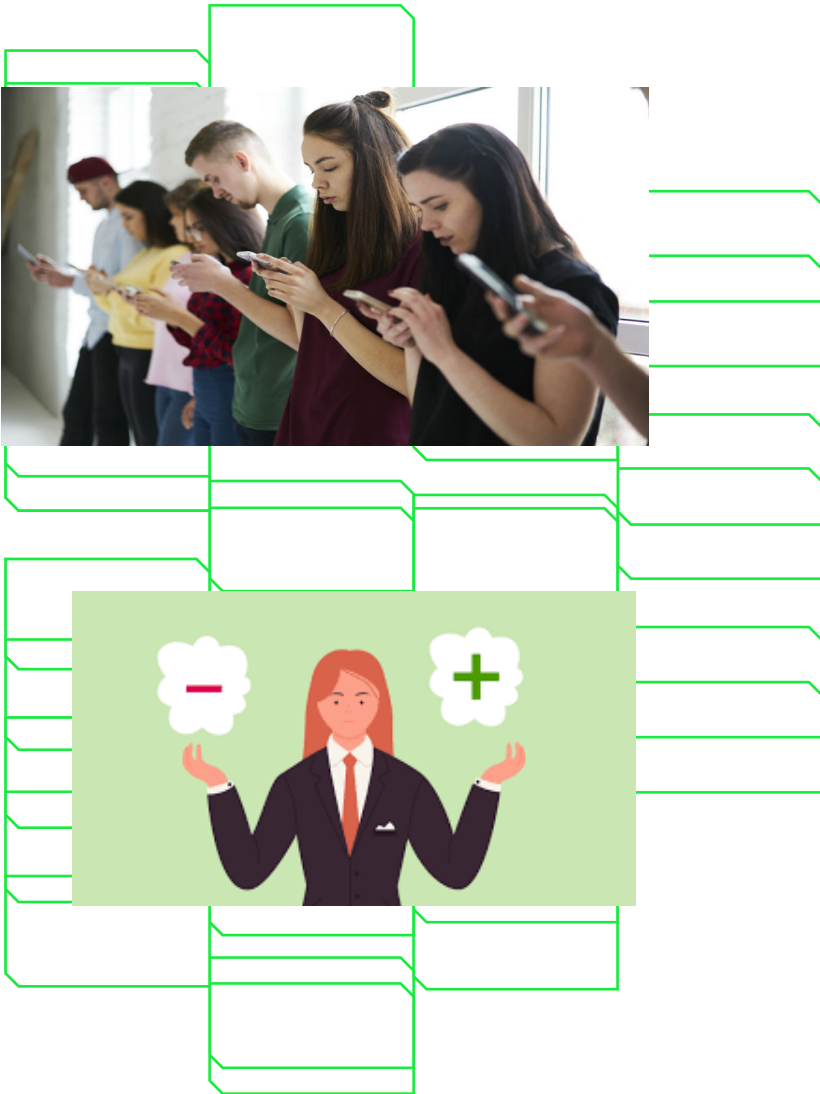
Average direct
impact costs per
institution

£2M



90% of successful cyber attacks start as a phishing email

The human factor in education and research



- Thousands of staff and students
- Multiple devices, some managed, many not
- But, people are the primary target, not technology
- User awareness is our first line of defence
- Investing in positive behavioral change pays dividends

Jisc cyber posture survey 2022

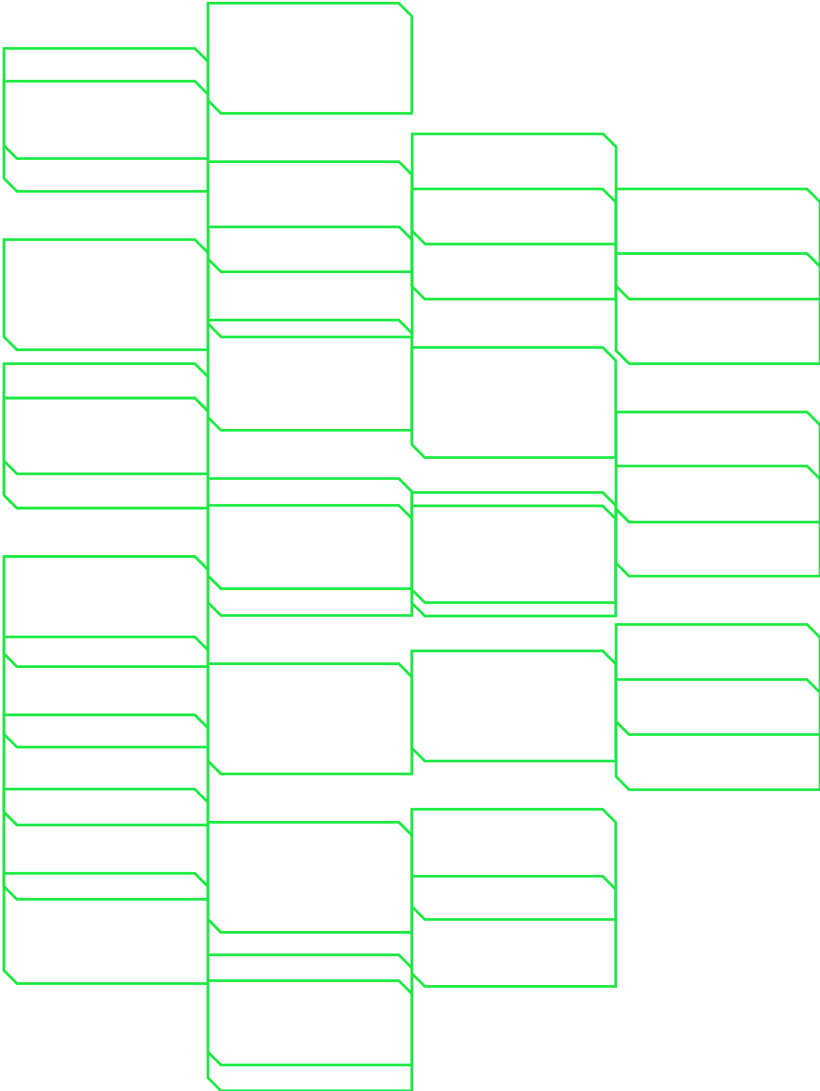
Top threat

Ransomware/malware is seen as the top threat for HE for a second year. The implementation of training for staff remains a priority, with a high proportion required to undertake this every year.

Top request

A range of responses were received, with cyber security training emerging as the biggest request, as in the previous year.

<https://www.jisc.ac.uk/reports/cyber-security-posture-surveys>



Awareness and training portfolio

- Annual security conference
- Cyber Security Community via Teams
- e-learning modules
- Wide range of free and paid for courses and clinics

[Cyber incident awareness workshop](#)

Improve your organisation's readiness in responding to phishing campaigns through this scenario-led workshop. This workshop is

[ISO 27001 clinic](#)

Ask us your questions about implementing the standard.

[Developing effective security awareness campaigns](#)

Creating a strong security culture and mindset at your organisation.

[Penetration testing - think like a hacker](#)

Learn how to test a computer system, network or web application to find security vulnerabilities.

[Information security e-learning module](#)

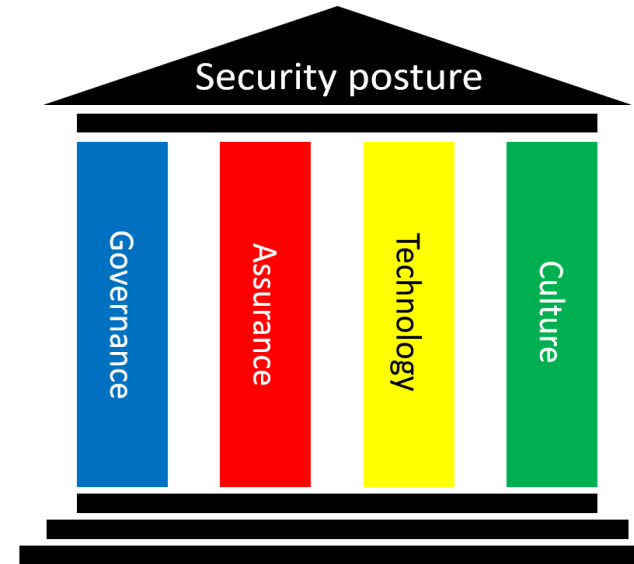
Online training module covering phishing, malware and password security.

[Incident response handling fundamentals workshop](#)

Work through the six phases of the incident response lifecycle to protect your organisation from cyber-related threats. This workshop is

[Ransomware incident response workshop](#)

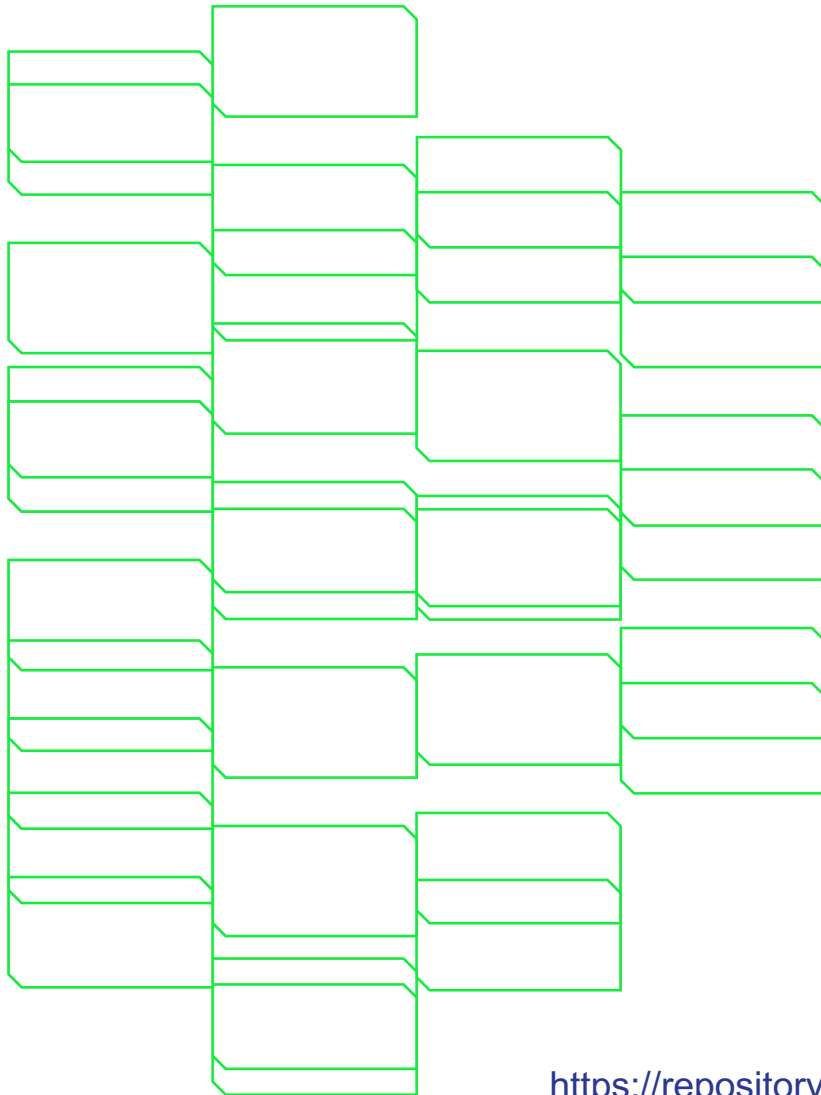
Test your infrastructure, policies and procedures with a realistic simulated incident. This



















Ransomware incident response workshop

- Pre workshop scoping exercise: PingCastle scan and review of existing major incident plans
- Full day workshop delivered in two parallel strands: IT and SMT
- Scenario shared with both teams: observe response, interaction between IT and SMT, decision making, delegated authority, comms...
- Designed to test: uncomfortable, stressful, highlight good practice and areas for improvement
- Concludes with a feedback session with both teams in one room
- Follow-up report covering observations and recommendations

Checklist for senior leaders

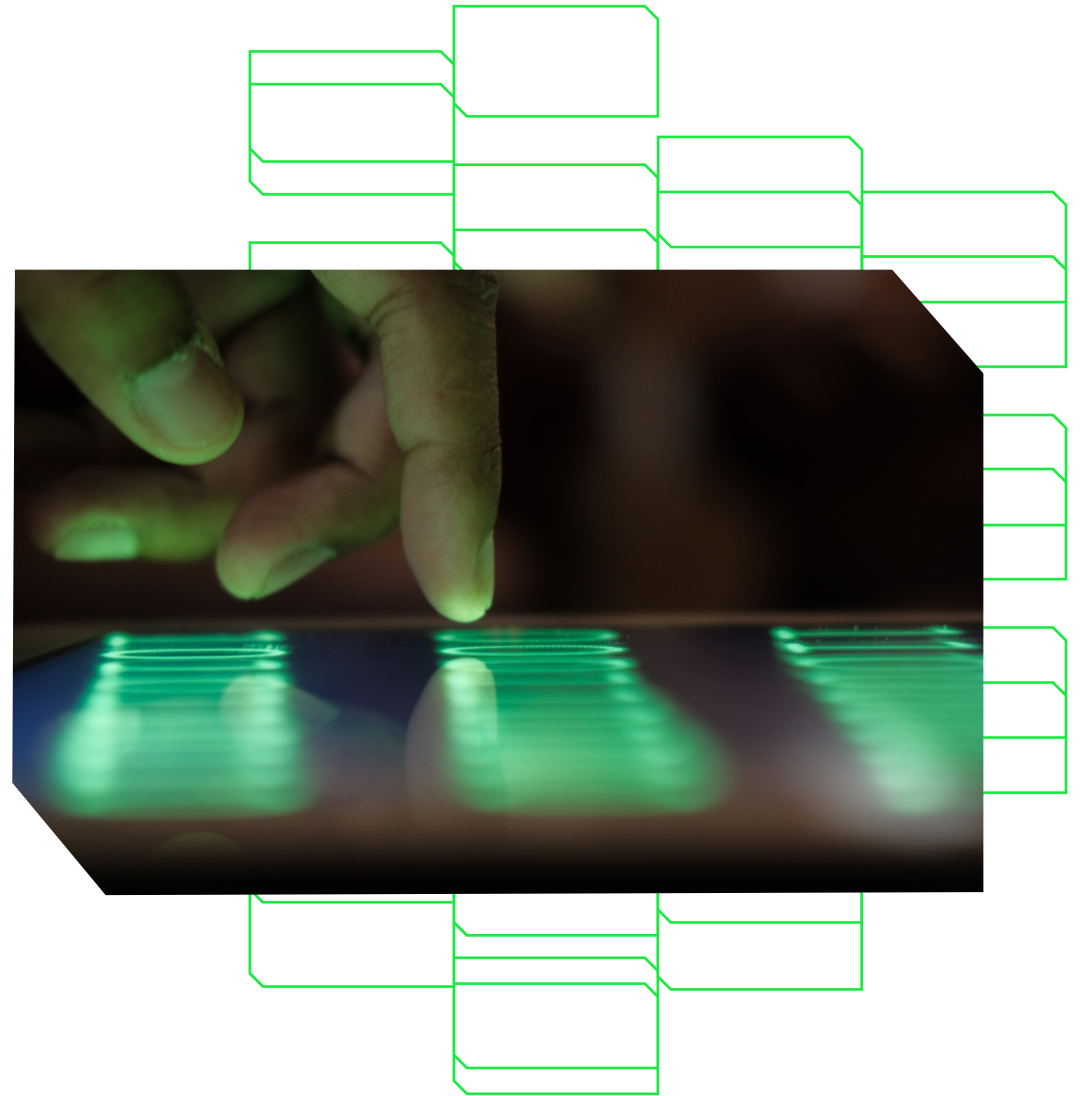


 <p>1. Do we have a data classification scheme to help identify sensitive information and ensure appropriate protections are in place?</p>	 <p>2. Do we have effective mechanisms for controlling access to resources, such as how we handle new starters, movers or when staff leave our organisation?</p>	 <p>3. Do we review user accounts and systems for unnecessary privileges on a regular basis?</p>
 <p>4. Do we enforce multifactor authentication for all systems and users?</p>	 <p>5. Do we have a tried and tested process for backing-up critical data in a manner resistant to disasters or cyber attacks?</p>	 <p>6. How long will it take us to recover critical business functions, assuming a loss of all infrastructure? What's the business impact of a loss of all digital infrastructure? How will we lead and co-ordinate business recovery in this scenario?</p>
 <p>7. Can the business tolerate a recovery period that could take several weeks or months? How is this effected by different critical time periods for our business?</p>	 <p>8. Do we have regularly rehearsed plans to deal with the most likely cyber events or disasters?</p>	 <p>11. How would our organisation identify an attacker's presence on the network?</p>
 <p>9. Are all of our hardware and software products free from vulnerabilities, supported by the vendor and regularly patched?</p>	 <p>10. Are our networks separated so that if an attacker gets access to one device, they will not have access to our entire estate?</p>	 <p>14. Are we doing everything necessary to support our staff, students and stakeholders to understand and be aware of cyber risk, via training advice and guidance?</p>
 <p>12. Do we regularly review our cyber risk management approach to ensure that the ways we have decided to manage risks remain effective and appropriate?</p>	 <p>13. Are all staff aware of and participate in effective cyber risk management processes?</p>	
 <p>15. Do we maintain an accurate record of our technology assets, including hardware, software, firmware, peripheral devices and removable media?</p>	 <p>16. Do we adequately understand our business-critical services and functions and their associated data, technology and supply chain dependencies?</p>	

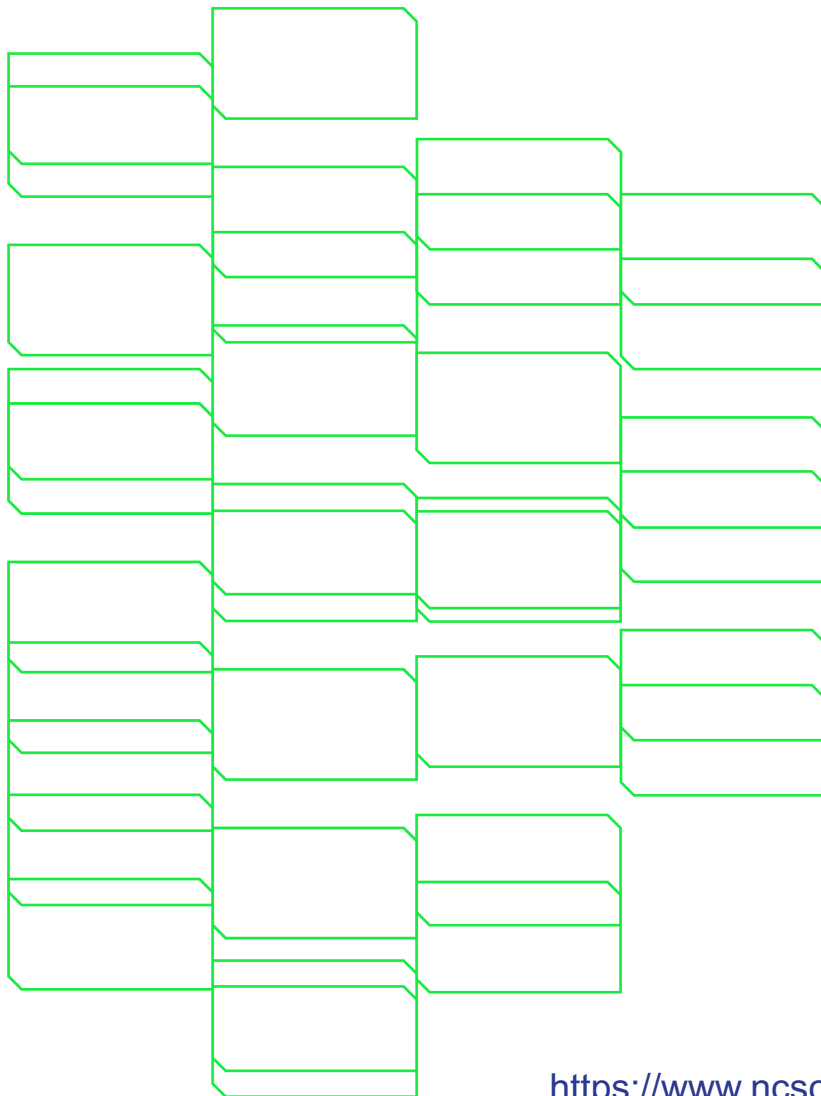
<https://repository.jisc.ac.uk/8549/1/cyber-security-16-questions-checklist.pdf>

Cyber posture self assessment

- Large UK university
- Used checklist to benchmark cyber posture
- Presented to board with three-year plan
- Significant increase in cyber budget
- Fivefold increase in dedicated cyber staff
- Increased awareness of cyber risk and its business impact



Working with partners



Stay safe online: Top tips for college staff

Regardless of the size or type of college you work for, it's important to understand how to defend yourself from cyber attacks. The advice summarised to the right is applicable to your college life and your home life.



Use strong passwords

Criminals will try the most common passwords (e.g. password1), or use publicly available information to try and access your accounts. If successful, they can use this same password to access your other accounts.

Most web browsers will offer to save your passwords for you. It's safe for you to do this (unless you're using a shared account at your college that other people can access).

Password

- Create a strong and memorable password for important accounts, such as by combining three random words. Avoid using predictable passwords, such as dates, family and pet names.
- Use a separate password for your college account. If an online account gets compromised, you don't want the criminal to also know your college password.
- If you write your passwords down, store them securely away from your device. Never reveal your password to anyone; your IT team or other provider will be able to reset it if necessary.
- Use 2 step verification (2SV) for important websites like banking and email. 2SV (which is also known as multi-factor authentication or MFA) provides a way of 'double checking' that you really are the person you are claiming to be when you're using online services.

Defend against phishing attacks

Phishing emails appear genuine, but are actually fake. They might try and trick you into revealing sensitive information, or contain links to a scam website or an infected attachment.



- Know the techniques that phishers use in emails. This can include urgency or authority cues that pressure you to act.
- Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more. If a message or call makes you suspicious, don't click the link in the message – instead use details from their official website.
- Anybody might click on a phishing email at some point. If you do, tell someone immediately to reduce the potential harm caused. Phishing emails appear genuine, but are actually fake. They might try and trick you into revealing sensitive information, or contain links to a scam website or an infected attachment.

If in doubt, call it out

Reporting incidents promptly – usually to your IT team or line manager – can massively reduce the potential harm caused by cyber incidents.

Secure your devices

The phones, tablets, laptops or desktop computers that you use can be targeted both remotely and physically, but you can protect them from many common cyber attacks.



- Don't ignore software updates – they contain patches that keep your device secure. Your college IT team may manage updates, but if you're prompted to install any, make sure you do.
- Always lock your device when you're not using it. Use a PIN, password, or fingerprint/face id. This will make it harder for a criminal to access a device if it is left unlocked, lost or stolen.
- Avoid downloading fake apps. Only use official app stores (like Google Play or the Apple App Store), which provide protection from viruses. Don't download apps from unknown vendors and sources.
- Cyber attacks can be difficult to spot, so don't hesitate to ask for further guidance or support when something feels suspicious or unusual.
- Report attacks as soon as possible – don't assume that someone else will do it. Even if you've done something (such as clicked on a bad link), always report what's happened.
- Don't be afraid to challenge policies or processes that make your job difficult. Security that gets in the way of people doing their jobs, doesn't work.



© Crown copyright 2024 Photographs and Infographics may include material under licence from third parties and are not available for re-use. Text content is licensed for re-use under the Open Government Licence v3.0 [ncsc.gov.uk](https://www.ncsc.gov.uk)

<https://www.ncsc.gov.uk/files/Stay-safe-online%20Final%201.png>

Any questions?

<https://www.jisc.ac.uk/staff/mark-tysom>

<https://beta.jisc.ac.uk/training?categories=3>

<https://www.jisc.ac.uk/cyber-security>

Security Days



Co-funded by
the European Union