



Delivering cyber security training and awareness to the education and research sector

Mark Tysom

Senior Cyber Security Product Manager

Jisc





Jisc – what we do

We provide the Janet Network - the UK's National research and education network (NREN)

It is used by **18 million** people

Carrying **6 petabytes** of data each day

It has built in, world class cyber security protection, utilising sector specific intelligence

Help the sector save time and money

Through our sector wide deals and shared services alone we save the sector around:

£300m (2023)

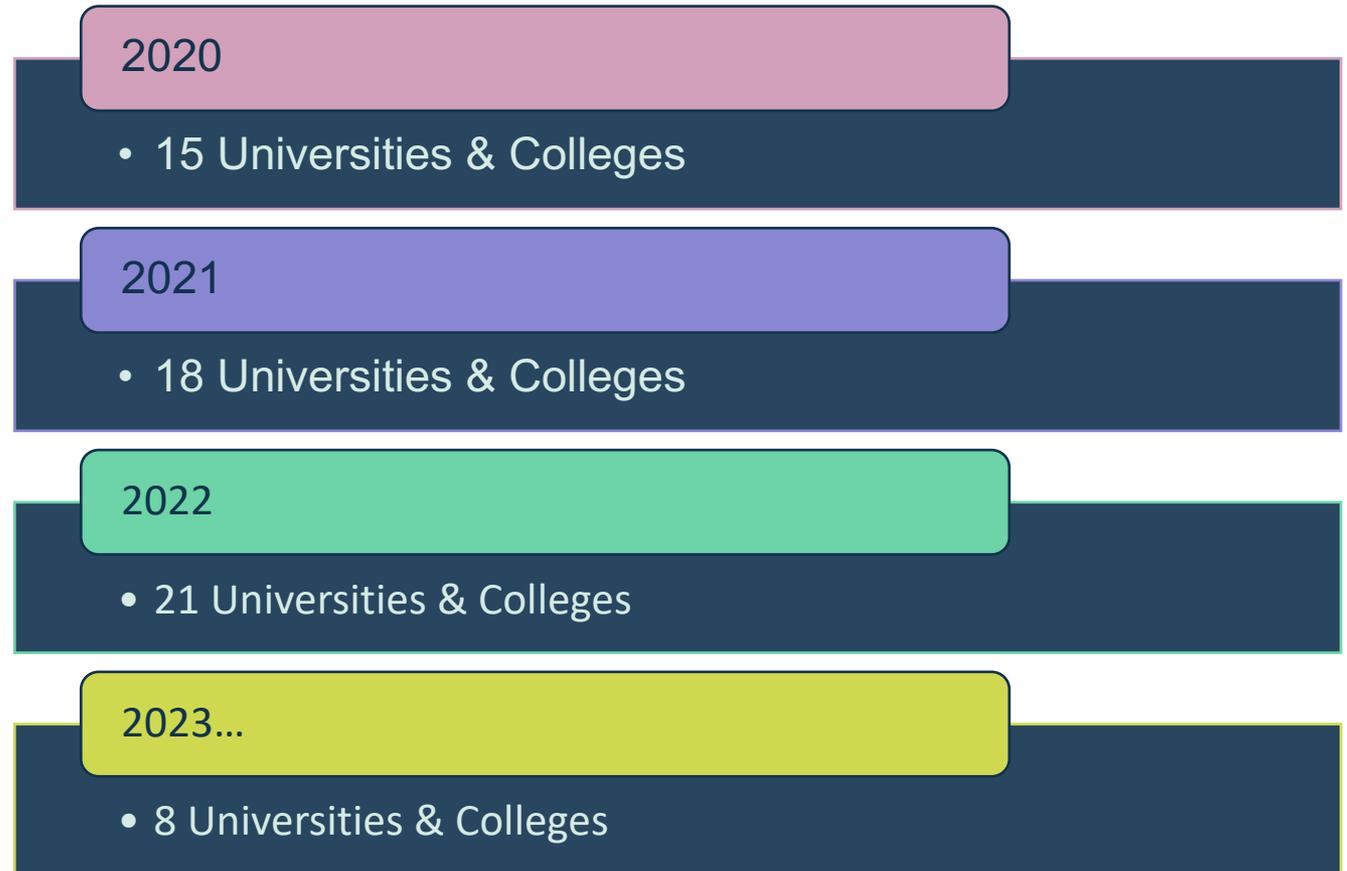
We provide trusted cyber advice and practical assistance:

- Providing insight, guidance and thought leadership
- Delivering training and events
- Building communities



A deteriorating landscape

- **Direct costs per institution c€2.3M**
- **Service disruption between 10 and 20 days**



The human factor

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

[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](#)

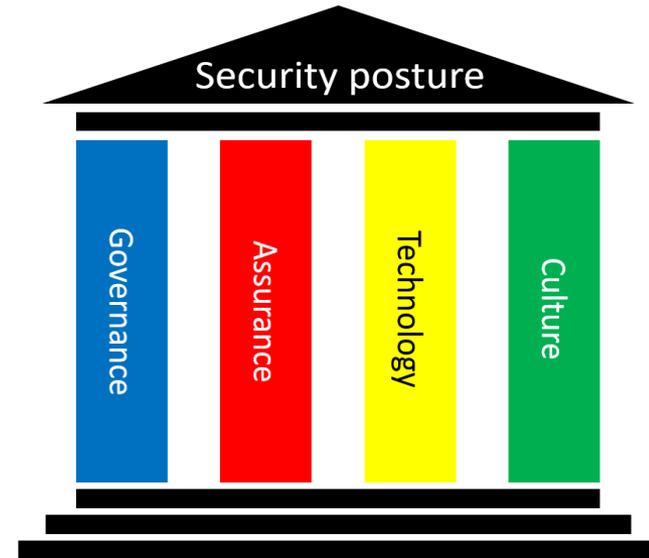
Online training module covering phishing, malware and password security.

[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



Facilitating conversations between technical and senior managers

 <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>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>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>	

- Large UK university
- Used questions 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





Thank you

Contact details:

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

Jisc cyber training portfolio:

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



ConfGARR23
SAPERI INTERCONNESSI