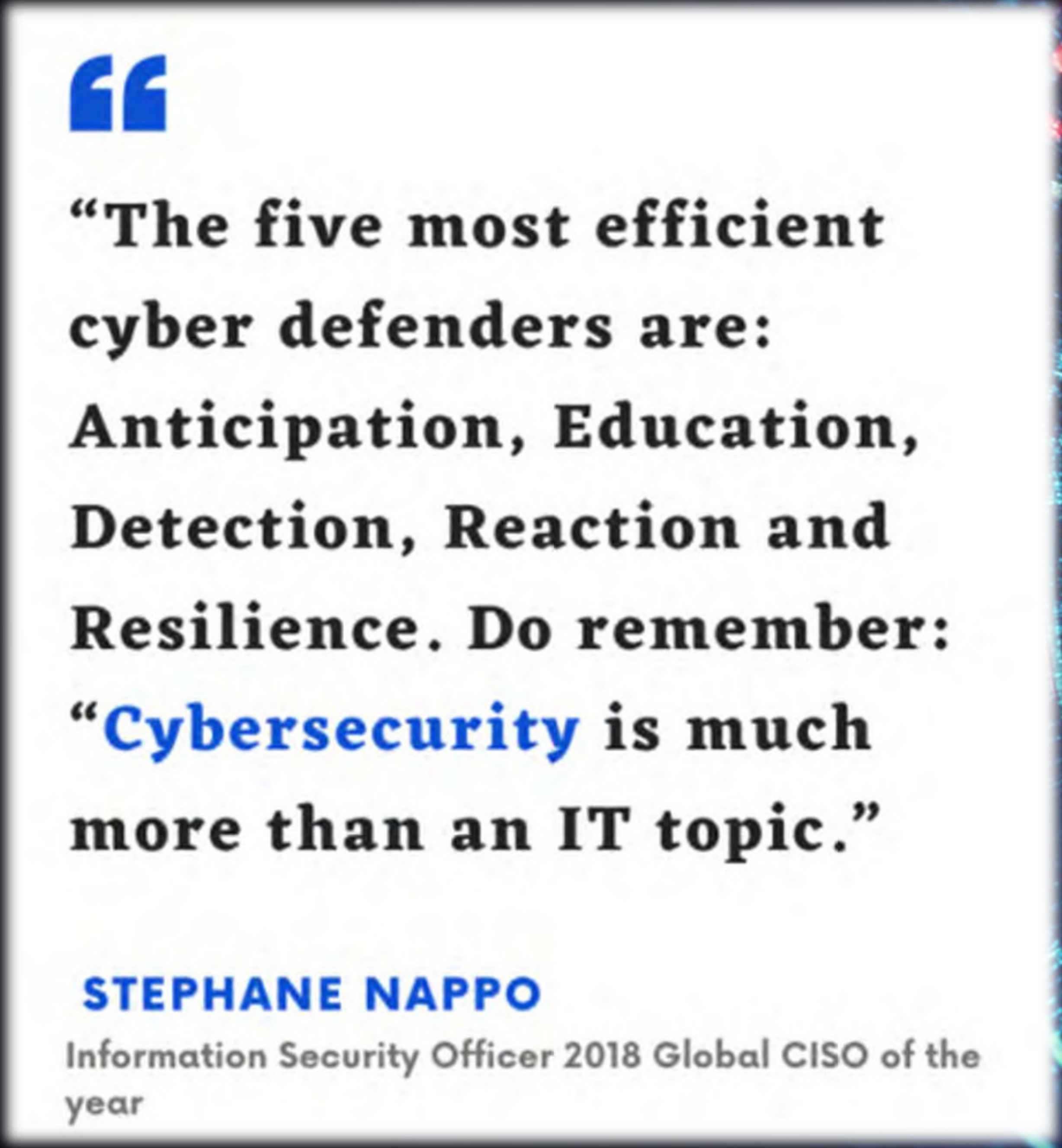
Association for Public Service Excellence

Cyber security: The risks and mitigating factors

David Batho, Head of Security, Jisc



> “The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: “Cybersecurity is much more than an IT topic.”

STEPHANE NAPPO

Information Security Officer 2018 Global CISO of the year

Setting the scene – What are the risks?

UK EDUCATION SECTOR – Key Attacks

Q1 2022:

- **4 Major incidents** (ransomware attacks, all via insecure remote access services)
- **84 DDoS** attacks targeting 37 institutions

Q2 2022:

- **8 Major incidents** (remote access, unpatched critical vulnerabilities, absent multi-factor authentication)
- **85 DDoS** attacks targeting 28 institutions

Q3 2022:

- **3 Major incidents** (Microsoft Exchange server compromise)
- **62 DDoS attacks** targeting 24 institutions

Q4 2022:

5 Major Cyber incidents

2 FE unable to operate

HE disruption to services and BAU

Student and business data exposed

EDUCATION Security Challenges

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

Service disruption between 10 and 20 days

Reputational Loss

Encrypting servers and workstations

Exfiltrating data – posting this information on dark web(HR or Student)

Partial to Full disruption of **ALL** services

Compromise cloud services (email and cloud services)

Jisc

Further targeted ransomware attacks on the UK education sector by cyber criminals

Cyber impact

The impact of cyber security incidents on the UK's further and higher education and research sectors

Observations, advice and recommendations

November 2020

If you don’t think you’re at risk, you’re…

Who’s targeting us?

- “Why would anybody want or bother to attack us?”

The “Lone Hacker” misconception

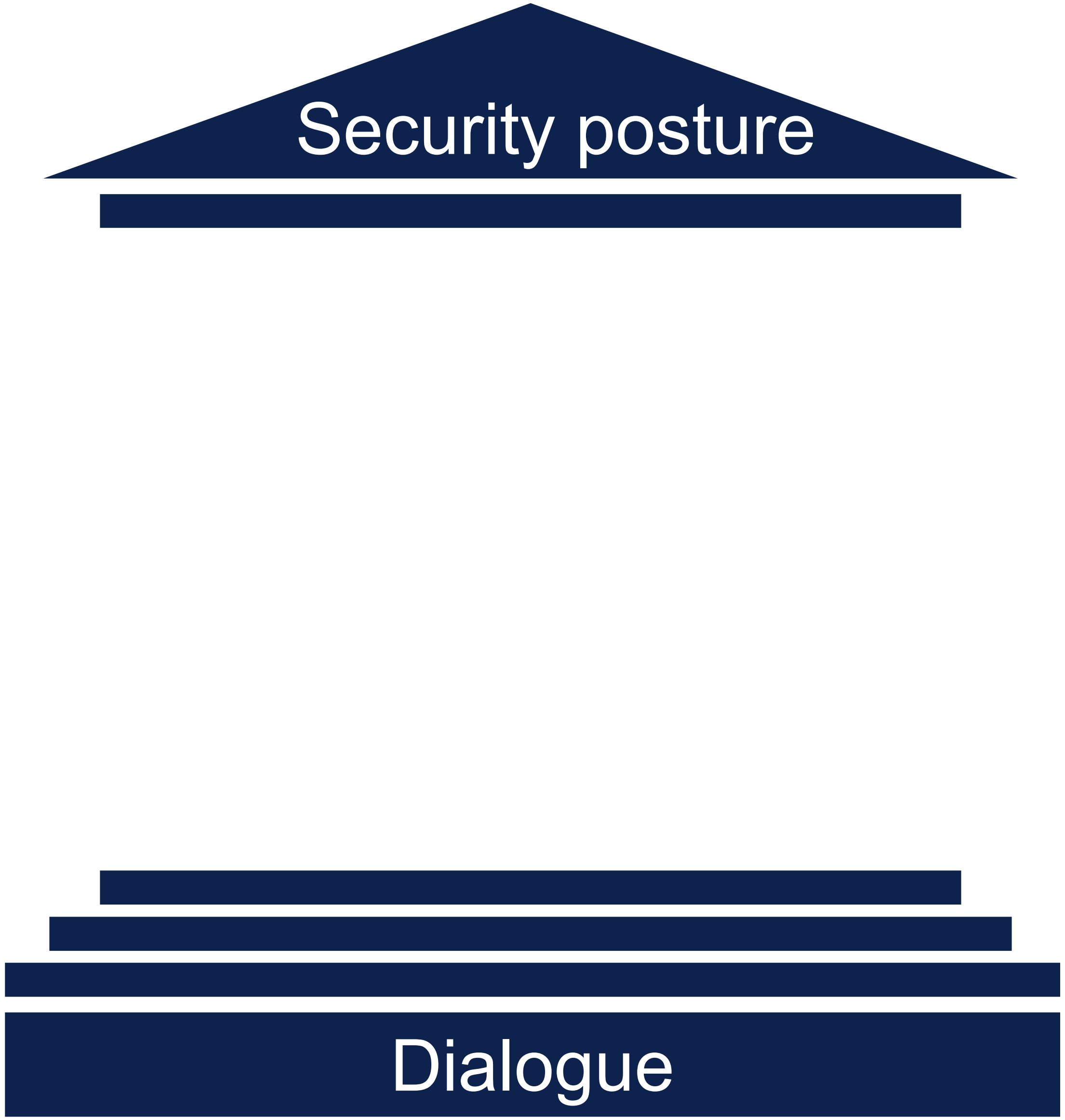
UK Local Authorities:

10,000 attempted cyber attacks per day

14% YOY increase

2 million+ incidents

Security posture



Security posture

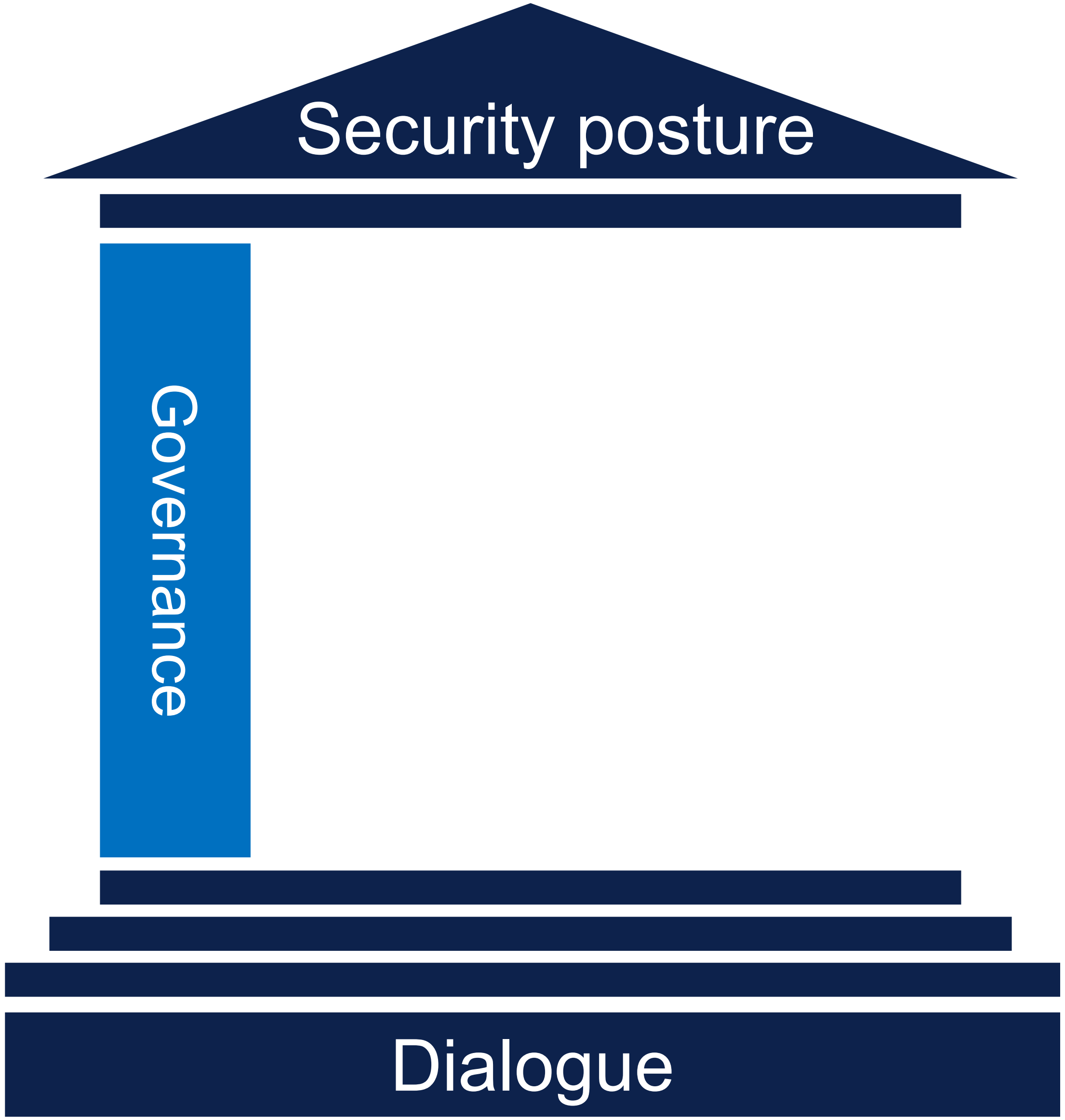
Dialogue

Constructive **dialogue** across the whole organisation is the **foundation** of a strong security posture

"I don't think any chief exec would get away with saying they don't need to understand legal risk because they have a General Counsel."

(Lindy Cameron, NCSC CEO)

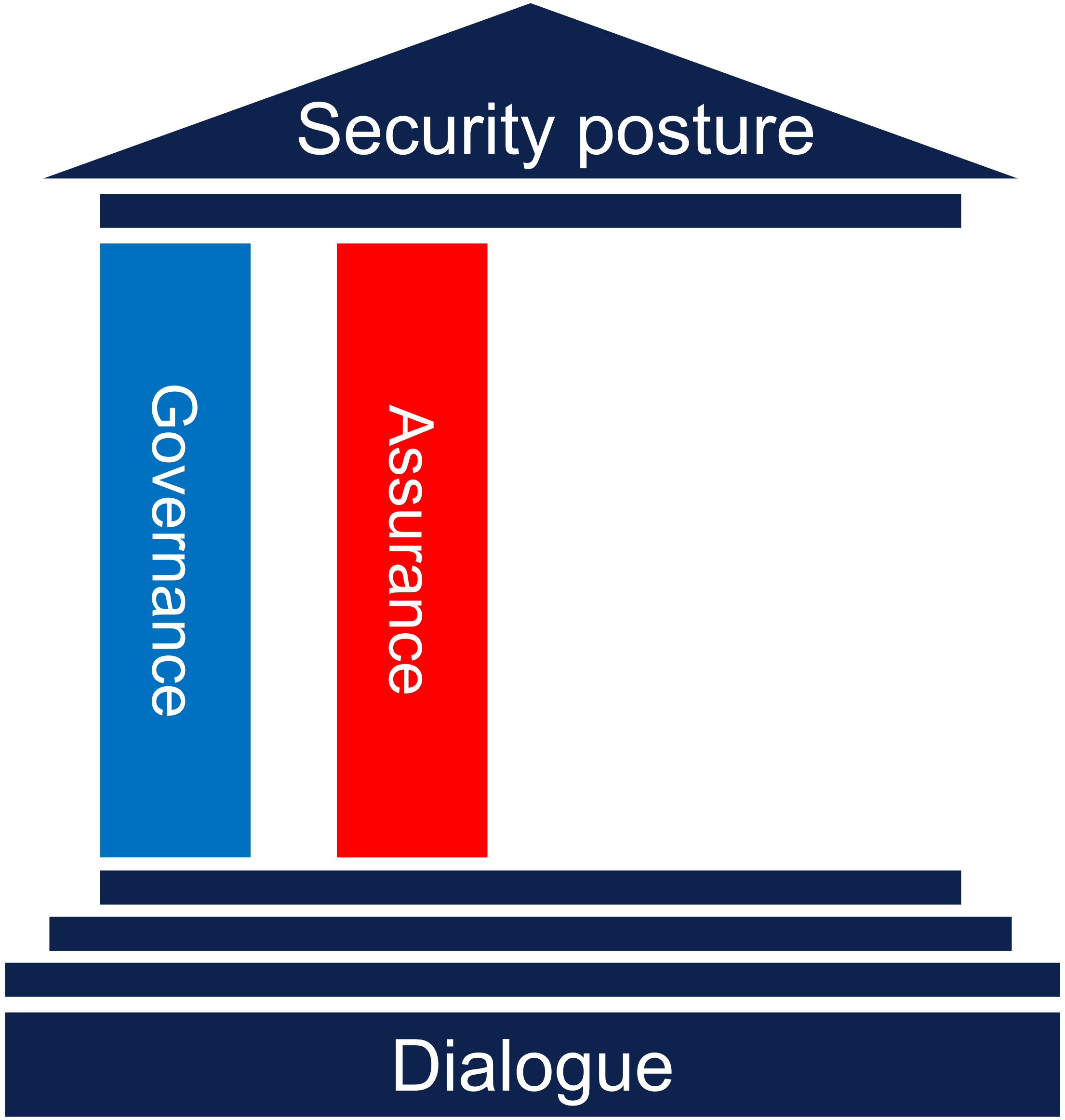
https://www.ncsc.gov.uk/speech/lindy-cameron-first-year



Do we have a strategy for our security, owned by senior leadership?

Is security just the IT team's responsibility, or everyone's?

Are our decision-making processes informed, effective and auditable?



Security posture

Governance

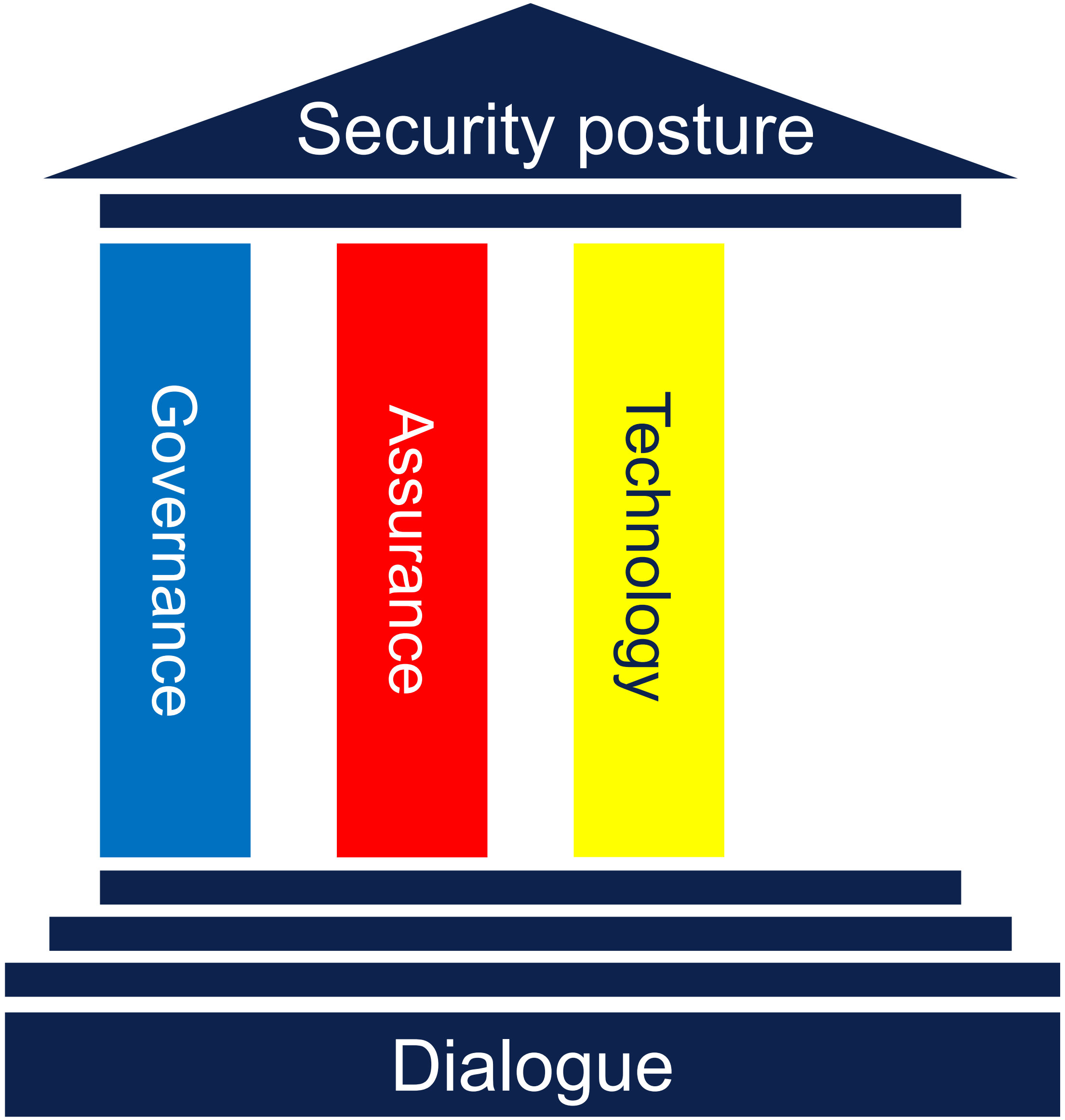
Assurance

Dialogue

Are we doing what we should be?

Are we doing things the way we should be?

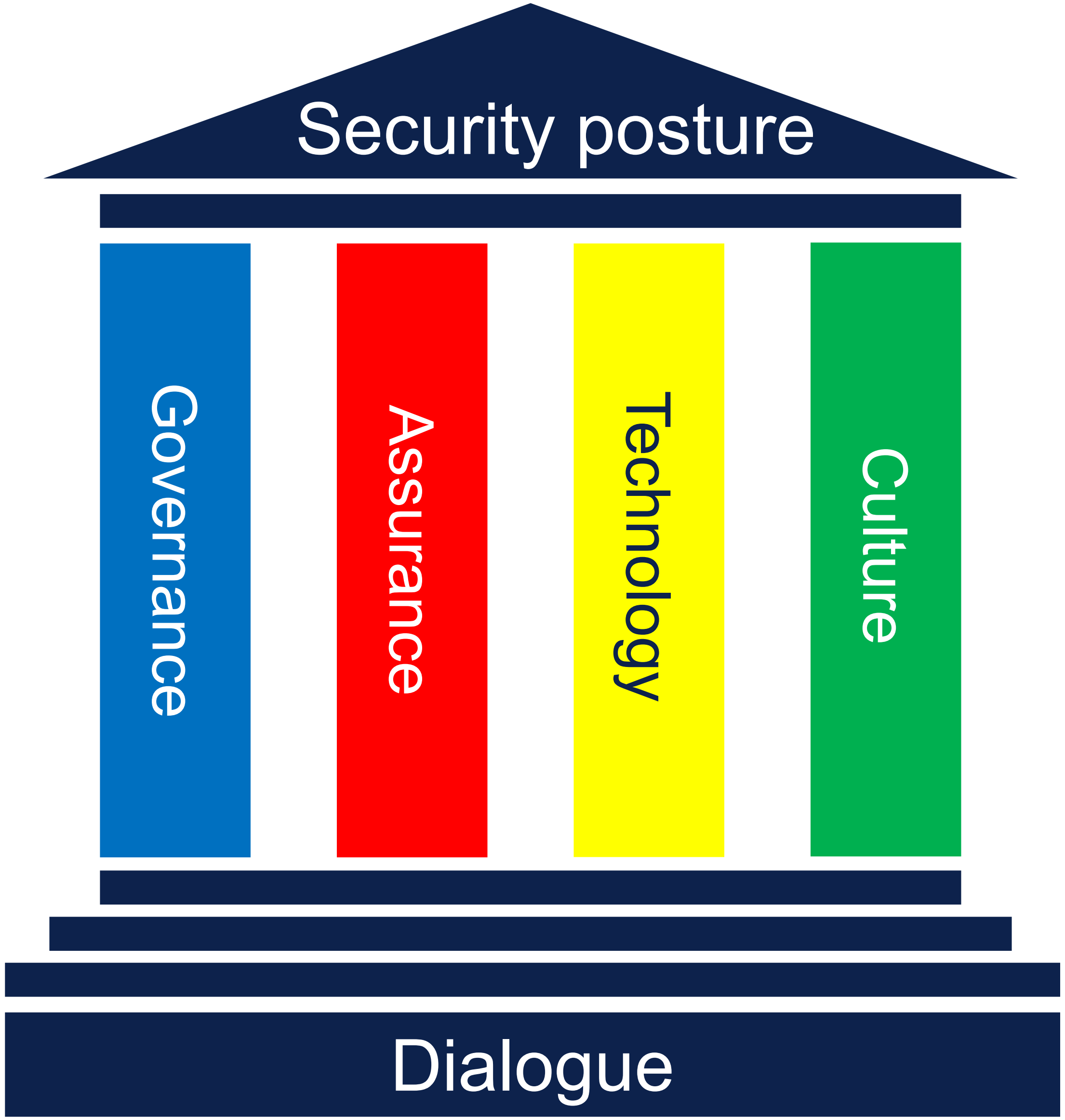
How do we benchmark and demonstrate our capability internally and externally?



Do we have the right technologies, processes and procedures in place?

Are we making best use of them?

Is security integral to our working practices and environments?



Do we train our staff and students about security?

Do we have a positive “no blame” culture?

Do we encourage and promote a security mindset?

▶

1. Do we have a data classification scheme to help identify sensitive information and ensure appropriate protections are in place?

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?

3. Do we review user accounts and systems for unnecessary privileges on a regular basis?

4. Do we enforce multifactor authentication for all systems and users?

5. Do we have a tried and tested process for backing-up critical data in a manner resistant to disasters or cyber attacks?

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?

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?

8. Do we have regularly rehearsed plans to deal with the most likely cyber events or disasters?

9. Are all of our hardware and software products free from vulnerabilities, supported by the vendor and regularly patched?

10. Are our networks separated so that if an attacker gets access to one device, they will not have access to our entire estate?

11. How would our organisation identify an attacker's presence on the network?

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?

13. Are all staff aware of and participate in effective cyber risk management processes?

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?

15. Do we maintain an accurate record of our technology assets, including hardware, software, firmware, peripheral devices and removable media?

16. Do we adequately understand our business-critical services and functions and their associated data, technology and supply chain dependencies?

“…cyber security is a **team sport**, and everyone has their role to play – it can’t just be a problem for anyone to ignore and assume somebody else is solving.”

(Lindy Cameron, NCSC CEO)

https://www.ncsc.gov.uk/speech/annual-review-2021

Thank you

David Batho

Head of Security

David.batho@jisc.ac.uk

help@jisc.ac.uk

jisc.ac.uk