CyBOK

Assessing the cross-disciplinary accessibility of CyBOK

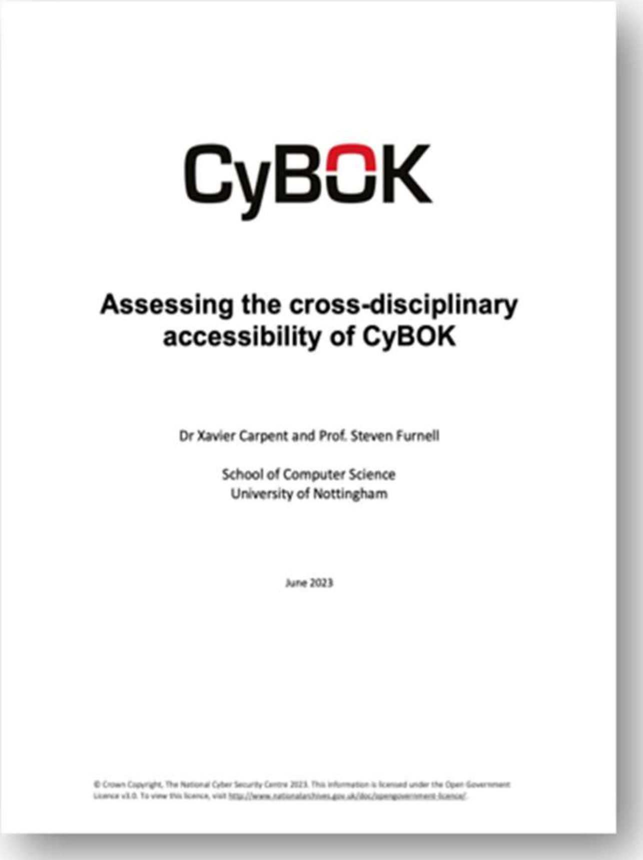
Xavier Carpent, Steven Furnell

University of Nottingham

contact@cybok.org
www.cybok.org

Introduction

- Cyber security commonly associated with computing/IT
- However, clearly relevant to a **wider audience,** e.g.
  - LR KA → law practitioners
  - HORA KAs → business and psychology
- Is CyBOK (in its current state) **accessible** to non-cyber sector?



CyBOK

Assessing the cross-disciplinary accessibility of CyBOK

Dr Xavier Carpent and Prof. Steven Furnell

School of Computer Science
University of Nottingham

June 2023

Our Methodology

- Gathering insights of IT-dependent professionals in non-security roles and non-tech sectors

- Establishing perception of cyber security + what is relevant in their context

- Identifying where sector has need for/contributes towards cyber security

Research Phases

- **Phase I: Online Survey**
  - Base statistics
  - Participants' perception of cybersecurity
  - What is relevant in the context of their discipline/sector
  - Capturing key words or phrases (KWoPs)
  - Attempt to map against CyBOK

  - 15 GBP vouchers incentive

  - 33 participants from various sectors

Research Phases

- **Phase II: Discussion Workshops**
  - Determine whether material covers expected aspects
  - Presentation (phrasing + level of content) meaningful?
  - How would content need to be reframed to make it accessible?
  - ~1h online workshop

  - 30 GBP vouchers incentive

  - 13 participants (grouped in 4 sector-specific workshops)
    - Includes a "cyber" workshop, for baseline

Phase I: Approach

CyBOK

- List any keywords or phrases that you **associate** with the cyber security **needs** of your organisation
- List any other keywords or phrases that you **associate** with cyber security as a **topic**
- Identify any topics that you feel that your sector **contributes** to cyber security

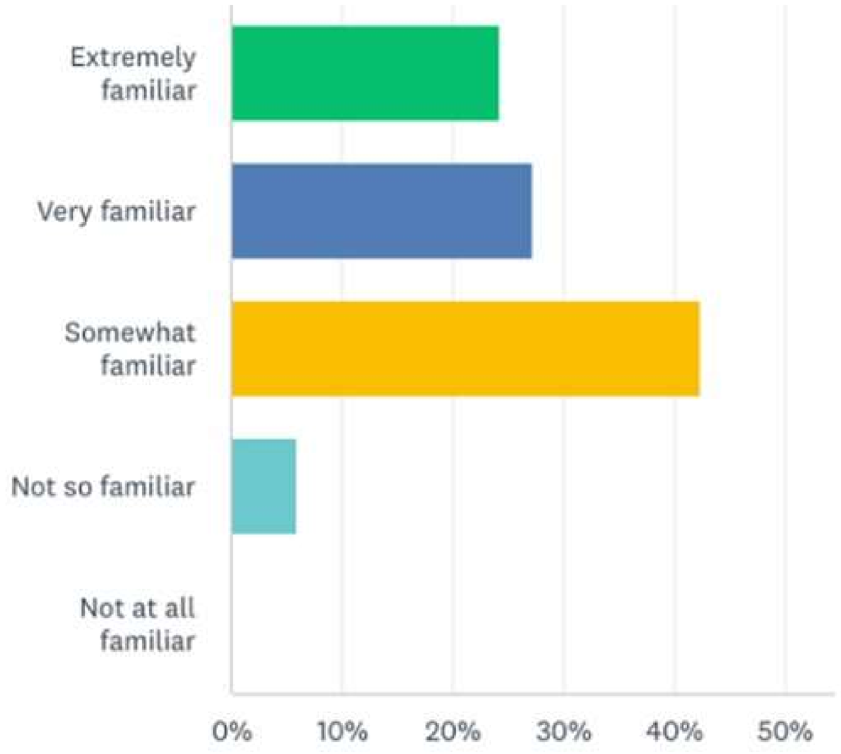
Basis for identifying indicative KWoPs from the sector

- Indicate your **understanding** of the different CyBOK Knowledge Areas and their **relevance** to your organisation

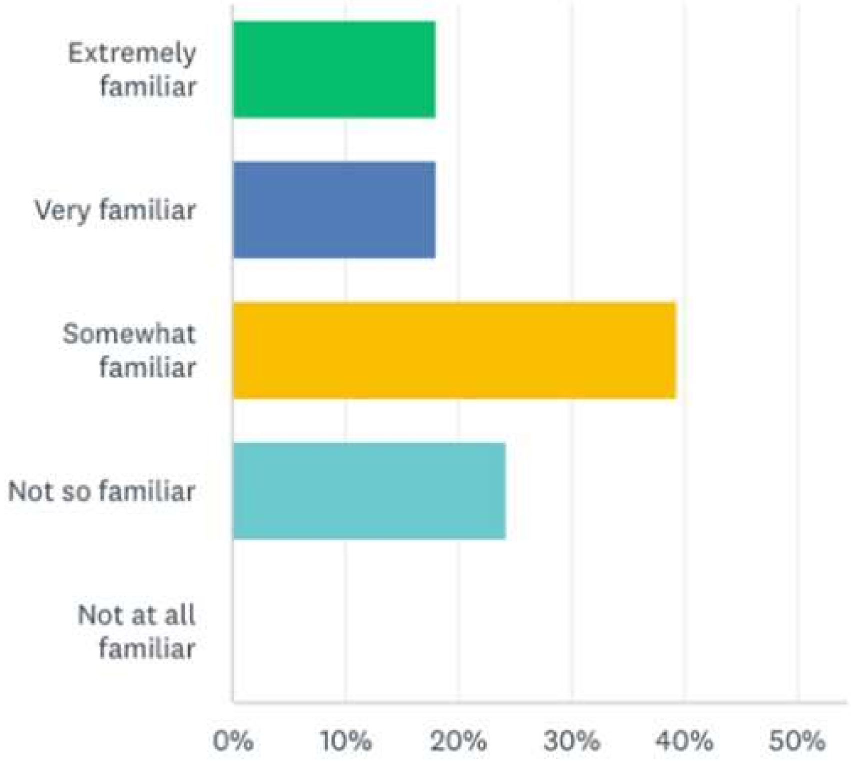
Indication of how ’meaningful’ the top-level descriptors are

Phase I: Results

CyBOK

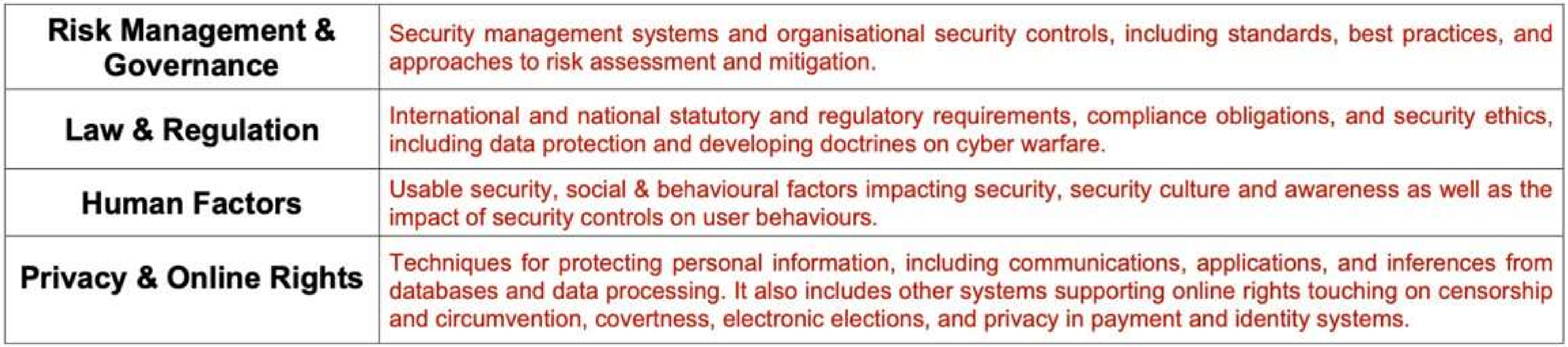


Familiarity with IT



Familiarity with Cybersecurity

Phase I: Results

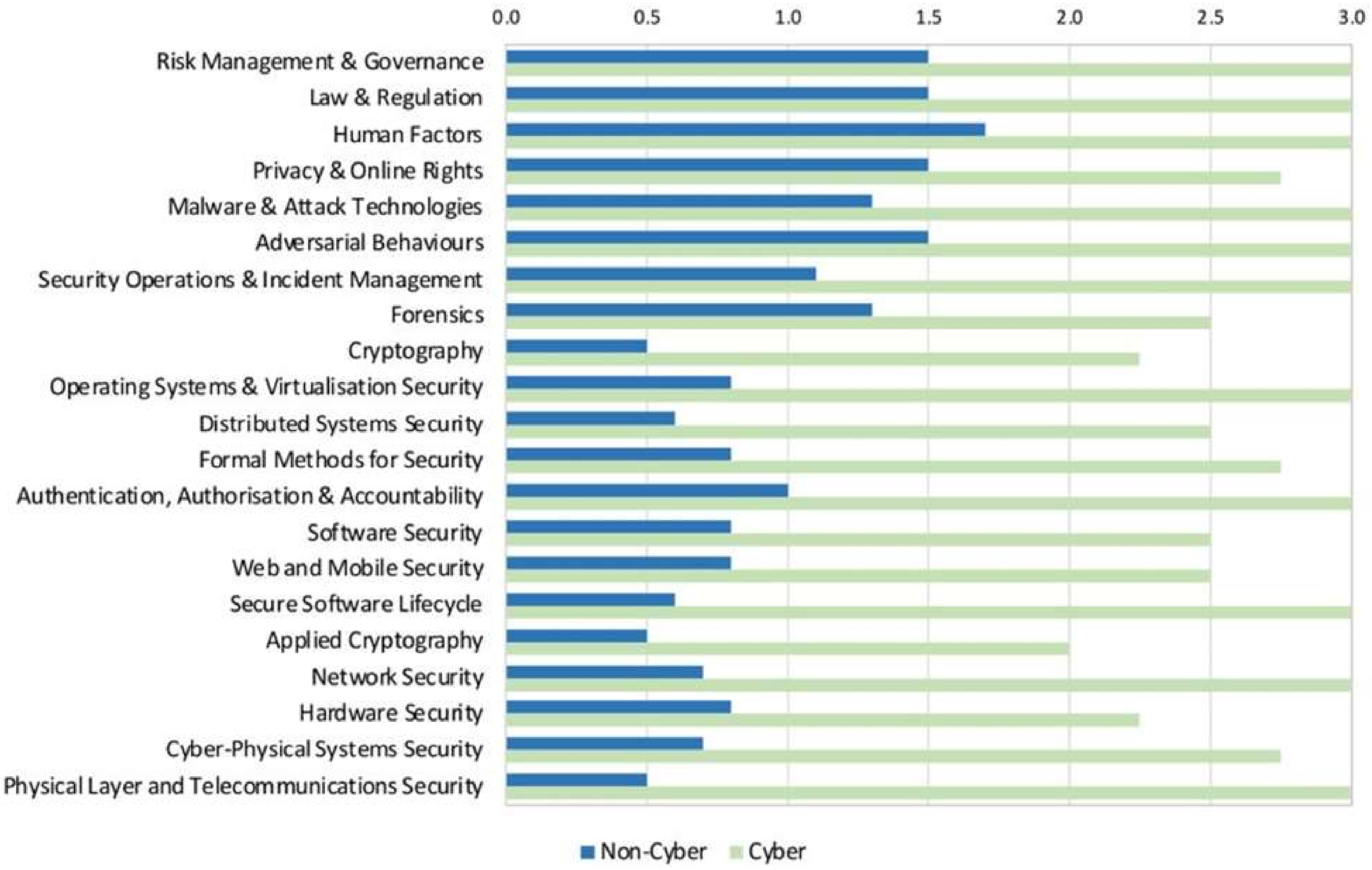


Risk Management & Governance	Security management systems and organisational security controls, including standards, best practices, and approaches to risk assessment and mitigation.
Law & Regulation	International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare.
Human Factors	Usable security, social & behavioural factors impacting security, security culture and awareness as well as the impact of security controls on user behaviours.
Privacy & Online Rights	Techniques for protecting personal information, including communications, applications, and inferences from databases and data processing. It also includes other systems supporting online rights touching on censorship and circumvention, covertness, electronic elections, and privacy in payment and identity systems.

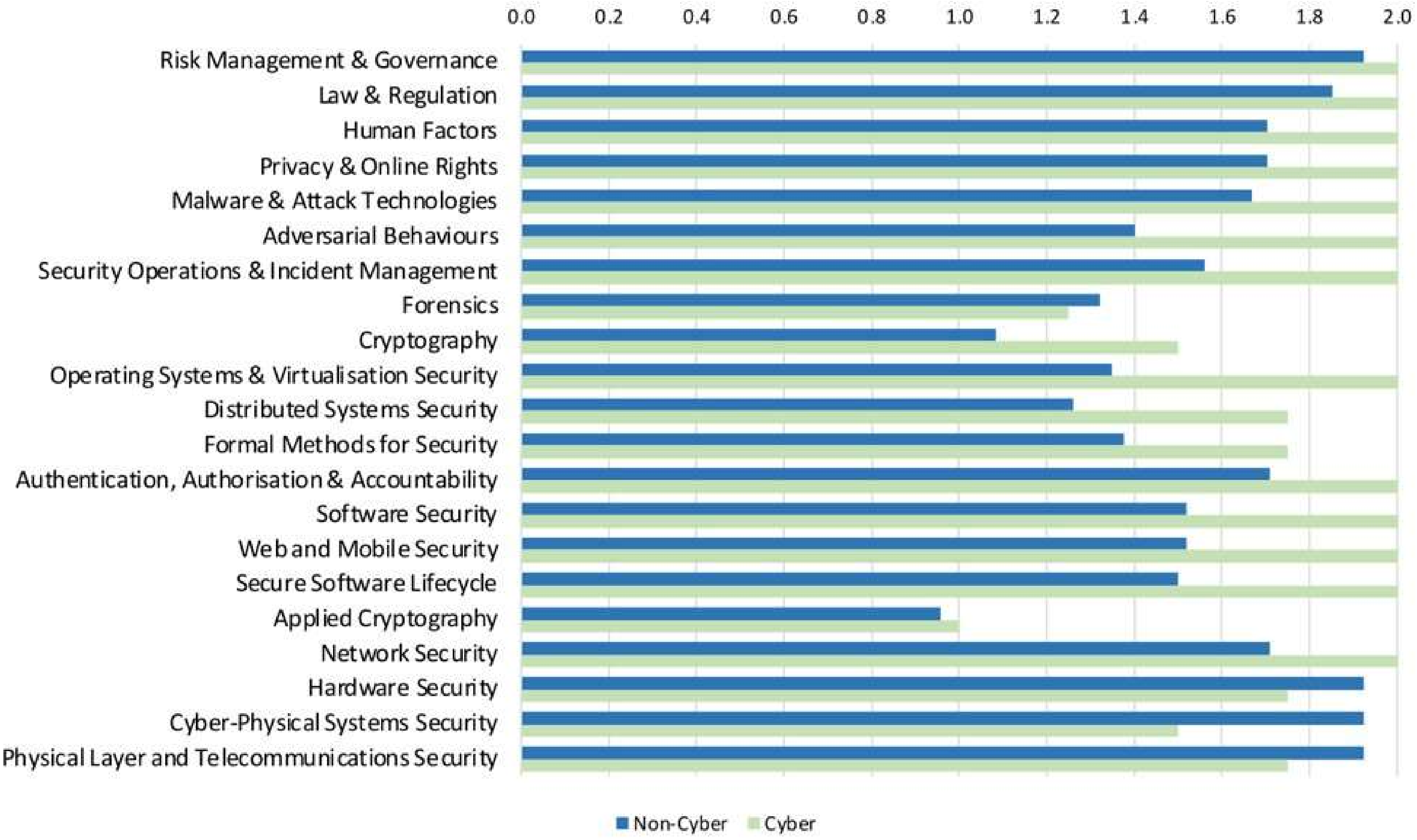
1. "Indicate **understanding** of different CyBOK KAs"
2. "Indicate perception of **relevance** of each KA to your organisation"

Phase I: Results

CyBOK



Phase I: Results



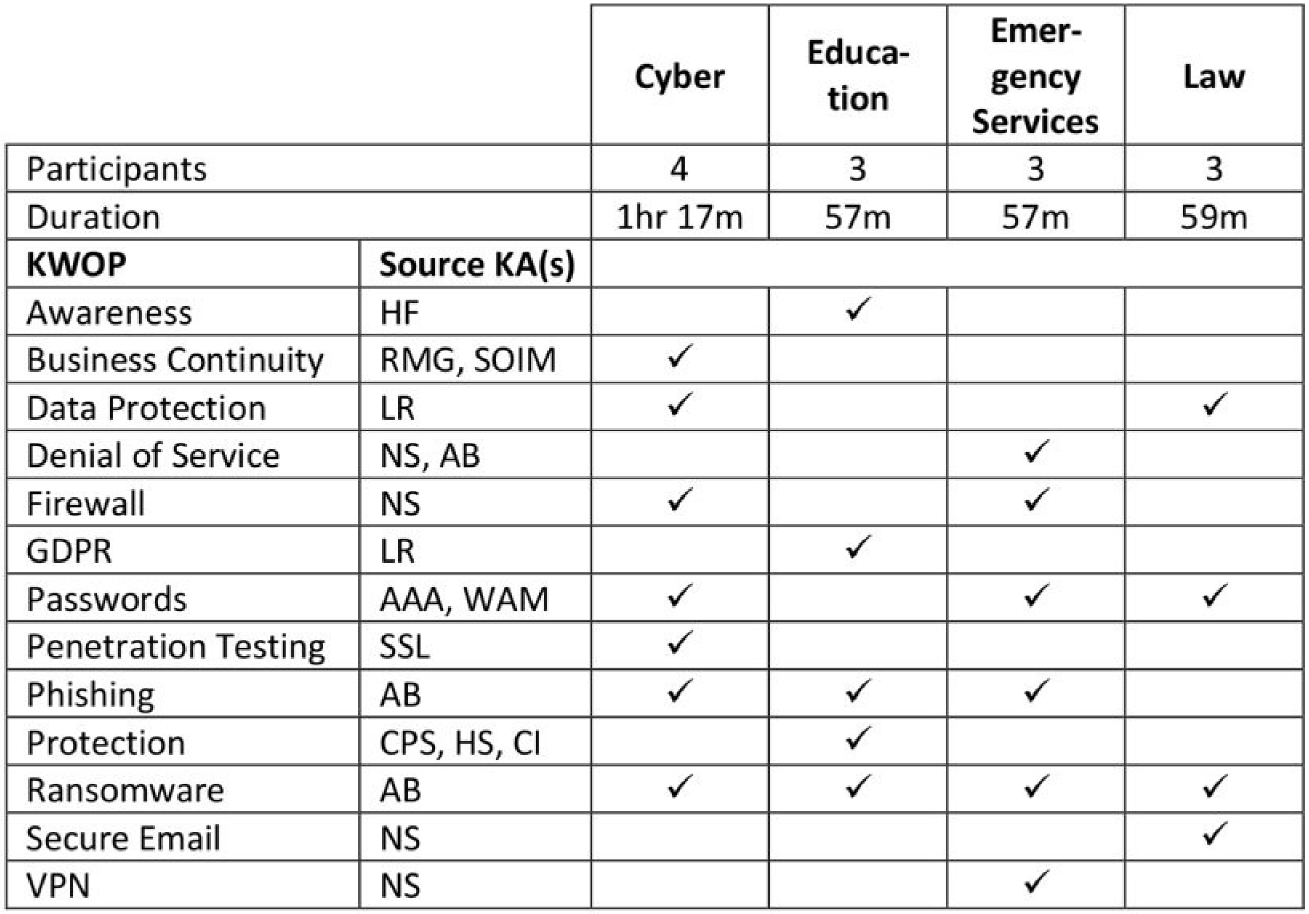
Phase I: Example Results (Law Sector)

- *Please list any keywords or phrases that you associate with cyber security needs of your organisation*
  - Encryption. Password. Confidential. Data Protection. Secure Backup
  - Hacking Data Protection
  - Privacy Sensitivity of data Data protection Personal information Encryption VPN Remote access Shared drive access Password Secured Drive Redaction of documents Secure e-mail accounts
  - Passwords, passcodes, dual authentication, secure email

Phase I: KWoP example mappings

KWoP	KA Mapping
Ransomware	SOIM AB LR MAT CPS RMG Also ‘Ransomware Detection’ in MAT
Secure email	Not found However, a range of KAs are associated with ‘Email’:
	EMAIL - WAM EMAIL ACCOUNT - LR EMAIL ADDRESS – AB AAA POR SOIM HF MAT EMAIL AND MESSAGING SECURITY - NS EMAIL ATTACHMENT - MATWAM EMAIL CLIENT - SOIM EMAIL ENCRYPTION - HF EMAIL LIST - AB EMAIL MESSAGE - F EMAIL REGULATION - AB EMAIL SECURITY SOLUTION - NS EMAIL SERVER – NS SOIM AB LR EMAIL SPAM - AB EMAIL SYSTEM - AAA POR SOIM HF PLT

Phase II: Workshops and KAs Discussed



		Cyber	Education	Emergency Services	Law
Participants		4	3	3	3
Duration		1hr 17m	57m	57m	59m
KWOP	**Source KA(s)**				
Awareness	HF		✓		
Business Continuity	RMG, SOIM	✓			
Data Protection	LR	✓			✓
Denial of Service	NS, AB			✓	
Firewall	NS	✓		✓	
GDPR	LR		✓		
Passwords	AAA, WAM	✓		✓	✓
Penetration Testing	SSL	✓			
Phishing	AB	✓	✓	✓	
Protection	CPS, HS, CI		✓		
Ransomware	AB	✓	✓	✓	✓
Secure Email	NS				✓
VPN	NS			✓	

Phase II: Key Findings

- Accessibility experience for non-cyber audience is **mixed**

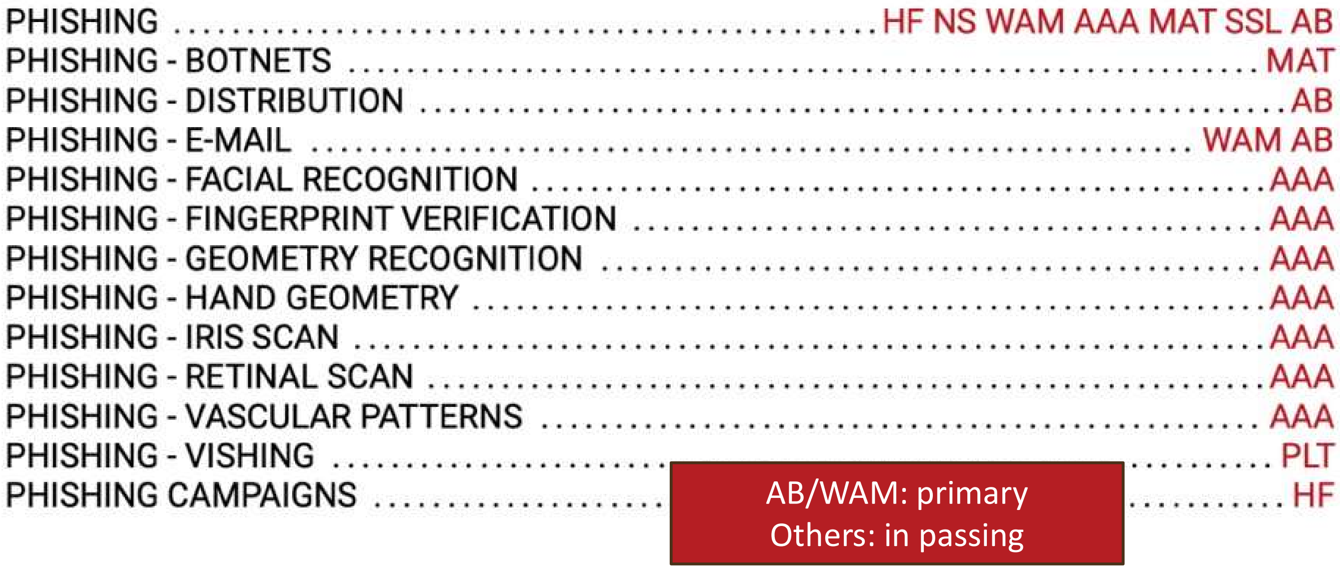
- Key issues:

  1. Locating the material
     - CyBOK’s Mapping Reference

  2. Understanding the material
     - Depends on background and KAs
     - Various comments and feedback

Phase II: Locating the Material

- Unclear introduction/entry point
- Often many different mappings with no clear primary



PHISHING	HF NS WAM AAA MAT SSL AB
PHISHING - BOTNETS	MAT
PHISHING - DISTRIBUTION	AB
PHISHING - E-MAIL	WAM AB
PHISHING - FACIAL RECOGNITION	AAA
PHISHING - FINGERPRINT VERIFICATION	AAA
PHISHING - GEOMETRY RECOGNITION	AAA
PHISHING - HAND GEOMETRY	AAA
PHISHING - IRIS SCAN	AAA
PHISHING - RETINAL SCAN	AAA
PHISHING - VASCULAR PATTERNS	AAA
PHISHING - VISHING	PLT
PHISHING CAMPAIGNS	HF

AB/WAM: primary
Others: in passing

Phase II: Understanding the Material

CyBOK

- Varies depending on KA
- E.g., Law sector: DP "written for lawyers" → digestible for them, but others?
- Technical terminology and acronyms: not accessible
- KAs written for different audiences, depending on perspective of author(s)
- Clarity (for given reader) varies across KAs (and sometimes within)
- Not specific to technical topics
  - E.g. "passwords" in different KAs landing very differently
- Idea evoked by participants: splitting technical non-technical descriptions
- Participants positively surprised that CyBOK free and available to all

Phase II: Cyber Sector Respondents

CyBOK

- Different perspective
- Accuracy and currency of some of the content (sometimes disagreeing with it)
- Various definitions/descriptions deemed outdated or too restricted
- Some others considered niche within the context of CyBOK

- Sheds light on problem of **maintaining** CyBOK's content to remain **current**
- Targeted at **academic** audience?
- Not possible/difficult to **dual-purpose** (practitioners + non-practitioners)

Phase II: Misc Comments

- Form factor: not ideal **accessibility** and **maintainability**
  - **Wikipedia**-like platform? (cross-referencing, etc.)

- Rapidly **evolving** nature of the discipline
  - Ability of the current format to remain **up-to-date**?

Conclusions

CyBOK

- CyBOK not *yet* ideally positioned for use by non-cyber sectors
  - **Accessibility** is mixed
  - Mapping Reference not fit to rapidly find primary source of information

- "**Sector Lens**" approach for CyBOK?
  - Clearly relevant for a wider audience
  - But challenging to realize (with the current content/structure)
  - Worth exploring further

- Insight for future direction for CyBOK?
  - Granular and layered
  - Audience in mind
  - Maintainability and agility

Thank you!

CyBOK

xavier.carpent@nottingham.ac.uk
steven.furnell@nottingham.ac.uk