CyBOK

A Framework for Organisational Knowledge Profiles

Awais Rashid, *Professor of Cyber Security, University of Bristol*
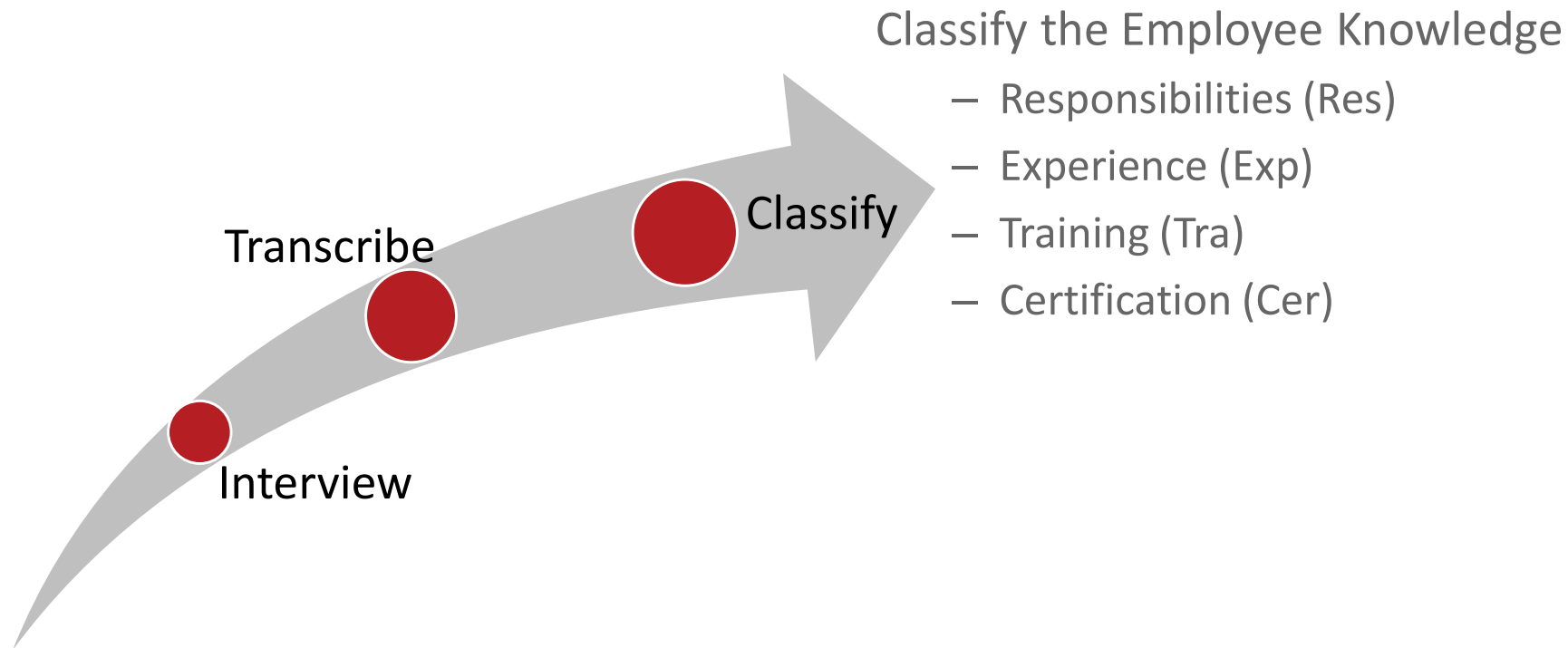**Lata Nautiyal,** *Research Associate, University of Bristol*

Benchmarking Knowledge Capacity in Organisations

- Identify where the focus lies, for example:

  - where the organisation needs to evolve its cyber security expertise; or
  - where such expertise may be outsourced drawing in knowledge capability from third parties.

- The CyBOK Knowledge Profile Framework can also be used as a basis for assessing the knowledge capability of such a third party.

Case Studies: Three teams (each from a different organization)

Interview

Transcribe

Classify

Classify the Employee Knowledge
- Responsibilities (Res)
- Experience (Exp)
- Training (Tra)
- Certification (Cer)

CyBOK Organisational Knowledge Profiling Framework

Built on top of the mapping framework and resources

- Professional Certification programme mappings.
- CyBOK Mapping Reference 1.2 (>8000 concepts mapped to CyBOK 1.0)
- CyBOK Knowledge Trees
- CyBOK Knowledge Area Text
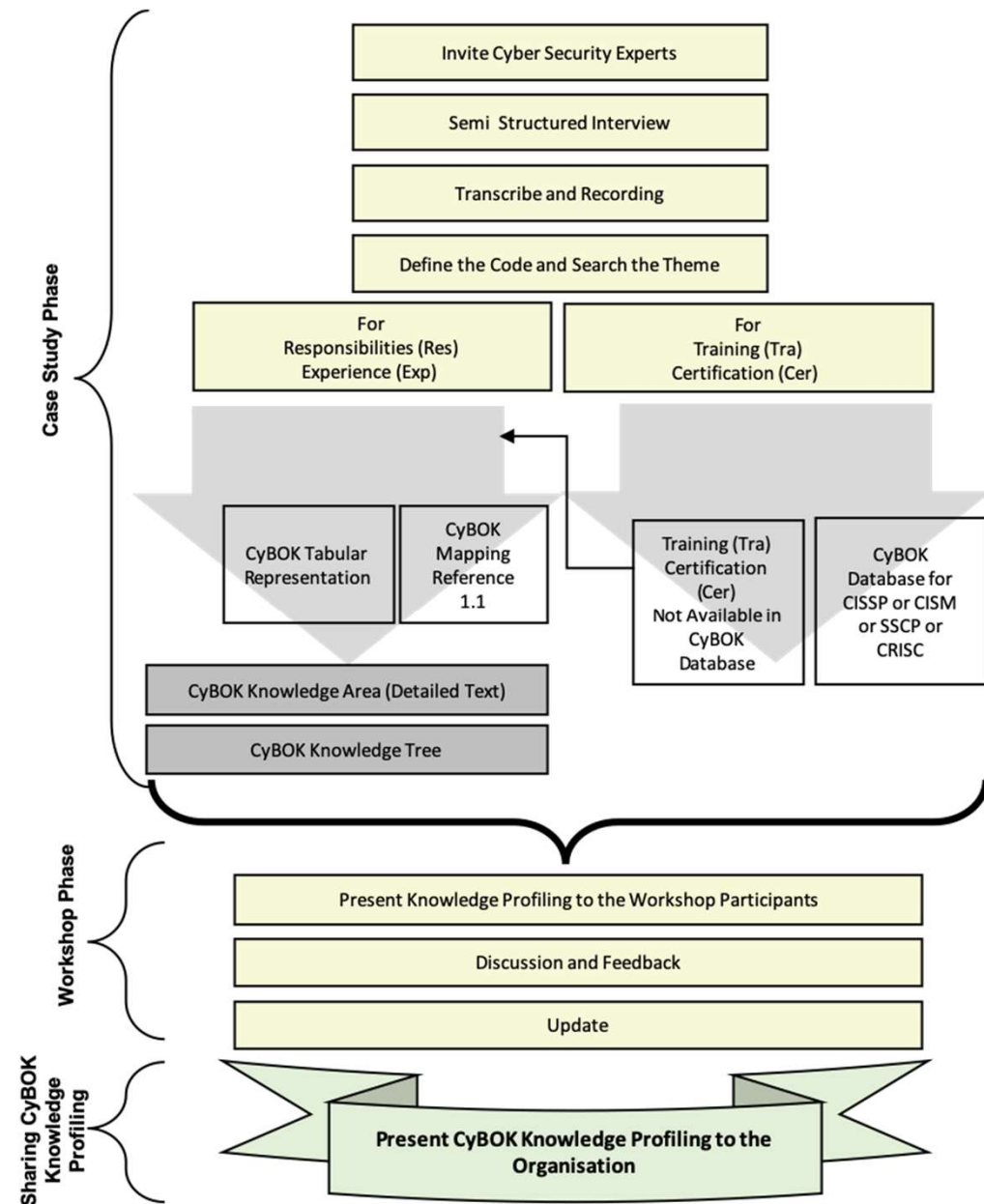
Knowledge Profiling Approach

- For each employee/team identify the **mapped** qualifications
  - These may be professional programmes such as CISSP, CISM, etc. resulting from the CyBOK Mapping framework with spider charts and bar charts as outcomes
  - These may also be NCSC certified degrees for which such mappings are available

- Initial knowledge profile = U U
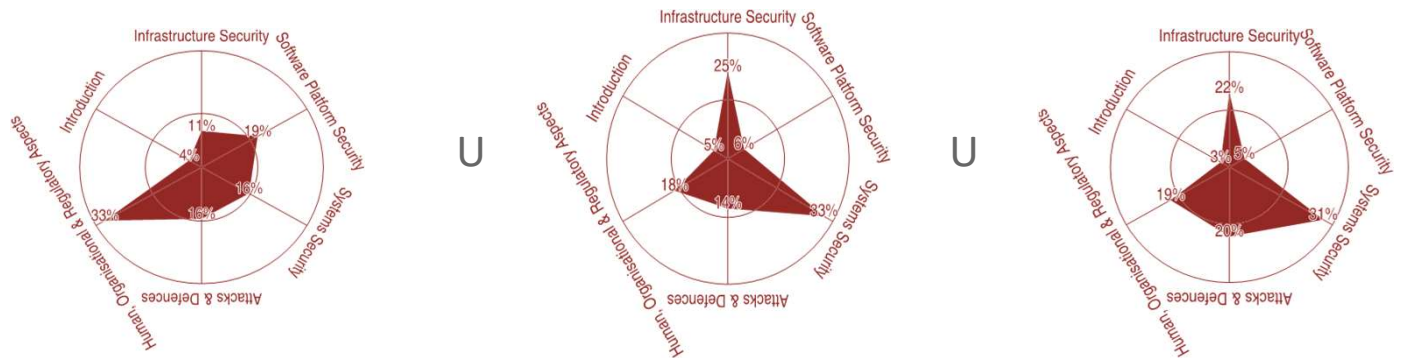
- For each employee/team for non-mapped training:
  - identify the list of topics that they have covered
  - map using CyBOK Mapping Framework for Professional Certification Programme

- Union with the Initial Knowledge Profile to derive the overall knowledge profile.

Knowledge Profiling of employee A1

Responsibilities –

Knowledge Listing S.No.	Cumulative Responsibiliti (Res) Knowledge Listing
Res_1	cyber incident director
Res_2	cyber threat intelligence.

U

Experience –

Knowledge Listing S.No.	Cumulative Experience (Exp) Knowledge Listing
Exp_1	Cloud-based solutions
Exp_2	Risk management

U

Training –

Knowledge Listing S.No.	Cumulative Certification (Tra) Knowledge Listing
Tra_1	Advanced IDS Concepts
Tra_2	DNS

U

Certification –

Knowledge Listing S.No.	Cumulative Certificatio Knowledge Listing
Cer_1	CISSP
Cer_2	CISM
Cer_3	ISO 27001 lead auditor

Knowledge Profile of employee A1
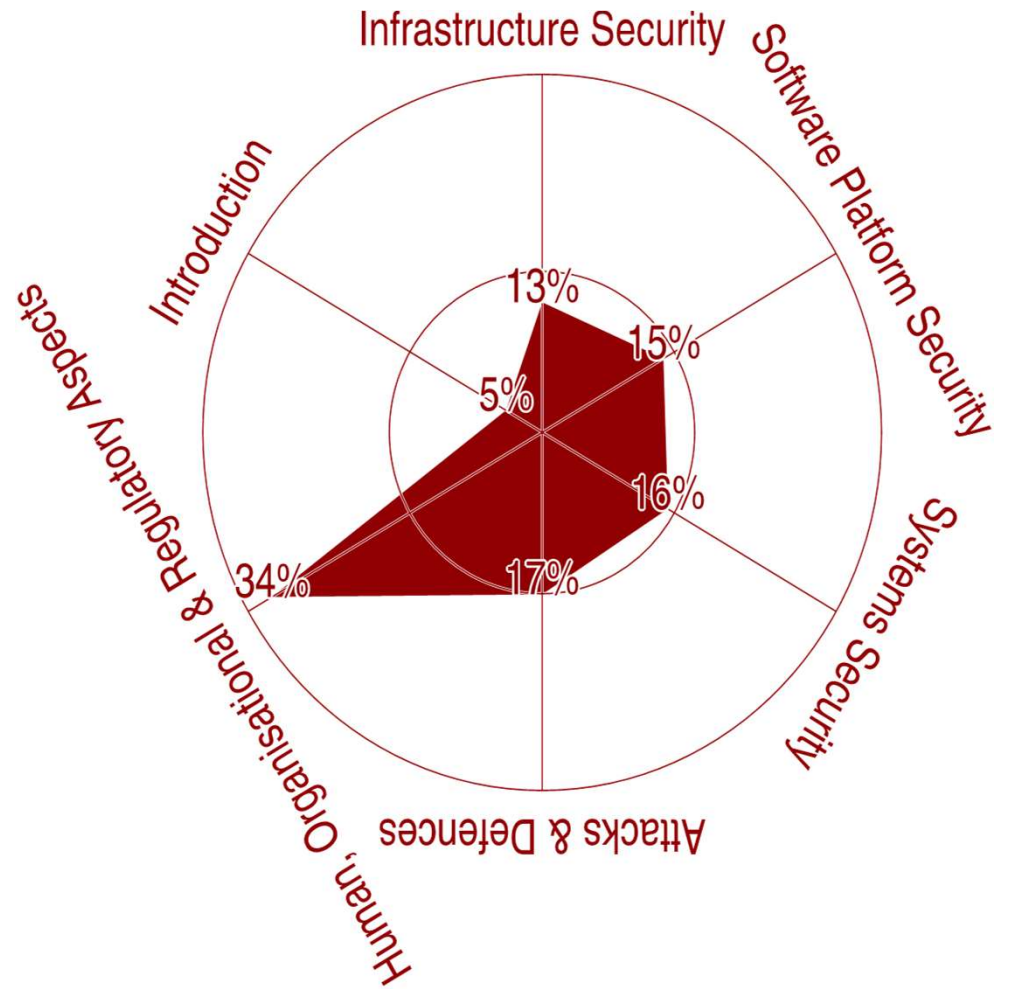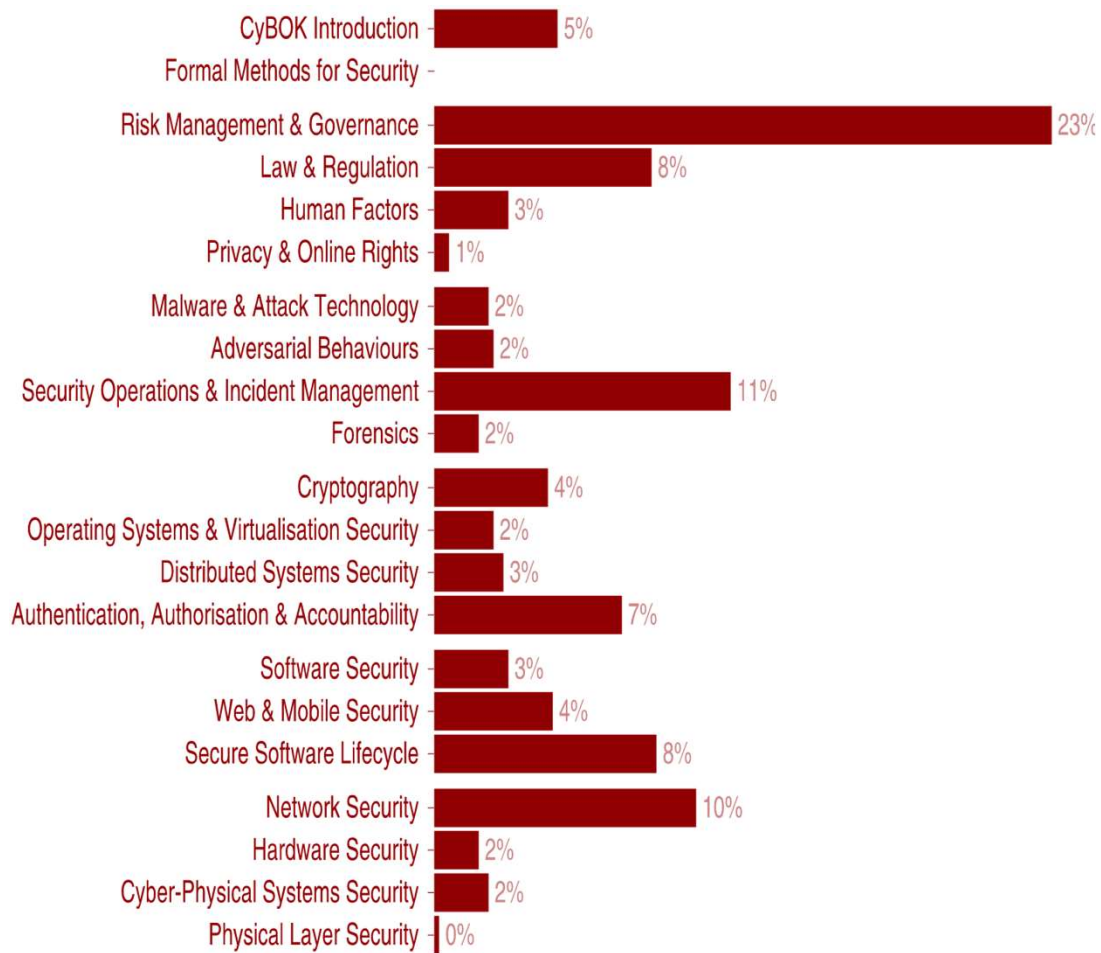
Knowledge Profiles of employee A2 and A3

Employee A2 (left chart):

Category	Value
CyBOK Introduction	6%
Formal Methods for Security	
Risk Management & Governance	9%
Law & Regulation	8%
Human Factors	2%
Privacy & Online Rights	1%
Malware & Attack Technology	3%
Adversarial Behaviours	2%
Security Operations & Incident Management	9%
Forensics	2%
Cryptography	6%
Operating Systems & Virtualisation Security	3%
Distributed Systems Security	3%
Authentication, Authorisation & Accountability	10%
Software Security	3%
Web & Mobile Security	7%
Secure Software Lifecycle	11%
Network Security	10%
Hardware Security	3%
Cyber-Physical Systems Security	3%
Physical Layer Security	0%

Employee A3 (right chart):

| Category	Value
CyBOK Introduction	5%
Formal Methods for Security	
Risk Management & Governance	9%
Law & Regulation	5%
Human Factors	2%
Privacy & Online Rights	2%
Malware & Attack Technology	1%
Adversarial Behaviours	2%
Security Operations & Incident Management	10%
Forensics	1%
Cryptography	14%
Operating Systems & Virtualisation Security	2%
Distributed Systems Security	2%
Authentication, Authorisation & Accountability	14%
Software Security	0%
Web & Mobile Security	2%
Secure Software Lifecycle	4%
Network Security	19%
Hardware Security	2%
Cyber-Physical Systems Security	2%
Physical Layer Security	2%

Knowledge Profile of Organisation Alpha – Based on the Union of Profile A1, A2, A3.. An
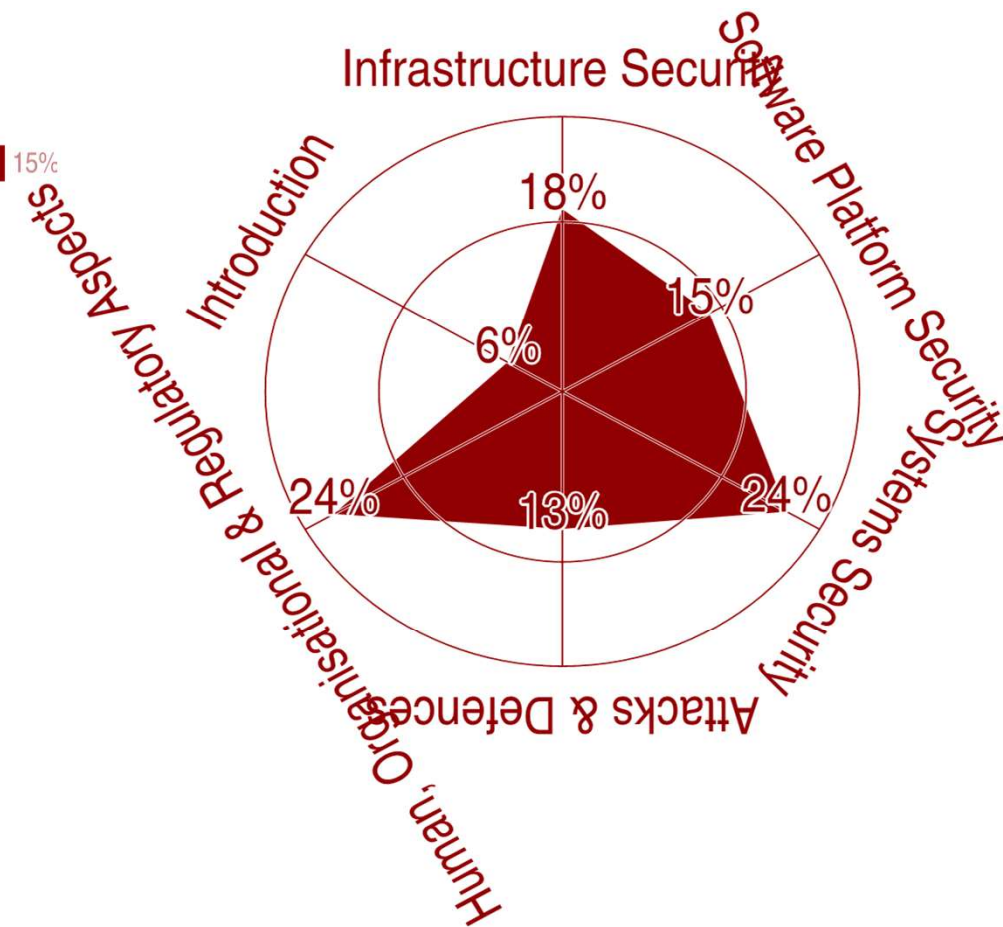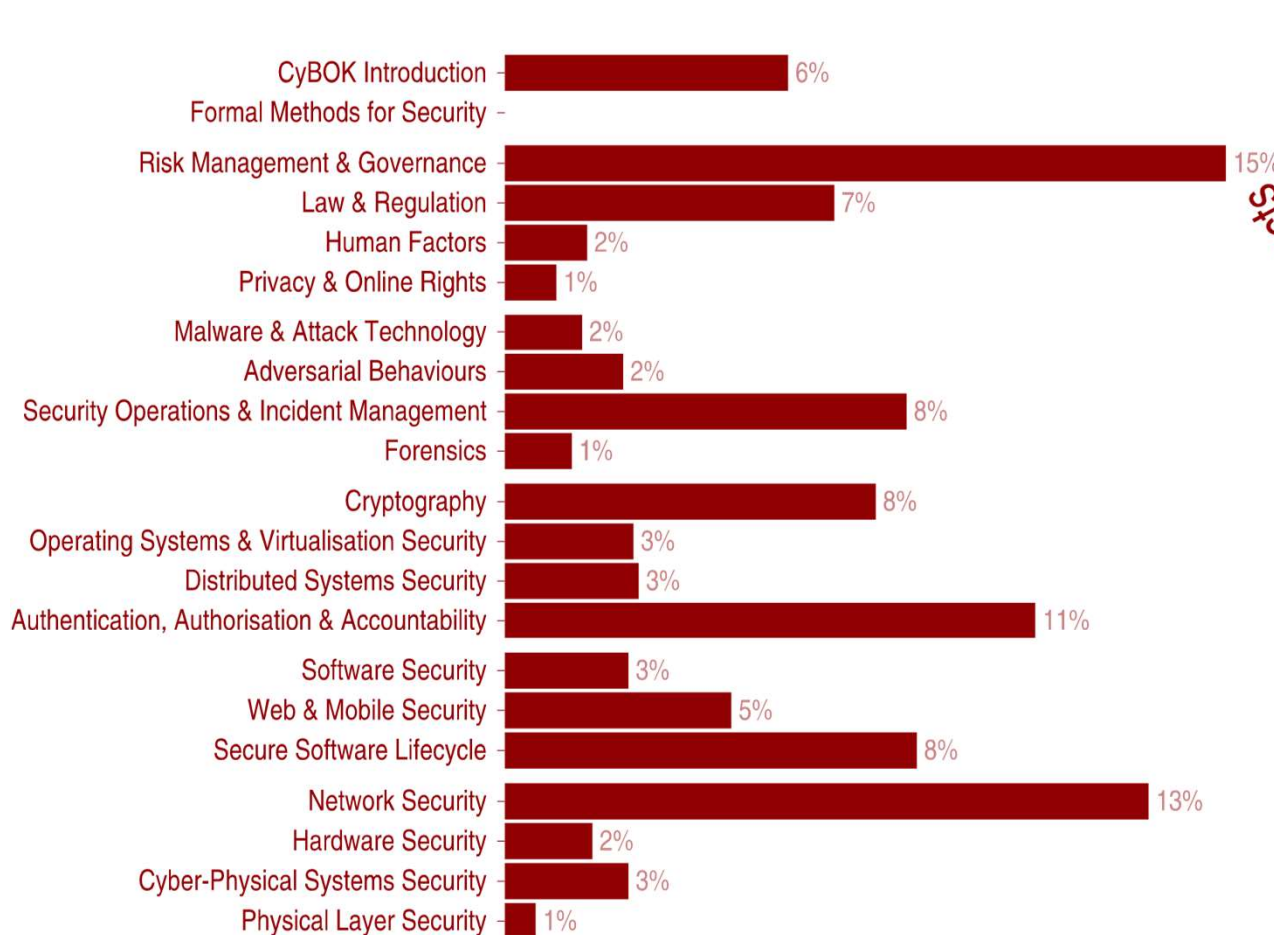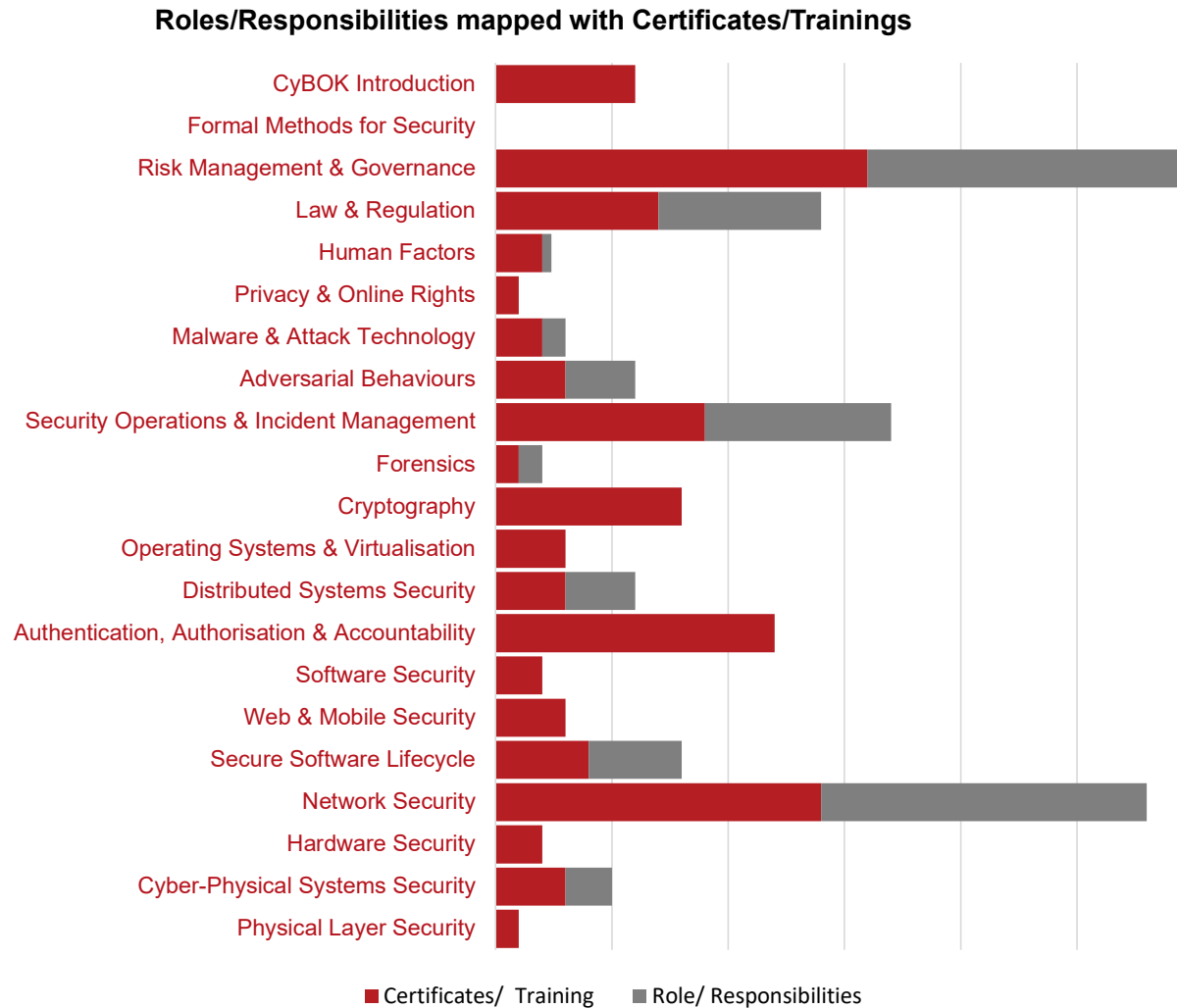
Phase 2: Workshops to gain feedback on the initial framework

- Two workshops: 1.5 hours each
- Eight attendees from industry and practitioner organisations
- Focus group discussion on the knowledge profile framework – what would work well; what needs to change/evolve?

What knowledge is "current" – Employee A1

Roles/Responsibilities mapped with Certificates/Trainings
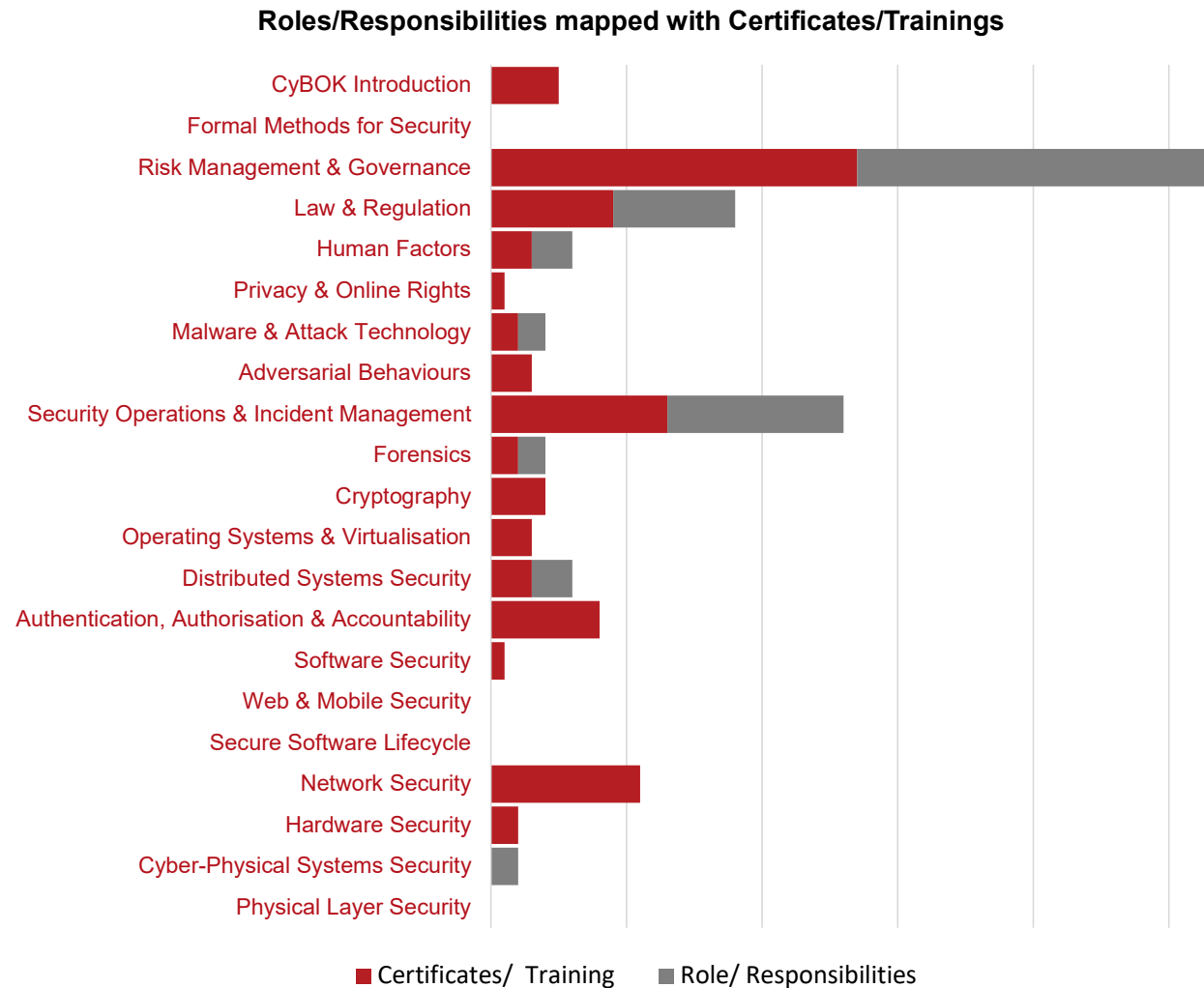
What knowledge is "current" – across the organisational profile

Roles/Responsibilities mapped with Certificates/Trainings

What type of visualisation and for whom?