CyBOK

The role of CyBOK in addressing recruitment challenges

Peter Loomes
Head of Training - The IASME Consortium

contact@cybok.org
www.cybok.org

Recruitment

- Questions:

  - How do we attract good people?
  - How do employers understand what they need?
  - How do we decode the profession?
  - Is there a skills shortage?

Jobs

- Excellent written, verbal, report writing and presenting skills.
- Excellent time management, planning, and organisational skills,
- Demonstrable Cyber / Information Security knowledge and experience.
- Good understanding of Risk Management and Security assessments within an IT or Security environment.
- Good understanding of Information Technology and software development vulnerabilities and risks.
- Experience of managing multiple streams of work.
- Knowledge of secure software development lifecycles and software security vulnerabilities.
- Awareness of threat modelling techniques.
- Awareness of secure software frameworks and guidelines such as OWASP, and NIST.
- A passion for detail and accuracy.
- An ability to analyse complex problems and understand root causes. Articulate, with the ability to explain things in non-technical language at all levels.
- Self-motivated with a desire to learn about new and evolving technologies, and associated Security threats, by seeking out resources to support personal development.

Role:

Run the Cyber Command Centre activities including SOC and Incident Response.

Main point of contact for Cyber incidents and Cyber escalations.

Focus on developing the SIEM further towards maturity.

Train and govern level 1 and 2 analysts

Produce metrics and reporting to accurately display the performance of the Cyber Operations program.

Requirements

A self-starter who can take initiative and make their ideas happen

Enthusiasm and a willingness to learn

An ability to work effectively under pressure

Forensic attention to detail

Sense of humour

Your Purpose

You will be responsible for assuring the safety of corporate data through the implementation of robust architecture, security standards and technology to manage security threats.

You will proactively work with the company to implement practices that meet policies and standards for cyber security.

Lead the cyber security function across the company to ensure consistent and high-quality information security management

- Review, strengthen and audit the company's disaster recovery and business continuity process
- Liaise with many teams across IT to build effective security and enterprise architectures
- Liaise with external agencies to ensure that the company sustains a strong security posture and is well-informed of relevant threats
- Promote and maintain a high level of security awareness throughout the business Your experience
- Working knowledge of cyber security technologies covering the corporate infrastructure
- Demonstrable understanding of disaster recovery and business continuity
- Experience in Multi Factor Authentication, Wireless Access Points and Enterprise Servers
- Demonstrable technical ability across a wide range of IT technologies and a good knowledge of industry standards and best practices

Cyber Security Specialist

Qualification Soup

CyBOK

ISO 27001Lead Auditor

ISO 27001 Lead Implementer

CISSP

CISM

C/CISO

MSc

CCP

CSTM
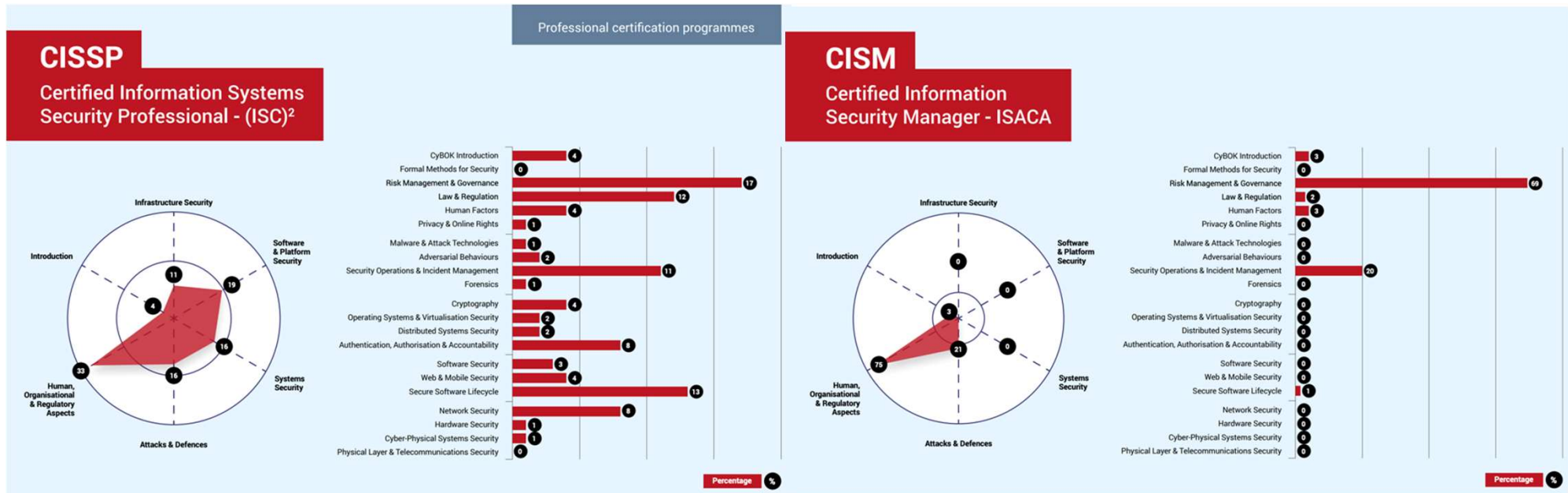
CSTL

ECSA

Security+

CEH

GSEC

SSCP

CASP

GCIH

OSCP

The qualification tautology

The successful candidate must hold the CISSP and CISM certifications
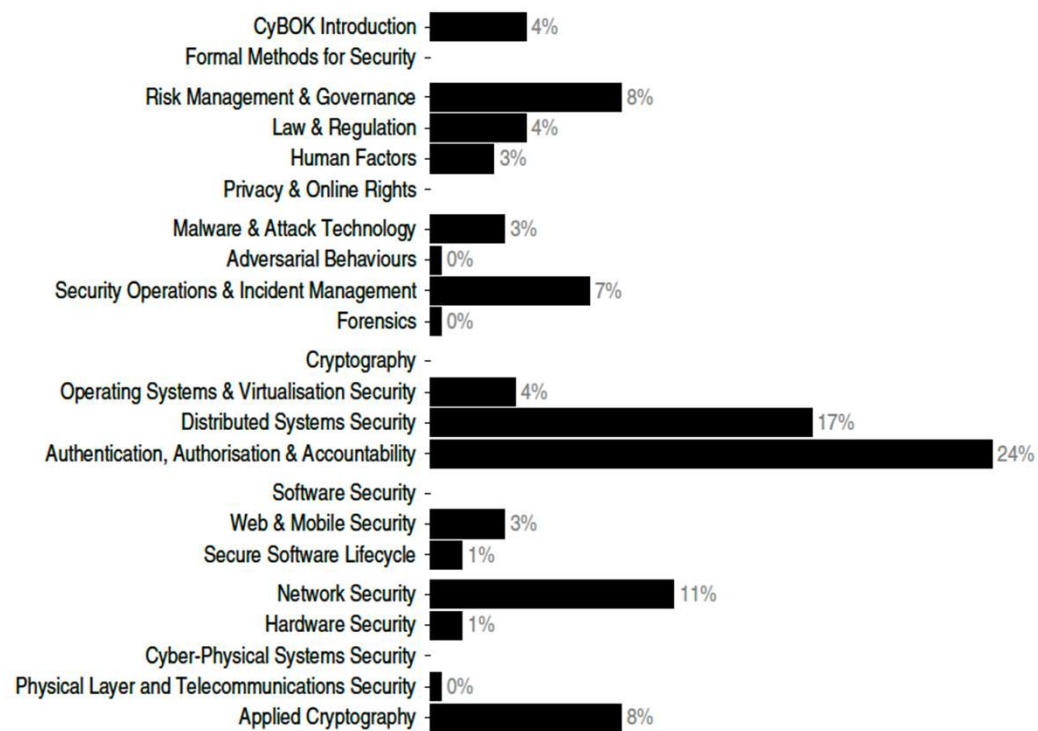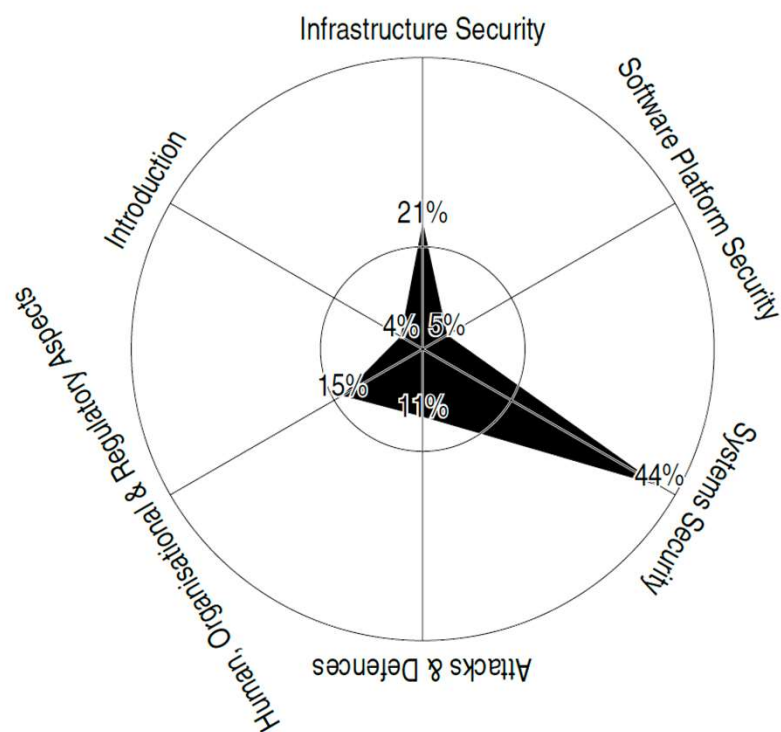
The Recruitment Industry

CyBOK

Infrastructure Security

Software Platform Security

Introduction

21%

4% 5%

15%

11%

44%

Systems Security

Human, Organisational & Regulatory Aspects

Attacks & Defences

CyBOK Introduction	4%
Formal Methods for Security	–
Risk Management & Governance	8%
Law & Regulation	4%
Human Factors	3%
Privacy & Online Rights	–
Malware & Attack Technology	3%
Adversarial Behaviours	0%
Security Operations & Incident Management	7%
Forensics	0%
Cryptography	–
Operating Systems & Virtualisation Security	4%
Distributed Systems Security	17%
Authentication, Authorisation & Accountability	24%
Software Security	–
Web & Mobile Security	3%
Secure Software Lifecycle	1%
Network Security	11%
Hardware Security	1%
Cyber-Physical Systems Security	–
Physical Layer and Telecommunications Security	0%
Applied Cryptography	8%

CyBOK

Responsibilities

1. Understand and document the threats to the organisation
2. Determine the vulnerabilities within the business
3. Analyse the possibility of issues arising
4. Make recommendations on reducing the risk

Job

Risk and Compliance Manager

CyBOK

What can we do?

- Work with:
  - Industry recruiters.
  - Industry leaders.
- Define a couple of roles
- Map roles to CyBOK
- Identify way to simplify mapping

Questions?

CyBOK