Building a Professional Cyber Security Workforce

Recognising Knowledge, Experience and Competence

Prof. Steven Furnell
Chair, IFIP Technical Committee 11

steven.furnell@nottingham.ac.uk

Short of what we need?

• (ISC)² Cybersecurity Workforce Study 2020 found that 64% of organisations reported some level of skills shortage
  • 42% characterized it as a slight shortage, 22% as significant
  • 56% considered themselves at moderate or extreme risk as a result
  • a global skills gap of 3.12 million

• What do we need to fill the gap and how to we recognise it?
  • different things (e.g. qualifications, certifications etc) signify different characteristics
  • e.g. qualifications don’t guarantee experience, and even the most widely known certifications don’t signify competence
No shortage of certifications ...

https://pauljerimy.com/security-certification-roadmap/

Some sense of structure?

- **Focus**
  - Broad (wide topic coverage)
  - Narrow (technology or product specific)

- **Skills**
  - General / Theoretical
  - Technical / Hands-on

- **Academic qualification**
  - (e.g. BSc/MSc course)

- **General Professional certification**
  - (e.g. CISSP, CISM)

- **Role-based certification**
  - (e.g. GCIA, CEH)

- **Vendor or technology-specific certification**
  - (e.g. Cisco Cybersecurity Specialist)
Knowledge, Experience, Competence?

Candidates must hold suitable entry qualifications and then study for n years, completing university-designed assessments.

No prior practitioner experience needed. Examined via 90 min exam based upon multiple choice and performance-based questions.

Candidates must have a minimum of 5 years cumulative paid full-time work experience in 2 or more of the 8 domains of the CISSP CBK.

---

CyBOK

19 Knowledge Areas

1. Risk Management & Governance
2. Cyber Physical Systems
3. Law & Regulation
4. Physical Layer and Telecommunications Security
5. Human Factors
6. Secure Software Lifecycle
7. Privacy & Online Rights
8. Operating Systems & Virtualisation Security
9. Adversarial Behaviours
10. Malware
11. Network Security
13. Cryptography
14. Software Security
15. Authentication, Authorisation & Accountability (AAA)
16. Web & Mobile Security
17. Hardware Security
18. Distributed Systems Security
19. Forensics
CIISec Developing Capability

CIISec Skills Framework

“Describes the range of competencies expected of Information Security and Information Assurance Professionals in the effective performance of their roles”
In more depth

CIISec individual membership levels

Full membership process:
Submit → Internal Review → Assessment → Interview → AC → Award
Chartered IT Professional (CITP)

Relevant qualifications
Accredited degree or certification

Supporter verification
Application reviewed by an employer, colleague or client above to offer a reliable opinion of your knowledge and experience

Assessor interview
10-min presentation of professional competence and questions to verify knowledge and competence (~1 hr total)

Concluding thoughts
• Knowledge and experience are both important, but:
  • having knowledge doesn’t guarantee you can put it into practice
  • having experience doesn’t guarantee competent use of skills

• The common target in cybersecurity recruitment is an ‘experienced practitioner’
  • the aspirational target ought to be ‘competent professional’

• None of this guarantees a competent cybersecurity professional, but the professional body schemes help
The cybersecurity workforce and skills

Steven Furnell

Computers & Security
Volume 100, 2021