



A Comparison Study of Cybersecurity Workforce Frameworks And Future Directions

Bradford Love (Presenter)

Dan T. Kim

Sanghun Kim

Preview

- Introduction
- Existing cybersecurity workforce frameworks
- A comparison between frameworks
- Discussion of issues
- Conclusion

Introduction Cont.



Introduction

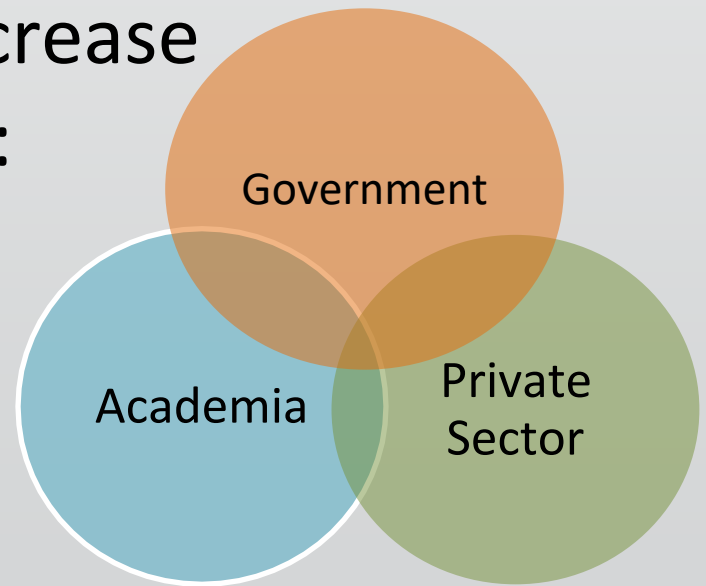


Introduction Cont.



Issues and Initiatives

- Lack of understanding on cybersecurity workforce from different perspectives
- Substantial initiatives to increase Cybersecurity workforce in:
 - Government
 - Academia
 - Private Sector



National Centers of Academic Excellence (CAE)

- CAE-CD (Cyber Defense)
 - CAE in CD Education
 - CAE in CD Research
- CAE-CO (Cyber Operations)

National Centers of Academic Excellence (CAE) Cont.

Basic Knowledge Units of CAE-CDE

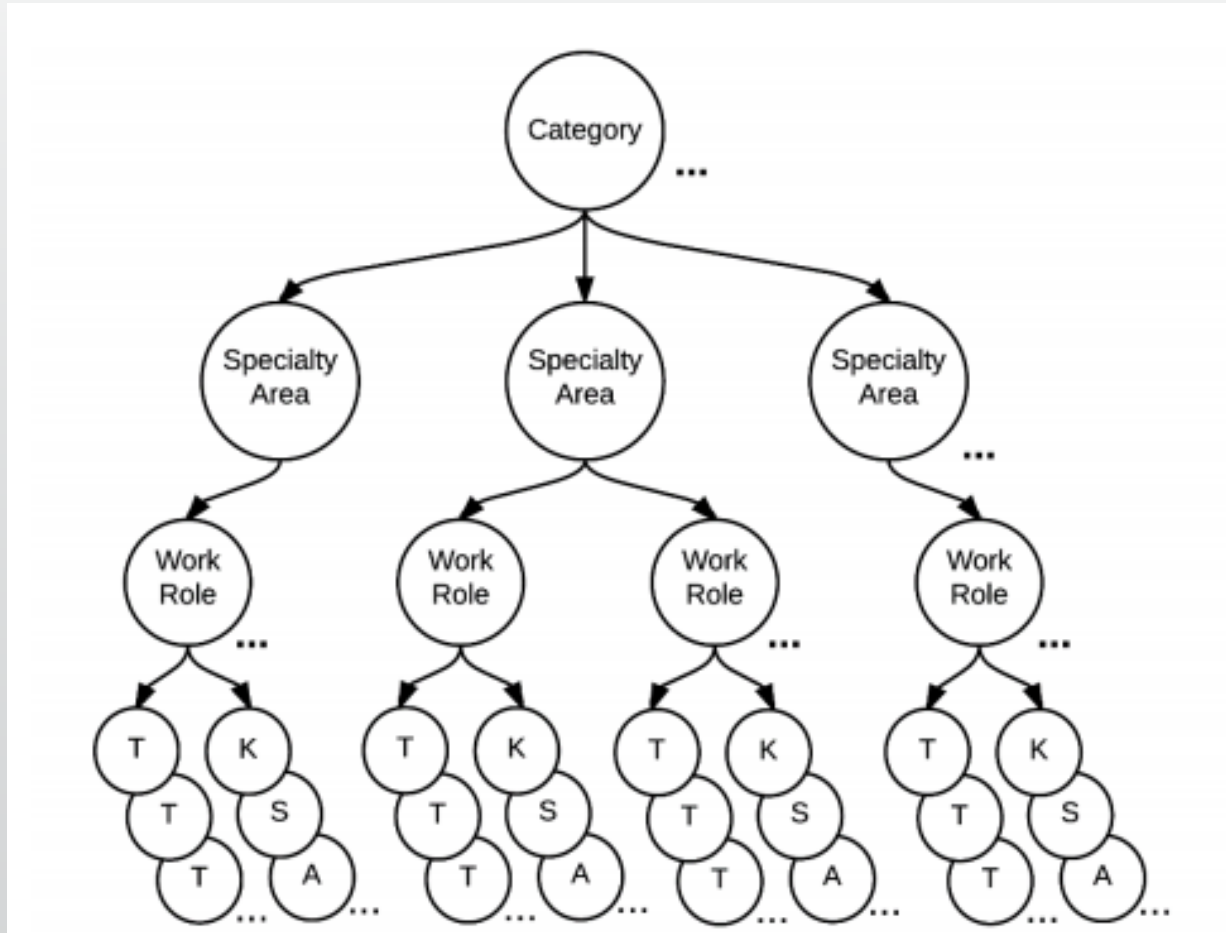
- A. Cybersecurity Foundations
- B. Cybersecurity Principles
- C. IT Systems Components
- D. Basic Cryptography
- E. Basic Networking
- F. Network Defense
- G. Operating Systems Concepts

- H. Cyber Threats
- I. Advanced Algorithms
- J. Algorithms
- K. Cyber Crime
- L. Data Structures
- M. Databases
- N. IA Compliance

NICE Cybersecurity Workforce Framework (NCWF)

- Categories (High-level grouping of common functions)
- Specialty Areas (Distinct areas of work)
- Work Roles (Knowledge, Skills, Abilities)

NICE Cybersecurity Workforce Framework (NCWF) Cont.



Department of Defense (DoD): DoD Directive 8570 and 8140

- DoDD 8570 (2005)
- DoDD 8570.01-M
- DoDD 8140.01 (2015)
- 8140 has no manual yet

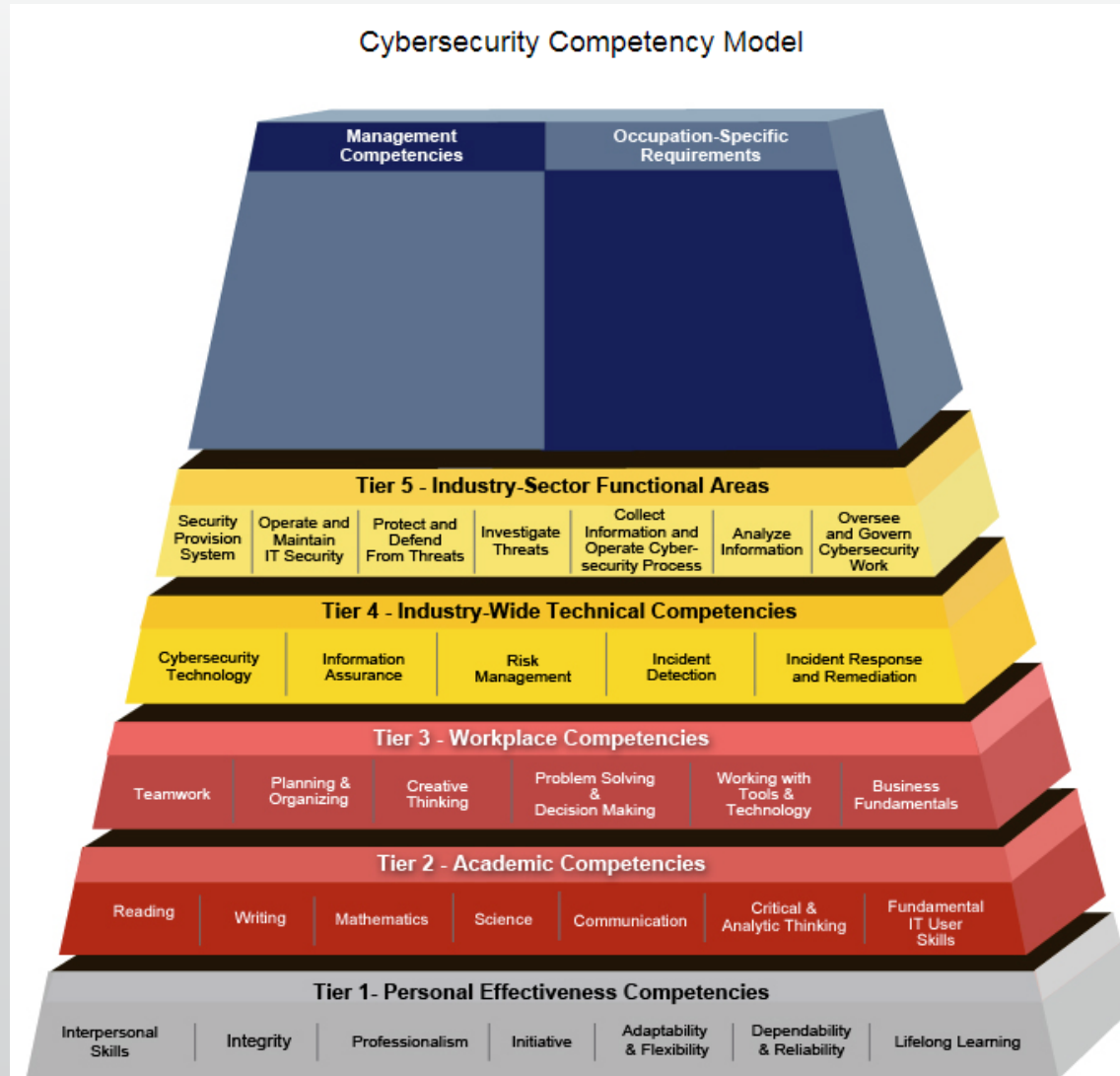
DoD Directive (DoDD) 8570 and 8140 Cont.

Approved Baseline Certifications		
IAT Level I A+ CE CCNA-Security Network+ CE SSCP	IAT Level II CCNA Security CSA+ GICSP GSEC Security+ CE SSCP	IAT Level III CASP CE CCNP Security CISA CISSP (or Associate) GCED GCIH
IAM Level I CAP GSLC Security+ CE	IAM Level II CAP CASP CE CISM CISSP (or Associate) GSLC	IAM Level III CISM CISSP (or Associate) GSLC
IASAE I CASP CE CISSP (or Associate) CSSLP	IASAE II CASP CE CISSP (or Associate) CSSLP	IASAE III CISSP-ISSAP CISSP-ISSEP
CSSP Analyst CEH CFR CSA+ GCIA GCIH GICSP SCYBER	CSSP Infrastructure Support CEH CSA+ GICSP SSCP	CSSP Incident Responder CEH CFR CSA+ GCFA GCIH SCYBER
CSSP Auditor CEH CSA+ CISA GSNA	CSSP Manager CISM CISSP-ISSMP	

Cybersecurity Industry Model

- Established by U.S. Department of Labor in 2014
- Complements the NCWF
- Tier system of competency areas

Cybersecurity Industry Model Cont.



Comparison of the Frameworks

	CAE-CD/CO	NCWF	DoDD 8570/8140	Cybersecurity Industry Model
Initiative organization	NSA and DHS	NIST (National Institute of Standard and Technology)	DoD (Department of Defense)	Department of Labor
Goal/Objective	Promotes higher education and research; and produces professionals with Cyber Operations (CO) and Cyber Defense (CD) expertise in various disciplines	Describes and categorizes cybersecurity work and identifies sample job titles, tasks, and KSAs (Knowledge, skills, and Abilities)	Provides the foundation for identifying education, training, and certification requirements to support cybersecurity personnel qualification	Provide a comprehensive overview of cybersecurity workforce competencies, including roles, training, and career paths for job seekers.
Audience	<ul style="list-style-type: none"> • 2-year, 4-year and graduate-level institutions in the U.S. seeking CAE designations 	<ul style="list-style-type: none"> • Employers • Current/Future cybersecurity workers • Training/Certification programs • Educators • Technology providers 	<ul style="list-style-type: none"> • Military, civilian, and contractor cybersecurity personnel • Training vendors, certification bodies, colleges, and continuing education providers 	<ul style="list-style-type: none"> • Current and future workforce (generally unemployed or under employed) participants, as well as employers, who need guidance on work role-KSA congruity
Mapping Component	<ul style="list-style-type: none"> • 3 Foundational KUs • 5 Core Technical KUs • 5 Core Non-Technical KUs • 57 Optional KUs 	<ul style="list-style-type: none"> • 7 Categories (Securely, Provision, Protect and Defend, Investigate, College and Operate, analyze, Operate and Maintain, Oversee and Govern) • 33 Specialty Areas • 52 Work Roles (KSA) 	<ul style="list-style-type: none"> • DoD work roles, tasks, functions and baseline KSAs • Under development awaiting DoD 8140.01 Manual 	<ul style="list-style-type: none"> • Pyramid: tapering from general skills and responsibilities to specialized competency areas at the top • Utilizes NICE Framework (NCWF), KSAs

Issues

- Starting point discrepancy
- Academic and private sector work experience discrepancy
- Lack of clear mapping components across sectors

Conclusion

- Lack of workforce seen
- Workforce frameworks are a great start
- No framework is perfect, but can always be tuned to evolve

Thank You.

Bradford Love

Email: bradfordlove@my.unt.edu

