Workforce Development for Cybersecurity: An Academic's Perspective

Dr. Thomas Meservy
Associate Professor of Information Systems
Brigham Young University

Systems Testing Excellence Program
FedEX Institute of Technology
University of Memphis

Essential Cybersecurity Skills

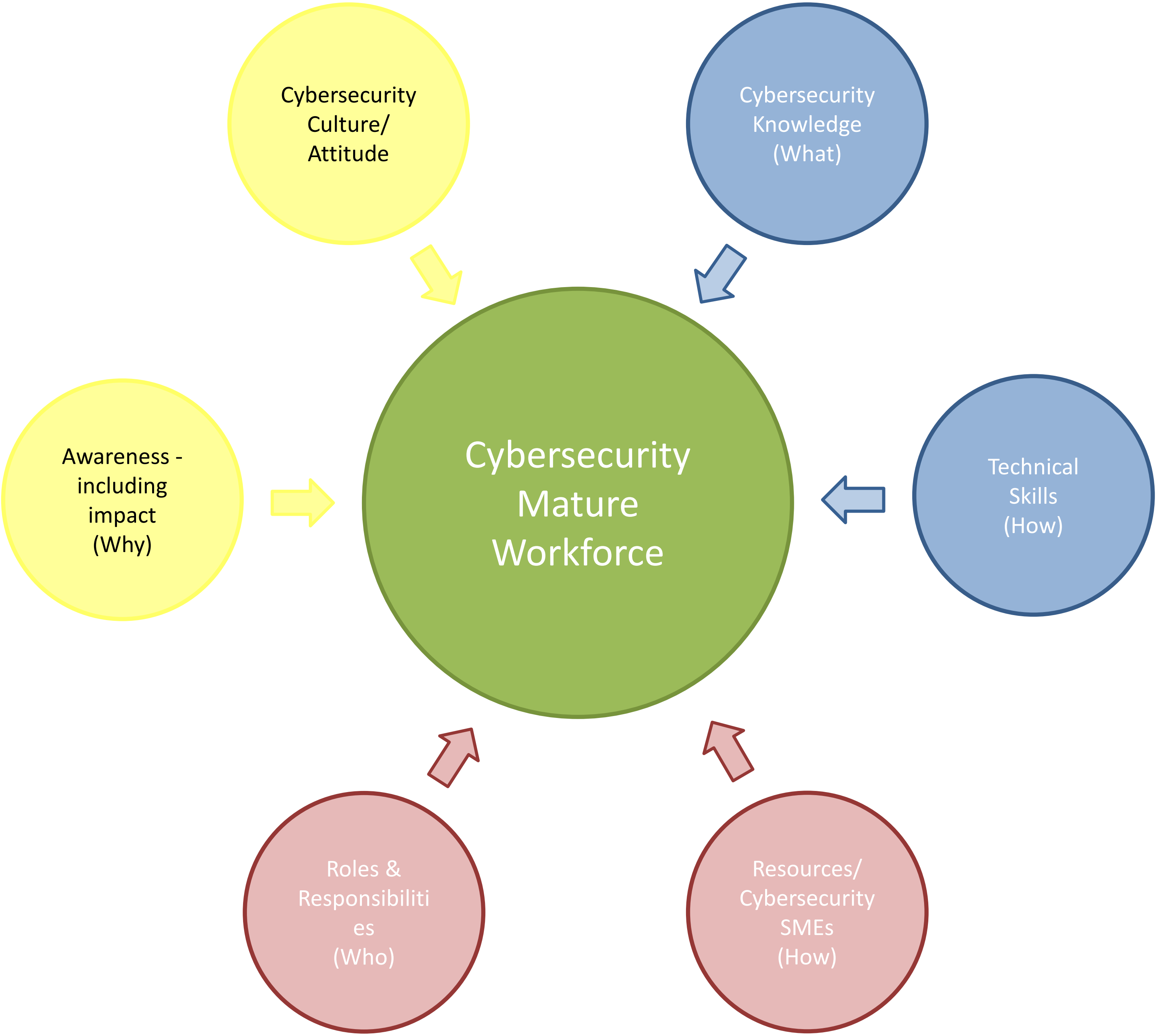
- Work Habits
  - Ability to work methodically and is very detail oriented
  - Eagerness to dig into technical questions and examine them from all sides
  - Enthusiastic and highly adaptable
  - Strong analytical and diagnostic skills
  - Demonstrated skills in innovation and collaboration
  - Keep a current understanding of vulnerabilities from the Internet
  - Maintaining awareness and knowledge of contemporary standards, practices, procedures and methods
  - Ability to get the job done
- Soft Skills
  - Excellent presentation and communications skills to effectively communicate with management and customers
  - Ability to clearly articulate complex concepts both written and verbally
  - Ability, understanding, and usage of active listening skills especially with customers
- Technical Skills
  - Understand architecture, administration, and management of operating systems, networking, and virtualization software
  - General programming/software development concepts and software analytical skills
  - Proficiency in programming in Java, C/C++, disassemblers, and assembly language and programming knowledge of two or more scripting languages (PHP, Python, Perl, or shell)
  - Understanding of how the different type of firewalls and network load balancers work
  - Deep understanding of how network routers and switches work
  - Evaluate and design systems and network architectures

https://insights.dice.com/cybersecurity-skills

Essential Cybersecurity Skills

- Platform Specific Skills
  - Open Source Applications
  - Linux Operating Systems
  - Microsoft Technologies
  - Wireless Technologies
  - Database Modeling
  - Web Application Technologies
  - Compiled and Interpreted Development Languages
  - Network Implementation (Operational and Security)
  - Telephony Technologies (Analog and IP)
  - Social Engineering
  - Physical Security
- Big Picture
  - Examine security from a holistic view, including threat modeling, specifications, implementation, testing, and vulnerability assessment
  - Understand security issues associated with operating systems, networking, and virtualization software
  - Understand Web application security concepts and practices
  - Understand the architecture of systems and network including identifying the security controls in place and how they are used
  - Understand database weaknesses and security best practices
  - Advanced understanding of general information security concepts and principles, system architectures and development
  - Expert knowledge of software development security principles, concepts, and best practices
  - Ability to write tools to automate certain security tasks
  - Ability to do Systems and Network hardening
  - Organize and coordinate technical Vulnerability Assessments including systems and network vulnerability assessments, penetration testing, web application assessments, social engineering assessments, physical security assessments, wireless security assessments and implementing secure infrastructure solutions
  - Recommend and set the technical direction for managing security incidents
  - Maintain the integrity of process and approach, as well as controls, for the whole incident management process including the ability to coordinate and manage major/highly sensitive investigations with potential for business wide impact/reputational damage
  - Be able to understand and forensically show how attacks from the Internet are done

https://insights.dice.com/cybersecurity-skills



Cybersecurity Culture/ Attitude

Cybersecurity Knowledge (What)

Awareness - including impact (Why)

Cybersecurity Mature Workforce

Technical Skills (How)

Roles & Responsibilities (Who)

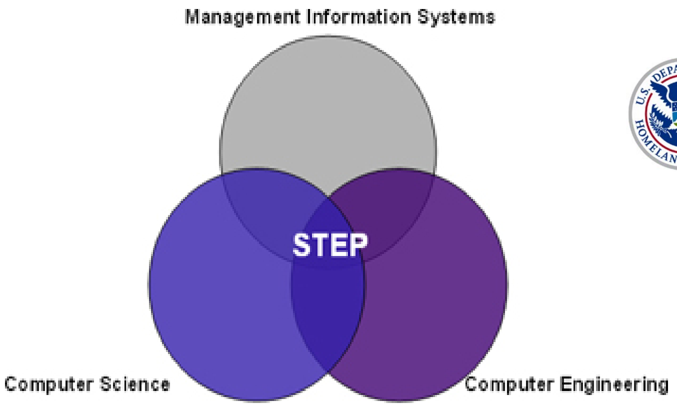
Resources/ Cybersecurity SMEs (How)

Major Challenges for Cybersecurity Workforce Development

- Knowledge needed
  - Increased complexity of environments/attacks
  - Frequency of attacks and variety of attacks
- Scarcity of resources
  - Limited resources including time
  - Public-private competition
- Competing priorities

A Partnership for Advancing the Science of Testing

System Testing Excellence Program



DISA
A Combat Support Agency

FedEx

Homeland Security

SYNTEL
Consider IT Done

SINCE 1884
DEHART CAPITAL, LLC

ELSEVIER

MPHASIS
an HP company

OAK RIDGE
National Laboratory

NRI
未来創発
Dream up the future.

COOK SYSTEMS INTERNATIONAL INCORPORATED

CISCO

AutoZone

Thomas&Betts

STEP Research-Based Certifications

- Foundational Certification in Systems T&E
  - Five Days (10 half-day modules and exam)
- Advanced Certification in Systems T&E
  - Ten Days (20 half-day modules and group project)
- Agile Development and T&E Boot Camp
  - Three Days
- DevSecOps/SecDevOps Training