Cyber Security Institute
University of Houston-Clear Lake

An Introduction of NICE Cybersecurity Workforce Framework

Dr. Kewei Sha

Dept. of Computing Sciences & Cyber Security Institute

University of Houston – Clear Lake

sha@uhcl.edu

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Agenda

- ❑ Motivation
- ❑ NICE and Cybersecurity Workforce Framework
- ❑ Designs of Cybersecurity Workforce Framework
- ❑ Adoption
- ❑ Concerns
- ❑ Conclusion

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

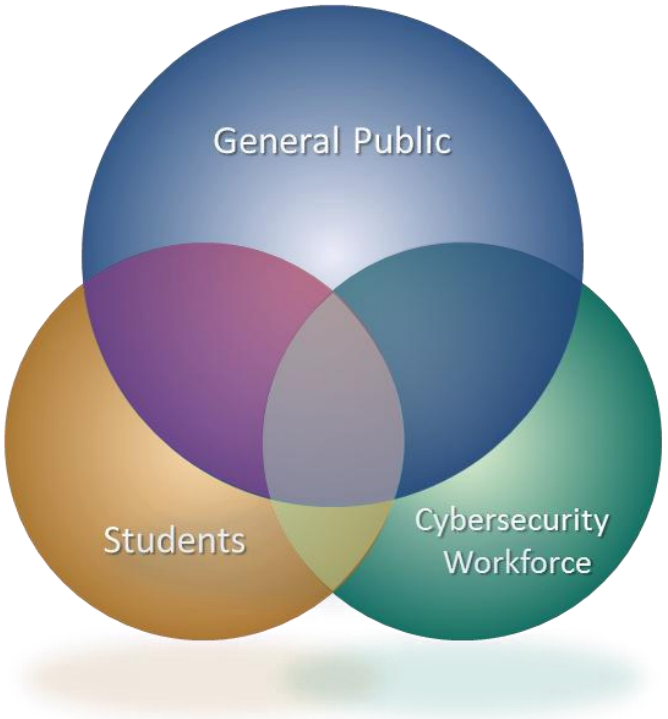
Motivation

- Interdisciplinary nature of cybersecurity
- Different perspectives from different disciplines
- Various stakeholders of cybersecurity: policy makers, employers, employees, educator/trainers, students
- Little consistency in terms of defining cybersecurity
- Strong needs of establishing consistency in how cybersecurity workforce is defined and classified

University of Houston Clear Lake

National Initiative for Cybersecurity Education (NICE)

Goal 1.
Raise national awareness about risks in cyberspace.



Goal 2.
Broaden the pool of individuals prepared to enter the cybersecurity workforce.

Goal 3.
Cultivate a globally competitive cybersecurity workforce.

Led by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce

University of Houston Clear Lake

History of Cybersecurity Workforce Framework

- Started in 2008 by the federal Chief Information Officers (CIO) Council
- Established NICE in 2010
- First release for comments: September 2012
- Version 1.0: April 2013
- Version 2.0: 2014 with the input from the Department of Homeland Security (DHS)
- Current version: NIST Special Publication 800-181, August 2017

Participating Organizations of Cybersecurity Workforce Framework

- Developed by NICE, led by NIST, Department of Commerce
- Other participating organizations

  Department of State, Department of Education, Department of Labor, Office of Management and Budget, Office of Personnel Management, Department of Defense, Department of Justice, Information Sciences & Technologies, Department of Homeland Security, Central Intelligence Agency, Defense Intelligence Agency, Director of National Intelligence, Federal Bureau of Investigation, National Security Agency, National Science Foundation, Department of Defense National Counterintelligence Executive, Federal Chief Information Officers Council

Overview (1)

- ***A dictionary*** defining the cybersecurity population consistently, and using standardized terms
- ***An essential step*** in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce
- ***A tool that*** provides the groundwork, or a baseline, by which organizations can develop their Human Capital Management programs, including defining roles, designing competency models, standardizing job descriptions, and providing specialized training
- ***An guidance*** to the federal government, will be made available to the private, public, and academic sectors for describing cybersecurity work and workforces, and related education, training, and professional development

Cyber Security Institute
University of Houston-Clear Lake

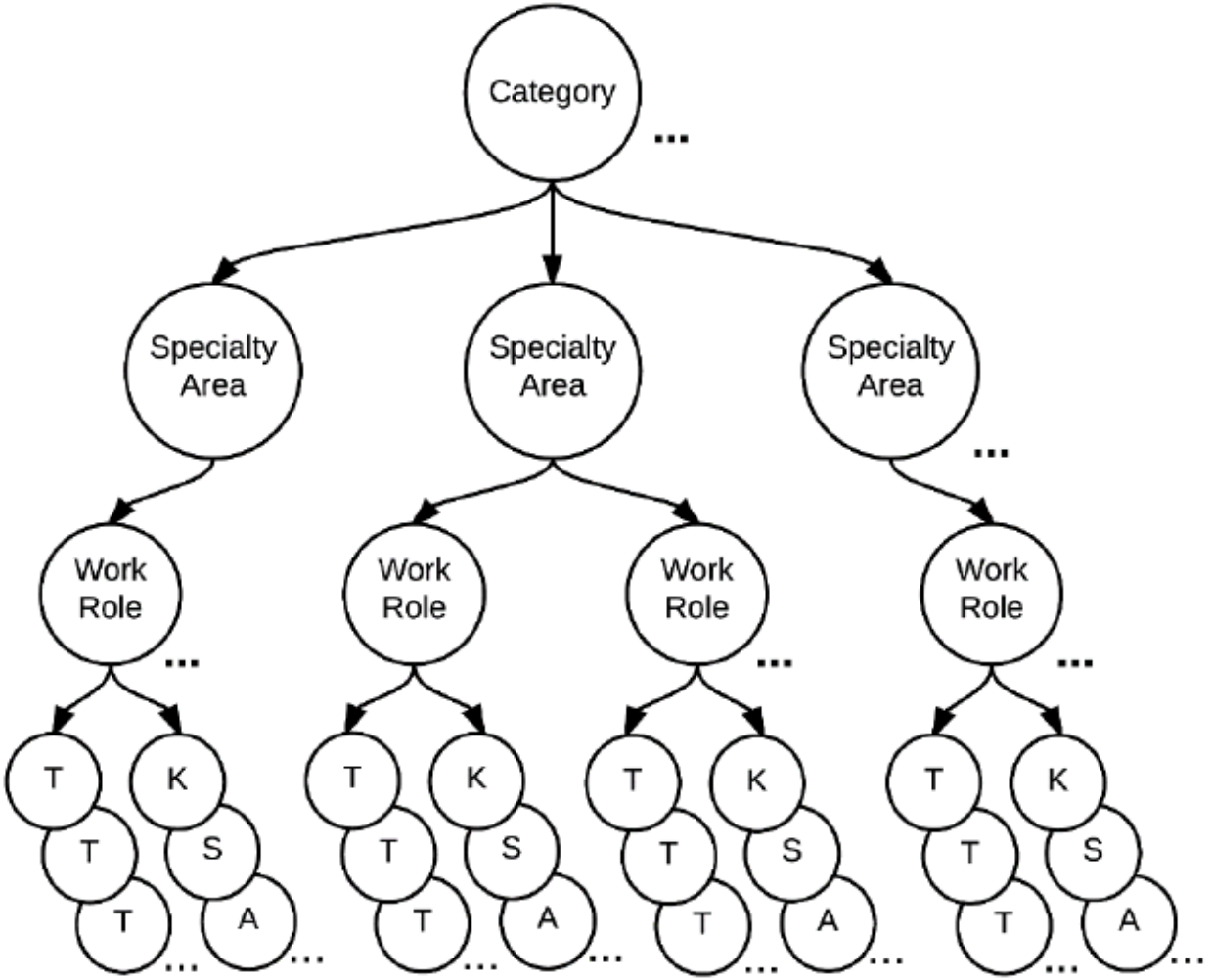
Overview (2)

- Lists and defines ***33 specialty areas*** of cybersecurity work and provides a description of each, in ***7 overall categories***
- Identifies common ***tasks*** and ***knowledge***, ***skills***, and ***abilities*** (KSAs) associated with each specialty area
- Collaborates with over 20 Federal departments and agencies and numerous national organizations from within academia and general industry

University of Houston Clear Lake

Relationships among NICE Framework Components

Group together work and workers that share common major functions, regardless of job titles or other occupational terms



Terms of Component (1)

- Categories (7)
  - The overarching organizational structure of the NICE Framework
- Specialty Areas (33)
  - Areas of concentrated work, or function, within cybersecurity and related work
- Work Roles (52)
  - The most detailed groupings of cybersecurity and related work that include a list of attributes required to perform that role in the form of KSAs and tasks performed in that role
- Competency
  - The capability of applying or using knowledge, skills, abilities, behaviors, and personal characteristics to successfully perform critical work tasks, specific functions, or operate in a given role or position

Terms of Component (2)

- Knowledge, Skills, and Abilities (KSAs)
  - ***Knowledge:*** A body of information applied directly to the performance of a function
  - ***Skill:*** An observable competence to perform a learned psychomotor act, in the psychomotor domain describe the ability to physically manipulate a tool or instrument like a hand or a hammer
  - ***Ability:*** Competence to perform an observable behavior or a behavior that results in an observable product
- Task
  - A specific defined piece of work that, combined with other identified Tasks, composes the work in a specific specialty area or work role

Cyber Security Institute
University of Houston-Clear Lake

Lists of 7 Categories

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Cyber Security Institute
University of Houston-Clear Lake

An Example Category: Investigate (IN)

NICE Specialty Area	NICE Specialty Area Definition	Work Role	Work Role Definition
Cyber Investigation (INV)	Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.	Cyber Crime Investigator	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.
Digital Forensics (FOR)	Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.	Law Enforcement /CounterIntelligence Forensics Analyst	Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.
		Cyber Defense Forensics Analyst	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

University of Houston Clear Lake

INV KSAs

Skill in preserving evidence integrity according to standard operating procedures or national standards.

Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.

Skill in using scientific rules and methods to solve problems.

Skill in evaluating the trustworthiness of the supplier and/or product.

Ability to find and navigate the dark web using the TOR network to locate markets and forums.

Ability to examine digital media on multiple operating system platforms.

Knowledge of computer networking concepts and protocols, and network security methodologies.

Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).

Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.

Knowledge of cybersecurity and privacy principles.

Knowledge of cyber threats and vulnerabilities.

Knowledge of specific operational impacts of cybersecurity lapses.

Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.

Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).

Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.

Knowledge of adversarial tactics, techniques, and procedures.

Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).

Knowledge of processes for seizing and preserving digital evidence.

Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).

Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.

Knowledge of types and collection of persistent data.

Knowledge of social dynamics of computer attackers in a global context.

Knowledge of electronic evidence law.

Knowledge of legal rules of evidence and court procedure.

Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.

Knowledge of covert communication techniques.

Knowledge of crisis management protocols, processes, and techniques.

Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity.

Knowledge of the judicial process, including the presentation of facts and evidence.

Knowledge of applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.

Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

Task ID	Task
T0031	Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects.
T0059	Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet.
T0096	Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals).
T0103	Examine recovered data for information of relevance to the issue at hand.
T0104	Fuse computer network attack analyses with criminal and counterintelligence investigations and operations.
T0110	Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.
T0112	Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations.
T0113	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.
T0114	Identify elements of proof of the crime.
T0120	Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations.
T0193	Process crime scenes.
T0225	Secure the electronic device or information source.
T0241	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.
T0343	Analyze the crisis to ensure public, personal, and resource protection.
T0346	Assess the behavior of the individual victim, witness, or suspect as it relates to the investigation.
T0360	Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks.
T0386	Provide criminal investigative support to trial counsel during the judicial process.
T0423	Analyze computer-generated threats for counter intelligence or criminal activity.
T0430	Gather and preserve evidence used on the prosecution of computer crimes.
T0433	Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.
T0453	Determine and develop leads and identify sources of information to identify and/or prosecute the responsible parties to an intrusion or other crimes.
T0471	Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking).
T0479	Employ information technology (IT) systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property.
T0523	Prepare reports to document the investigation following legal standards and requirements.

INV Tasks

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Adoption

STEP 1

Define Cybersecurity Roles

Assess your cybersecurity workforce and ensure your roles are consistent with the Framework. Click HERE to see an example process that can help guide your work. These are the cybersecurity roles developed by the Federal Chief Information Officers Council (Fed CIOC), which you can use within your own organization.

STEP 2

Develop Cybersecurity Competency Models

Once you define your organization's Framework-based cybersecurity roles, you can then develop competency models for these individuals. (Federal guidance requires every department and agency to develop competency models for workers.) Click HERE for an example of how this is being done by DHS's Cybersecurity Workforce Initiative.

STEP 3

Conduct Workforce Planning

Use your newly defined cybersecurity roles to gather and assess data that can be used for future workforce planning efforts. Click HERE to see an example of the methodology you can use.

STEP 4

Plan for the Future

Once those activities are accomplished, and based on the gaps found after completing workforce planning, you can develop strategies for other Human Capital efforts within your organization, such as recruitment, selection, succession planning, and employee development.

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Concerns

- Still some inconsistency
  - Inputs from many organizations
- Work role may not complete
  - Missing disaster recovery/business
  - Privacy not emphasized
- Lists of Tasks, Knowledge, Skills, & Abilities
  - Not in any order
  - Some description is ambiguous
  - Some redundancy
- Needs better mapping between this framework with
  - Knowledge Units in NSA/DHS Centers of Academic Excellence
  - ACM/IEEE-CS curricula in IT and Cybersecurity
  - ABET Accreditation Standards

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Conclusion

- An introduction of NICE Cybersecurity Framework
  - Goals and history
  - Major components
  - An example category
- Adoption and concerns
  - 4 steps to adopt the framework
  - Suggestions to improve the framework

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Thank you!

University
of Houston
Clear Lake