# Cybersecurity Education

May 25, 2022

8:30 – 11:30 am, Todd 203

Dr. Sola Adesope, Dr. James Crabb, Dr. Chris Hundhausen,
Slater Weinstock (Casaba)

# Agenda

| Time | Activity | Facilitator |
|---|---|---|
| 8:30 – 8:45 | Welcome and Introductions | Chris Hundhausen |
| 8:45 – 9:30 | A day in the life of a cybersecurity professional | Slater Weinstock |
| 9:30 – 9:45 | Review of cybersecurity academic recommendations | James Crabb |
| 9:45 – 10:15 | Assessing cybersecurity knowledge with Bloom's Taxonomy | James Crabb |
| 10:15 – 10:30 | Break | |
| 10:30 – 11:30 | Designing curricula and technologies to facilitate cybersecurity education | Sola Adesope<br>James Crabb<br>Chris Hundhausen |
| 11:30 – 11:45 | Discussion and wrap-up | Chris Hundhausen |

# Introductions

Sola Adesope
Chris Hundhausen
James Crabb
Slater Weinstock

WASHINGTON STATE UNIVERSITY

casaba

# A day in the life of a cybersecurity professional

Slater

# Assessing cybersecurity knowledge with Bloom's Taxonomy

James

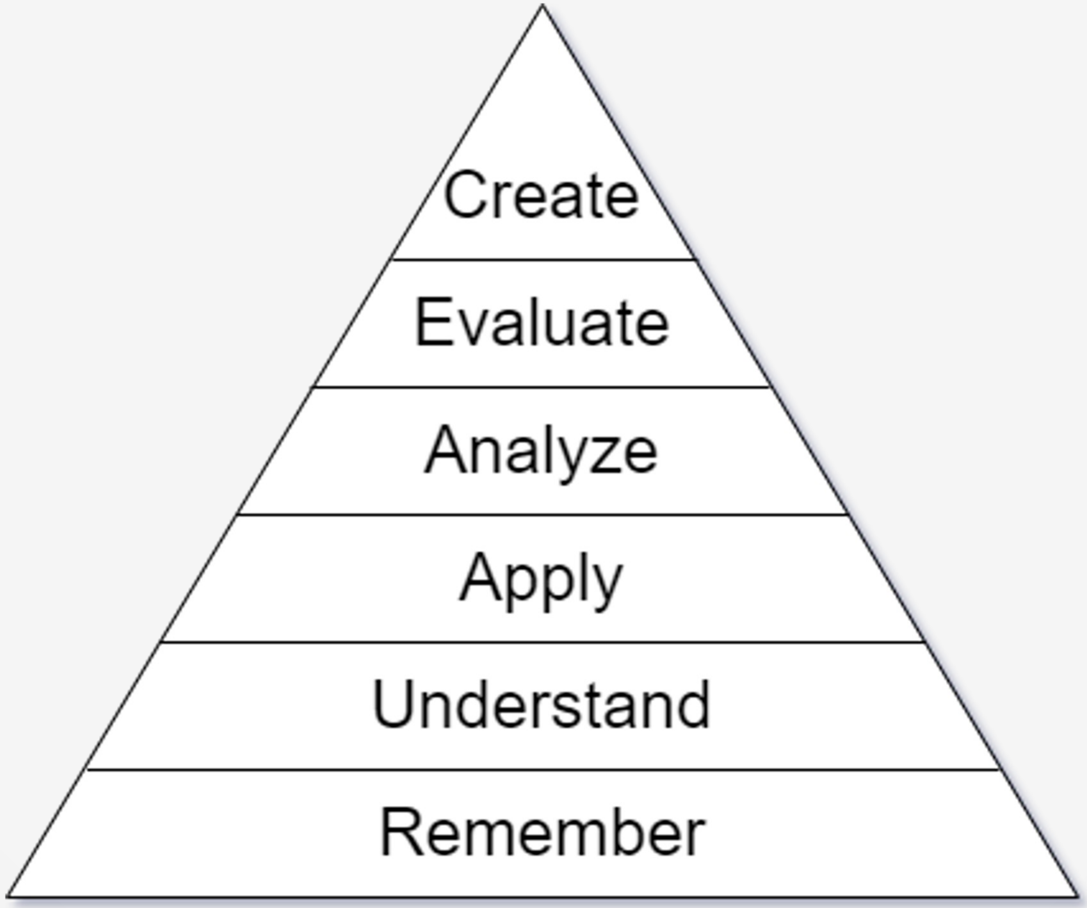
WASHINGTON STATE
UNIVERSITY

# Bloom's Taxonomy

*Taxonomy of educational objectives: The classification of educational goals*. Handbook I: Cognitive domain. Bloom et al, 1956.

*A Taxonomy for learning, teaching, and assessing: A revision of Bloom's Taxonomy of educational objectives*. Anderson and Krathwohl (eds.), 2001.

# Bloom's Taxonomy



Create

Evaluate

Analyze

Apply

Understand

Remember

# Bloom's Taxonomy

REMEMBER

Recognize or recall knowledge from memory.

Ex: Remember the function prototype for malloc().

# Bloom's Taxonomy

UNDERSTAND

Construct meaning from material.

Ex: Understand what malloc() does.

# Bloom's Taxonomy

APPLY

Use knowledge to implement a procedure or solve a related problem.

Ex: Use malloc() properly in your own code.

# Bloom's Taxonomy

ANALYZE

Differentiate, organize, and attribute components and functionality of a concept.

Ex: Decide whether to use malloc(), calloc(), or realloc().

# Bloom's Taxonomy

EVALUATE

Perform checking and critiquing of materials based on standards and criteria.

Ex: Test code that uses malloc().

# Bloom's Taxonomy

CREATE

Put elements together or reorganize them into a new pattern to form a functional whole

Ex: Write a new implementation of malloc().

# Bloom's Taxonomy

ASSESSING AT EACH LEVEL

- **Remember** a fact
- **Understand** its details
- **Apply** it to a problem
- **Analyze** different options
- **Evaluate** the potential outcomes
- **Create** a novel solution

# Review of cybersecurity education recommendations

James

WASHINGTON STATE UNIVERSITY

# Existing sources

- Cybersecurity Assessment Tools (CATS) - University of Maryland, Baltimore County
  1. Cybersecurity Concept Inventory
  2. Cybersecurity Curriculum Assessment
- Cybersecurity Curricula 2017 – ACM, IEEE, others
- NICE Framework – National Institute of Standards and Technology

# Cybersecurity Assessment Tools

What is a *concept inventory*?

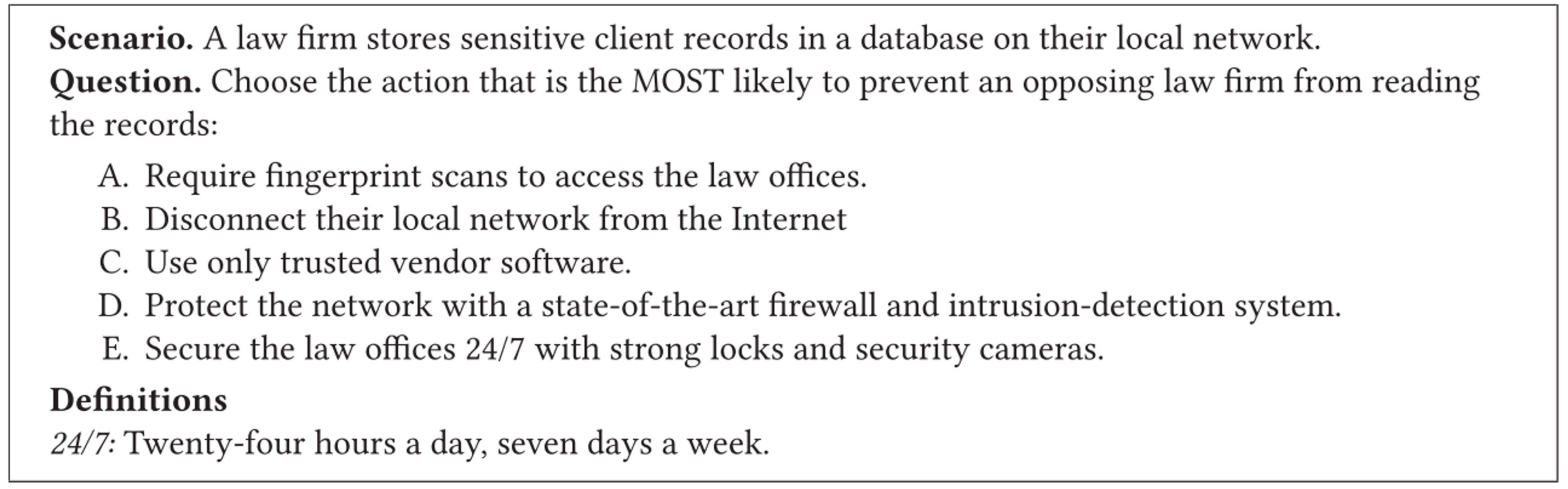
- Tool for assessment of knowledge in a specific domain
- Evaluate the effectiveness of a course or program
- Rigorous development process
- Statistically validated

# Cybersecurity Assessment Tools

Development of the Cybersecurity Concept Inventory (CCI)

- *Identifying core concepts of cybersecurity: Results of two Delphi Processes*. Parekh et al, 2018
- *Student misconceptions about cybersecurity: Analysis of think-aloud interviews*. Thompson et al, 2018.
- *Initial validation of the Cybersecurity Concept Inventory: Pilot testing and expert review*. Offenberger et al, 2019.
- *Psychometric evaluation of the Cybersecurity Concept Inventory*. Poulsen et al, 2021.

# Cybersecurity Assessment Tools



**Scenario.** A law firm stores sensitive client records in a database on their local network.
**Question.** Choose the action that is the MOST likely to prevent an opposing law firm from reading the records:

A. Require fingerprint scans to access the law offices.
B. Disconnect their local network from the Internet
C. Use only trusted vendor software.
D. Protect the network with a state-of-the-art firewall and intrusion-detection system.
E. Secure the law offices 24/7 with strong locks and security cameras.

**Definitions**
*24/7:* Twenty-four hours a day, seven days a week.

Fig. 8. CCI Question 23 probes the concept “Devise a Defense.” This question had the highest discrimination of all the questions on the test.

*Psychometric evaluation of the Cybersecurity Concept Inventory*. Poulsen et al, 2021.

# Cybersecurity Assessment Tools

Validation of the Cybersecurity Concept Inventory (CCI)

Each question is evaluated for:

- Reliability – same student will have same score over multiple measurements
- Difficulty – number of students who answer correctly vs. incorrectly
- Discrimination – whether weaker students get lower scores than stronger students

# Cybersecurity Assessment Tools

Cybersecurity Concept Inventory

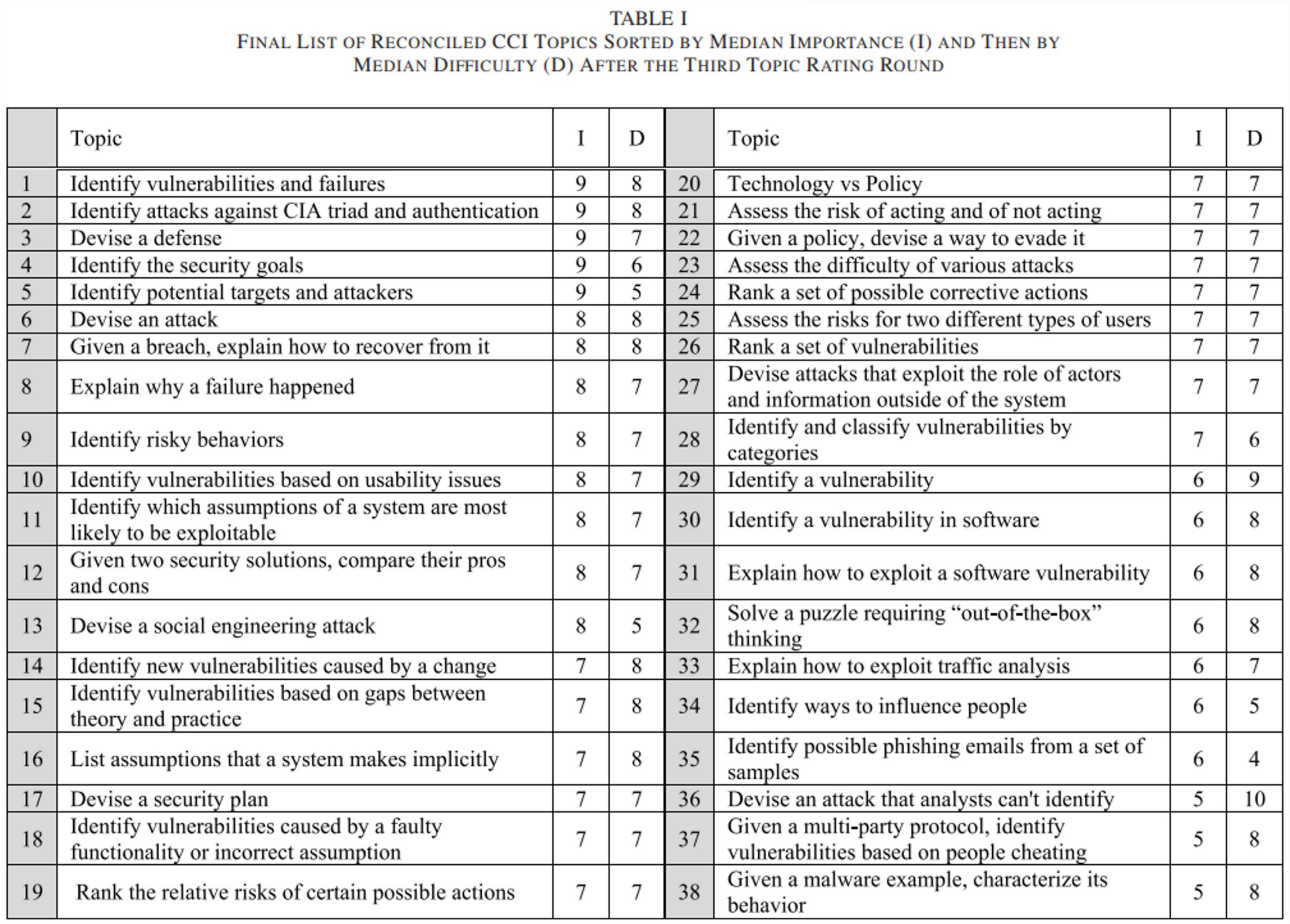


TABLE I
FINAL LIST OF RECONCILED CCI TOPICS SORTED BY MEDIAN IMPORTANCE (I) AND THEN BY MEDIAN DIFFICULTY (D) AFTER THE THIRD TOPIC RATING ROUND

| | Topic | I | D | | Topic | I | D |
|---|---|---|---|---|---|---|---|
| 1 | Identify vulnerabilities and failures | 9 | 8 | 20 | Technology vs Policy | 7 | 7 |
| 2 | Identify attacks against CIA triad and authentication | 9 | 8 | 21 | Assess the risk of acting and of not acting | 7 | 7 |
| 3 | Devise a defense | 9 | 7 | 22 | Given a policy, devise a way to evade it | 7 | 7 |
| 4 | Identify the security goals | 9 | 6 | 23 | Assess the difficulty of various attacks | 7 | 7 |
| 5 | Identify potential targets and attackers | 9 | 5 | 24 | Rank a set of possible corrective actions | 7 | 7 |
| 6 | Devise an attack | 8 | 8 | 25 | Assess the risks for two different types of users | 7 | 7 |
| 7 | Given a breach, explain how to recover from it | 8 | 8 | 26 | Rank a set of vulnerabilities | 7 | 7 |
| 8 | Explain why a failure happened | 8 | 7 | 27 | Devise attacks that exploit the role of actors and information outside of the system | 7 | 7 |
| 9 | Identify risky behaviors | 8 | 7 | 28 | Identify and classify vulnerabilities by categories | 7 | 6 |
| 10 | Identify vulnerabilities based on usability issues | 8 | 7 | 29 | Identify a vulnerability | 6 | 9 |
| 11 | Identify which assumptions of a system are most likely to be exploitable | 8 | 7 | 30 | Identify a vulnerability in software | 6 | 8 |
| 12 | Given two security solutions, compare their pros and cons | 8 | 7 | 31 | Explain how to exploit a software vulnerability | 6 | 8 |
| 13 | Devise a social engineering attack | 8 | 5 | 32 | Solve a puzzle requiring “out-of-the-box” thinking | 6 | 8 |
| 14 | Identify new vulnerabilities caused by a change | 7 | 8 | 33 | Explain how to exploit traffic analysis | 6 | 7 |
| 15 | Identify vulnerabilities based on gaps between theory and practice | 7 | 8 | 34 | Identify ways to influence people | 6 | 5 |
| 16 | List assumptions that a system makes implicitly | 7 | 8 | 35 | Identify possible phishing emails from a set of samples | 6 | 4 |
| 17 | Devise a security plan | 7 | 7 | 36 | Devise an attack that analysts can't identify | 5 | 10 |
| 18 | Identify vulnerabilities caused by a faulty functionality or incorrect assumption | 7 | 7 | 37 | Given a multi-party protocol, identify vulnerabilities based on people cheating | 5 | 8 |
| 19 | Rank the relative risks of certain possible actions | 7 | 7 | 38 | Given a malware example, characterize its behavior | 5 | 8 |

*Identifying core concepts of cybersecurity: Results of two Delphi Processes*. Parekh et al, 2018

# Cybersecurity Assessment Tools

Cybersecurity Curriculum Assessment

- Developed in parallel with CCI
- Key differences:
  - Targeted at curriculum rather than individual course
  - Assumes students have broader base of knowledge

# Cybersecurity Assessment Tools

## Cybersecurity Concept Assessment

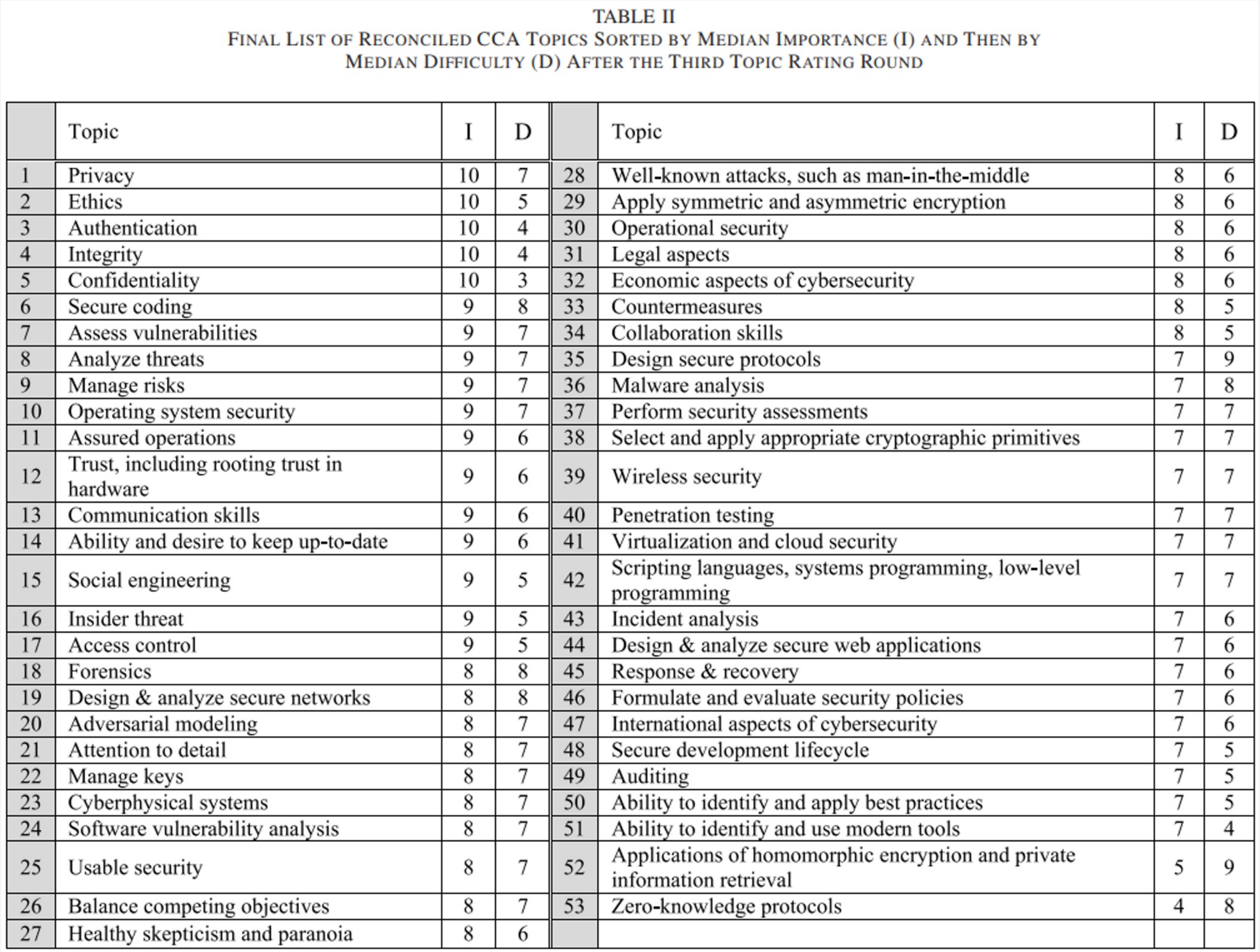


TABLE II
Final List of Reconciled CCA Topics Sorted by Median Importance (I) and Then by Median Difficulty (D) After the Third Topic Rating Round

| | Topic | I | D | | Topic | I | D |
|---|---|---|---|---|---|---|---|
| 1 | Privacy | 10 | 7 | 28 | Well-known attacks, such as man-in-the-middle | 8 | 6 |
| 2 | Ethics | 10 | 5 | 29 | Apply symmetric and asymmetric encryption | 8 | 6 |
| 3 | Authentication | 10 | 4 | 30 | Operational security | 8 | 6 |
| 4 | Integrity | 10 | 4 | 31 | Legal aspects | 8 | 6 |
| 5 | Confidentiality | 10 | 3 | 32 | Economic aspects of cybersecurity | 8 | 6 |
| 6 | Secure coding | 9 | 8 | 33 | Countermeasures | 8 | 5 |
| 7 | Assess vulnerabilities | 9 | 7 | 34 | Collaboration skills | 8 | 5 |
| 8 | Analyze threats | 9 | 7 | 35 | Design secure protocols | 7 | 9 |
| 9 | Manage risks | 9 | 7 | 36 | Malware analysis | 7 | 8 |
| 10 | Operating system security | 9 | 7 | 37 | Perform security assessments | 7 | 7 |
| 11 | Assured operations | 9 | 6 | 38 | Select and apply appropriate cryptographic primitives | 7 | 7 |
| 12 | Trust, including rooting trust in hardware | 9 | 6 | 39 | Wireless security | 7 | 7 |
| 13 | Communication skills | 9 | 6 | 40 | Penetration testing | 7 | 7 |
| 14 | Ability and desire to keep up-to-date | 9 | 6 | 41 | Virtualization and cloud security | 7 | 7 |
| 15 | Social engineering | 9 | 5 | 42 | Scripting languages, systems programming, low-level programming | 7 | 7 |
| 16 | Insider threat | 9 | 5 | 43 | Incident analysis | 7 | 6 |
| 17 | Access control | 9 | 5 | 44 | Design & analyze secure web applications | 7 | 6 |
| 18 | Forensics | 8 | 8 | 45 | Response & recovery | 7 | 6 |
| 19 | Design & analyze secure networks | 8 | 8 | 46 | Formulate and evaluate security policies | 7 | 6 |
| 20 | Adversarial modeling | 8 | 7 | 47 | International aspects of cybersecurity | 7 | 6 |
| 21 | Attention to detail | 8 | 7 | 48 | Secure development lifecycle | 7 | 5 |
| 22 | Manage keys | 8 | 7 | 49 | Auditing | 7 | 5 |
| 23 | Cyberphysical systems | 8 | 7 | 50 | Ability to identify and apply best practices | 7 | 5 |
| 24 | Software vulnerability analysis | 8 | 7 | 51 | Ability to identify and use modern tools | 7 | 4 |
| 25 | Usable security | 8 | 7 | 52 | Applications of homomorphic encryption and private information retrieval | 5 | 9 |
| 26 | Balance competing objectives | 8 | 7 | 53 | Zero-knowledge protocols | 4 | 8 |
| 27 | Healthy skepticism and paranoia | 8 | 6 | | | | |

*Identifying core concepts of cybersecurity: Results of two Delphi Processes*. Parekh et al, 2018

# Cybersecurity Curricula 2017

"A Report in the Computing Curricula Series Joint Task Force on Cybersecurity Education"

Version 1.0: 31 Dec 2017

(provided in the share folder)

# Cybersecurity Curricula 2017

Chapter 4: Content of the Cybersecurity Curricular Framework

Knowledge areas

- Data security
- Software security
- Component security
- Five more …

# Cybersecurity Curricula 2017

Chapter 4: Content of the Cybersecurity Curricular Framework

Knowledge units in data security

- Cryptography
- Digital forensics
- Data integrity and authentication
- Access control
- More …

# Cybersecurity Curricula 2017

Chapter 4: Content of the Cybersecurity Curricular Framework

Topics in cryptography

- Basic concepts
- Advanced concepts
- Mathematical background
- More ...

# Cybersecurity Curricula 2017

Chapter 4: Content of the Cybersecurity Curricular Framework

Essentials and learning outcomes

"Students are required to demonstrate proficiency in each of the essential concepts through achievement of the learning outcomes.  Typically, the learning outcomes lie within the understanding and applying levels in the Bloom's Revised Taxonomy." (p. 30)

# Cybersecurity Curricula 2017

## Chapter 4: Content of the Cybersecurity Curricular Framework

| Essentials | Learning Outcomes |
|---|---|
| Basic cryptography concepts | Describe the purpose of cryptography and list ways it is used |
| | Explain how public key infrastructure supports digital signing and encryption |
| Digital forensics | Describe what a digital investigation is, the sources of digital evidence, and the limitations of forensics |
| | Compare and contrast variety of forensics tools |

# NICE Framework

NICE Framework Program Office – NICEframework@nist.gov

- NIST Special Publication 800-181 rev. 1: *Workforce Framework for Cybersecurity*
- "Provides a set of building blocks for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work …" (p. vi)

# NICE Framework

NICE Framework: Building Blocks

- Tasks
- Knowledge
- Skills
- Pre-existing T/K/S
- Extensible

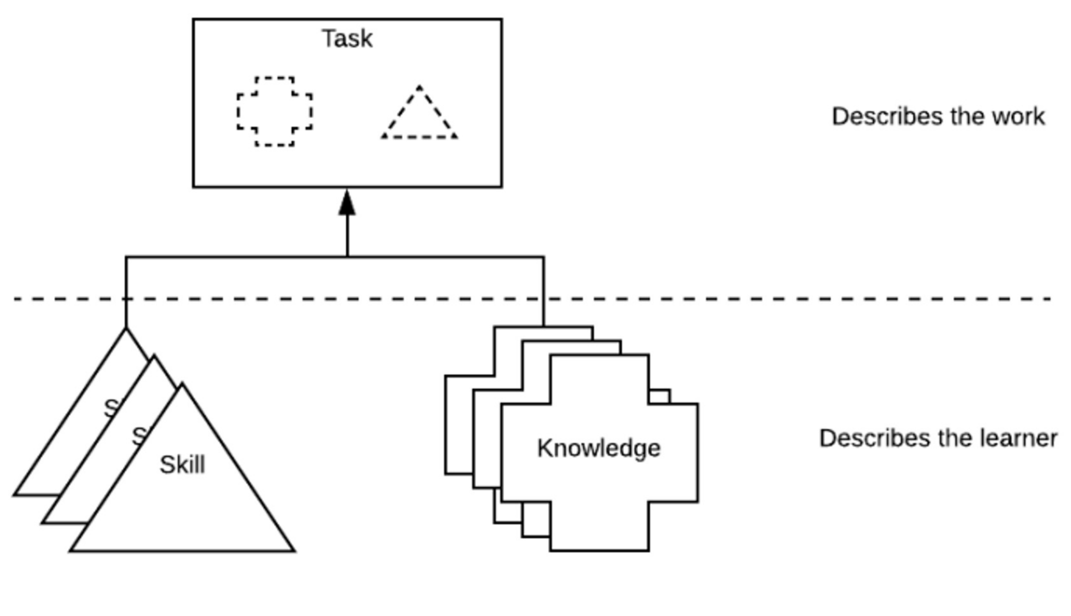


**Figure 1 - NICE Framework Building Blocks Approach**

(p. 1)

# NICE Framework

NICE Framework: Building Blocks

Task

- An activity that is directed toward the achievement of organizational objectives.
- Ex: Troubleshoot system hardware and software.

# NICE Framework

NICE Framework: Building Blocks

Knowledge

- A retrievable set of concepts within memory.
- "Organizations developing Knowledge statements should consider the learners' different levels of knowledge … described in Bloom's Taxonomy" (p. 5)
- Ex: Knowledge of cyberspace threats and vulnerabilities.

# NICE Framework

NICE Framework: Building Blocks

Skill

- The capacity to perform an observable action.
- "use terms that facilitate observability and assessment of the learner" (p. 5)
- Ex: Skill in recognizing the alerts of an Intrusion Detection System.

# NICE Framework

NICE Framework: Specialty Areas and Work Roles

https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice

NICE Framework Data – Reference Spreadsheet

# NICE Framework

NICE Framework: Specialty Areas and Work Roles

SP-DEV-001: Software Developer

- T0009 – Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.
- T0014 – Apply secure code documentation.

# NICE Framework

NICE Framework: Specialty Areas and Work Roles

SP-DEV-001: Software Developer

- K0005 – Knowledge of cyber threats and vulnerabilities.
- K0060 – Knowledge of operating systems.
- S0014 – Skill in conducting software debugging.
- S0174 – Skill in using code analysis tools.

# Applying Bloom's Taxonomy

SPECIFICALLY ADDRESSED IN:

- NICE Framework
- Cybersecurity Curricula 2017

# Applying Bloom's Taxonomy

NICE FRAMEWORK

- T0111 – Identify basic common coding flaws at a high level. (**Analyze**)
- T0009 – Analyze information to determine, recommend, and plan the development of a new application. (**Evaluate**)
- T0176 – Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities. (**Create**)

# Applying Bloom's Taxonomy

CYBERSECURITY CURRICULA 2017

Data Security Learning Outcomes

- Explain the concepts of authentication, authorization, access control and data integrity (**Understand**).
- Describe the purpose of cryptography (**Understand**) and list ways it is used in data communications (**Apply**).
- Compare and contrast variety of forensics tools (**Analyze**).

# Applying Bloom's Taxonomy

CYBERSECURITY CONCEPT INVENTORY

Assessment activities for "Identify vulnerabilities and failures"

- Remember: list types of vulnerabilities
- Understand: define (list key features of) vulnerabilities
- Apply: identify causal vulnerabilities of a security failure
- Analyze: identify vulnerabilities of a system
- Evaluate: perform risk assessment of a system
- Create: fix the vulnerabilities in a system

# Applying Bloom's Taxonomy

1. START WITH WELL-DEFINED LEARNING OUTCOMES
2. USE THOSE TO DEVELOP ASSESSMENTS
3. USE ASSESSMENTS TO DEVELOP LESSONS

# Break time!

Resuming in 15 minutes

WASHINGTON STATE UNIVERSITY

# Designing curricula and tools to facilitate cybersecurity education

Sola

WASHINGTON STATE UNIVERSITY

# Developing Assessments using Bloom's Taxonomy

## Length

30 minutes

## Goal

Learn how to classify different levels of student knowledge and apply appropriate assessments

## Group sizes

3-4

## Online materials

tiny.cc/cysered

# Group Reports & Wrap-Up

Chris

WASHINGTON STATE
UNIVERSITY