Developing a Workforce for Security Awareness and Behavior Change

A NICE Framework Workshop

Wednesday, September 29, 2021
1-5 p.m. ET (10 a.m. - 2 p.m. PT)

CAE in Cybersecurity Community Virtual Event
https://www.caecommunity.org

Today's Agenda

- Opening and Welcome
- Security Awareness: Managing Human Risk
- NICE Framework: Competencies & Work Roles
- *Break*
- Break-out Session: Identifying What is Unique in Security Awareness
- Integrating Security Awareness into the NICE Framework: Coming to Consensus
- *Break*
- Integrating Security Awareness into the NICE Framework: Building the Content
- Closing Session: Where We Go From Here

Today's Goals

Understand **what is unique about Cybersecurity Awareness work** and how to best translate that for workforce application

Discuss sample Cybersecurity Awareness scenarios to determine **existing content and gaps** in the NICE Framework.

Understand NICE Framework **Work Roles and Competencies** to determine the best approach to incorporating Cybersecurity Awareness.

Identify **Cybersecurity Awareness tasks** for inclusion in the NICE Framework.

Housekeeping & Ground Rules

- Slides will be shared following the event
- Recording of main sessions for internal review only
- Mute when not speaking
- A workshop report will follow

- Be present
- Share *and* listen
- Keep an open mind
- Watch out for rabbit holes

NICE
NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION

Opening & Welcome

Rodney Petersen
Director, National Initiative for Cybersecurity Education (NICE)

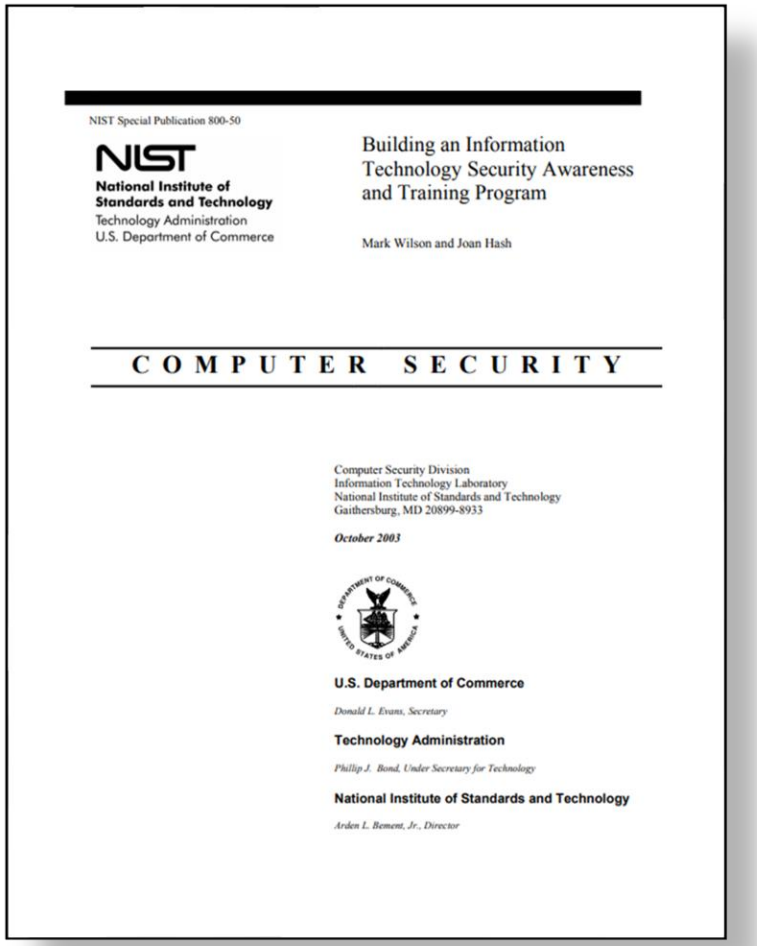
NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Cybersecurity Enhancement Act of 2014 – Section 401

Director of National Institute of Standards and Technology (NIST), in consultation with [public and private sectors], shall continue to coordinate a National Cybersecurity Awareness and Education Program, that includes activities such as

- facilitating Federal programs to advance cybersecurity education, training, and workforce development
- supporting formal cybersecurity education programs at all education levels
- promoting initiatives to evaluate and forecast future cybersecurity workforce needs
- ***increasing public awareness of cybersecurity, cyber safety, and cyber ethics***

PRE-DRAFT Call for Comments: Building a Cybersecurity and Privacy Awareness and Training Program



NIST Special Publication 800-50

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Building an Information Technology Security Awareness and Training Program

Mark Wilson and Joan Hash

COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8933

October 2003

U.S. Department of Commerce
Donald L. Evans, Secretary

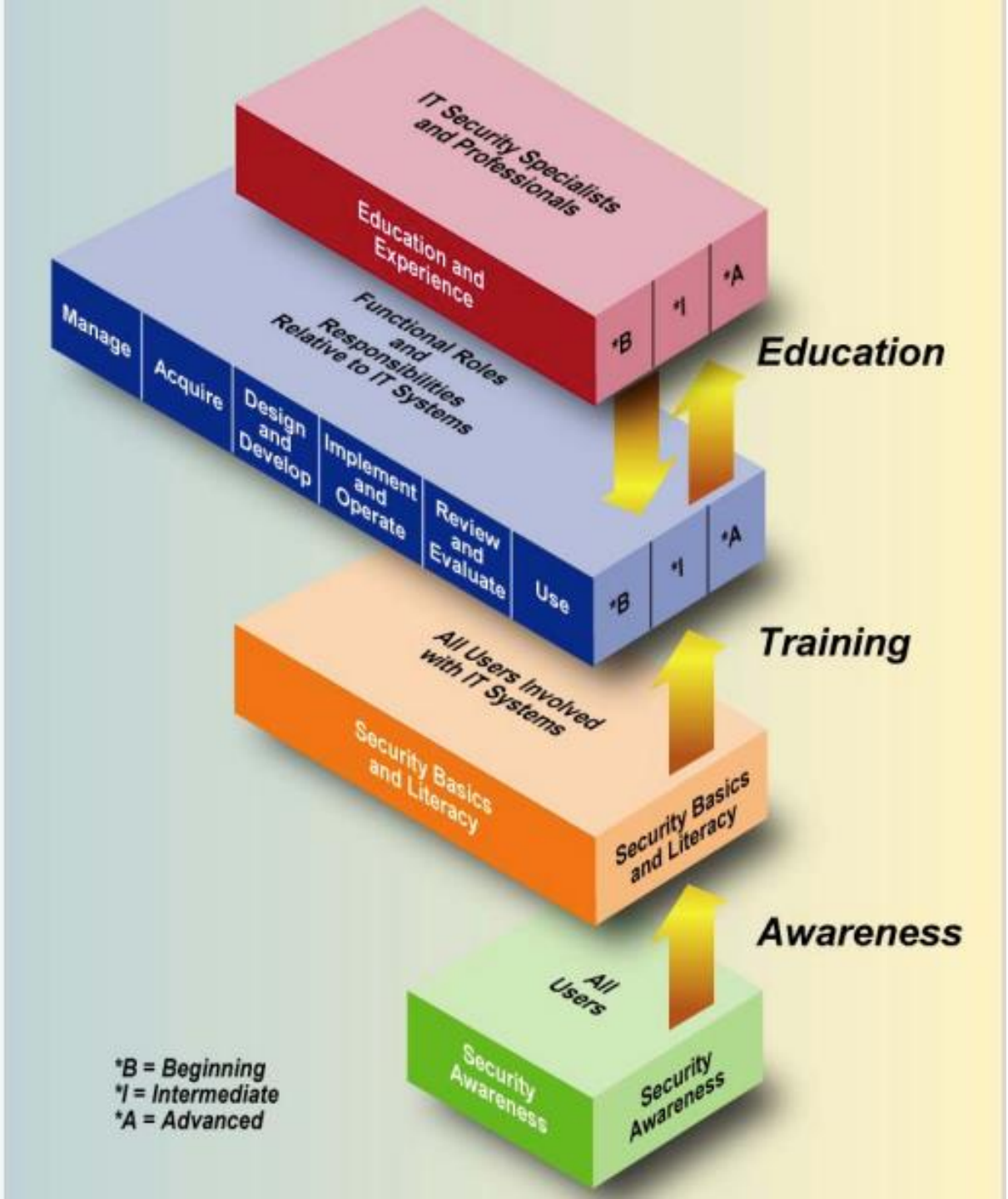
Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

Submit your comments by November 5, 2021.

Learn more: https://go.usa.gov/xMU4y

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION



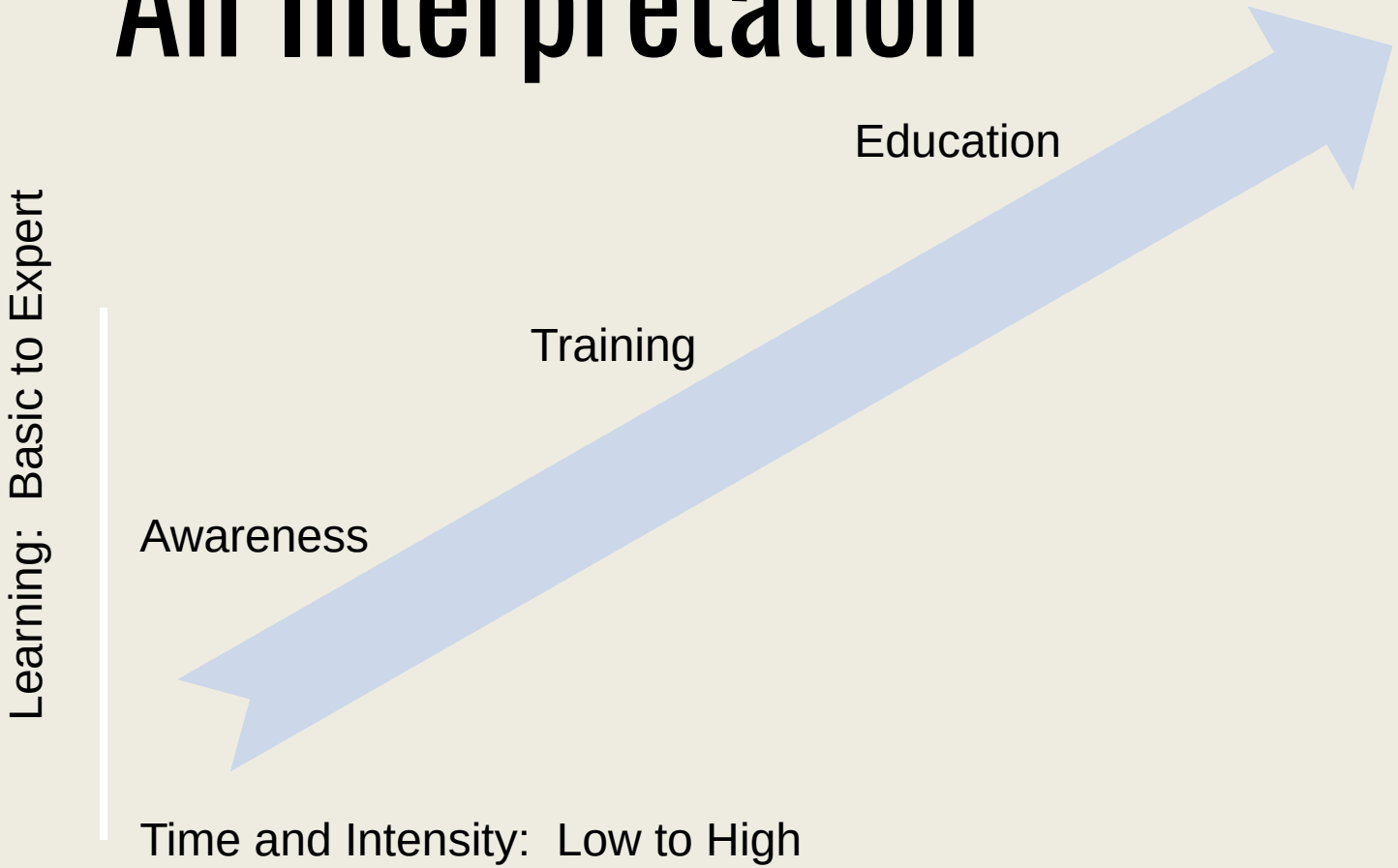
The IT Security Learning Continuum

Awareness Defined

Awareness is not training.
The purpose of awareness presentations is simply to focus attention on security.
Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.
In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role.
Awareness relies on reaching broad audiences with attractive packaging techniques.
Training is more formal, having a goal of building knowledge and skills to facilitate the job performance.

Source: NIST Special Publication 800-16 – A Role-Based Model for Federal Information Technology and Cybersecurity Training

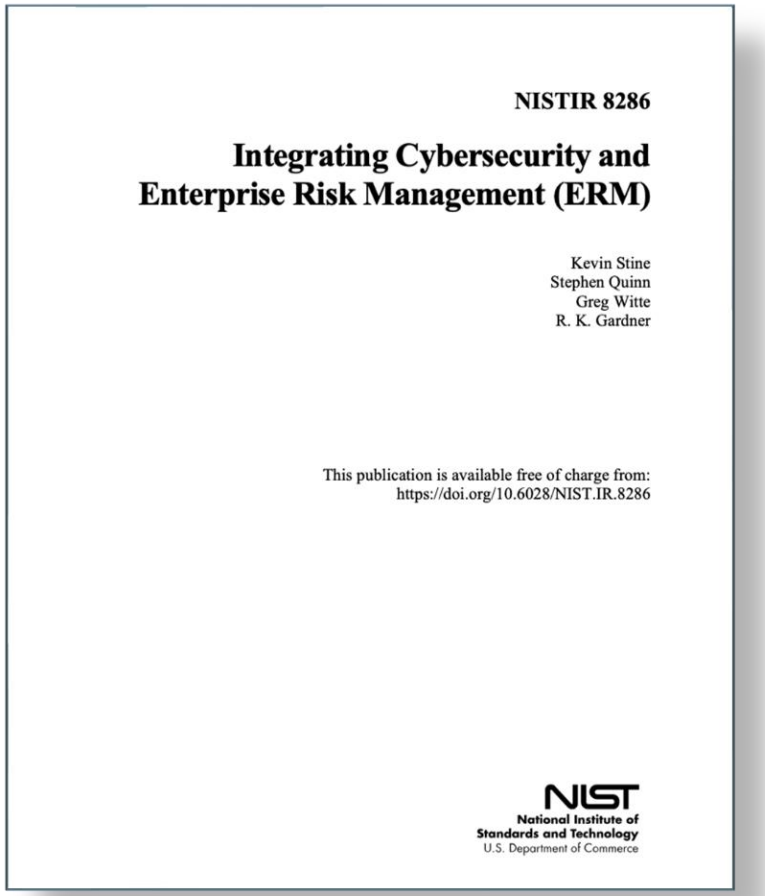
The Learning Continuum: An Interpretation



Integrating Cybersecurity and Enterprise Risk Management

People = Workforce, Training, and Education

https://csrc.nist.gov/publications/detail/nistir/8286/final

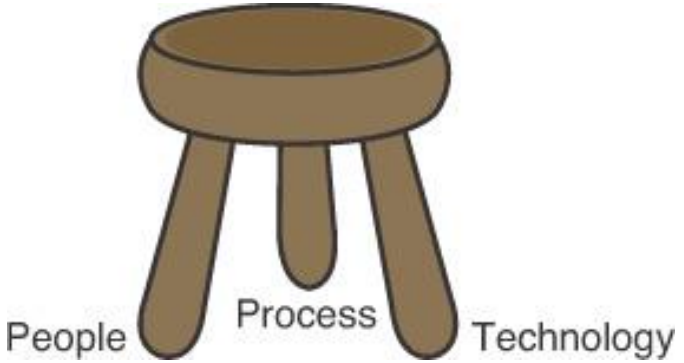

NISTIR 8286

Integrating Cybersecurity and Enterprise Risk Management (ERM)

Kevin Stine
Stephen Quinn
Greg Witte
R. K. Gardner

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8286

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Security Awareness: Managing Human Risk

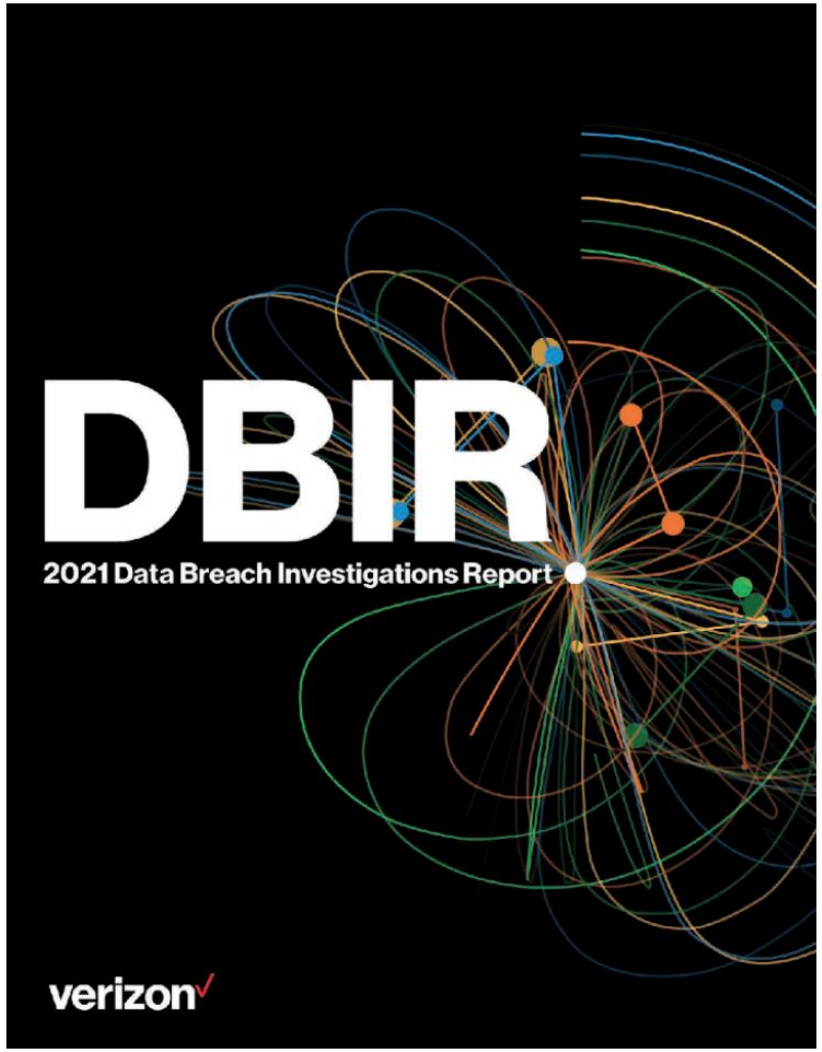
Lance Spitzner
Director, SANS Security Awareness

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

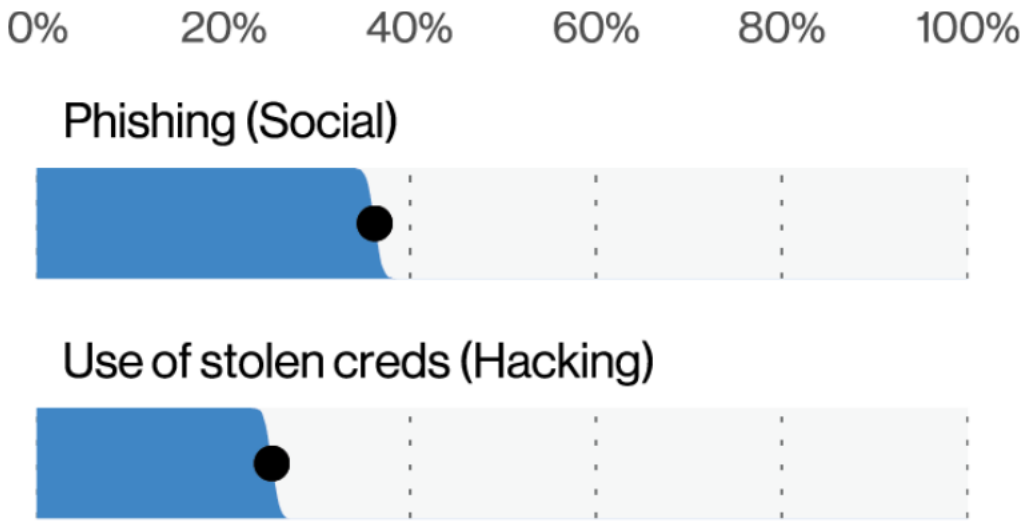
Security Awareness - Managing Human Risk

Lance Spitzner
lspitzner@sans.org

The Problem



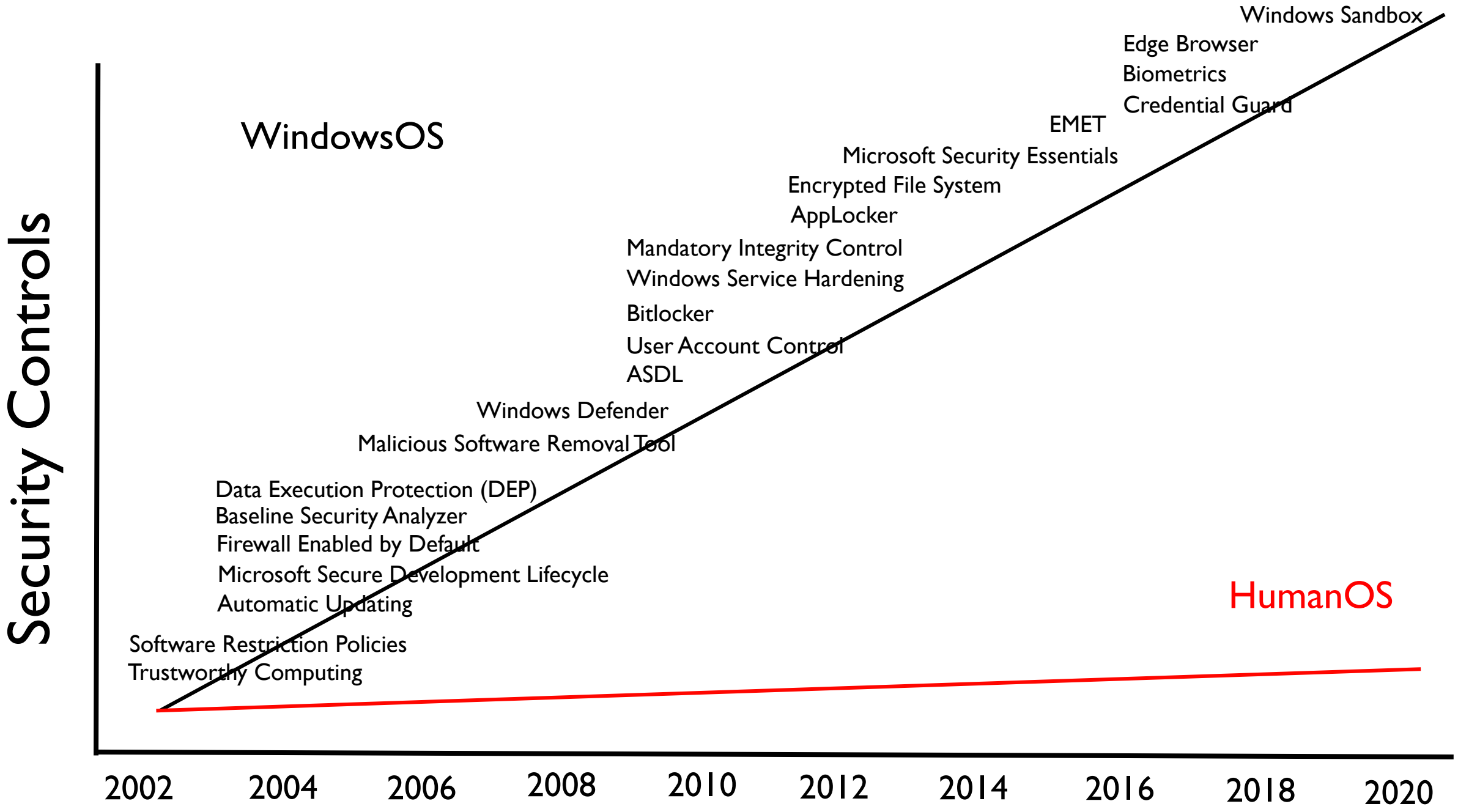
85% of breaches involve the human element



Cybersecurity Perceived as Technical

- Cybersecurity is perceived by too many as purely a technical challenge
- In today's world we also have to address the human side of cybersecurity
- No human focused work role in NIST NICE

16


Security Controls
WindowsOS
HumanOS
Windows Sandbox
Edge Browser
Biometrics
Credential Guard
EMET
Microsoft Security Essentials
Encrypted File System
AppLocker
Mandatory Integrity Control
Windows Service Hardening
Bitlocker
User Account Control
ASDL
Windows Defender
Malicious Software Removal Tool
Data Execution Protection (DEP)
Baseline Security Analyzer
Firewall Enabled by Default
Microsoft Secure Development Lifecycle
Automatic Updating
Software Restriction Policies
Trustworthy Computing
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020

People are not the weakest link - they are the primary attack vector


THE SOLUTION

Security Awareness

Influence

Culture

Engagement

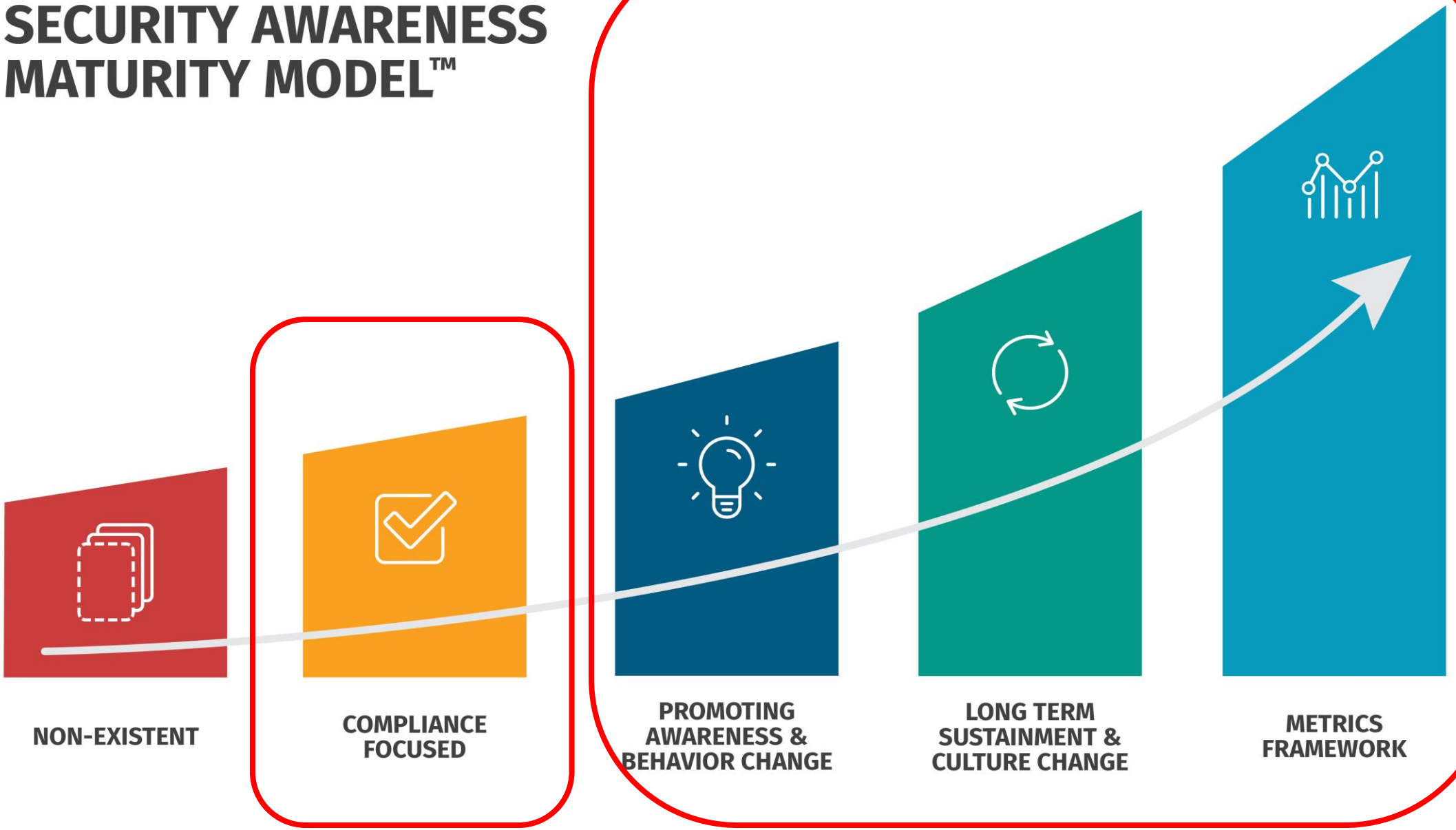
Training

Communication

Education

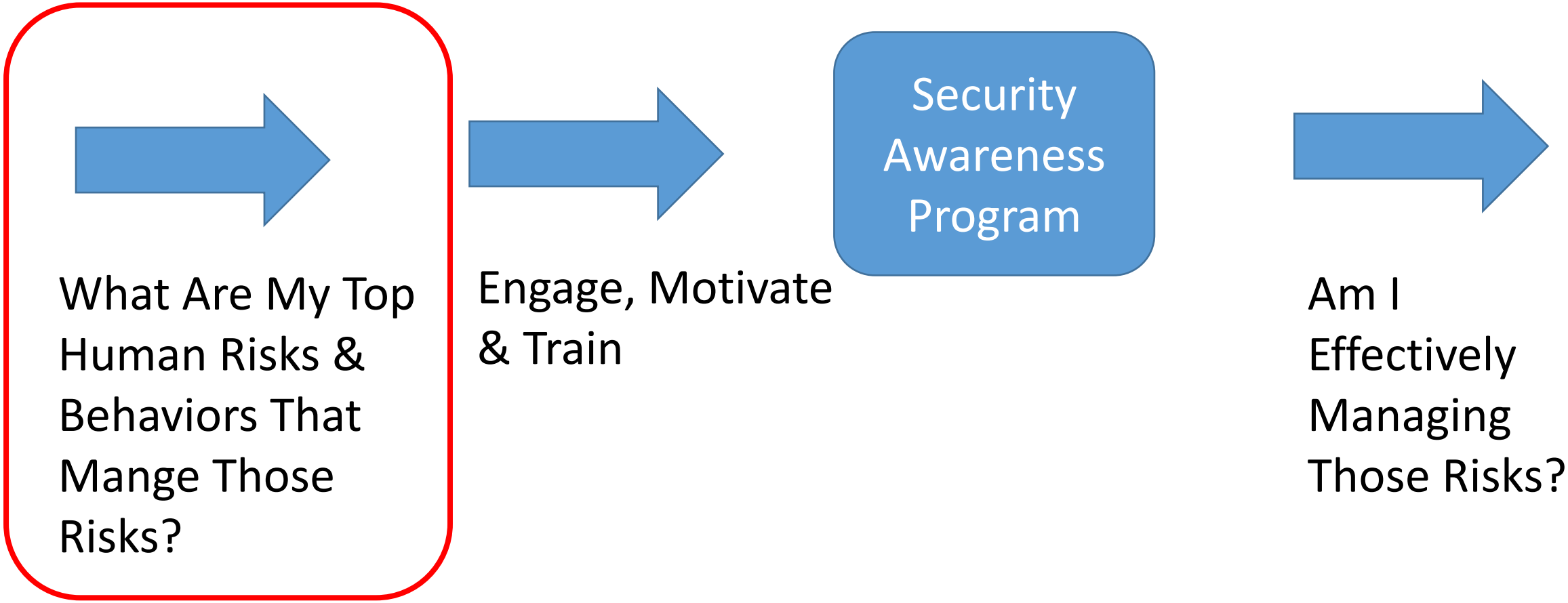
Manage human risk by changing human behavior

SECURITY AWARENESS MATURITY MODEL™



SANS SECURITY AWARENESS

3 Steps to Managing Human Risk



1. What Are My Top Human Risks?

- To effectively manage human risk you need to first identify and prioritize your human risks
- These decisions should be driven by data, not emotion

Data Sources

- Past incidents / breaches
- Past assessments / audits
- Industry risk reports
- Human risk / behavior assessments
- Cyber Threat Intelligence (CTI)

2. Engage and Train

- Engage, train and motivate behavior change, often working with communications, marketing or Human Resources
- Always start with WHY (Golden Circle)
- Curse of Knowledge

3. Measure Change & Impact

- Identify your top human risks
- Identify the key behaviors that manage those risks

Measure those behaviors

Interactive Metrics Matrix

Tab	Description
Impact Metrics – Behaviors	These metrics measure the impact of your security awareness training. Specifically, is the training changing people's behaviors.
Impact Metrics - Culture	These metrics measure the impact of your security awareness program or other security initiatives. Specifically, are they changing peoples attitudes, beliefs and norms concerning security.
Impact Metrics – Strategic	These metrics measure how your security awareness program is supporting your organization's overall security program, and ultimately the mission of your organization. These are the types of metrics senior leadership are more likely to be interested in.
Compliance Metrics	These metrics measure what your awareness program is doing, specifically who you are training and how. These metrics are most valuable for compliance and auditing purposes.
Ambassador Program Metrics	These metrics measure the activity and impact of a security ambassador program.
Human Risk Score	Proof of concept Human Metrics Dashboard that measures your overall human risk based on index of your top human risks. Designed for senior leadership.

Our goal is defining a role in managing human risk

NICE Framework: Competencies & Work Roles

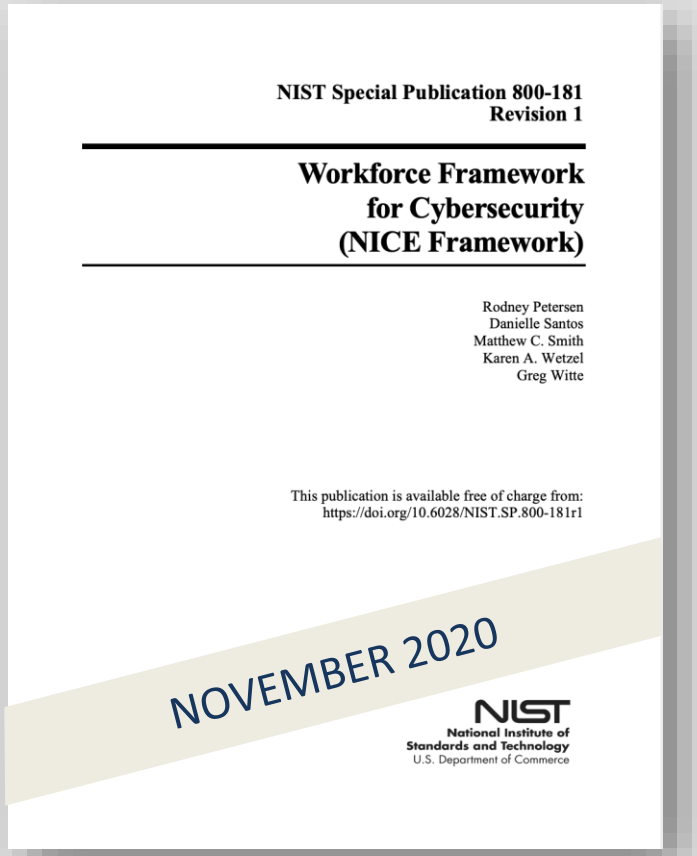
Danielle Santos
Manager of Communications,
National Initiative for Cybersecurity Education (NICE)

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

What is it?

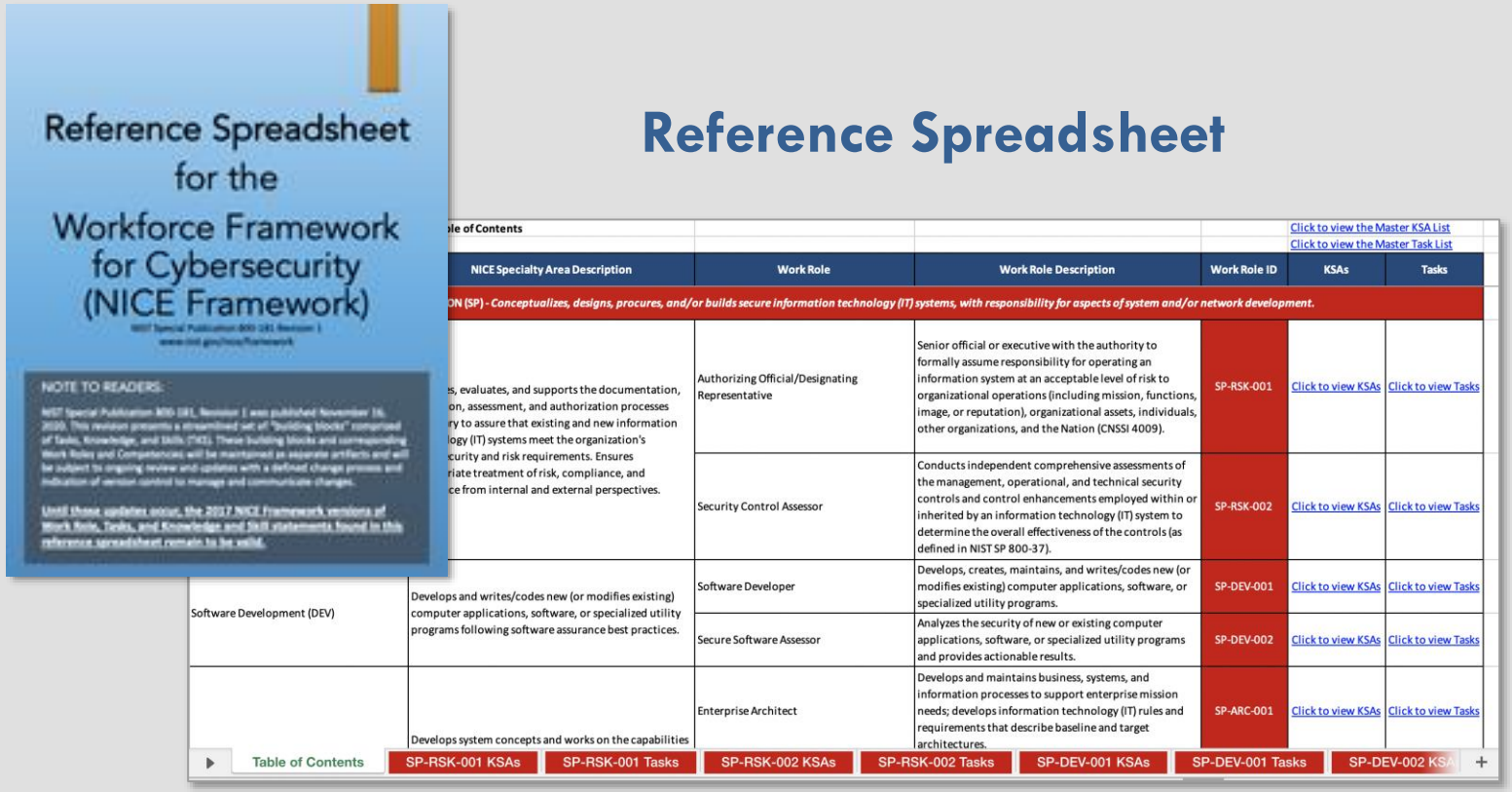
Workforce Framework for Cybersecurity (NICE Framework)

Framework Document



nist.gov/nice/framework

Reference Spreadsheet



www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-supplemental-material

HOW CAN I USE THE NICE FRAMEWORK?

Employers

- Track workforce capabilities
- Position descriptions
- Assess learner capabilities
- Develop teams

Education & Training Providers

- Develop a learning program
- Align teaching with NICE Framework
- Assess whether learners have achieved capabilities

Learners

- Learn about a defined area of expertise
- Understand an organization's workforce needs
- Self-assessment

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

SLIDESMANIA.COM

NICE Framework by the Numbers

Categories

High-level way to sort Work Roles into related areas. Includes: Securely Provision, Operate and Maintain, Oversee and Govern, Protect and Defend, Analyze, Collect and Operate, and Investigate.

Work Roles

A grouping of work for which someone is responsible or accountable. Consist of Tasks that constitute the work to be done..

Competencies

A mechanism for organizations to assess learners. Consist of TKS statements that define the area of work. May be additive to Work Roles.

Task Statements

Define the work to be done

Knowledge Statements

Define what someone must know to complete a Task.

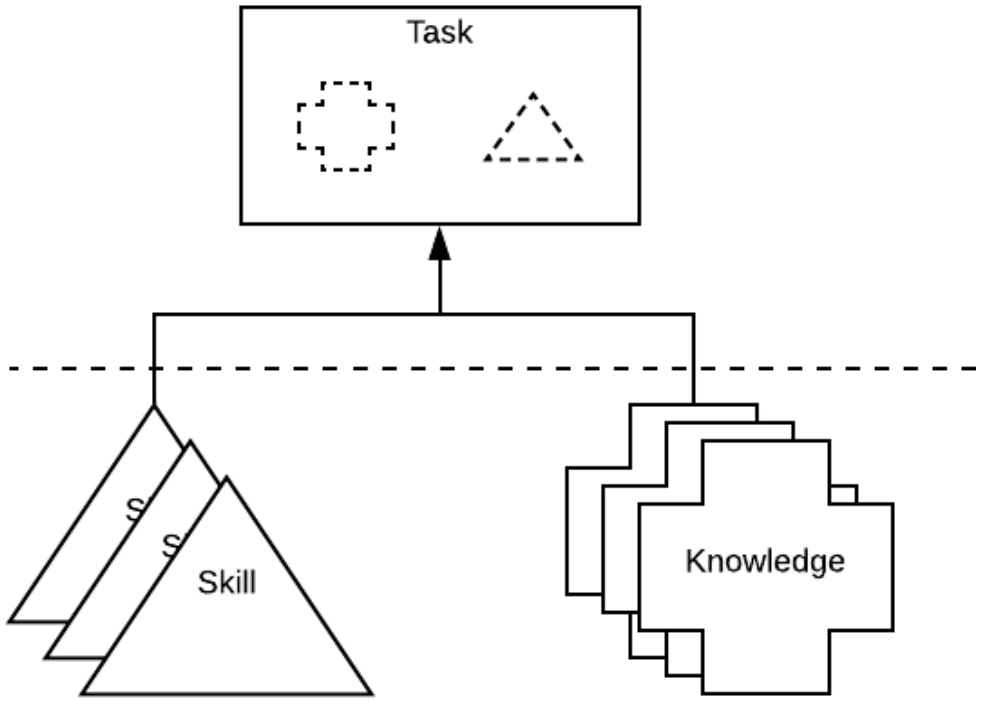
Skill Statements

Define what someone must be able to do to complete a Task.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Framework Building Blocks

Task, Knowledge, and Skill (TKS) Statements



Using the NICE Framework: **Building Block Applications**

TEAMS

- Defined by Competencies or Work Roles

COMPETENCIES

- Groupings of TKS
- Means of assessing a learner

WORK ROLES

- Groupings of Tasks
- Work someone is responsible for

Work Roles & Competencies

What do they offer?

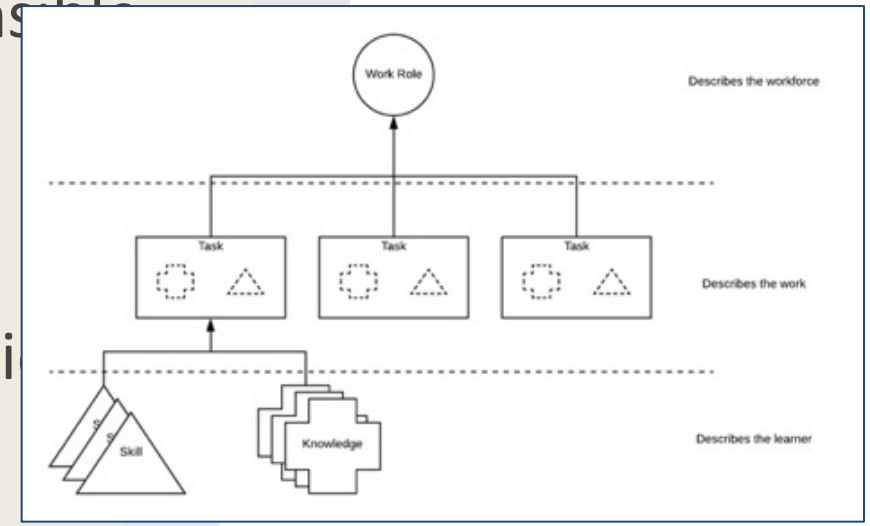
- A common language to describe cybersecurity work
- A way to identify job and qualification requirements
- Assessment-based hiring and promotion
- A means to identify current gaps and training needs and anticipate future requirements
- A way to align work with organizational objectives
- A way to align education and training to organizational goals
- A flexible approach – can be combined with other Work Roles and Competencies

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Framework Work Roles

Work Role:

A grouping of work for which someone is responsible or accountable



Work Roles:

- Are not synonymous with job titles or occupati
- May apply to many varying job titles
- Can be combined to create a particular job

Consist of:

- Tasks that constitute the work to be done

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Related NICE Framework Work Roles

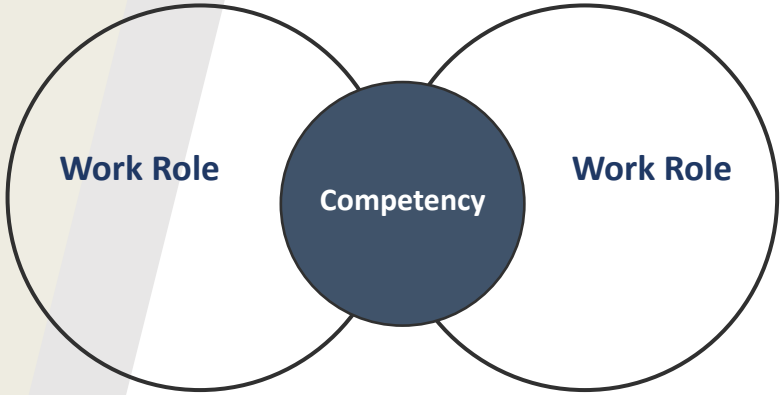
Category	OVERSEE & GOVERN (OV): Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Work Role	**Cyber Instructional Curriculum Developer:** Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs. **Cyber Instructor:** Develops and conducts training or education of personnel within cyber domain.
TKS Statements	*47* Tasks (38 unique) and ~150 Knowledge and Skill statements
Some Potential Related Competencies	• Education and Training Delivery • Education and Training Curriculum Development • Professional Competencies (E.g., Communication, Interpersonal Skills) • Organizational Awareness • Risk Management • Law, Policy, and Ethics

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Framework Competencies

Competency:

A mechanism for organizations to assess learners (including students, job-seekers, and employees) as well as a means for learners to demonstrate capability in a particular domain.



Competencies are:

- Defined via an employer-driven approach
- Learner-focused
- Can apply to multiple Work Roles, although a Work Role can also stand independent of the Competency

Consist of:

- Competency title
- Competency description
- Associated TKS statements

Draft NISTIR 8355

NICE Framework Competencies: Assessing Learners for Cybersecurity Work

https://csrc.nist.gov/publications/detail/nistir/8355/draft

NICE Framework Competency Examples

Competency Title	Competency Type	Competency Description
Contracting and Procurement	Organizational	This Competency describes a learner's capabilities related to procuring, negotiating, administering, and managing various types of contracts, including application of contracting or procurement techniques and requirements according to applicable laws and policies.
Infrastructure Design	Technical	This Competency describes a learner's capabilities related to the architecture and topology of software, hardware, and networks, including LANS, WANS, and telecommunications systems, their components and associated protocols and standards, and how they operate and integrate with one another and with associated controlling software.
Strategic Planning	Leadership	This Competency describes a learner's capabilities related to formulating effective tactics and metrics associated with the vision, mission, goals, and objectives of the organization or business unit.
Communication	Professional	This Competency describes a learner's capabilities related to the process of clearly and effectively expressing information or ideas to individuals or groups in a variety of ways (verbal, nonverbal, written, and visual). Includes understanding when and how to adapt messages for different audiences as well as listening to others' instructions, ideas and intentions, attending nonverbal cues, and responding appropriately.

How Do They Differ?

Competencies

- Learner focused
- Help address employer needs
- Assessment is typically based on the competency as a whole

Work Roles

- Work focused
- Help define positions and responsibilities
- Assessment typically occurs at the task level

Where is security awareness work already referenced?

- NIST SP 800-181: NICE Framework
  - Cyber Instructional Curriculum Developer Work Role
  - Cyber Instructor Work Role
- NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations, Section 3.2 Awareness and Training
  - Policy and Procedures
  - Literacy Training and Awareness
  - Role-Based Training
  - Training Records
  - Training Feedback
- NIST SP 800-50: Building an Information Technology Security Awareness and Training Program
  - Designing the program
  - Developing the awareness and training material
  - Implementing the program
- NIST Cybersecurity Framework: Framework for Improving Critical Infrastructure Cybersecurity version 1.1
  - Awareness and Training (PR.AT) Category: The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Discussion

- What is driving the need for Security Awareness in the NICE Framework?
- What are the biggest challenges for us to address?
- What questions do you have?

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Break

Rejoin at 2:25 p.m. ET

11:25 a.m. PT

Break-out Session: Identifying What is Unique in Security Awareness

Becky Foreman, Facilitator

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Integrating Security Awareness into the NICE Framework: Coming to Consensus

Becky Foreman, Facilitator

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Break

Rejoin at 4:10 p.m. ET

1:10 p.m. PT

Integrating Security Awareness into the NICE Framework: Building the Content

Becky Foreman, Facilitator

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Closing Session: Where We Go From Here

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

How to Engage

Visit the NICE Framework Resource Center
www.NIST.gov/NICE/Framework

Contribute your Success Stories or **Ask** questions
niceframework@nist.gov

Join the NICE Framework Users Group to discuss and learn more

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Contact me at karen.wetzel@nist.gov

THANK YOU