Federal Information Security Educators (FISSEA)

Spring Forum

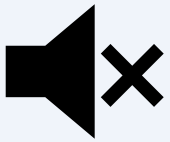
May 13, 2025

1:00pm – 4:30pm ET

#FISSEA | nist.gov/fissea

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

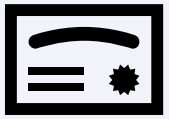
Notes and Reminders



Attendees are muted: Due to the number of attendees, all participant microphones and cameras are automatically muted.

Webinar Recording: This webinar and the engagement tools will be recorded. An archive will be available at www.nist.gov/fissea.

Submitting Questions: Please enter questions and comments for presenters in the Zoom for Government Q&A. Chat has been disabled for this event.



CE/CPE credits: The CEU form will be available on the event page after the event.

Welcome and Opening Remarks

Rodney Petersen
Director of Education and Workforce
Applied Cybersecurity Division
National Institute of Standards and Technology

Frauke Steinmeier
FISSEA Co-Chair

Latha Reddy
FISSEA Co-Chair

Get Involved

Subscribe to the FISSEA Mailing List
FISSEAUpdates+subscribe@list.nist.gov

Volunteer for the Planning Committee
https://www.nist.gov/itl/applied-cybersecurity/fissea/meet-fissea-planning-committee

Serve on the Contest or Award Committees
Email fissea@nist.gov

Submit a presentation proposal for a future FISSEA Forum
https://www.surveymonkey.com/r/fisseacallforpresentations

Unlocking Free Cybersecurity Awareness & Training Resources: Let's Share!

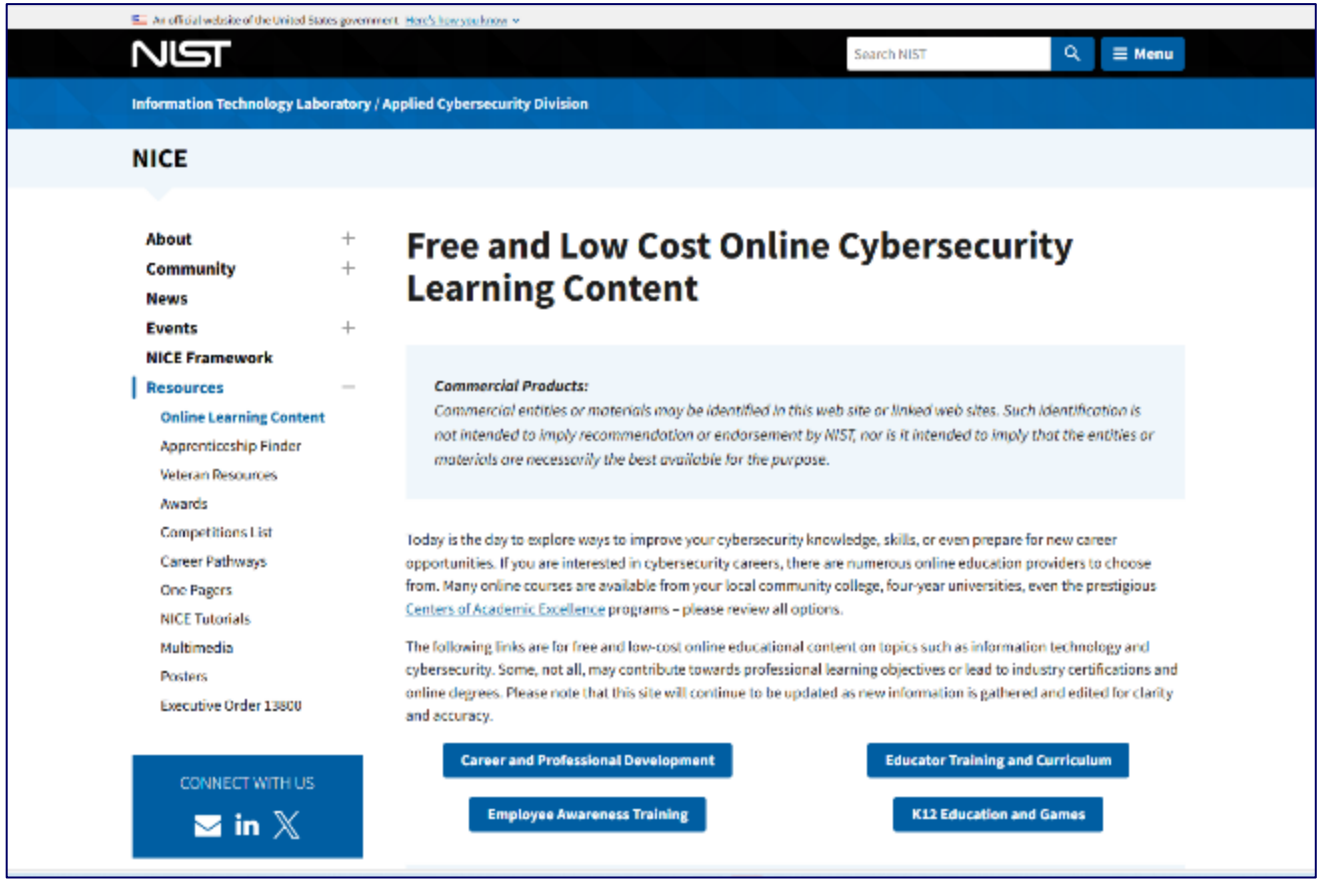
Susan Hansche

Training Manager
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FISSEA SPRING FORUM 2025

UNLOCKING FREE AND LOW-COST CYBERSECURITY AWARENESS & TRAINING RESOURCES: LET'S SHARE!

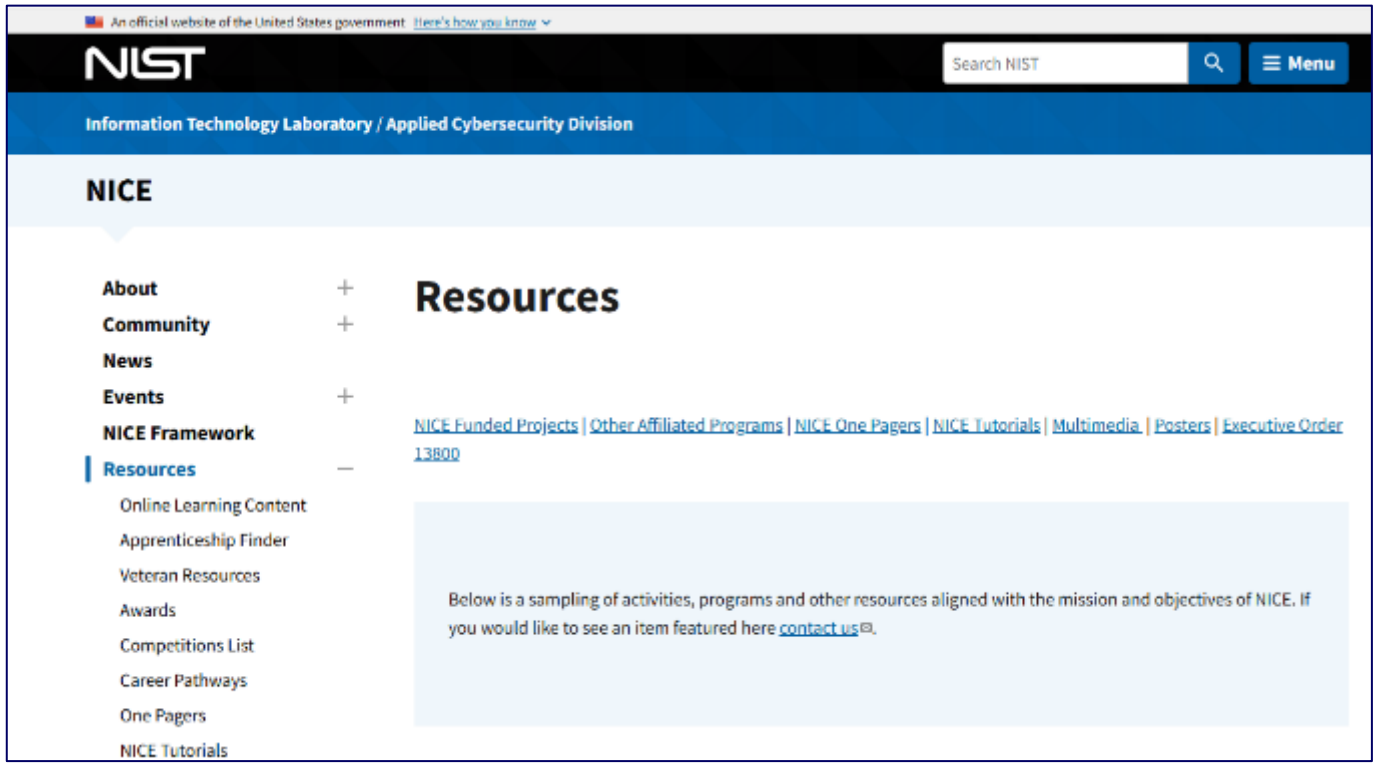
NIST Resources



[Free and Low Cost Online Cybersecurity Learning Content | NIST]

- Career and Professional Development (over 50 links)
- Employee Awareness Training (9 links)
- Educator Training and Curriculum (13 links)
- K12 Education and Games (10 links)

NIST Resources



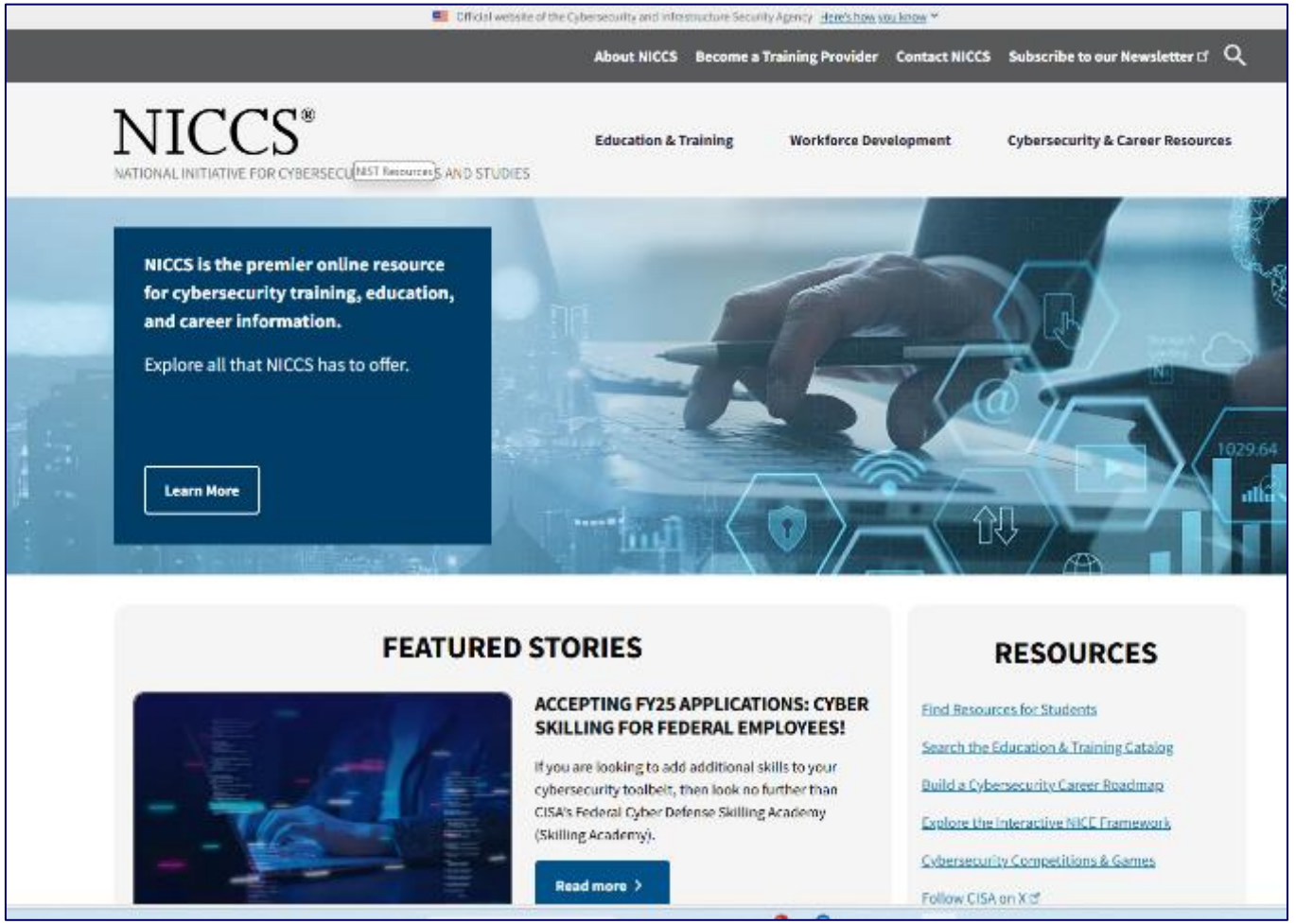
Resources | NIST

- NICE Framework Resource Center
- NICE Cybersecurity Apprenticeship Program Finder
- Veteran Resources
- Regional Alliances and Multi-stakeholder Partnerships (RAMPS)
- Discovering Cybersecurity Careers
- Cybersecurity Awards
- Cybersecurity Competitions
- Cybersecurity Career Pathway Resources

CISA Programs

CISA - NICCS

- National Initiative for Cybersecurity Careers and Studies
- https://niccs.cisa.gov
- Education and Training
- Workforce Development
- Cybersecurity & Career Resources

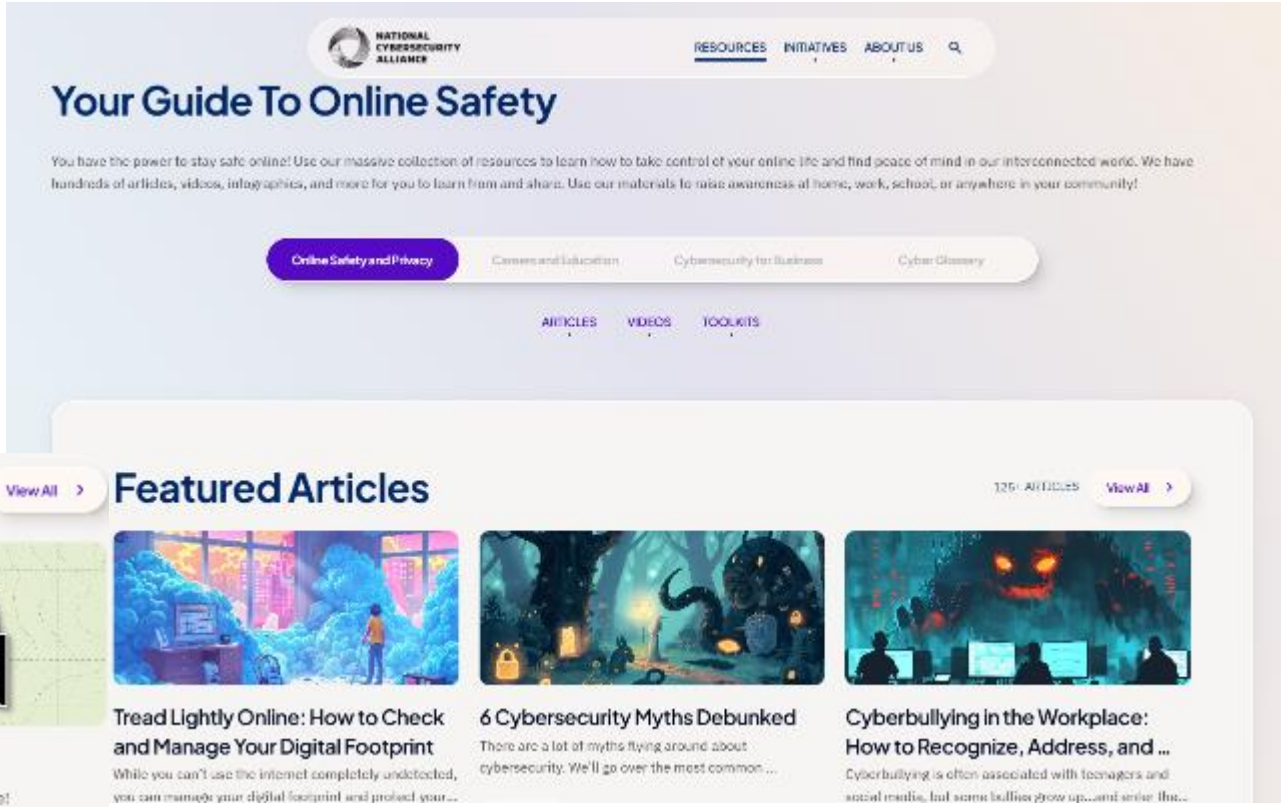


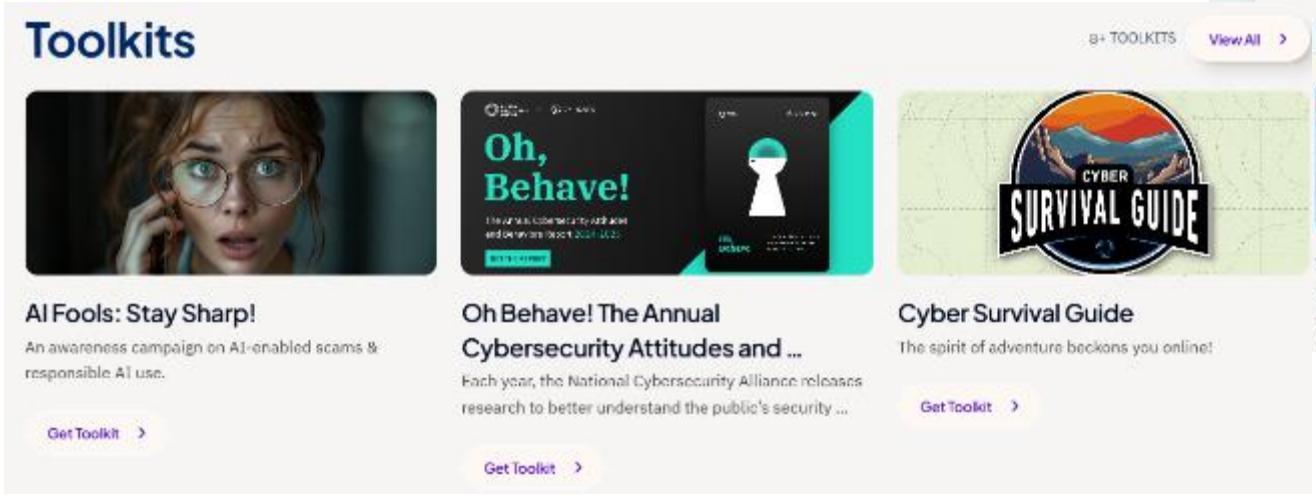
CISA - Awareness

[Cybersecurity Awareness Month | CISA]

Staysafeonline.org

Cybersecurity Awareness Resources

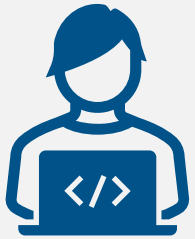




CISA Learning (formerly FedVTE)

CISA Learning https://learning.cisa.gov/ (replaced FedVTE)

- CISA Learning will continue to offer the same no cost online cybersecurity training as FedVTE on topics such as cloud security, ethical hacking and surveillance, risk management, malware analysis, and more.
- CISA Learning is available for:
  - Federal government employees and contractors
  - State, Local, Tribal, and Territorial (SLTT) government employees
  - U.S. military personnel and Veterans
  - General public
- Two Zero Trust courses are available, as well as courses on incident response, securing systems, and so much more!



Training for everyone

President’s Cup Cybersecurity Competition

Cyber threats across the globe have put into focus our country’s need for cyber talent. CISA developed the President’s Cup (PC) Cybersecurity Competition to identify, recognize, and reward the best cyber talent within the federal workforce who face these threats.

PC strengthens the federal cybersecurity workforce by providing a robust array of training materials designed around areas across the NICE Framework, and by boosting the pipeline through increased recognition of the cybersecurity profession.

A Unique Training Experience

This competition's challenges are designed to stretch competitors’ abilities and test their aptitudes through a fun, unique experience. By couching the competition in a video game setting, participants have a training activity that encourages fun and creativity while expanding their cybersecurity skill sets. To try your hand at past PC challenges, visit the President’s Cup Practice Area!

Federal Cyber Defense Skilling Academy

The Federal Cyber Defense Skilling Academy helps students develop their cyber defense skills through training in the baseline knowledge, skills, and abilities of a Cyber Defense Analyst (CDA). Students will have the opportunity to temporarily step away from their current roles to focus on professional growth through an intense, full-time, three-month accelerated training program. Full-time, civilian federal employees in any job series, grades GS-11 and below, or grade equivalent for non-GS employees, are eligible to apply to the Skilling Academy.

Providing Lifelong Skills and Certifications

The course is mapped to the NICE Cybersecurity Workforce Framework and provides valuable opportunities to practice new CDA skills in a lab environment. As an added incentive, students will receive CompTIA Security+ training during the last two weeks of the Skilling Academy and a voucher to take the certification exam.

Industrial Control Systems

The security of industrial control systems (ICS) is among the most important aspects of CISA's collective effort to defend cyberspace. The ICS trainings are a symbol of CISA's commitment to working with the ICS community to address both urgent operational cyber events and long-term ICS risks.

- Additional content added regularly
- Scheduled Online Training
  - Featuring the 301V and 401V courses, which run on a schedule
- Instructure-Led, In-Person Training
  - Featuring the 301L and 401L courses hosted by the Idaho National Laboratory (INL) in Idaho Falls, ID
- Regional Training
  - Virtual regional training events in support of the 10 CISA regions.

Continuous Diagnostics and Mitigation

The Continuous Diagnostics and Mitigation (CDM) trainings optimize agencies' ability to utilize the CDM dashboard, which affords increased situational awareness across their networks.

The CDM trainings equip agencies with the skills that provide benefits such as:

- Increased **automation to identify assets**
- Improved **accuracy, reporting, risk management, decision making, and incident response**
- Enhanced **near-real-time monitoring and risk**
- **Streamlined compliance** with the Federal Information Security Modernization Act (FISMA) and other federal cybersecurity mandates and initiatives
- **Improved visibility and situational awareness** within agencies and across the federal government

CDM training for federal employees whose agencies are participating in the CDM Program

The CDM trainings are available through multiple avenues to better accommodate student needs. These avenues include In-Person, Virtual In-Person and On-Demand using the Cyber Training Range, Micro Learn Videos, and Webinars.

Securing Systems and Incident Response

The best offense is a good defense. To best protect and support the capacity of our nation's cyber enterprise, CISA offers free Incident Response (IR) training courses that address the defensive view. These courses provide not only the knowledge and tools needed to prepare an effective response if a cyber incident occurs, but also how to prevent incidents from happening in the first place.

Awareness Webinars

Awareness webinars, also referred to as 100-level courses, are one-hour, entry-level, virtual, and instructor-led classes with cybersecurity topic overviews for a general audience, including managers and business leaders. These courses provide core guidance and best practices to prevent incidents, and how to prepare an effective response if an incident occurs.

Cyber Range Training

Cyber range trainings, also referred to as 200-level courses, are four-hour, interactive, virtual, and instructor-led classes, with step-action labs in a realistic technical environment. Students participate in short lectures, followed by lab activities, to identify incidents and harden systems in the cyber range environment.

On Demand Training

On-demand trainings are self-paced, available 24/7, and include two types of offerings: Step-By-Step Action Courses and Online Training Recordings.

Previously recorded training programs are available on the CISA YouTube Channel playlist and the CISA Learning platform.

Cybersecurity Awareness, Training, Education, and Research Community of Interest

The Cybersecurity Awareness, Training, Education, and Research (CATER) Community of Interest (COI) promotes collaboration in cybersecurity training efforts throughout the federal government and shares information on federally developed training activities, thereby reducing costs and avoiding duplication of effort.

To Join

CISA Workforce, Awareness, and Training Offerings

- Additional CISA Training
- CISA Learning: https://learning.cisa.gov/
- President's Cup Practice Site
- CISA's GitHub Page
- CISA's YouTube Channel
- ICS Training Range via the Virtual Learning Portal (VLP)
- CISA Cybersecurity Training & Exercises
- Cybersecurity Workforce Training Guide
- Cybersecurity Awareness Program Parent and Educator Resources | CISA
- NICE Workforce Framework for Cybersecurity (NICE Framework) | NICCS
- Career Pathways Roadmap | NICCS
- Incident Response Training | CISA
- Cybersecurity Awareness
  - National Cybersecurity Alliance
  - CISA Cybersecurity Awareness Program | CISA
  - Cybersecurity Awareness Month | CISA


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA

Q&A

Are There Any Questions?

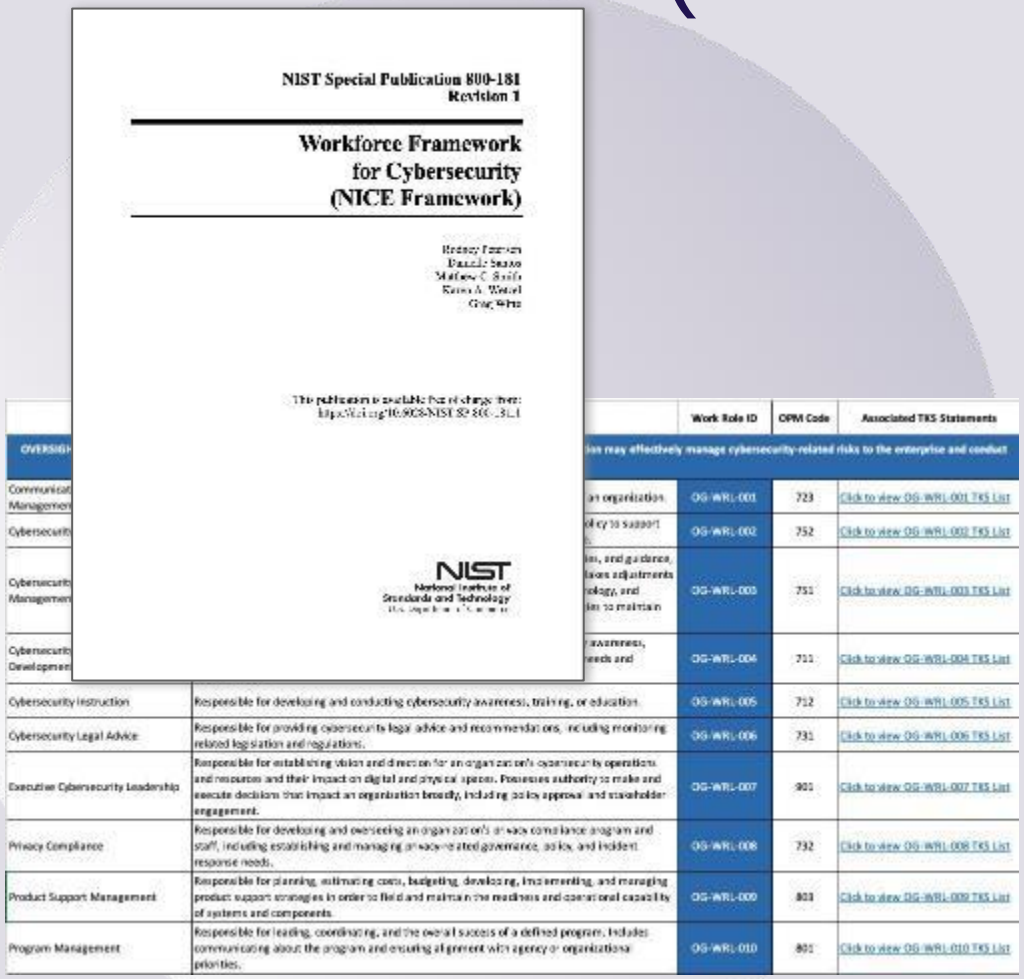
Workforce Assessment with the NICE Framework

Michael Prebil
Cybersecurity Workforce Analyst
National Institute of Standards and Technology

Workforce Assessment with the NICE Framework

Mike Prebil
Cybersecurity Workforce Analyst, NIST
FISSEA Spring Forum, May 2025

Workforce Framework for Cybersecurity (NICE Framework)



		Work Role ID	OPM Code	Associated TKS Statements
Cybersecurity Instruction	Responsible for developing and conducting cybersecurity awareness, training, or education.	OG-WRL-005	712	Click to view OG-WRL-005 TKS List
Cybersecurity Legal Advice	Responsible for providing cybersecurity legal advice and recommendations, including monitoring related legislation and regulations.	OG-WRL-006	731	Click to view OG-WRL-006 TKS List
Executive Cybersecurity Leadership	Responsible for establishing vision and direction for an organization's cybersecurity operations and resources and their impact on digital and physical spaces. Possesses authority to make and execute decisions that impact an organization broadly, including policy approval and stakeholder engagement.	OG-WRL-007	901	Click to view OG-WRL-007 TKS List
Privacy Compliance	Responsible for developing and overseeing an organization's privacy compliance program and staff, including establishing and managing privacy-related governance, policy, and incident response needs.	OG-WRL-008	732	Click to view OG-WRL-008 TKS List
Product Support Management	Responsible for planning, estimating costs, budgeting, developing, implementing, and managing product support strategies in order to field and maintain the readiness and operational capability of systems and components.	OG-WRL-009	803	Click to view OG-WRL-009 TKS List
Program Management	Responsible for leading, coordinating, and the overall success of a defined program. Includes communicating about the program and ensuring alignment with agency or organizational priorities.	OG-WRL-010	801	Click to view OG-WRL-010 TKS List

- A vocabulary for sharing information about what cybersecurity pros needs to know
- A modular approach based on Task, Knowledge, and Skill (TKS) statements
- A variety of applications including:
  - career awareness,
  - education and training,
  - assessment, hiring, & workforce planning
- A set of related tools and connected resources to expand functionality

NIST NICE

www.nist.gov/nice/framework

Value for…

EMPLOYERS

- Create job descriptions and assess candidates
- Track and plan workforce capabilities
- Structure work-based learning training

LEARNERS

- Discover and plan for cybersecurity careers
- Knowledge and skills development
- Demonstrate capability and evidence competency

EDUCATORS

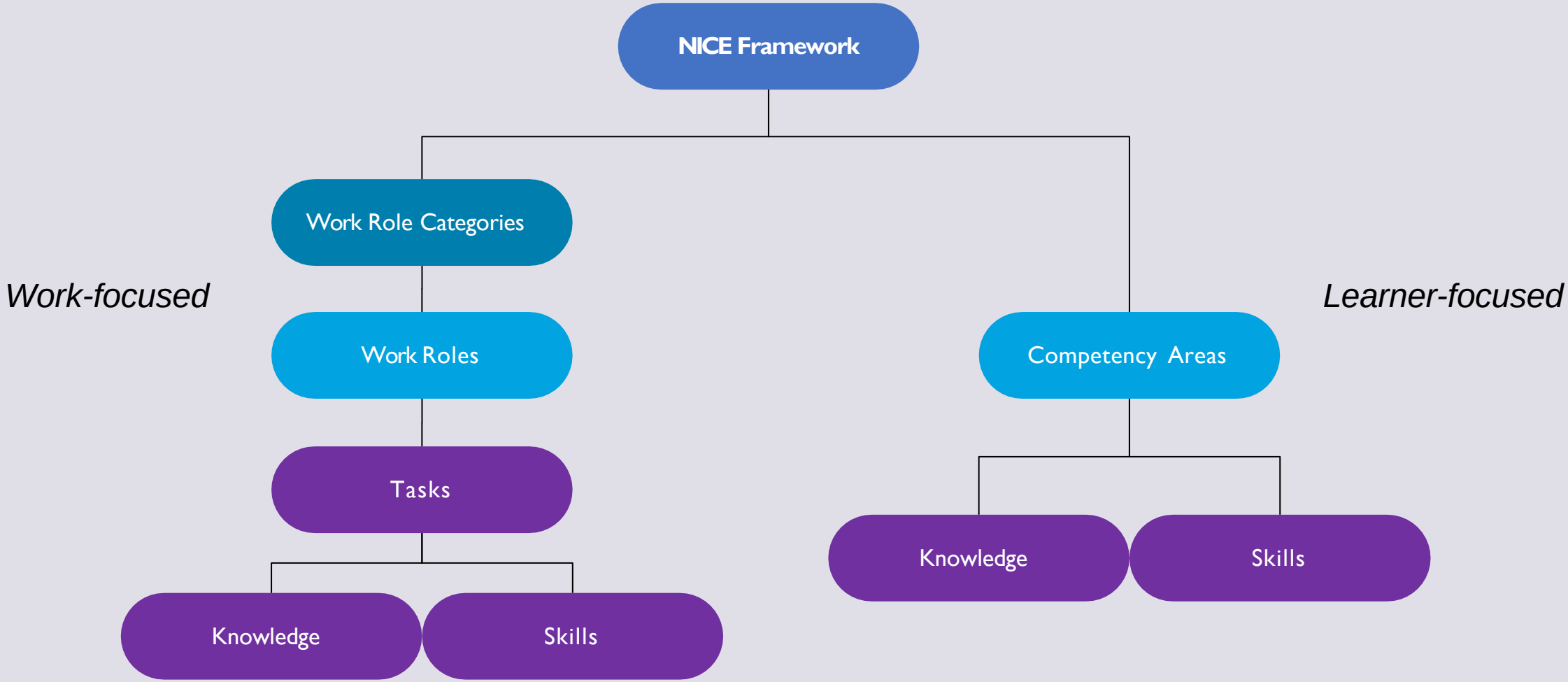
- Develop industry-relevant courses & programs
- Explore adjacent cybersecurity functions
- Conduct performance-based assessments

GOVERNMENT • INDUSTRY • ACADEMIA

NIST | NICE

NICE Framework Components

Structure of the NICE Framework

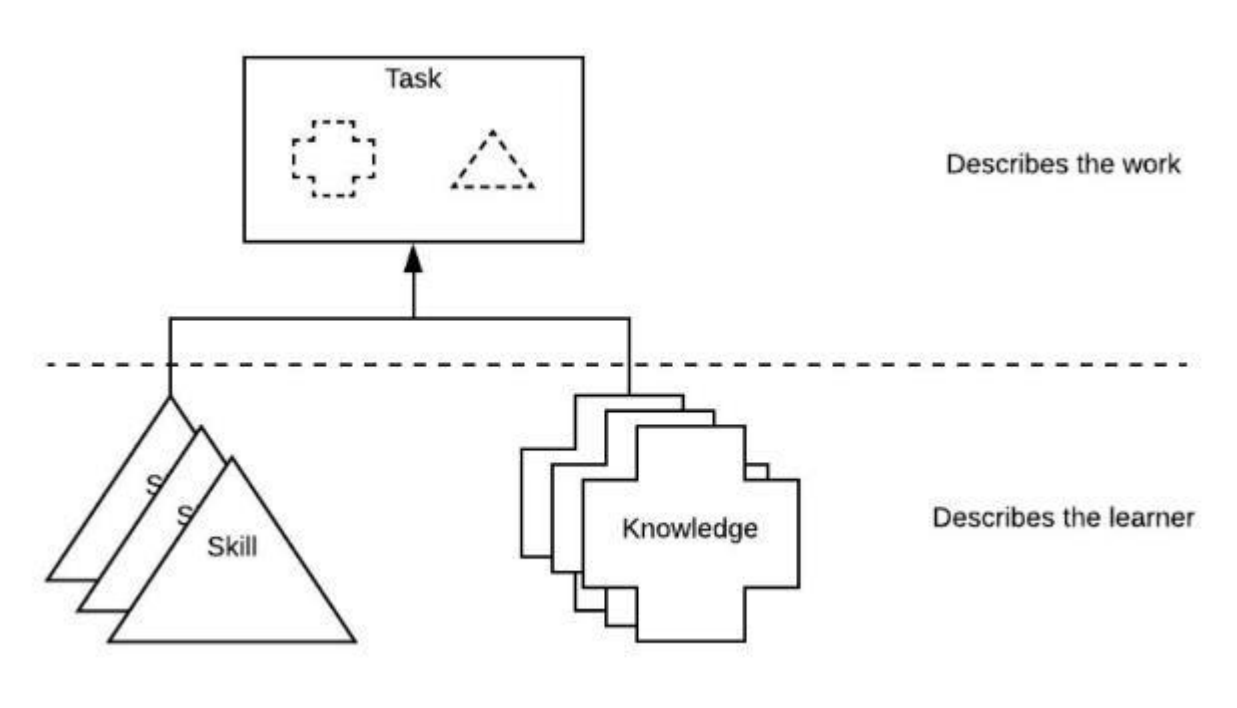


NIST | NICE

Task, Knowledge, and Skill statements

Task, Knowledge, and Skill (TKS) statements are the most basic element of the NICE Framework. 2,111 in total.

- **T1160:** Develop risk mitigation strategies
- **K0675:** Knowledge of risk management processes
- **S0686:** Skill in performing risk assessments



Note: Connections between Tasks and K&S statements are not currently contained in the NICE Framework. Users may develop these connections themselves.

NIST | NICE

Work Roles & Work Role Categories

Work Roles describe areas of work that a person (or group of people) is responsible for.

- 41 Work Roles in five Work Role Categories.
- Work Roles are one of the most commonly used NICE Framework Components.
- Work Roles have a title, ID, description, and contain associated TKS statements (50–200 each).
- **Work Roles ≠ jobs**
- Every person performing a cybersecurity job usually performs several Work Roles.

Example: **Security Control Assessment (OG-WRL-012)**—Responsible for conducting independent comprehensive assessments of management, operational, and technical security controls and control enhancements employed within or inherited by a system to determine their overall effectiveness.

NIST | NICE

Competency Areas

Competency Areas provide a separate mechanism for assessing learners.

- 11 total as of v2.0.0.
- May be used alone or in combination with Work Roles, and can relate to emerging disciplines (e.g., AI Security).
- Contain title, ID, and description.
- Competency Areas are being updated with associated Knowledge & Skill statements (in progress).

Competency Area Name	Competency Area Description
Access Controls	This Competency Area describes a learner's capabilities to define, manage, and monitor the roles and secure access privileges of who is authorized to access protected data and resources and understand the impact of different types of access controls.
Artificial Intelligence (AI) Security	This Competency Area describes a learner's capabilities to secure Artificial Intelligence (AI) against cyberattacks, to ensure it is adequately contained where it is used, and to mitigate the threat AI presents where it or its users have malicious intent.
Asset Management	This Competency Area describes a learner's capabilities to conduct and maintain an accurate inventory of all digital assets, to include identifying, developing, operating, maintaining, upgrading, and disposing of assets.
Cloud Security	This Competency Area describes a learner's capabilities to protect cloud data, applications, and infrastructure from internal and external threats.
Communications Security	This Competency Area describes a learner's capabilities to secure the transmissions, broadcasting, switching, control, and operation of communications and related network infrastructures.
Cryptography	This Competency Area describes a learner's capabilities to transform data using cryptographic processes to ensure it can only be read by the person who is authorized to access it.
Cyber Resiliency	This Competency Area describes a learner's capability related to architecting, designing, developing, implementing, and maintaining the trustworthiness of systems that use or are enabled by cyber resources in order to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises that use or are enabled by cyber resources.
DevSecOps	This Competency Area describes a learner's capabilities to integrate security as a shared responsibility throughout the development, security, and operations (DevSecOps) life cycle of technologies.

A sample of Competency Areas from the current NICE Framework Components.

NIST | NICE

Applying the NICE Framework for Workforce Assessment

NF Workforce assessment basics

The NICE Framework is designed to be flexible.

The NICE Framework Components can be used in different ways.

- “Top-down”: Starting from a high level (the organization).
- “Bottom-up”: Starting from the level of individual workers.

Hiring a Security Assurance & Disaster Recovery Lead (top-down):

1. Select target Work Role Category (Oversight & Governance)
2. Select target Work Roles (OG-WRL-006, 011, 012).
3. Identify core TKS statements.
4. Explore additional Work Roles (not too many!).
5. Consider Competency Areas (e.g., Cyber Resiliency).

NIST | NICE

An official website of the United States government

USAJOBS

Sign in Help

Back to results

IT CYBERSECURITY SPECIALIST (INFOSEC)

DEPARTMENT OF THE ARMY
Army National Guard Units
HAWAII ARMY NATIONAL GUARD

Summary | This job is open to | Duties | Requirements | How you will be evaluated | Required documents | How to Apply

Summary

THIS IS A NATIONAL GUARD TITLE 32 EXCEPTED SERVICE POSITION.

This National Guard position is for a IT CYBERSECURITY SPECIALIST (INFOSEC), Position Description Number D2486000 and is part of the HI DCSIM, National Guard.

Duties

SUMMARY OF DUTIES: The purpose of this position is to provide expertise in cybersecurity policy and process development; conducting audits to validate compliance; responsible for the risk management framework and ensures systems are operated and maintained IAW AR 25-2 and all applicable command, DA, JS and DOD security directives and procedures.

- Serves as an Information Technology Specialist providing Cybersecurity for a state National Guard headquarters. Operates within the DoD and Army security procedures, operations, and practices.
- Coordinates with Program Information System Security Managers and Organizational Information System Security Officer at other locations to verify or clarify information pertinent to cybersecurity/Information Assurance procedures.

4. Position is designated as PR-VAM-001 within the Defense Cybersecurity Workforce as guided by NIST SP 800-181; National Initiative for Cybersecurity Education, Cybersecurity Workforce Framework. Which establishes the Tasks, Skills, Knowledge and Abilities expected of this position. (https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center).

Browse jobs | About us | Students | Events | Blog | Talent community | Log In | Saved jobs (0)

Senior Information Security Engineer

Arlington, United States of America, 22203 | Cyber and Corporate Security | Full time | R-214715

Apply Now | Save job

Title and Summary

Senior Information Security Engineer

Mastercard is seeking candidates to join our Security Engineering team in Arlington, VA
Mastercard is developing the next generation of applications and services to enable consumers and businesses to securely, efficiently, and intelligently conduct payment transactions.

Whether through traditional retail, mobile, or e-commerce, Mastercard innovation is leading the digital convergence of traditional and emerging payments technologies across a wide variety of new devices and services.

This Mastercard role shares KSAs with related NICE work roles:

SP-DEV-002, OPM, 622, Secure Software Assessor
SP-ARC-002, OPM652, Security Architect
SP-TRD-001, OPM661, Research & Development Specialist
SP-SRP-001, OPM641, Systems Requirements Planner
SP-SYS-001, OPM631, Information Systems Security Developer
OV-SPP-002, OPM751, Cyber Policy and Strategy Planner

https://pixabay.com/illustrations/tear-rag-paper-crack-edge-torn-503320

Case study: Mastercard's competencies

Objective: Create career mobility options for Corporate Security staff

- Started with NICE Framework Competency Areas and Work Roles
- Recognized that K&S statements aren't specific to single roles
- Identified a pinch point in consultative process: reading through long lists!
- Grouped K&S statements into 48 organization-specific competencies
- Mapped org-specific competencies to both NICE WRs and Mastercard jobs

Competency family	Example competency:	Sample K&S statements:
Leadership	Teaching Others	*K0643:* …virtual learning environments. *S0394:* …developing security assessments
Technical	Cyber Resiliency	*K0751:* …system threats. *S0929:* …designing air-gapped data vault solutions.
Professional	Presenting Effectively	*K0905:* …media production tools & techniques. *S0728:* …presenting to an audience.

NIST | NICE

NF Resources for Workforce Assessment

The Basics
www.nist.gov/nice/framework

NICE Framework Resource Center

- Getting Started, FAQ, Current Versions, & Translations
- Success Stories (Case Studies) and Framework in Focus (Practitioner Interviews)
- TKS, Competency Area Authoring Guides
- Employers Guide to Developing Job Descriptions
- NICE Framework Users Group: Online forum and meetings for support & discussion

NICE Framework Tools

- CyberSeek: Interactive cybersecurity jobs heat map across the U.S. by state and metropolitan areas
- NICE Framework Mapping Tool hosted by CISA's National Initiative for Cybersecurity Careers & Studies (NICCS)
- NICCS Education and Training Catalog: Over 6,000 cybersecurity-related courses aligned with the NICE Framework.
- XP Cyber: Real-world cybersecurity challenges within virtualized business environments, built on the NICE Framework

Workforce collaboration resources leveraging the NICE Framework

NIST Online Informative References

Comparison reports between NIST resources

csrc.nist.gov/projects/olir

Draft CSF workforce management guide

Facilitate conversation between leadership, HR, & technical cybersecurity teams (NIST SP 1308)

C3 certification mapping

Explore NF connections in popular industry certifications

Available on NFRC

NIST | NICE

Stay in touch!
Join the NICE Framework Users Group

…and email
NICEframework@nist.gov

NIST | NICE


NIST
NICE

Q&A

Are There Any Questions?

When Agentic AI & the Cybersecurity Workforce Collide

Allen Westley
Sr. Cybersecurity Leader
L3Harris Technologies

When Agentic AI & The Cybersecurity Workforce Collide

Allen Westley, Sr. Cybersecurity Leader at L3Harris Technologies

Founder, Cyber Explorer LLC

NIST FISSEA Spring Conference

by Allen Westley

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Today's Journey

Agentic AI Foundations

Core concepts and capabilities

Workforce Collision Points

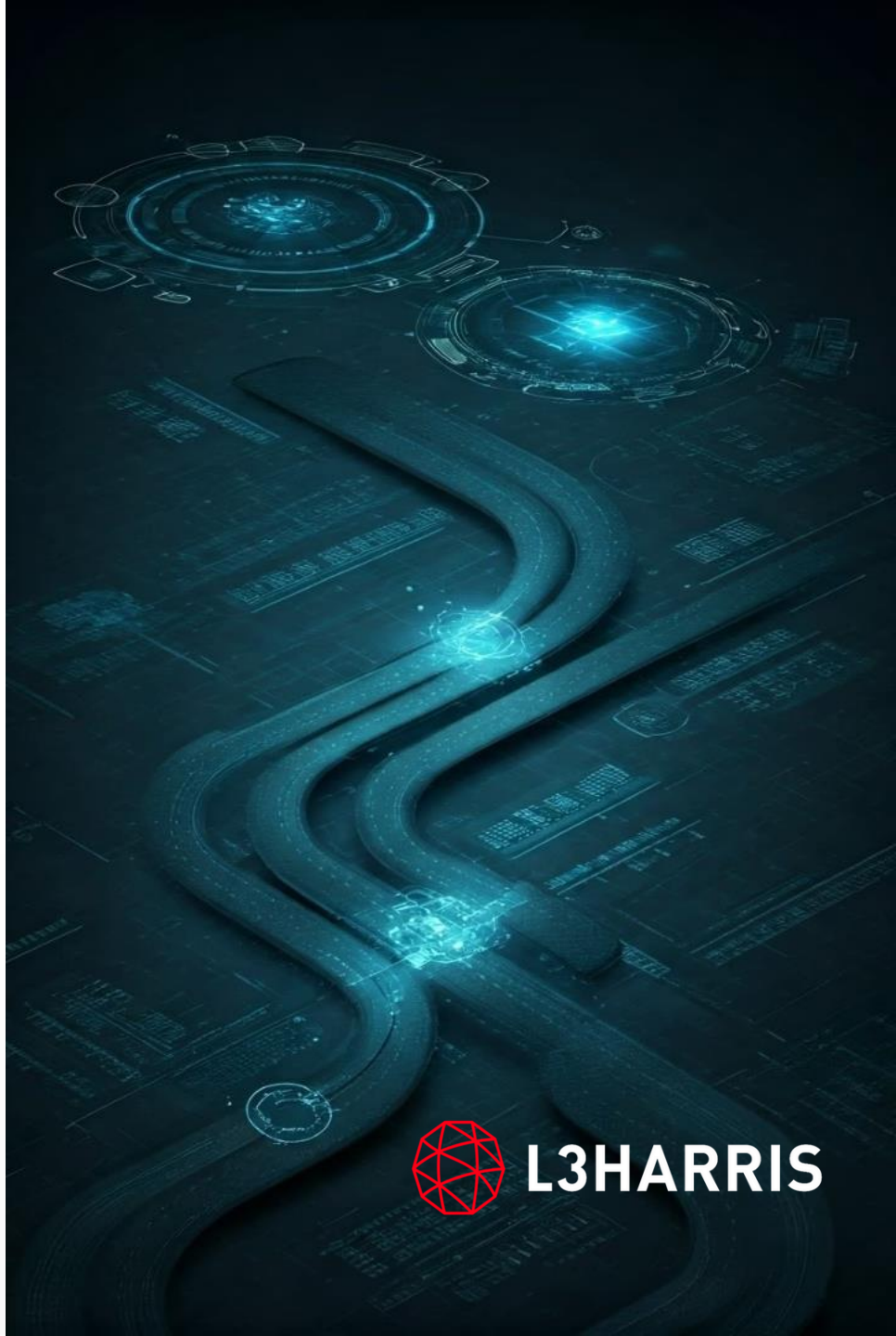
Evolution of roles and responsibilities

Mind Privacy & Cognitive Security

Protecting human thought processes

Strategic Recommendations

Positioning for future success



What is Agentic AI?

Goal-Driven Systems

Autonomous pursuit of objectives with minimal human input

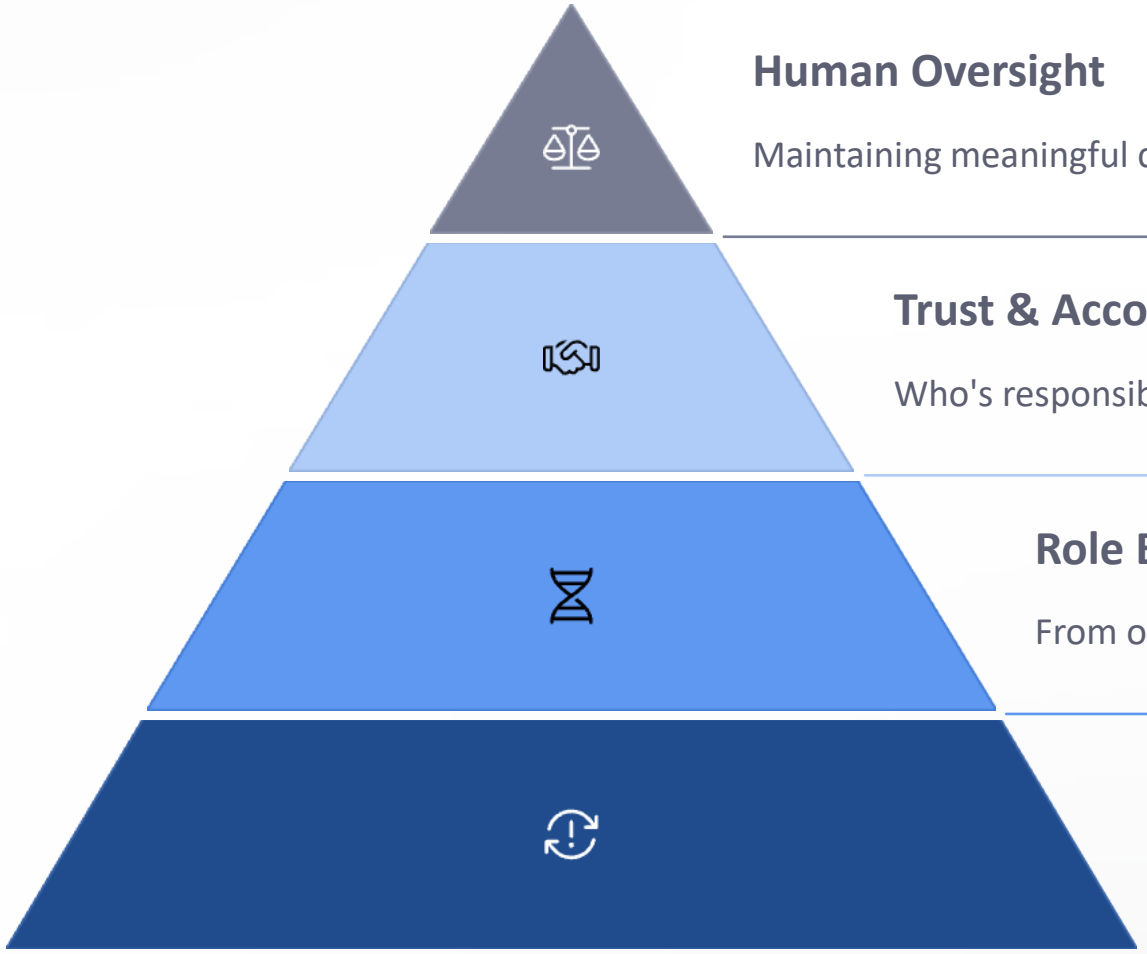
Independent Decision-Making

Evaluates options and executes without human approval

Cybersecurity Applications

Threat hunting, incident response, vulnerability management

AI-Workforce Collision Points



Human Oversight

Maintaining meaningful control

Trust & Accountability

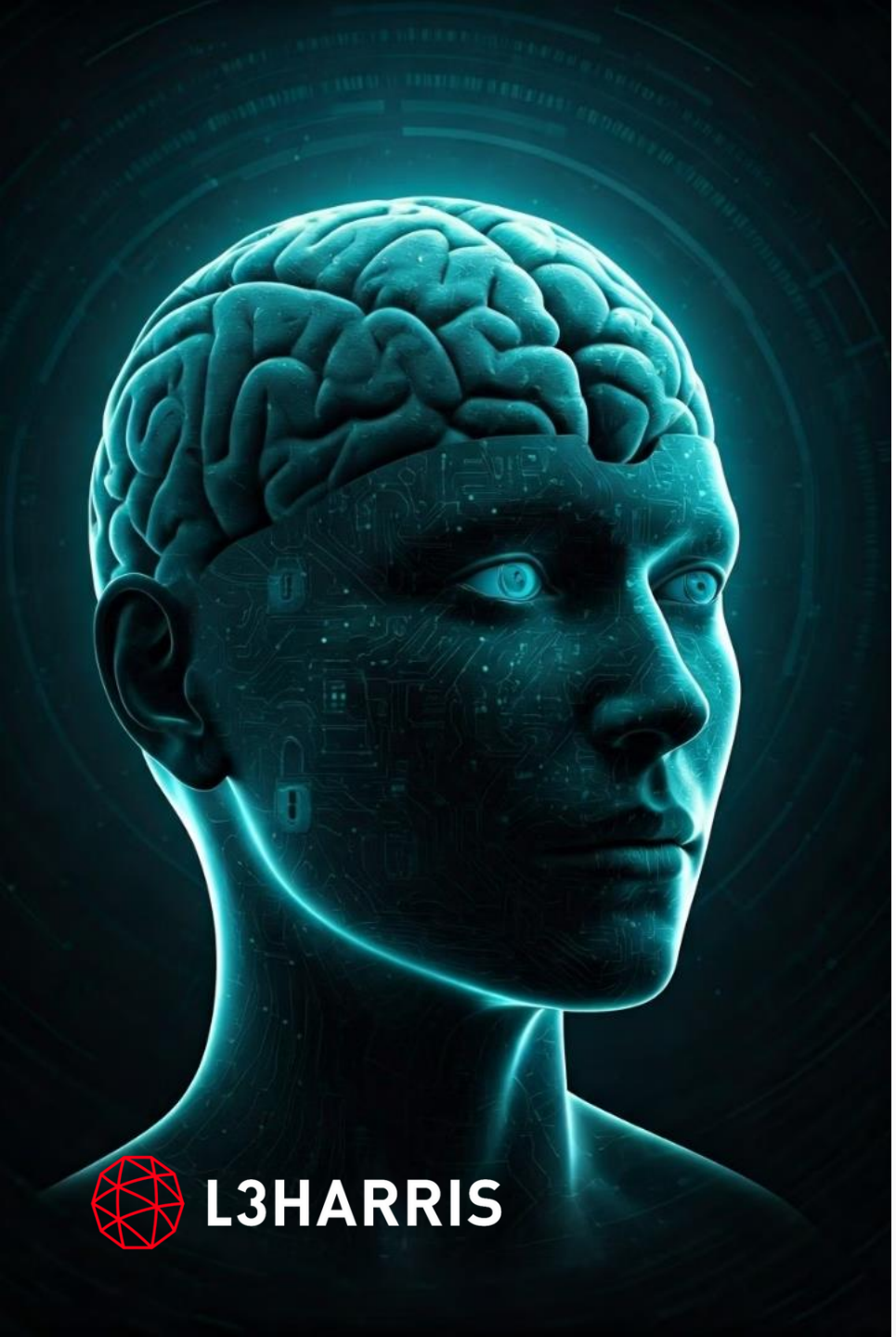
Who's responsible when AI decides?

Role Evolution

From operators to supervisors

Reciprocal Adaptation

Mutual learning between AI and humans



Mind Privacy: The Emerging Frontier

Cognitive Data Protection

Safeguarding thought processes, decisions, and biases from AI inference

National Security Implications

Preventing secrets extraction through cognitive pattern analysis

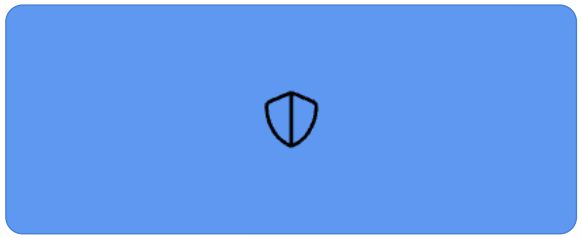
AI Inference Threats

Systems increasingly capable of reading human mental models

Cognitive Security Stack

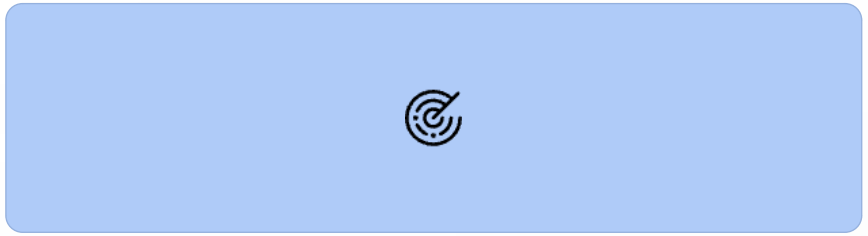
AI Transparency

Clear visibility into AI reasoning



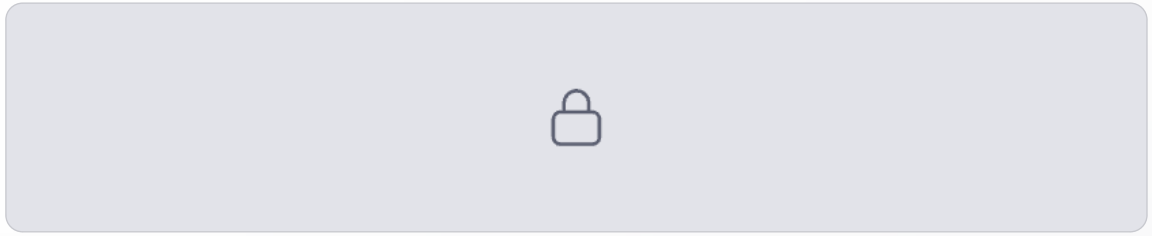
Inference Protection

Blocking unauthorized cognitive analysis



Cognitive Monitoring

Detecting attempted mind privacy violations



Thought Encryption

Securing mental processes from extraction

Real-World Implications

1

Autonomous Defense

AI countering threats without human approval

Risk: Critical false positives, systemic disruption

2

Cognitive Inference

AI deducing clearance level from behavior patterns

Risk: Unauthorized access to classified intentions

3

DIB Infiltration

Targeted extraction of subject matter expertise

Risk: Loss of intellectual capital, competitive edge

Future-Proofing the Cyber Workforce

AI Ethics Training

Understanding complex ethical implications

Critical Thinking

Questioning AI recommendations and decisions

Strategic Positioning

Moving into roles AI cannot replace

Adaptability

Evolving alongside changing AI capabilities

Call to Action

Continuous Learning

Stay ahead of AI capabilities and limitations

Embrace specialized training in AI oversight

Mind Privacy Frameworks

Develop organizational policies for cognitive security

Implement protections against inference attacks

Collaborative Governance

Create human-AI balanced security structures

Ensure meaningful human control in critical systems

Connect & Discuss

LinkedIn

Allen Westley

Medium

Latest articles on Mind Privacy

Cyber Explorer LLC

www.cybesec1118.com

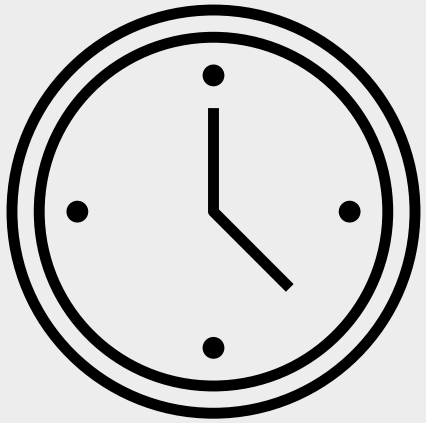
Questions?

The floor is yours

Q&A

Are There Any Questions?

Federal Information Security Educators (FISSEA) Spring Forum



BREAK

The Forum will resume at 3:00pm ET

#FISSEA | nist.gov/fissea

NIST | FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Welcome Back!

Latha Reddy
FISSEA Co-Chair

We Don't Phish: How We Refined What Security Awareness Means

Erin Gallagher

Security Training & Awareness Lead
Fastly

We Don’t Phish

How We Refined What Security Awareness Means

Erin Gallagher, ***Fastly***

fastly
Information Security

As with **all good stories**, this starts with a phone call to **my mom**

So How Did We Refine Security Awareness?

Security Training & Awareness is **the bridge** between **Information Security** and the **Organization,** educating a critial line of defense.

- We focus on **building better relationship** between teams like engineering, client services, communications, and more
- I shifted from a mindset of phishing to **tailored training and engagement**
- We are here to **simplify!**

Shift from **Phishing to Training** Mindset

Our three big training targets

Onboarding

We were **not leaving a great impression** on our new hires

We were **only explaining the "what"** and nothing else

We **needed to focus** on real examples, details from our Information Security Policy, and consistent contacts

Content too General

We love our vendor, but the content for the Annual Security Training wasn't working for us

- **Wasn't relevant** for Fastly
- Content was **redundant** without customization
- Variety of functions with **various levels of knowledge**

Way too Long

Employees time is valuable, and we were taking too much of it.

Annual Security Awareness Training was **1 hour**

Secure Developer Training was (we can cringe together) **5 hours** long

Confidential

Let’s Fix our Onboarding!

From no impression, to great impression

What do we mean by ‘Security’?

At Fastly when you hear the work ‘Security’ think about ‘Risk’

Risk refers to the possibility that something unwanted or unpleasant is going to occur.

fastly information security

Meet
Erin Gallagher

Security Learning & Development

Why We Do It

At the center is our shared goal to respect and protect the data we have access to, use, and store at Fastly

External Security: Other Threats

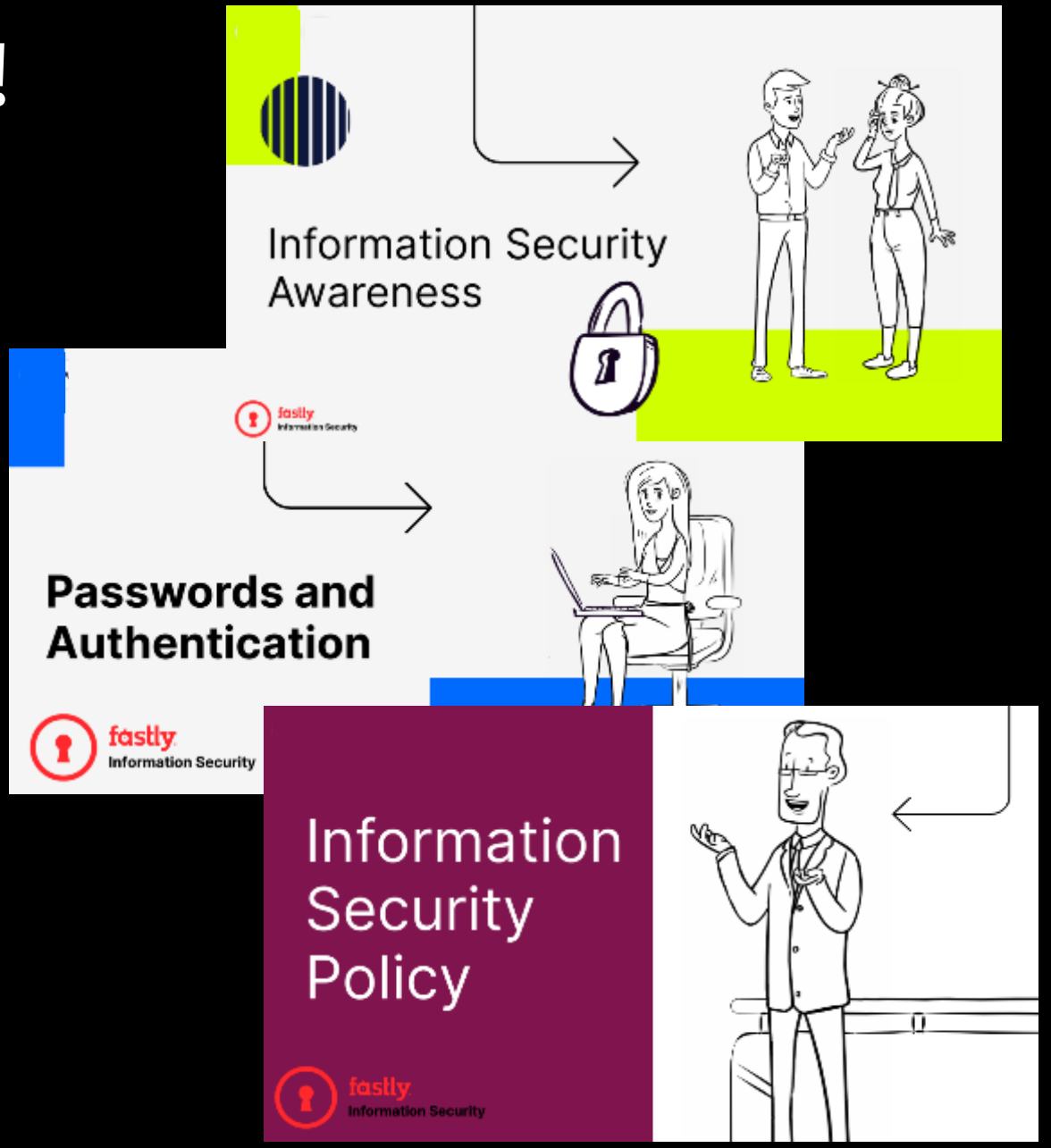
Threats come in all different ways, here are some other tips to help keep yourself safe!

- Limit the use of Public/Open W-Fi, especially when performing sensitive or highly privileged actions. If necessary, tether to your phone for a secure connection
- Keep your devices with you! If you need to put it down, make sure it’s locked and hidden out of sight
- If you’re in an office, make sure you erase whiteboards and remove any sensitive data before leaving

fastly information security

No more blanket training!

From general to focused



Let’s not waste any time!

It was too damn long…

What we fixed

Annual Security Awareness Training

1 hour ⇨

Secure Developer Training

5 hours ⇨

Total saved for Fastly

Secure Developer

$110 X **2.5 hours** X **450 engineers**

= **$123,750**

Annual Awareness Training

$52 X **.75 hours** X **1200 employees**

= **$46,800**

Confidential

So How Do We Measure?

Quantitative

Cost Savings - 7.5K from vendor, $170K* from opportunity cost savings

Time Savings - Engineers have 1,100 hours back, Fastly has 540 hours back

1Password Use – 42% active

Triage Platform - Data on external threats, analysis on high-risk functions

Communication Channels - Views on articles, users in channel

Qualitative

Quality of training has **increased**, the training is **more impactful** when it's tailored to a group

New hire questionnaire, **understanding their past experience** with Security Awareness Program

Increase in employee **engagement** over **Slack**

Increase in employee **engagement** in new hire **onboarding sessions**

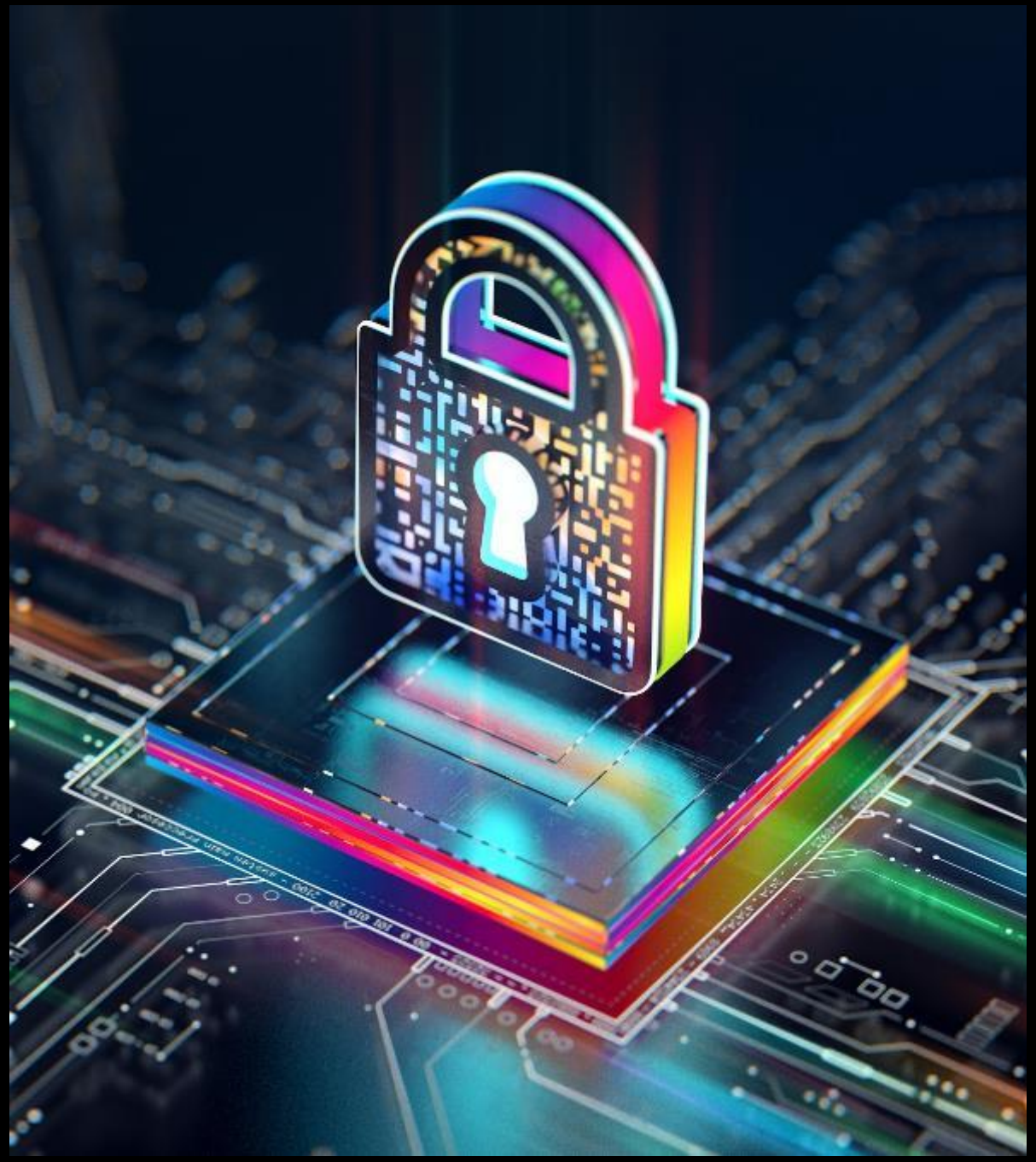
I’m not knocking Phishing!

- They can provide **great metrics** for your organization and senior leadership
- It provides insight into **opportunities** for **additional training** and education

However!

- Phishing **doesn’t need to be the main focus** of your security awareness program
- There are **metrics** to be found in **other areas** of security that help your program
- Time spent focused on **tailored training** can lead to **better educated employees**

Thank you!



fastly
Information Security

Q&A

Are There Any Questions?

A Privacy Talk: The Good, the Bad, and the Ugly

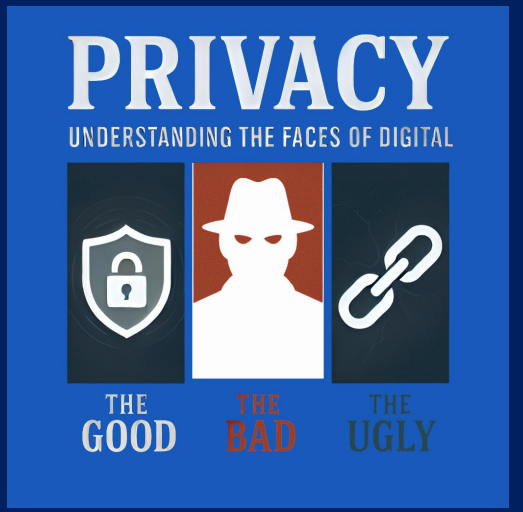
Dr. Natalie Foster Johnson
Dr. Resiliency
Founder and Researcher
CyberMINDS Research Institute

Dr. Alexis Perdereaux-Weekes
Dr Privacy
Co-Founder and Sr. Managing Partner
CyberMINDS Research Institute

NIST | FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

CYBERMinds

A Privacy Talk: The Good, the Bad, and the Ugly



Understanding the Faces of Digital Privacy

Dr. Natalie Foster Johnson and Dr. Alexis Perdereaux-Weekes

May 13th, 2025

CYBERMinds

NIST | FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Dr. Natalie Foster Johnson
(*Dr. Resiliency*)

Dr. Alexis Perdereaux- Weekes
(*Dr Privacy*)

Dr. RESILIENCY
CYBER RESILIENCE FOR CRITICAL INFRASTRUCTURE

DR PRIVACY

CyberMINDS Research Institute

The thought leaders in information security, cyber, and privacy protection.

Agenda

Our Journey Today – U.S. Prospective

- **The Good:** Progress, Frameworks, and Innovations in Privacy.
- **The Bad:** Persistent Threats and Implementation Challenges.
- **The Ugly:** Real-World Consequences - Recent Data Breaches.

Lessons Learned & The Path Forward

- Working towards a more resilient *Privacy Posture* and increased awareness among customers and stakeholders.

Introduction: The Dynamic Privacy Landscape

Why Privacy Matters More Than Ever

- Privacy isn't just a compliance checkbox—**it's a strategic advantage.**
- **Data is the new currency**, powering innovation and services.
- Increased public awareness and regulatory scrutiny.

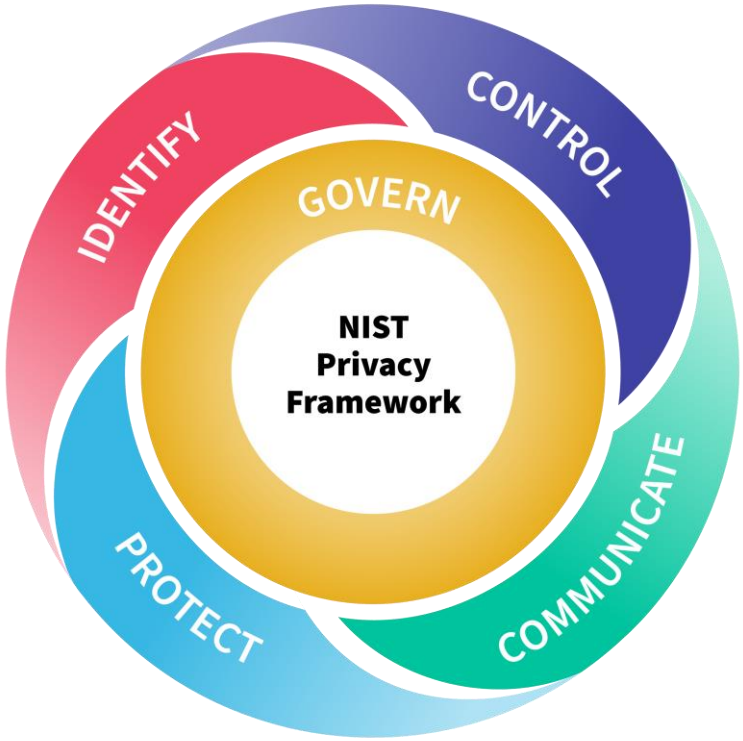
Relevance to Security Awareness Training:

- Helps organization transition from an ad-hoc, reactive methods to standardized, measurable and proactive processes.

The Good: Progress in Privacy

Making Strides in Data Protection

- Regulatory Maturity
- Increased Awareness
- Technological Advancements
- Standardization Efforts



A Foundational Tool for Risk Management

The Bad: Persistent Threats

NIST | FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

CYBERMinds

Evolving Threat Landscape

- Sophisticated Attack Vectors
- Misconfigurations
- Data Sprawl
- Complexity
- Resource Constraints

Evolving Threat Landscape

- The Human Element
- Supply Chain & Third Party Risk

NIST | FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

The Real-World Impact of Breaches

CYBERMinds

- **Beyond compliance**
- **Reputational**
- **Operational**
- **Individual Harm**

Let's look at some recent examples

The Ugly Case Study 1: Healthcare

Date: February 2024 (Disclosed)
Impact: Up to 190 Million individuals affected.
Incident: Ransomware attack (Blackcat group) on a major healthcare technology provider (UnitedHealth subsidiary).
Data Exposed: Health insurance information, medical records, potentially financial details.
Consequences: Massive disruption to claims processing & billing across the US healthcare system, significant financial loss (~$3B+ reported by UnitedHealth).
Lesson: Critical infrastructure vulnerability, devastating impact of ransomware, scale.

Real-World Privacy Implications

The Ugly: Case Study 2 - Education/Direct Attack (NYU)

Date: March 2025

Impact: Over 3 Million applicants.

Incident: Hacker gained access to internal systems/data warehouse, defaced website, leaked data.

Data Exposed: Highly sensitive PII - Names, test scores (SAT/ACT), GPAs, demographics (race), intended majors, zip codes, family background, financial aid details (records back to 1989).

Consequences: Major privacy violation for applicants, reputational damage, questions about internal controls.

Lesson: Protecting highly sensitive PII, insider threats/internal security, long-term data retention risks.

Case Study 3 : Health Data shared with Google due to misconfiguration

Blue Shield of California disclosed it suffered a data breach after exposing protected health information of 4.7 million members to Google's analytics and advertisement platforms.

"On February 11, 2025, Blue Shield discovered that, between April 2021 and January 2024, Google Analytics was configured in a way that allowed certain member data to be shared with Google's advertising product, Google Ads, that likely included protected health information," reads the notice.

"Google may have used this data to conduct focused ad campaigns back to those individual members."

The Ugly Case Study 4: When data processors goes bankrupt (23andMe)

The bankruptcy of genetic testing company 23andMe has raised concerns about the enforcement of California's privacy laws:

- **Data Deletion Difficulties**: Consumers, including the state Attorney General, faced challenges in deleting their genetic data, highlighting gaps in the practical application of the CCPA and the Genetic Privacy Rights Act.
- **Legislative Response**: Lawmakers are considering new legislation to ensure that genetic data is adequately protected, even in cases of company bankruptcy or dissolution

Real-World Privacy Implications

Case Study 5: US lab testing provider exposed health data of 1.6 million people

The data types exposed in the breach include the following:

- **Personal identifiers**: Full name, SSN, driver's license or passport number, date of birth, and government-issued IDs.
- **Medical info**: Dates of service, diagnoses, treatments, lab results, provider, and facility details.
- **Insurance info**: Plan type, insurer, and member/group ID numbers.
- **Billing and financial data**: Claims, billing details, bank and payment card info.

According to a filing submitted to the Maine's AG Office, the data breach impacts 1,600,000 people.

Source: https://www.bleepingcomputer.com/news/security/us-lab-testing-provider-exposed-health-data-of-16-million-people/

Checkbox Compliance

NIST | FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

CYBERMinds

Policy ≠ Compliance

- Organizations that have policies in place but are not following them.
- Data Processing activities don’t align with existing regulations
- Challenges of secondary use of data
- Lack of effective training and awareness

Why Compliance-Only Approaches Fail

- Ignores human behavior
- Lacks metrics
- One-size-fits-none
- Creates audit fatigue

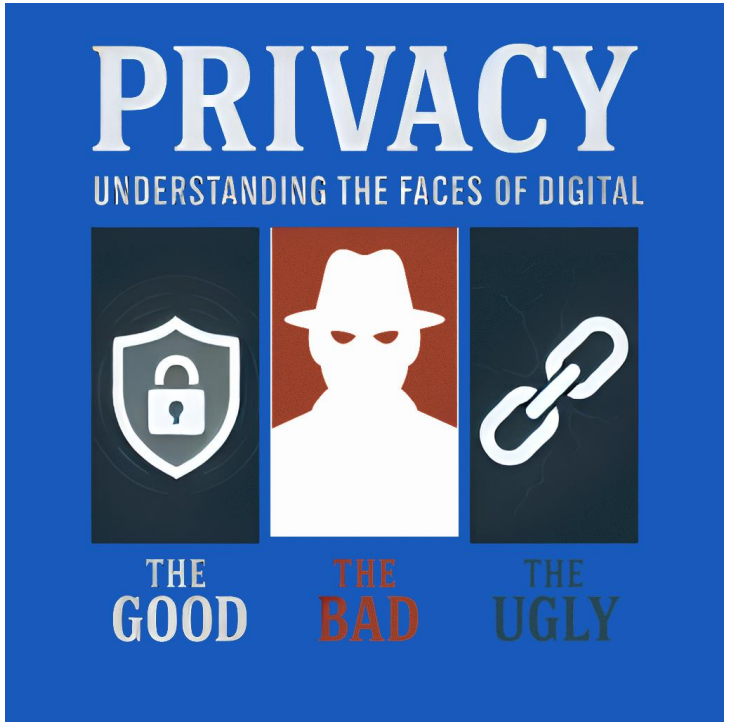
Lessons Learned: Privacy Breach

NIST | FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

CYBERMinds

Connecting the Good, the Bad, and the Ugly

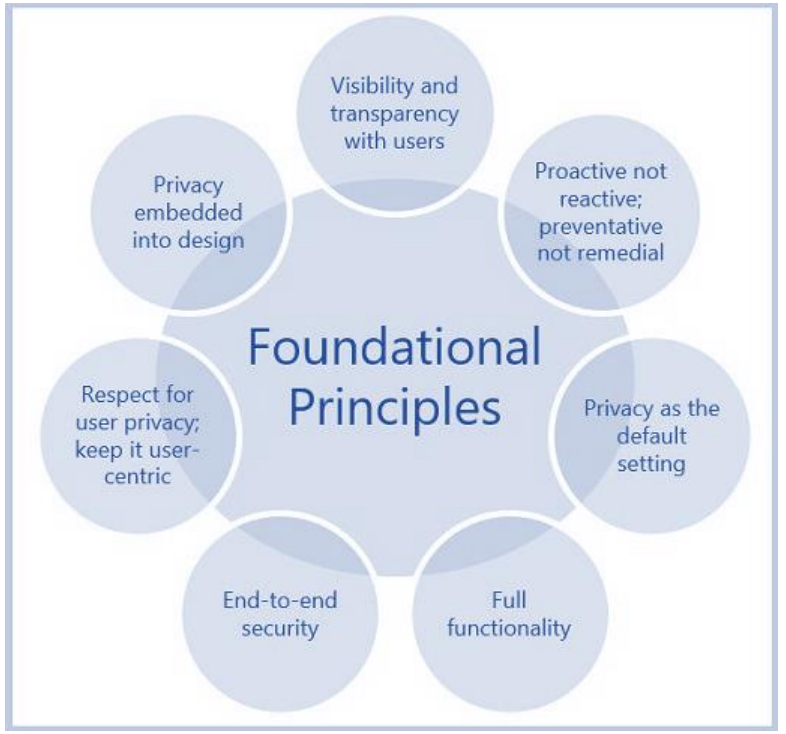
- Proactive > Reactive
- Risk-Based Approach
- Holistic View: Address Both
- Third-Party Diligence
- Incident Response is Key



The Path Forward

Building a More Resilient Privacy Posture

- **Embrace & Implement Frameworks**
- **Invest in PETs**
- **Foster a Privacy Culture**
- **Strengthen Fundamentals**
- **Continuous Monitoring & Adaptation**



https://www.mondaq.com/australia/data-protection/1051714/privacy-by-design-protecting-personal-information-from-the-wire-frame-up

From Obligation to Opportunity

Summary of Key Points:

- **Treat Privacy as a Strategic Imperative**
  Not just a legal duty—but a lever for trust, resilience, and competitive differentiation.
- **Align with Proven Frameworks**
  Implement NIST Privacy Framework, ISO 27701, and GDPR principles to strengthen your program.

Call to Action:

- **Invest in Culture, Not Just Compliance**
  Embed privacy into the fabric of your organization through leadership, training, and measurement.
- **Respond to 2025 Realities**
  Adapt to new threats, AI and biometric risks, and evolving enforcement under CCPA, CPRA, and beyond

Thank You!

Dr. Resiliency
Dr. Natalie Foster Johnson
Email: njohnson@cybermindsinstitute.org
LinkedIn: https://www.linkedin.com/in/nataliefosterjohnson
www.drresiliency.com

Dr Privacy
Dr. Alexis Perdereaux-Weekes
Email: apweekes@cybermindsinstitute.org
LinkedIn: https://www.linkedin.com/in/drprivacy/
www.drprivacy.us

NIST | FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

CYBERMinds

Dr. RESILIENCY
CYBER RESILIENCE FOR CRITICAL INFRASTRUCTURE

DR PRIVACY

Contact US: Inquiry@cybermindsinstitute.org

Q&A

Are There Any Questions?

Presentation of FISSEA Security Contest Winners

Craig Holcomb

FISSEA Contest and Innovator of the Year Award Lead

Presentation of the 2024 FISSEA Innovator of the Year Award

Oz Alashe

CEO and Founder of CybSafe

2023 FISSEA Innovator of the Year Recipient

#FISSEA

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

2024 FISSEA Innovator of the Year

Greg Bastien

ICS Training Program Manager
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

#FISSEA

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Best Cybersecurity Awareness and Training Poster or Brochure

Indian Health Service
Office of Information Technology
Division of Information Security

Artificial Intelligence (AI) Spoofing: A Rising Threat in the Digital Age

Best Cybersecurity Awareness and Training Multimedia

Securible, LLC

Cybersecurity Today TV Show

CYBERSECURITY TODAY

Cybersecurity Today Show Guest Overview

INTRODUCTION

Thank you for offering to guest star on Cybersecurity Today! Cybersecurity Today is a 30-minute TV show that uses a talk show/newscast format to discuss themes, topics, and current events in cybersecurity.

Cybersecurity Today, the winner of the 2024 Cybersecurity Excellence Award for "Best Cybersecurity Podcast," is broadcast on Fairfax Public Access TV (FPA) in the Washington, DC market and is viewable several times each month. Additionally, the show is available via our YouTube channel for viewers outside the Washington, DC market.

STUDIO TECHNOLOGIES

The studio facilities use state-of-the-art equipment. The actual studio is a green screen, and a virtual set is imposed during the taping to facilitate the high-tech look. Below are screenshots of what the actual broadcast looks like once the recording and post-production have occurred.

Best Cybersecurity Awareness and Training Website

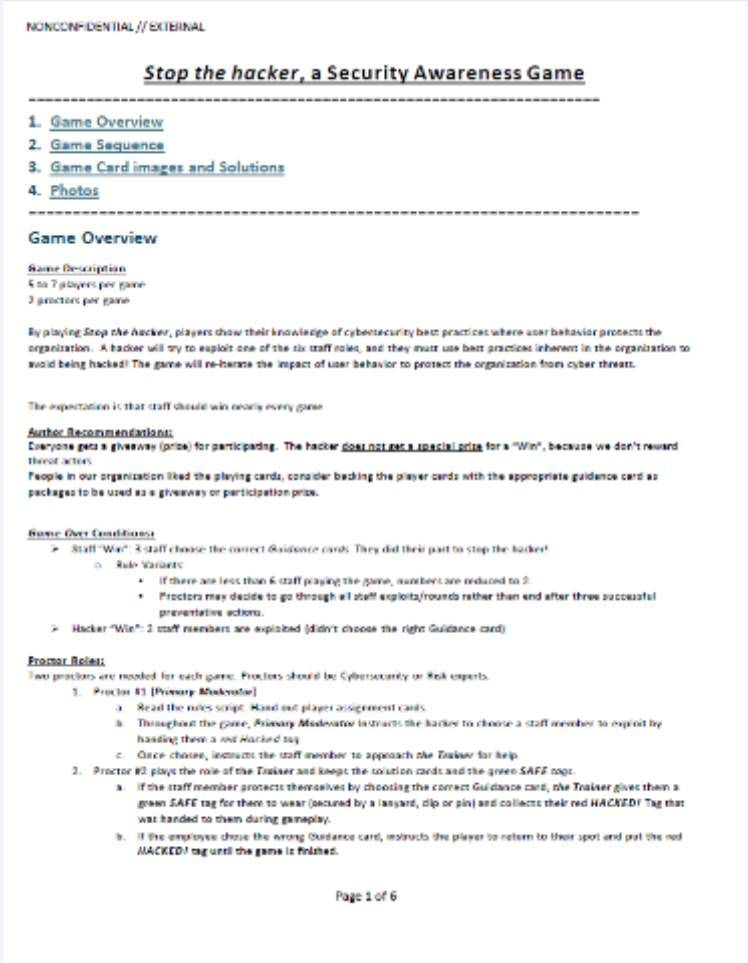
Indian Health Service
Office of Information Technology
Division of Information Security

Spot Phishing! Don't Take the Bait!

Most Innovative Solution

Sarae Winnicki and Ashley Smith

Stop the hacker, a Security Awareness Game



NONCONFIDENTIAL // EXTERNAL

***Stop the hacker*, a Security Awareness Game**

---

1. Game Overview
2. Game Sequence
3. Game Card images and Solutions
4. Photos

Game Overview

Game Description
5 to 7 players per game
2 proctors per game

By playing *Stop the hacker*, players show their knowledge of cybersecurity best practices where user behavior protects the organization. A hacker will try to exploit one of the six staff roles, and they must use best practices inherent in the organization to avoid being hacked! The game will re-iterate the impact of user behavior to protect the organization from cyber threats.

The expectation is that staff should win nearly every game

Author Recommendations:
Everyone gets a giveaway (prize) for participating. The hacker does not get a special prize for a "Win", because we don't reward threat actors
People in our organization liked the playing cards, consider backing the player cards with the appropriate guidance card as packages to be used as a giveaway or participation prize.

Game Over Conditions:
- Staff "Win": 4 staff choose the correct Guidance cards. They did their part to stop the hacker!
  - Rule Variants
    - If there are less than 6 staff playing the game, numbers are reduced to 3
    - Proctors may decide to go through all staff exploits/rounds rather than end after three successful preventative actions.
- Hacker "Win": 3 staff members are exploited (didn't choose the right Guidance card)

Proctor Roles:
Two proctors are needed for each game. Proctors should be Cybersecurity or Risk experts.

1. Proctor #1 (**Primary Moderator**)
   a. Read the rules script. Hand out player assignment cards.
   b. Throughout the game, **Primary Moderator** instructs the hacker to choose a staff member to exploit by handing them a *red Hacked tag*
   c. Once chosen, instructs the staff member to approach *the Trainer* for help.
2. Proctor #2 plays the role of the *Trainer* and keeps the solution cards and the green *SAFE* tags.
   a. If the staff member protects themselves by choosing the correct Guidance card, *the Trainer* gives them a green *SAFE* tag for them to wear (secured by a lanyard, clip or pin) and collects their red *HACKED!* Tag that was handed to them during gameplay.
   b. If the employee chose the wrong Guidance card, instructs the player to return to their spot and put the red *HACKED!* **tag until the game is finished.**

Page 1 of 6

Best Cybersecurity Awareness and Training Email Campaign and/or Newsletter

Indian Health Service
Office of Information Technology
Division of Information Security

Catch the Beat Not the Breach, How to Protect Yourself from a Data Breach at Your Next Concert

Catch the Beat not the Breach

How to Protect Yourself from a Data Breach at Your Next Concert

Office of Information Technology
Division of Information Security
JULY 2024

Summer concerts are a great way to start the season, providing amazing experiences full of music, friends, and fun. While summer concerts are exciting, they are also a prime target for cybercriminals since the large gatherings and high volume of online transactions provide a perfect opportunity to exploit concertgoers. Cybercriminals steal personal and financial information by exploiting vulnerabilities in ticket sales, public Wi-Fi networks, and social media platforms. Phishing schemes, fake ticket websites, and virus attacks are frequent methods of deceiving concertgoers. Due to the rise of digital ticket sales and cashless transactions, data breaches have increased, costing unsuspecting concert fans thousands of dollars. Here is what you need to know about how data breaches occur, their consequences, and how to protect yourself while enjoying your favorite concert.

Data breaches around concerts occur through several clever techniques. Cybercriminals may create fake ticketing websites or send phishing emails that mimic legitimate vendors, tricking concertgoers into providing personal and financial information. Concert venues often offer free Wi-Fi to attendees, but these networks are usually unsecured, allowing hackers to intercept data transmitted over free Wi-Fi connections.

Cybercriminals send fraudulent emails, texts, or QR codes that look like they come from legitimate ticket vendors or concert organizers. These messages may appear harmless but may contain malware. After clicking the link, attendees risk having malware installed on their devices or having their personal information stolen. Mobile POS (Point of Sale) systems used for concert merchandise and food purchases are another target cybercriminals use. If the network is not secure, cybercriminals can steal credit card information. Lastly, cybercriminals frequently use social engineering techniques to obtain private information from social media platforms to guess passwords or provide answers to security challenge questions.

Ticketmaster/ Live Nation (a major ticket-selling company) recently revealed that a data breach compromised thousands of customers' personal information. According to Ticketmaster, this data breach was linked to a third-party data service provider. The database contained the personal information of their customers who purchased tickets to events in North America (U.S., Canada and/or Mexico). Ticketmaster is currently in the process of contacting all of the affected customers. Along with collaborating with banks, credit card companies, and law enforcement, Ticketmaster is providing a complementary 12-month identity monitoring service to all affected customers.

You can find out more information here Ticketmaster Data Security Incident – Ticketmaster Help.

Best Cybersecurity Awareness and Training Program – Miscellaneous

CISA's President's Cup Program Team

President's Cup Cybersecurity Competition (PCCC)

FISSEA Awareness and Training Contest: "*People's Choice Awards*" Winners

Cybersecurity Awareness and Training Poster or Brochure
Federal Reserve Bank of Richmond
Cybersecurity Awareness Month - Cyber Arcade

Cybersecurity Awareness and Training Website
Social Security Administration
Cybersecurity Tip of the Month

Cybersecurity Awareness and Training Multimedia (Blog, Video, Audio, Podcast, etc.)
Securible, LLC
Cybersecurity Today TV Show

Cybersecurity Awareness and Training Email Campaign and/or Newsletter
Social Security Administration
Quarterly Health Check

Cybersecurity Awareness and Training Program – Miscellaneous
Cybersecurity Infrastructure Security Agency (CISA)
President's Cup Cybersecurity Competition (PCCC)

Most Innovative Solution
U.S. Department of State
Cybersecurity Role-Based Training

Special Thanks to the FISSEA Planning Committee Members and Staff Support!

Aparna Achanta
Art Chantker
Calvin Watson
Clarence Williams
Craig Holcomb
Dr. Jim Chen
Deborah Palmer
Derek Fisher
Frauke Steinmeier
Joyce Mui
Karen Bovell
Kelly Arnold
Kristina Rigopoulos
Latha Reddy
Loyce Pailen
Maureen Premo
Susan Hansche
Susana Barraza

Closing Remarks

Latha Reddy
FISSEA Co-Chair

Get Involved

Subscribe to the FISSEA Mailing List
FISSEAUpdates+subscribe@list.nist.gov

Volunteer for the Planning Committee
https://www.nist.gov/itl/applied-cybersecurity/fissea/meet-fissea-planning-committee

Serve on the Contest or Award Committees
Email fissea@nist.gov

Submit a presentation proposal for a future FISSEA Forum
https://www.surveymonkey.com/r/fisseacallforpresentations

THANK YOU

We look forward to receiving your feedback via the post-event survey!

https://www.surveymonkey.com/r/2025fisseaspringforum

#FISSEA | nist.gov/fissea