Please Note…

This webinar will be recorded

An archive will be available at nist.gov/fissea

Federal Information Security Educators (FISSEA) Summer Forum

STRONGER TOGETHER

June 17, 2021

1:00pm – 4:00pm EDT

#FISSEA2021 | nist.gov/fissea

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

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

Welcome and Opening Remarks from National Institute of Standards and Technology

Rodney Petersen

Director
National Initiative for Cybersecurity Education (NICE)
National Institute of Standards and Technology (NIST)

Welcome and Opening Remarks from FISSEA Chair

Sarah Moffat

Chief of the Office of Communications & Outreach
National Institutes of Health

NIST Research Activities on Cybersecurity Awareness: *Federal Security Awareness Study*

Julie Haney

National Institute of Standards and Technology

NIST Federal Cybersecurity Awareness Survey

Julie Haney, Jody Jacobs, & Susanne Furman
Visualization & Usability Group, Information Technology Lab
National Institute of Standards and Technology

RESEARCH EFFORTS

Purpose: To better understand the needs, challenges, practices, and professional competencies of federal security awareness teams and programs

Focus Groups

8 focus groups of 29 feds working in departments, agencies in departments, & independent agencies

Online, Anonymous Survey

Survey a broader population of federal security awareness professionals & organizations

TAKE THE SURVEY, MAKE AN IMPACT!

Tell us what works for your security awareness program and what doesn't to help inform resources for federal security awareness programs.

NIST SP 800-50 Revision

"Building an IT Security Awareness and Training Program"

Best Practices

Successful approaches/strategies & lessons learned

Sharing Platforms/Forums

Facilitation of sharing among federal programs

SURVEY INFORMATION

- Eligibility:
  - ✓ Federal employee
  - ✓ Have security awareness responsibilities or manage/oversee the security awareness program (e.g., as a manager, CISO, or CIO) in your organization
  - ✓ Be knowledgeable about the program's approaches & challenges
- Participation is voluntary, and responses are anonymous
- Takes ~20 minutes to complete with option to save and return later
- Please pass to the survey to colleagues in and outside your organization!

Survey open now through July 2

https://nistusability.checkbox.com/security-awareness

Julie.Haney@nist.gov

For questions during the survey: Jody.Jacobs@nist.gov or Susanne.Furman@nist.gov

NIST Research Activities on Cybersecurity Awareness: *NICE Framework Cybersecurity Awareness Work Roles and Competencies*

Karen Wetzel

Manager of the NICE Framework
NIST

NICE

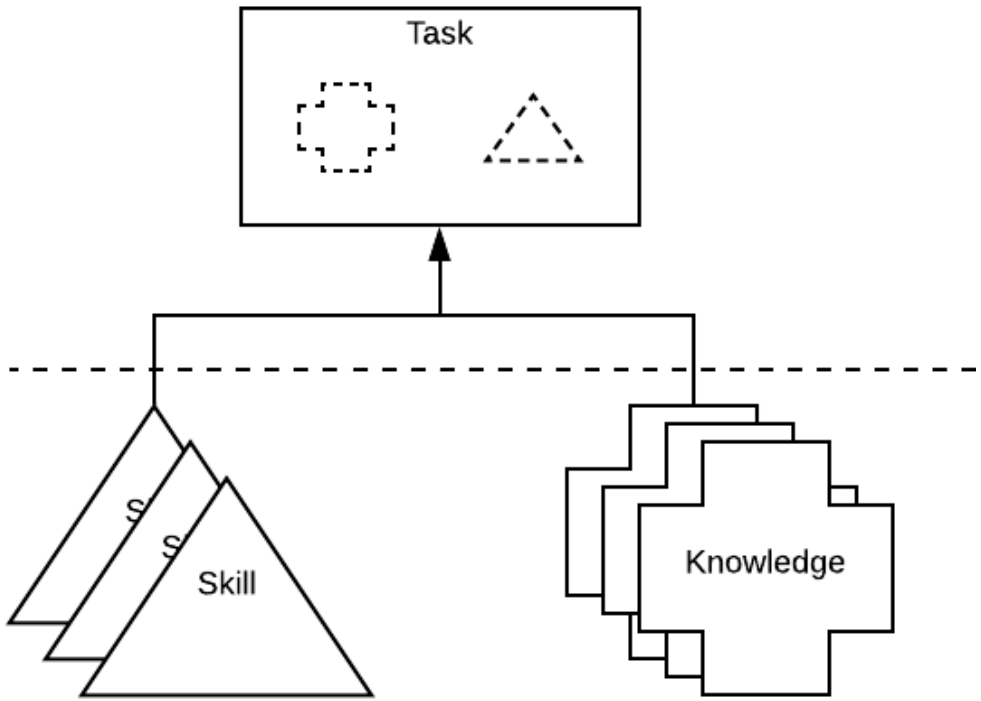
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Framework Competencies and Work Roles: An Awareness and Training Perspective

Karen Wetzel, Manager of the NICE Framework

June 2021 • FISSEA Summer Forum

NICE Framework Building Blocks:
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

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Awareness & Training Work Roles

OVERSEE and GOVERN (OV) - Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.

Instructional Curriculum Developer (OPM Code 711)

- Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.
- 17 Task Statements, e.g.,
  - Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.
- 40 KSA Statements

Instructor (OPM Code 712)

- Develops and conducts training or education of personnel within cyber domain.
- 30 Task Statements, e.g.,
  - Conduct interactive training exercises to create an effective learning environment.
- 93 KSA Statements

✓ 9 Common Tasks
✓ 33 Common KSAs

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Awareness & Training Competencies

Education and Training Delivery

- This Competency describes a Learner's capabilities related to helping others acquire knowledge or develop skills. Includes training of personnel within pertinent subject domain, including cybersecurity awareness for users of computers and other electronic telecommunication devices.

Education and Training Curriculum Development

- This Competency describes a Learner's capabilities related to developing, planning, coordination, delivery, and evaluation of training courses, methods, and techniques.

Related OPM Competencies:

- Teaching Others
- Learning

Competency Model for Cybersecurity (2/16/2011)

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Framework Virtual Workshop: A Focus on Cybersecurity Awareness

- September 29, 2021
- 1-5 p.m. ET
- An exploration of more focused content – including Competencies, Work Roles, and TKS – for cybersecurity awareness
- A Collaboration with CAE Community

Questions?
Contact me at karen.wetzel@nist.gov

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

KEYNOTE

Cybersecurity Human Risk Management

Ashley Rose

CEO and Founder
Living Security

Cybersecurity Human Risk Management

Ashley Rose
CEO and Founder, Living Security

livingsecurity.com

Overview

- Introduction
- What is Cybersecurity Human Risk Management and how does it differ from Security Awareness Training?
- What's in the human risk management training toolkit today?
- Shifting the mindset from Training Program to CORE SECURITY PRIORITY
- 7 steps to truly changing behavior and mitigating risk

What's wrong with my Cybersecurity Training?

- Low Engagement
- Low Retention
- Poor Behavior Change

Transform employees in to your greatest security asset

1

Implement training that meets compliance AND provide engaging, fun, and effective programs for the end users that produce PROVEN LASTING CHANGE in behavior and culture

2

Measure and predict Cybersecurity Human Risk and Security Awareness Training ROI accurately

Tired of having no answers when asked:

“How do we tell if our Security Awareness Training is working?”

Assess

- **What are the strengths of your current cybersecurity awareness program?**

- **Where are you struggling? What departments are most vulnerable?** Many companies have little or no security monitoring and reporting and simply don't have the data to identify vulnerabilities. If you're not auditing your security, how do you know where you need to improve?

- **What bilndspots are your end users most vulnerable to?** Cybercriminals just keep getting savvier and new threats emerge daily. Organizations that don't invest in security training often have no clue what their employees know and don't know.

- **How can you get more buy-in internally from other departments?** A lot of employees and managers assume that cybersecurity awareness will be time-consuming and mind-numbing, and frankly won't actually make a difference. Consider ways to get staff and managers excited again. How can you convince other teams that security matters just as much as their other initiatives?

- **Do you provide training that doesn't taste like medicine? Why should your managers and employees care about training?** Start thinking in terms of motivations. How can you make security training attractive and less laborious? How can you reward participants for their time and effort? How can you make it interesting and engaging?

- **How do you have training *so good* that end users own it, look forward to it and tell other employees how awesome it is?** That's a loaded question right? Even if you get your employees and management interested in your security training, how do you get them personally invested? How do you make them eager to keep learning and encourage others to have better security habits?

Human **Risk Management**

Finally defining the program, not the parts

- Security Awareness and Training programs generally target **Human Risk**.
- **Risk Management** is an assessment of a security problem followed by actions to accept, ignore, transfer or mitigate that risk.

Security awareness programs are intended (assumed!) to accomplish HRM but most are not positioned within their security organization to be truly effective.

Our Training Toolkit

Training Metrics:

- Compliance
- Completion
- Participation

Phishing Programs:

- Subjective levels of difficulty
- Role-Based Implementation
- Cultural alignment - danger of distrust

Implementation

- One size fits all, get-through- it approach
  - LMS battles and lack of time)
- Leave the “engagement” to culture and awareness activities.

Training Program Or Core Security Priority

Buy a training program → Solving a core security vulnerability

Training budget is the first thing cut, despite it being widely regarded as the biggest risk.

-Why is this?

It's extremely difficult to measure the ROI past compliance. How do you accurately measure effectiveness or demonstrate a positive impact on a security priority for the organization?

We Must Uplevel The Data

Human Risk Metrics

- Computer Based Training
- Awareness Events
- Gamification
- Phishing Results
- Marketing and Comms

Risk Management

- Reduce Risk
- Enable the Business
- Secure the Enterprise
- Save Money
- Process Efficiency

We Must Uplevel The Data

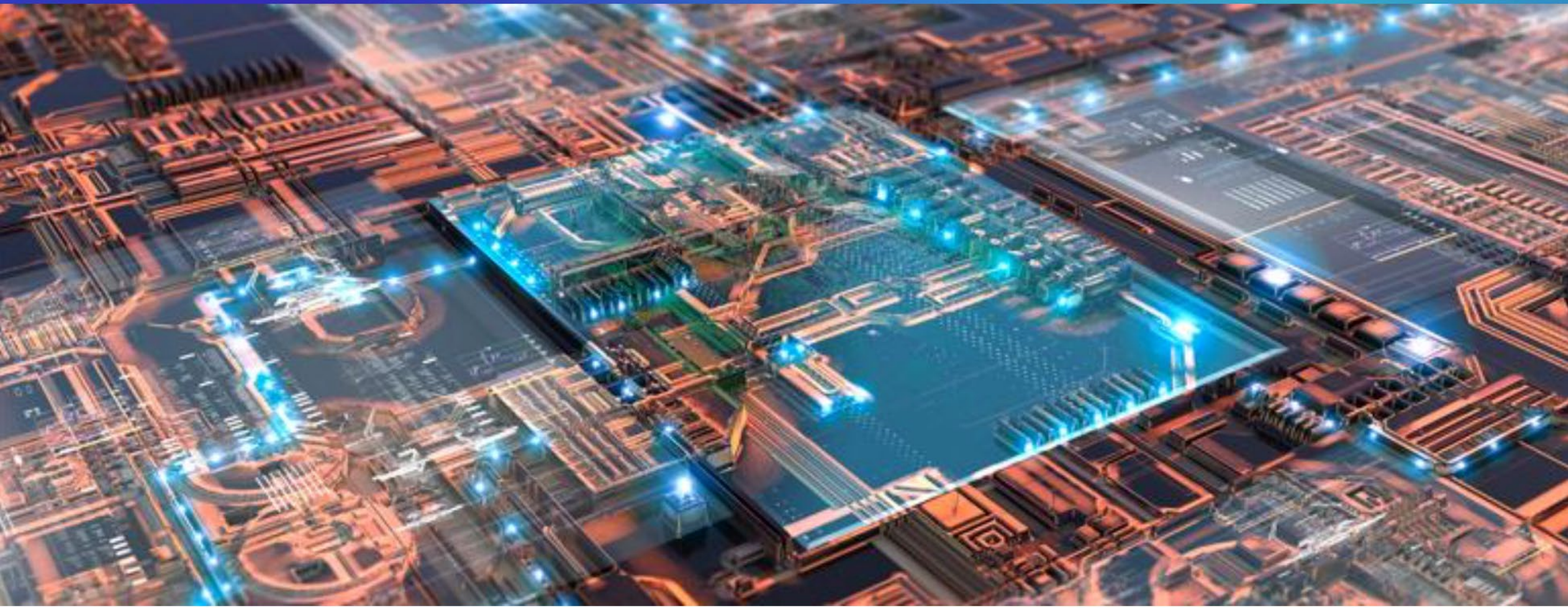
Integration of training data with operational security systems allows for the combination of these data points to inform decision making and enable ***Human Risk Management***

7 steps to truly changing behavior and mitigating risk

1. Make your employees your best allies

2. The importance of integration

3. Leverage automation

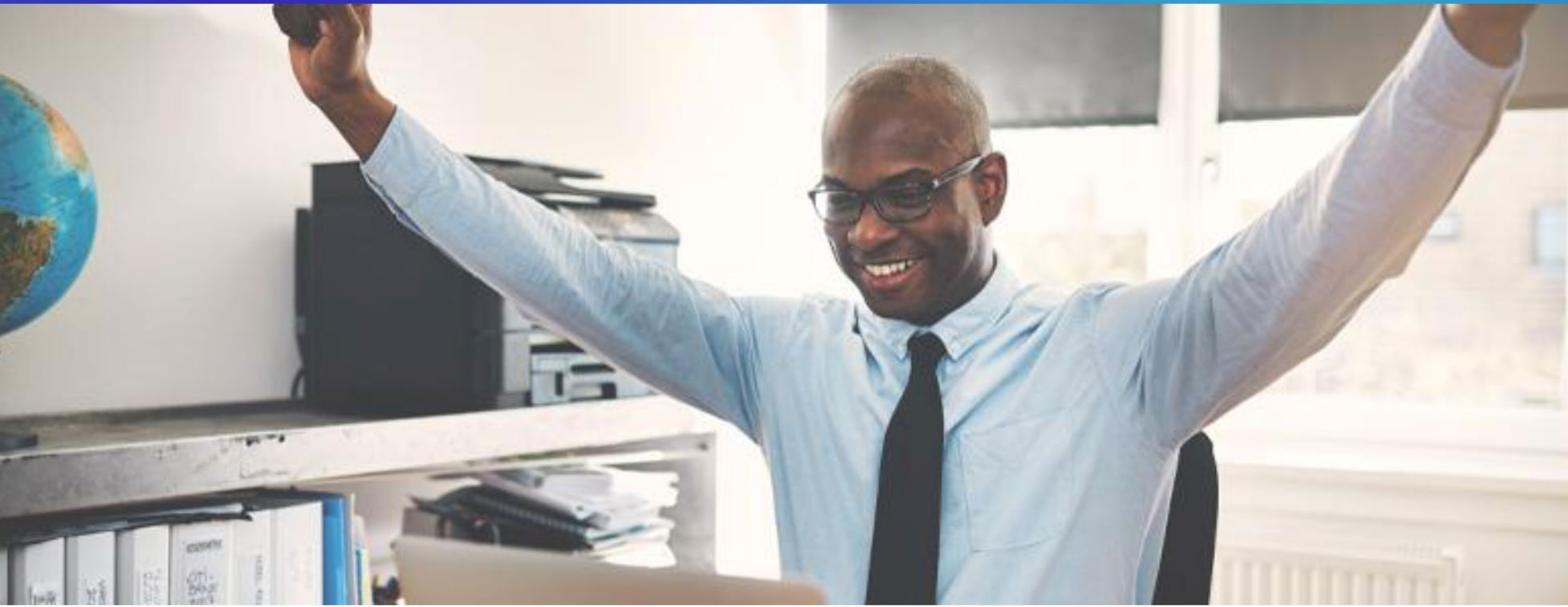


4. Manage and measure the data

5. Build a positive security culture

6. Personalize through micro-learning

7. Gamification done right



BREAKING SECURITY AWARENESS

Virtual Conference | June 24, 2021

- Human Risk Management
- Social Engineering
- DEI in Cybersecurity
- Enterprise Security Awareness
- Remote Working Security
- Ransomware

Register Today: breakingsecurityawareness.com

FEATURED SPEAKER

A Federal CISO's Perspective on Cybersecurity Awareness and Training

Janet Vogel

Chief Information Security Officer
Office of Information Security
Department of Health and Human Services

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

HHS Cybersecurity

OFFICE OF INFORMATION SECURITY (OIS) FISSEA Presentation

June 17, 2021

Cybersecurity Stakeholder Communities

Protect our House

Protect our Neighborhood

Protect all Healthcare

HHS

Federal Partners

HPH Sector

HHS Cybersecurity Today and Tomorrow

The HHS Cybersecurity Program is tasked with preparing for and facing cybersecurity threats as well as protecting the critical information with which the Department is entrusted

2020

HHS maintains

760

systems

379,310

endpoints subject to attack

86

High Value Assets (HVAs)—critical systems that support HHS' mission

65+

legislative mandates that HHS' cybersecurity and privacy program are required to satisfy

HHS experienced

209 billion

attempts to compromise our systems resulting in

7,557

incidents

HHS implemented systems to aid in the fight against

COVID-19

when they became attractive cyber targets worldwide

2021 and Beyond

Growing sophistication of cyber attacks

requiring more technical abilities to better prevent, defend and mitigate threats

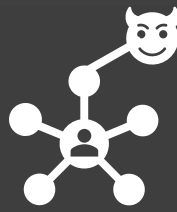
Increased data exposure

because of increased cloud migration and access by authorized and bad actors

Increased phishing & spear-phishing attempts

Based on current trends

New threat vectors



Introduced by a more distributed workforce using unapproved tools and technologies while teleworking

Importance of Cybersecurity Awareness Training

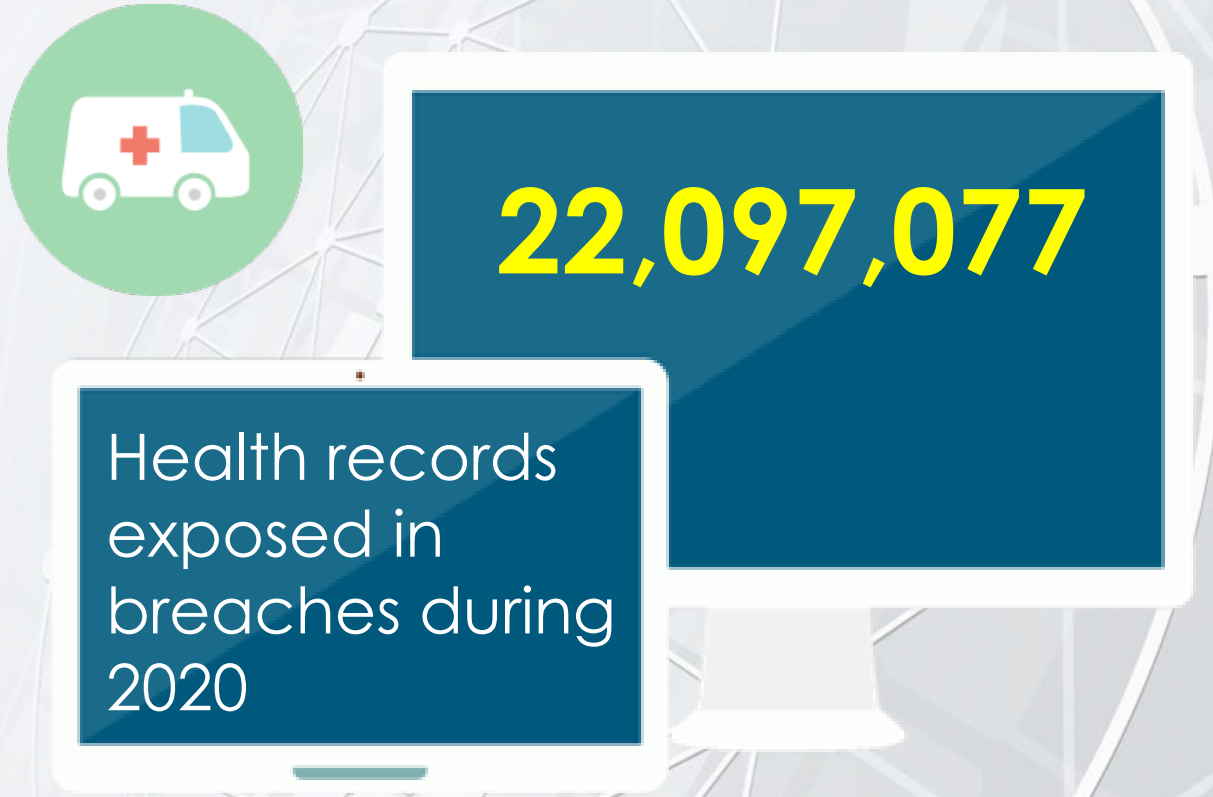
$7.13 MILLION

The average cost of a data breach in the healthcare sector was **$7.13 million** in 2020.

Organizations that willfully neglect HIPAA Rules and make no effort to protect sensitive patient data could be fined **up to**

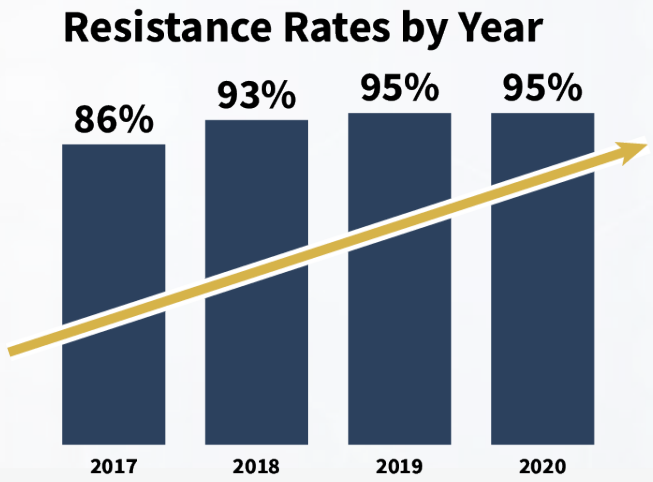
$1.5 million

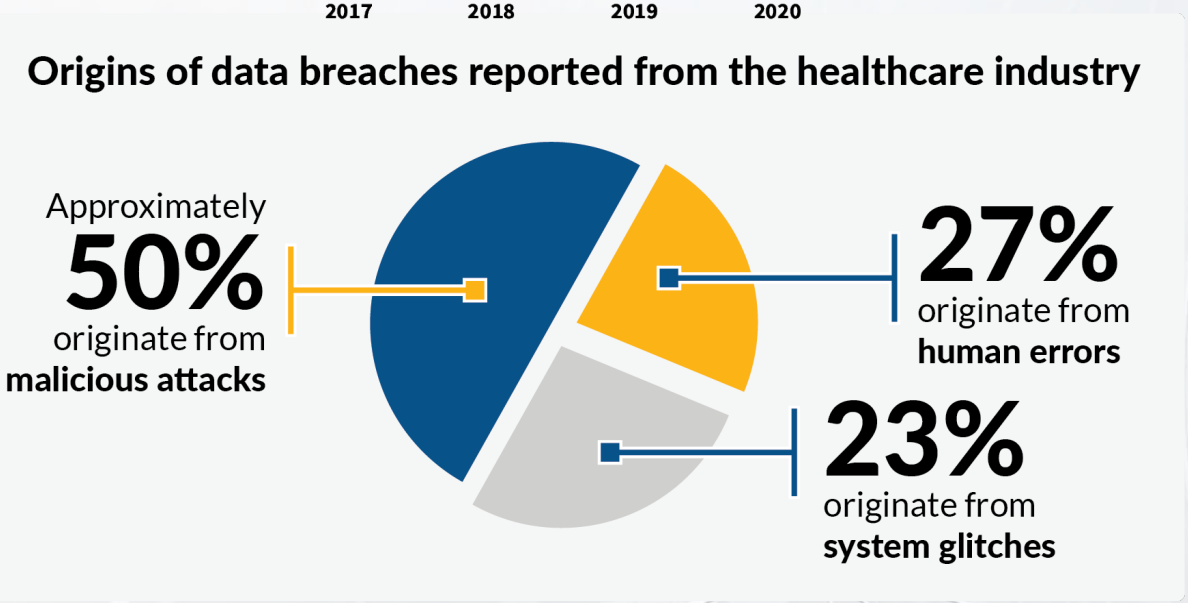
per year.



96% of cyber attacks start from an email

Threats Are Constantly Evolving – So Must Security Awareness Training





HHS Cybersecurity Awareness Training and 405(d) Program

HHS CyberCARE
Communication, Awareness, Response & Education

ALIGNING HEALTH CARE INDUSTRY SECURITY APPROACHES
HHS 405(d)

Cybersecurity Awareness Training Will Remain Critical

For the **10th** year in a row, healthcare has had the **highest** average breach cost

6.48 million (2019)

7.13 million (2020)

10% increase from 2019

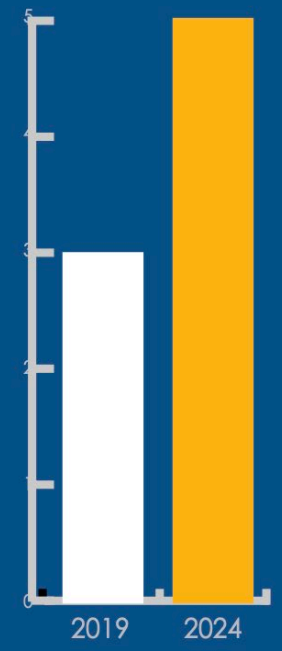
It is estimated that the cost of data breaches will rise from

$3 trillion

each year to over

$5 trillion

by 2024



Verizon Data Breach Report (2019)

Cybersecurity Awareness – Do I have your attention now?

- **Visit www.hhs.gov/hc3 for threat briefs and health sector alerts.**
- **Visit www.phe.gov/405d and follow us @ask405d on your favorite social media platform for cybersecurity tips, awareness products, and to learn about 405(d) outreach events for the HPH sector.**

Cybersecurity Awareness – Do I have your attention now?

Questions?

Federal Information Security Educators (FISSEA) Summer Forum

BREAK

The Forum will resume at 2:30pm EDT

#FISSEA2021 | nist.gov/fissea

fissea
FEDERAL
CYBERSECURITY | INNOVATION, AWARENESS, TRAINING

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

Innovator of the Year Award Recognition

Loyce Pailen

Senior Director, Center for Security Studies
University of Maryland Global Campus
(Committee Chair)

Shehzad Mirza

Director of Operations
Global Cyber Alliance
(2019 Award Recipient)

CONGRATULATIONS TO:

Deborah Coleman

Cybersecurity Awareness and Training Program Manager
U.S. Department of Education
FISSEA Innovator of the Year

Stu Sjouwerman

Founder and CEO
KnowBe4, Inc.
FISSEA Innovator of the Year

FISSEA Innovator of the Year Fireside Chat

Loyce Pailen
Moderator

Senior Director, Center for Security Studies
University of Maryland Global Campus
(FISSEA Committee Chair)

Deborah Coleman
Panelist

Cybersecurity Awareness and
Training Program Manager
U.S. Department of Education
(FISSEA Innovator of the Year)

Stu Sjouwerman
Panelist

Founder and CEO
KnowBe4, Inc.
(FISSEA Innovator of the Year)

Breakout Groups

Breakout Group One:
Cybersecurity Awareness Challenges and Solutions for a Remote Federal Workforce

Facilitators:

Art Chantker
President
Potomac Forum

Frauke Steinmeier
Cybersecurity & Infrastructure Security Agency
Department of Homeland Security

Breakout Group Two:
Creating Virtual Training for Federal Employees – What's Working, What's Not

Facilitators:

Susan Hansche
Cybersecurity & Infrastructure Security Agency
Department of Homeland Security

Clarence Williams
Senior Advisor, Cyber Workforce Management Department of Veterans Affairs

Closing Remarks

Susan Hansche

Cybersecurity & Infrastructure Security Agency
Department of Homeland Security

NICEatNIST.checkbox.com/fisseaevents

FISSEA Contest

Submissions are due by June 30th!

- Awareness Poster
- Innovative Solutions
- Awareness Website
- Awareness Newsletter
- Awareness Video
- Cybersecurity Blog
- Cybersecurity Podcast
- Technical Training Scenario or Exercise

Email submissions to: fissea-contest@nist.gov

Get Involved

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

Volunteer for the Planning Committee

Serve on the Contest or Award Committees for 2022

Email fissea@list.nist.gov

STRONGER TOGETHER

FISSEA Fall Forum

September 28, 2021

1:00pm – 4:00pm EDT

REGISTER TODAY: nist.gov/fissea

SAVE THE DATE

STRONGER TOGETHER

Federal Information Security Educators (FISSEA) Conference

May 18-19, 2022

#FISSEA2021 | nist.gov/fissea

fissea FEDERAL
CYBERSECURITY | INNOVATION, AWARENESS, TRAINING

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