Federal Information Security Educators (FISSEA) Fall Forum

STRONGER TOGETHER

September 28, 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 FISSEA Chair

Susan Hansche

FISSEA Chair

Cybersecurity & Infrastructure Security Agency

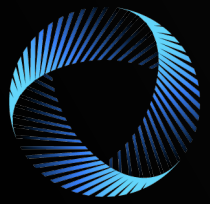
Department of Homeland Security

Kick-Off to Cybersecurity Awareness Month

Lisa Plaggemier

Interim Executive Director

National Cyber Security Alliance



NATIONAL
CYBERSECURITY
ALLIANCE

The Power of the Collective

Lisa Plaggemier
Interim Executive Director | National Cyber Security Alliance

27 September 2021

We empower a more secure, interconnected world.

Our alliance stands for the safe and secure use of all technology.

We encourage everyone to do their part to prevent digital wrongdoing of any kind.

We build strong partnerships, educate and inspire all to take action to protect ourselves, our families, organizations and nations.

Only together can we realize a more secure, interconnected world.

CYBERSECURITY AWARENESS MONTH

CyberSecure MY BUSINESS

IDENTITY MANAGEMENT DAY2021

DATA PRIVACY DAY

Millions of people turn to the National Cybersecurity Alliance for information

- 1.7+ million pageviews StaySafeOnline.org
- 350,000+ social media followers
- 150+ free resources
- Thousands of webinar attendees
- 3,000 CyberSecure My Business attendees


mimecast


Lilly


WELLS
FARGO


DISCOVER


TERRANOVA
SECURITY


PAUBOX


Microsoft


COFENSE


ADP


mastercard


VISA


proofpoint


BANK OF AMERICA


Raytheon


LA Z BOY


facebook


usbank


eset


KnowBe4
Human error. Conquered.


servicenow


AIG


NortonLifeLock

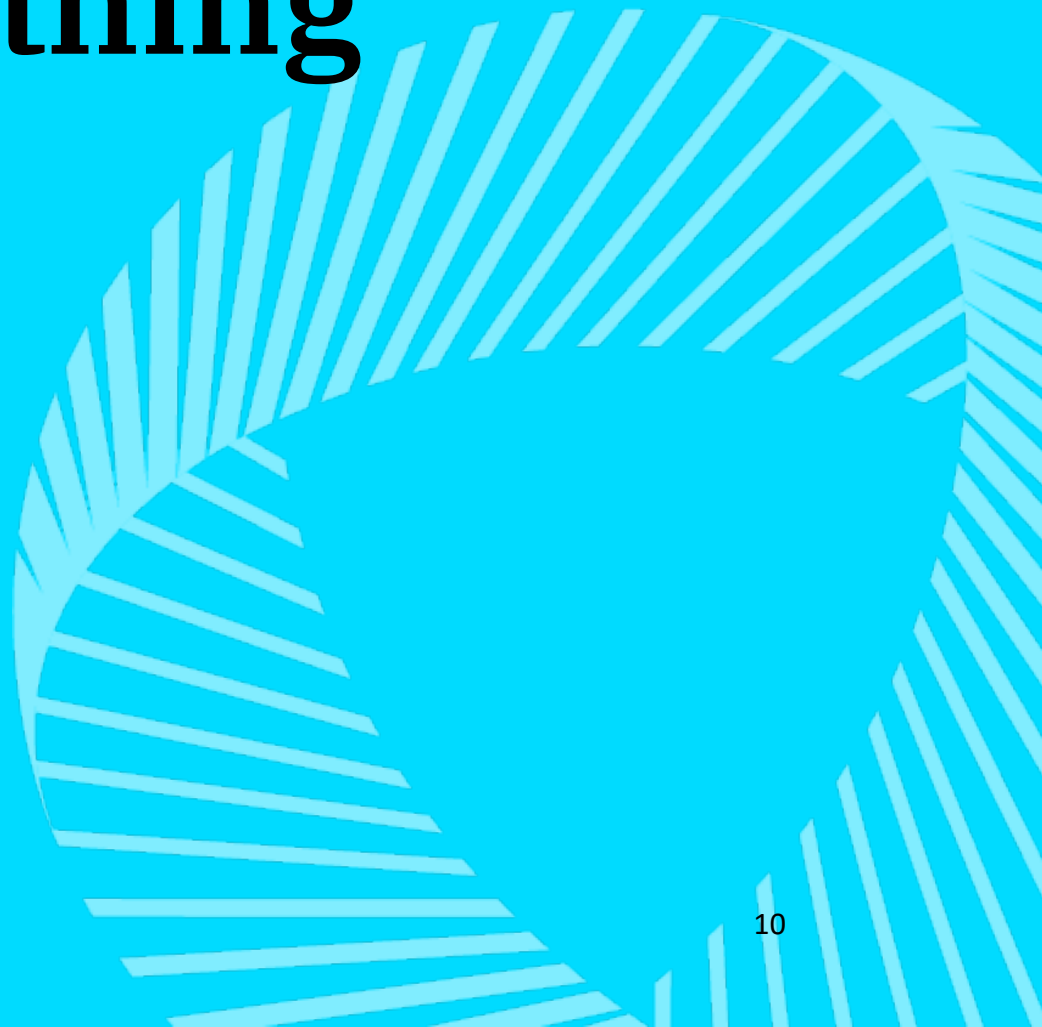

MARRIOTT


Lenovo

NATIONAL
CYBERSECURITY
ALLIANCE

NATIONAL
CYBERSECURITY
ALLIANCE

Be a part of something bigger



102,514,520

8,425 unique articles published with a global reach of over **3.1 billion**

Of those articles, **1,366** referenced "Do Your Part. #BeCyberSmart", resulting in **487 million** global views

NATIONAL CYBERSECURITY ALLIANCE

StaySafeOnline.org

188.4k

sessions

26%

increase from 2019

157k

unique visitors

27%

increase from 2019

367.6k

page views

10%

increase from 2019

#BeCyberSmart

- 77,117 tweets in 2020
- 70% increase from 2019
- 752M total impressions in 2020
- 94% increase from 2019

6.4M followers

Twitter Support
@TwitterSupport

October is National Cybersecurity Awareness Month in the US, but staying safe online is something you can do anywhere at any time.

Over the next few weeks, we'll be sharing some tips to keep your account safe and secure. #BeCyberSmart

1:04 PM · Oct 12, 2020 · Sprinklr

202 Retweets **30** Quote Tweets **603** Likes

4.1M followers

BlackBerry
@BlackBerry

#BeCyberSmart Tip: In #healthcare, a Zero Trust model can ensure 24x7 access to critical information.

Visit bit.ly/31mNkK0 to get a live demo of BlackBerry solutions, learn how to apply #ZeroTrust to earn patient trust and protect patient data.

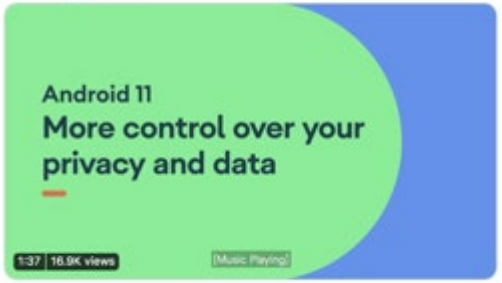
12:01 PM · Oct 19, 2020 · Salesforce - Social Studio

4 Retweets **12** Likes

10.5M followers

Android
@Android

#Android11 puts you in control of what permissions you want to share with apps on your phone. Hear from Senior Product Manager Charmaine D'Silva on the new privacy features that help keep you better protected. #BeCyberSmart



12:04 PM · Oct 7, 2020 · Sprinklr

75 Retweets **3** Quote Tweets **577** Likes

820.5K followers

FEMA
@fema

October is a National Cyber Security Awareness Month. #BeCyberSmart by reviewing your online privacy settings and updating your passwords regularly.

Follow @StaySafeOnline & @CISAgov for more useful tips: cisa.gov/national-cyber...

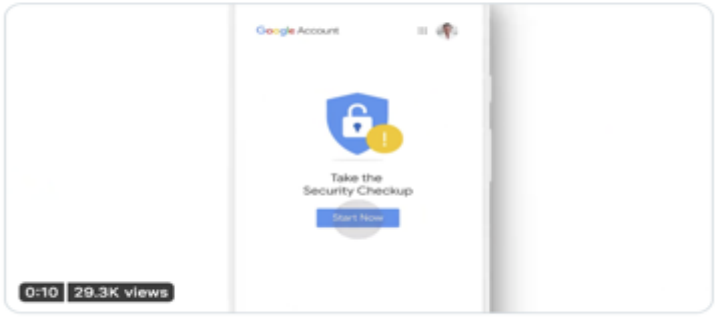
9:46 AM · Oct 23, 2020 · Hootsuite Inc.

11 Retweets **1** Quote Tweet **15** Likes

22.M followers

Google
@Google

It's Cybersecurity Awareness Month—the perfect reminder to take a quick Security Checkup to strengthen your account security → goo.gle/3ktQ7IF



12:08 PM · Oct 1, 2020 · Twitter Web App

135 Retweets **12** Quote Tweets **645** Likes

6.2M followers

Department of Defense
@DeptofDefense

It's National Cybersecurity Awareness Month! Press ▶ to hear a message from Defense Secretary @EsperDoD. Remember: Do your part! #BeCyberSmart.

4:00 PM · Oct 1, 2020 · Twitter Media Studio

16 Retweets **2** Quote Tweets **33** Likes

2M followers

CDC Emergency
@CDCemergency

#DYK personal medical devices can be vulnerable to cybersecurity incidents, such as cyberattacks? #BeCyberSmart by learning how to protect your internet-connected devices. Learn more: ow.ly/rgl850BYHXR #PrepYourHealth

5:50 PM · Oct 22, 2020 · Hootsuite Inc.

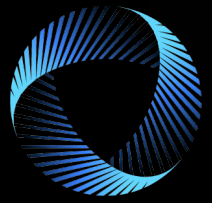
9 Retweets **19** Likes

813.3K followers

Robert Herjavec
@robertherjavec

October is Cybersecurity Awareness Month! Are you #cyberaware? Test your cybersecurity knowledge and download the resource kit from @HerjavecGroup at HerjavecGroup.com/BeCyberSmart Oh and send me your toughest cybers Qs ! #BeCyberSmart

Stay safe online.



NATIONAL
CYBERSECURITY
ALLIANCE

Website
StaySafeOnline.org

Twitter
@staysafeonline

Facebook
/staysafeonline

LinkedIn
/national-cyber-security-alliance

Email
info@staysafeonline.org

Featured Topic: *Security Awareness Training Research Study*

Julie Haney

Usable Cybersecurity Program Lead
National Institute of Standards and Technology

Jody Jacobs

IT Specialist
National Institute of Standards and Technology

NIST Security Awareness Study

Julie Haney, Jody Jacobs, and Susanne Furman
National Institute of Standards and Technology
September 2021

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

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Problem

Organizational security awareness programs face numerous challenges.

- May lack tools, resources, and appropriate competencies to effectively manage and execute programs
- May be compliance (vs. impact) focused

Unclear if these challenges apply to U.S. Government programs

Study Overview

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

Focus Groups

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

Online, Anonymous Survey

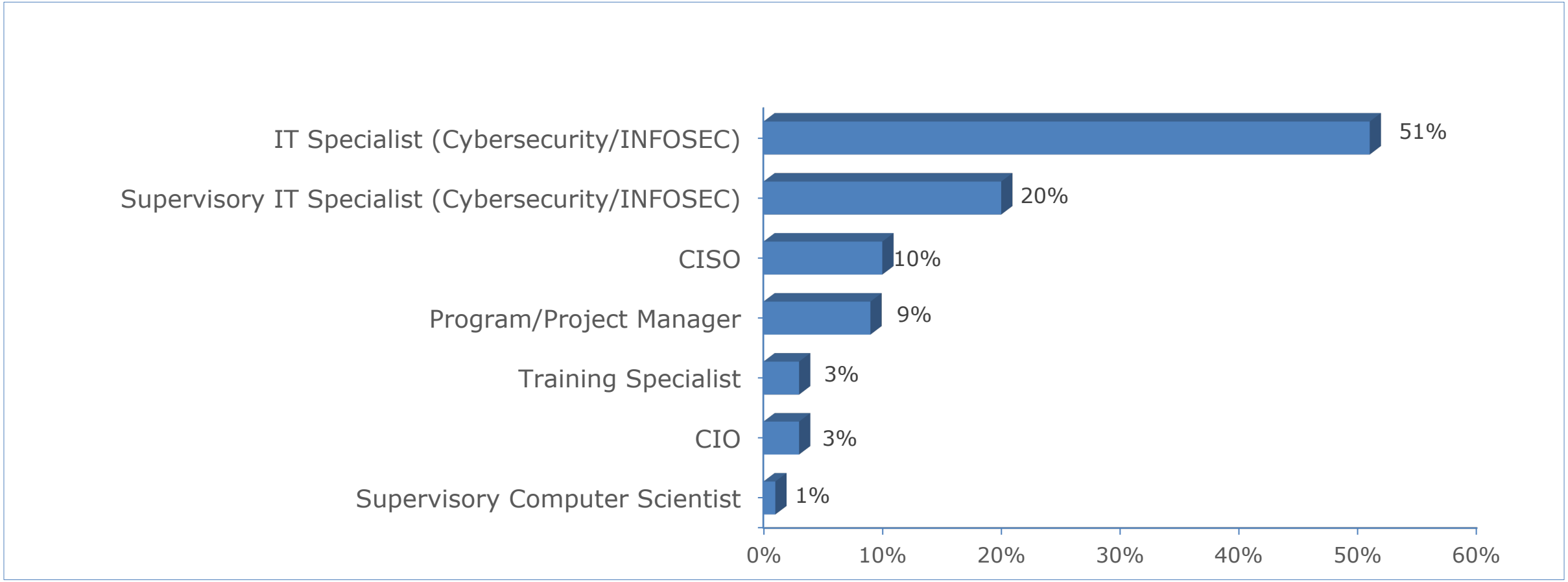
Survey of a broader population (n=96) of federal security awareness professionals

Study Participants and Organizations

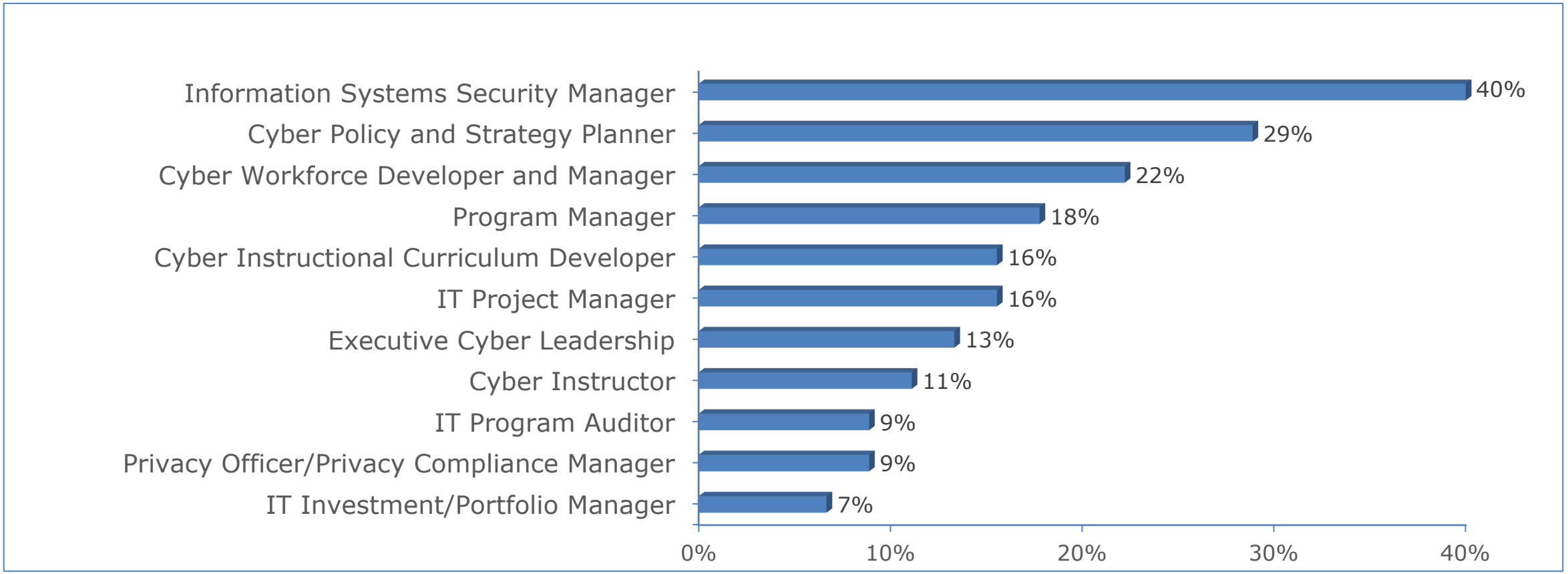
Security Awareness Involvement

	Focus Groups	Survey
Security awareness role	**76%** program leads 10% program team members 14% managers/CISOs	**45%** program leads 36% program team members 21% managers/execs (~52% leads)
% of time on security awareness	**93%** are part-time 38% <= ¼ of their time	**90%** are part-time 56% <= ¼ of their time
Security awareness experience	**69%** with > 5 years **all** with > 1 year	74% with > 5 years **99%** > 1 year

Job Classifications (survey)

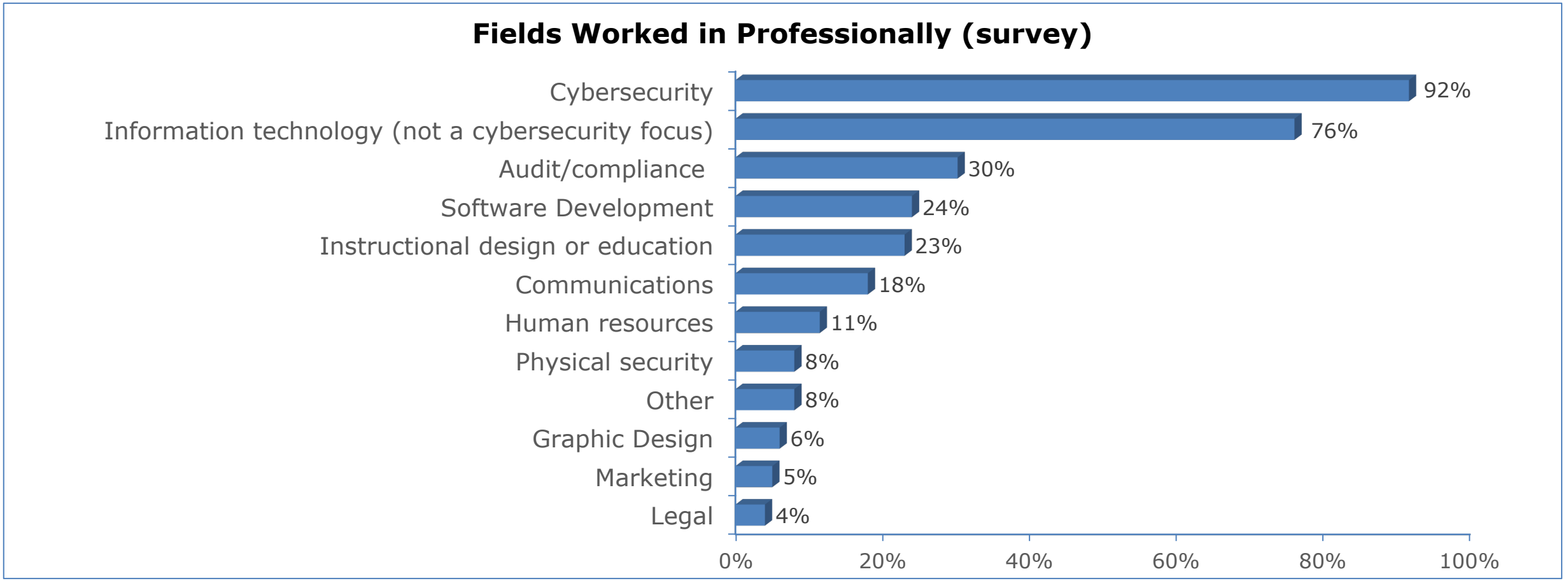


NICE Framework Work Roles (survey)

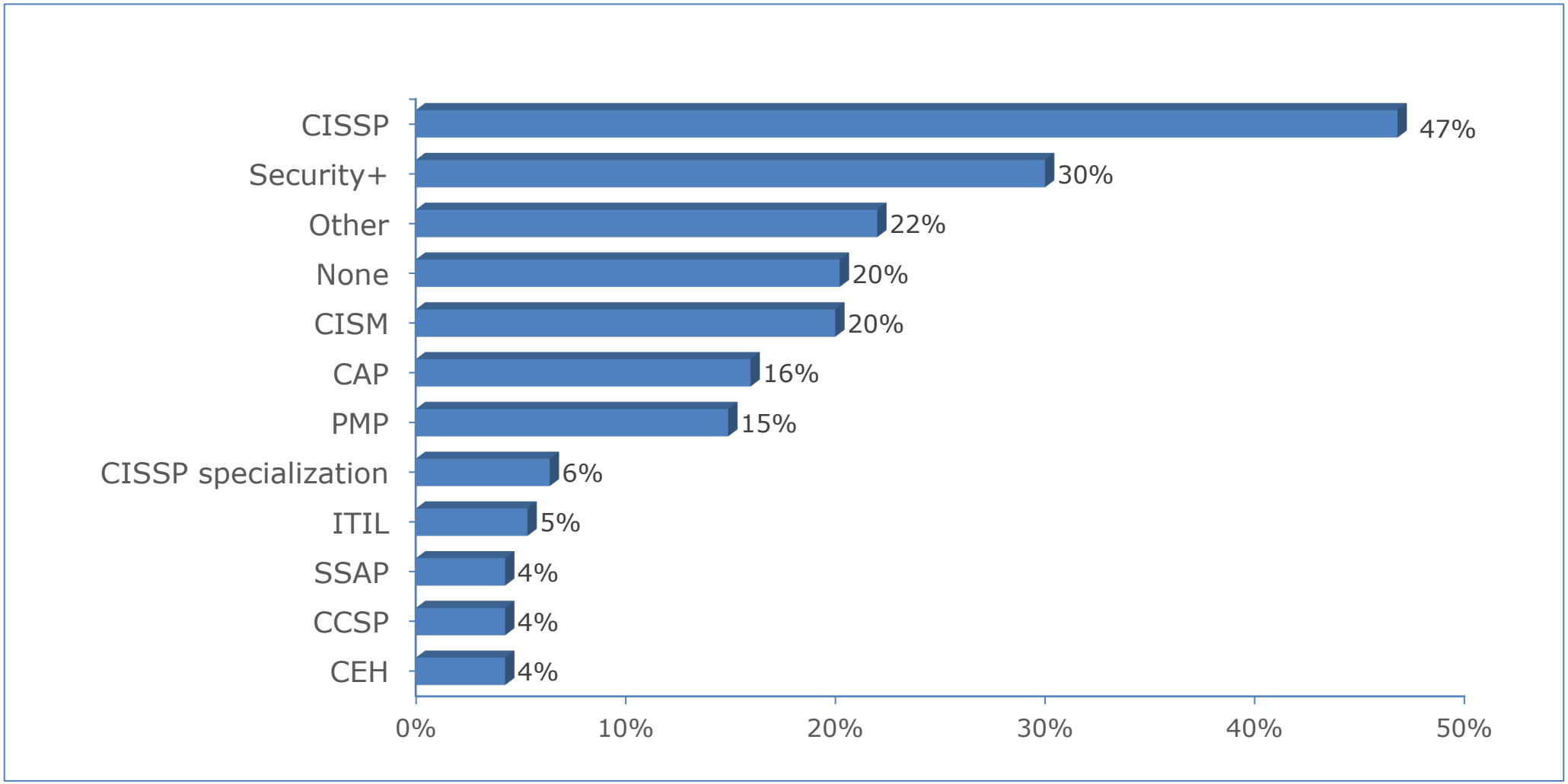


Discipline Diversity

83% of ***focus group*** and **68%** of ***survey*** participants had at least one non-computing degree



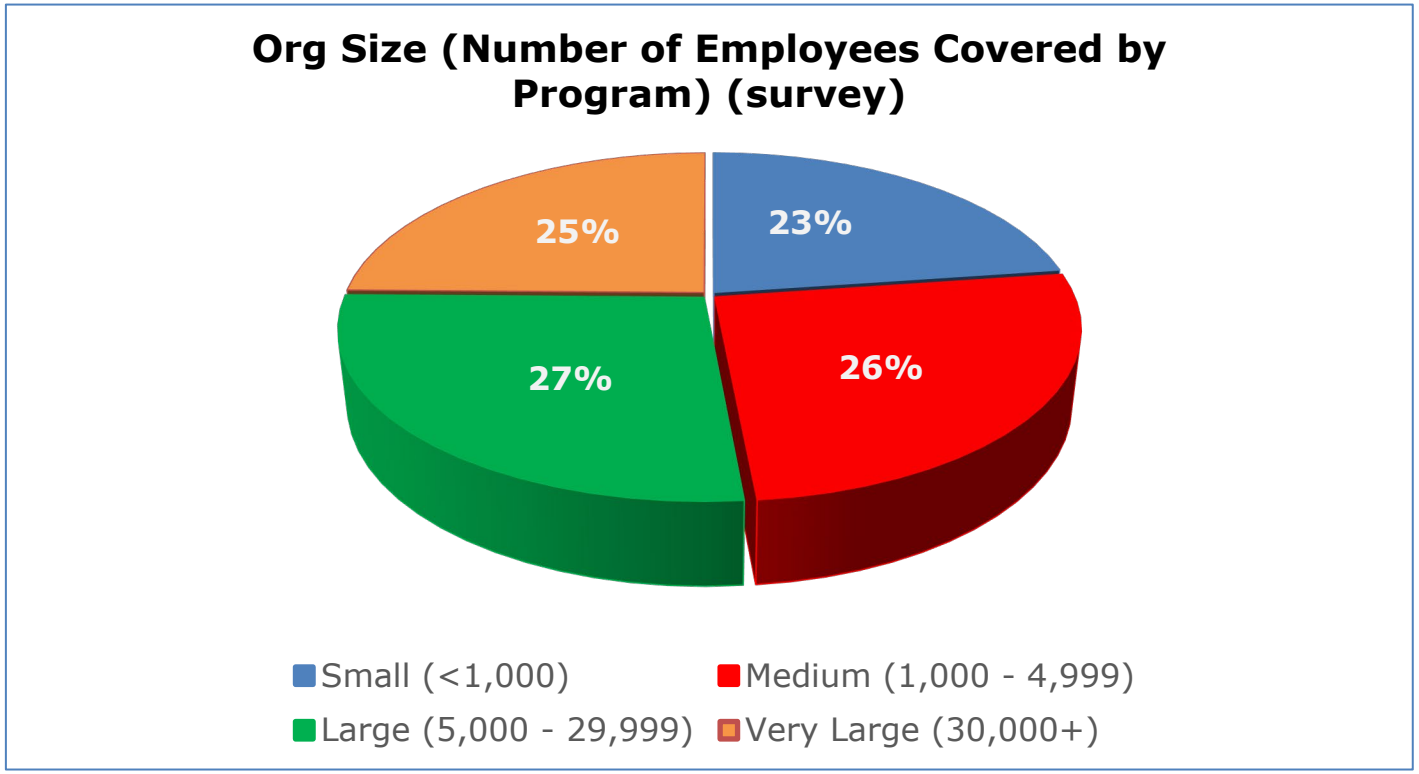
Industry-recognized Certifications (survey)



Represented Organizations

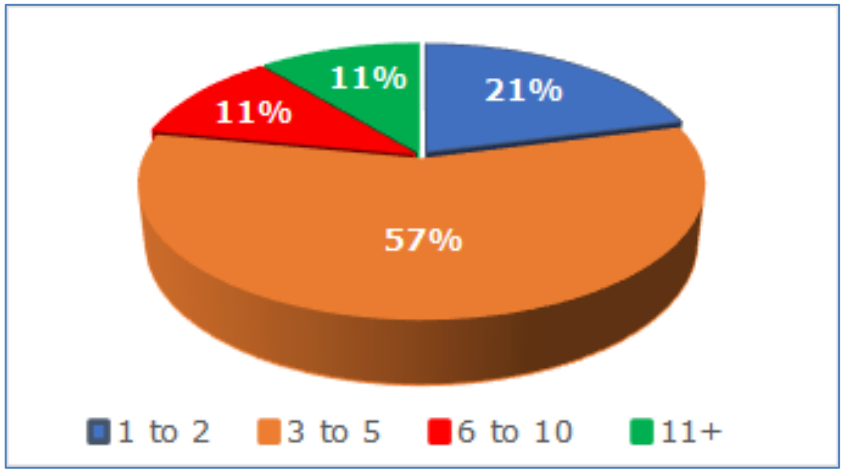
Focus Groups: ~21% from departments
38% sub-components
41% independents

Survey: ~32% departments
31% sub-components
35% independents

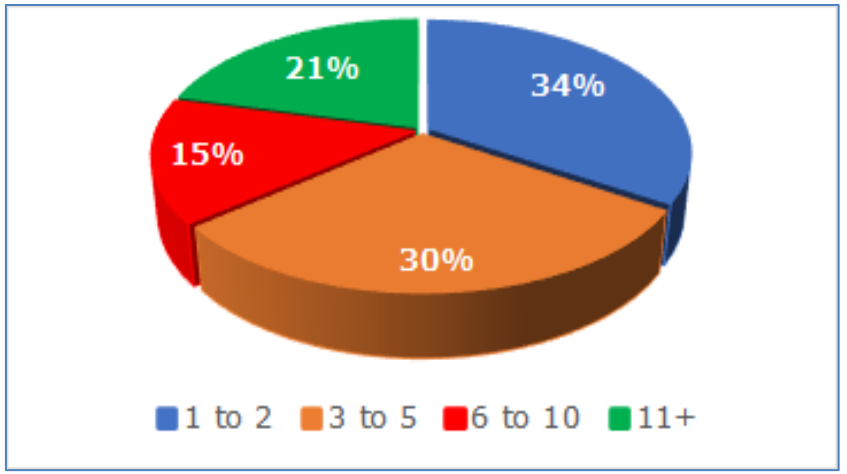


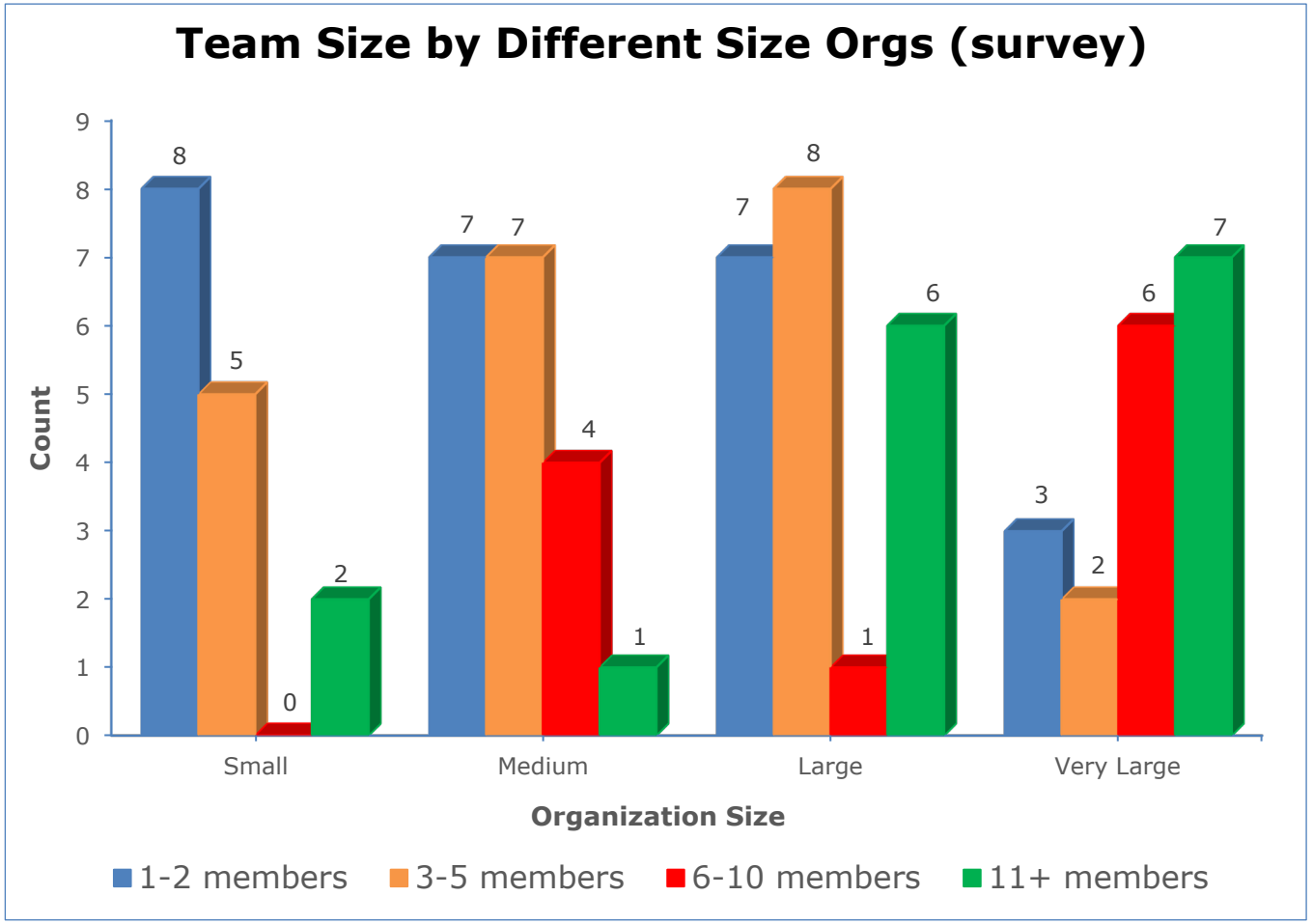
Security Awareness Team Size

Focus Groups



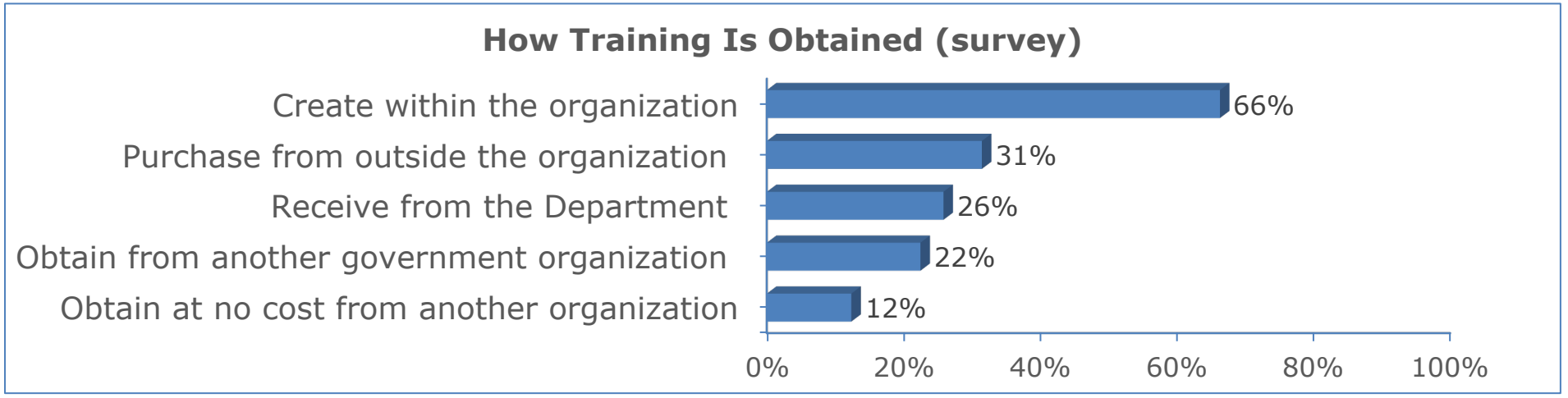
Survey





Results

Required Annual Cybersecurity Training



- Training delivered online, computer-based or live events
- Training is obtained from variety of sources
- **80%** update training at least once per year
- The handling of non-compliance varied from email reminders to **~75%** disabling account or network access

Required Annual Training Challenges

47% Getting employees to complete training

23% Finding course materials

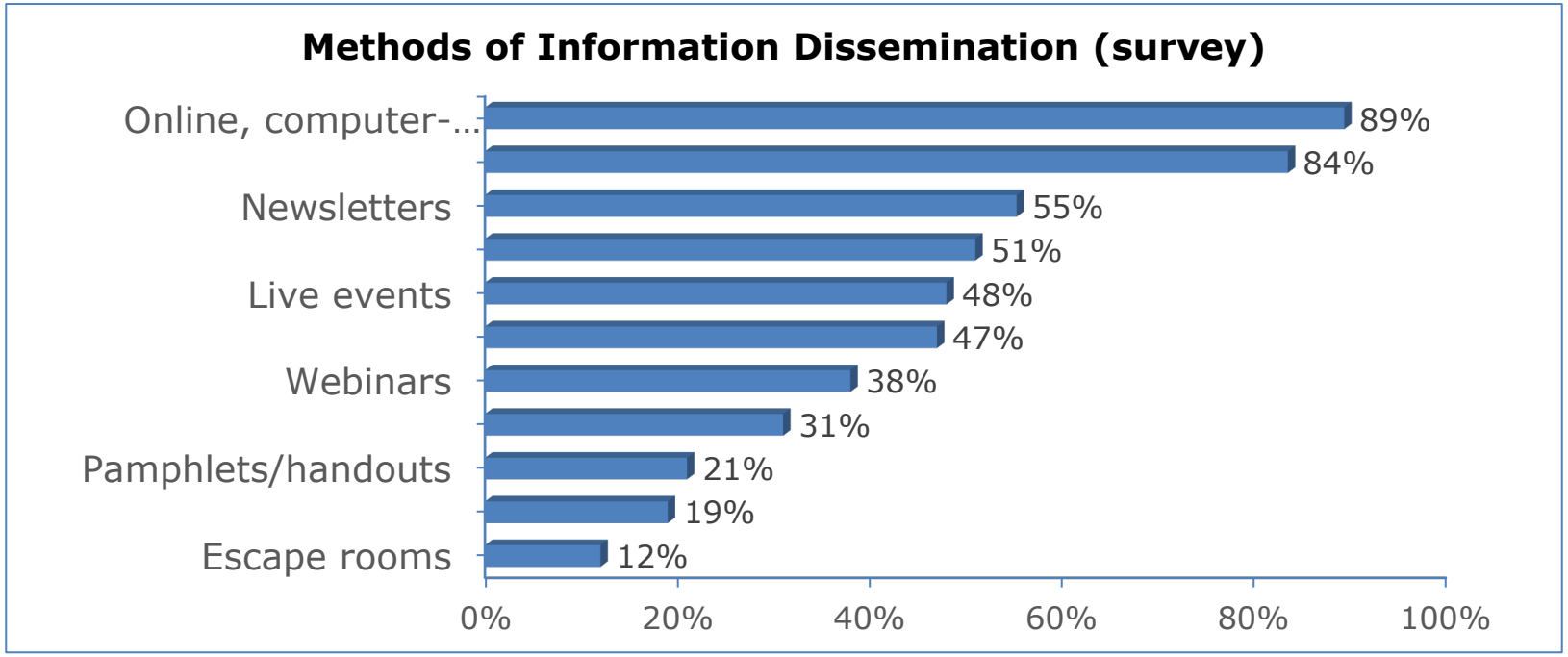
22% Finding guidance on what to include

Focus Groups: Lack of course content standardization across agencies

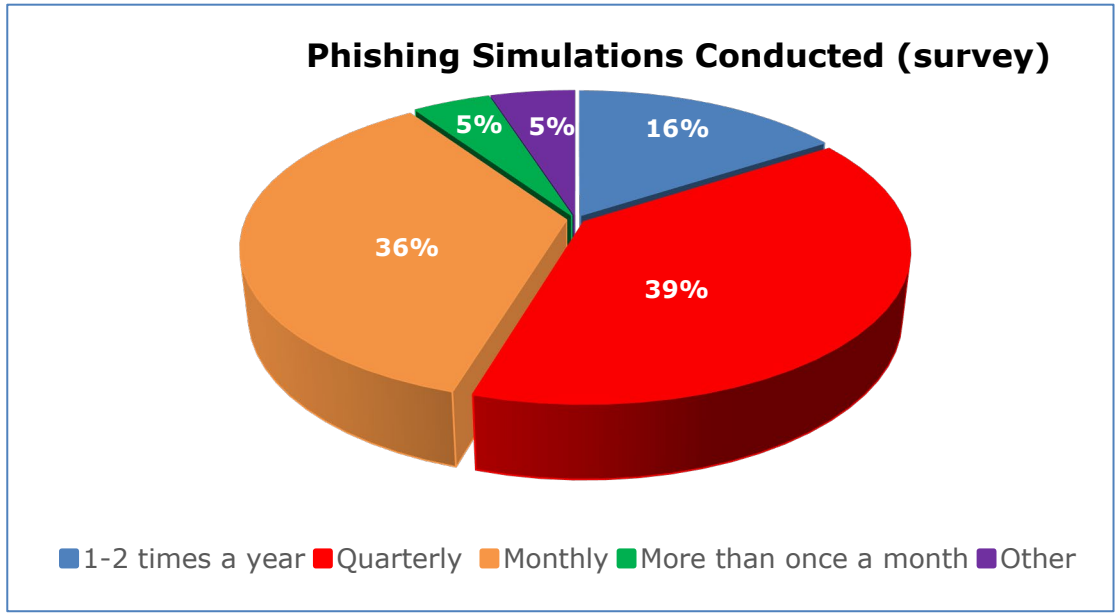
"There are some topics, probably 80% of the topics, everybody needs to know about. So why are we buying that over and over again at each agency?" (D01)

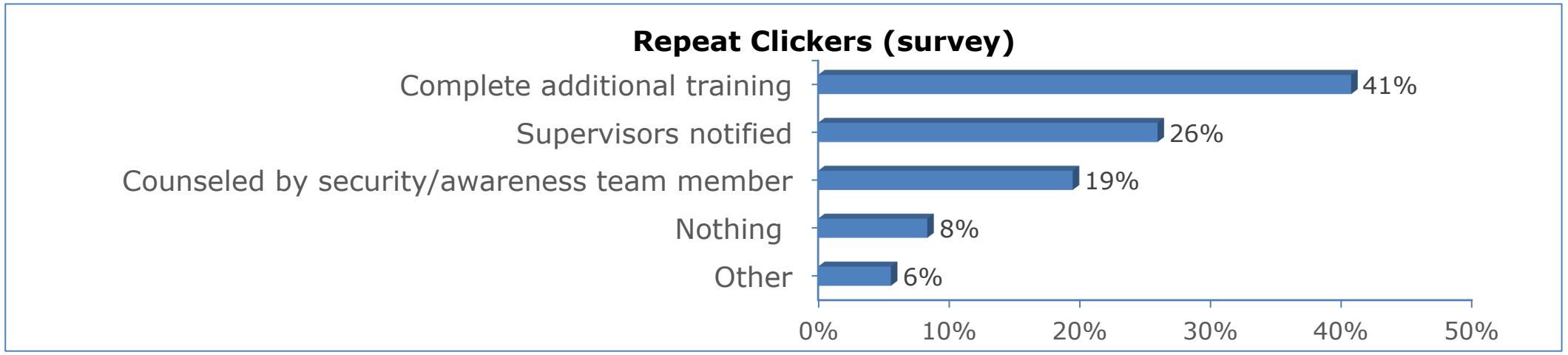
Approaches

- **21%** have no security awareness events or interactive activities beyond required training or phishing simulations
- **56%** don't recognize or reward employees for good security behavior
- Disseminate information using various methods: **7%** only use 1 method, **41%** 2-4 , **30%** 5-7, **22%** 8+



Phishing Simulations





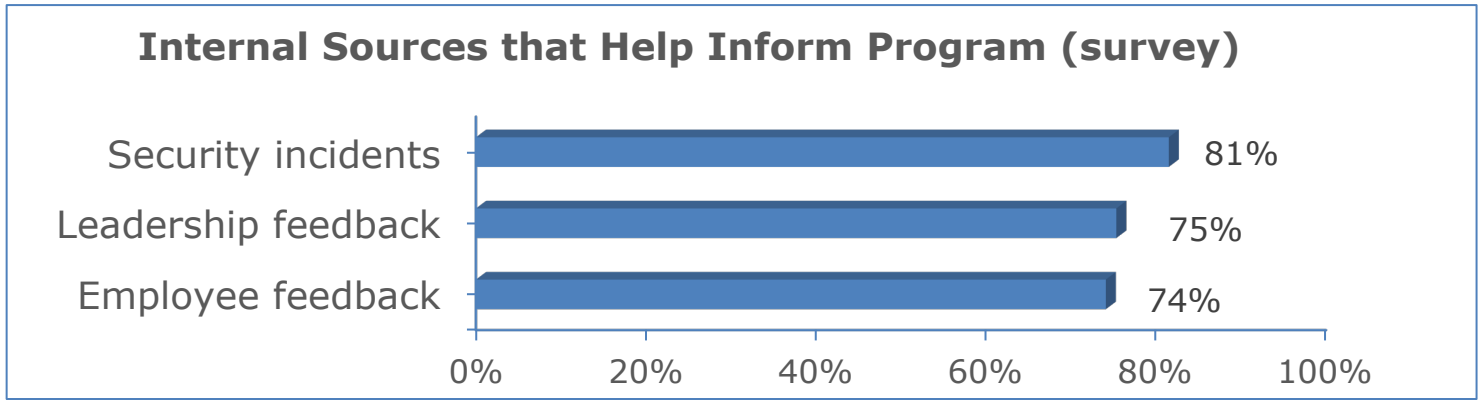
Approaches Challenges

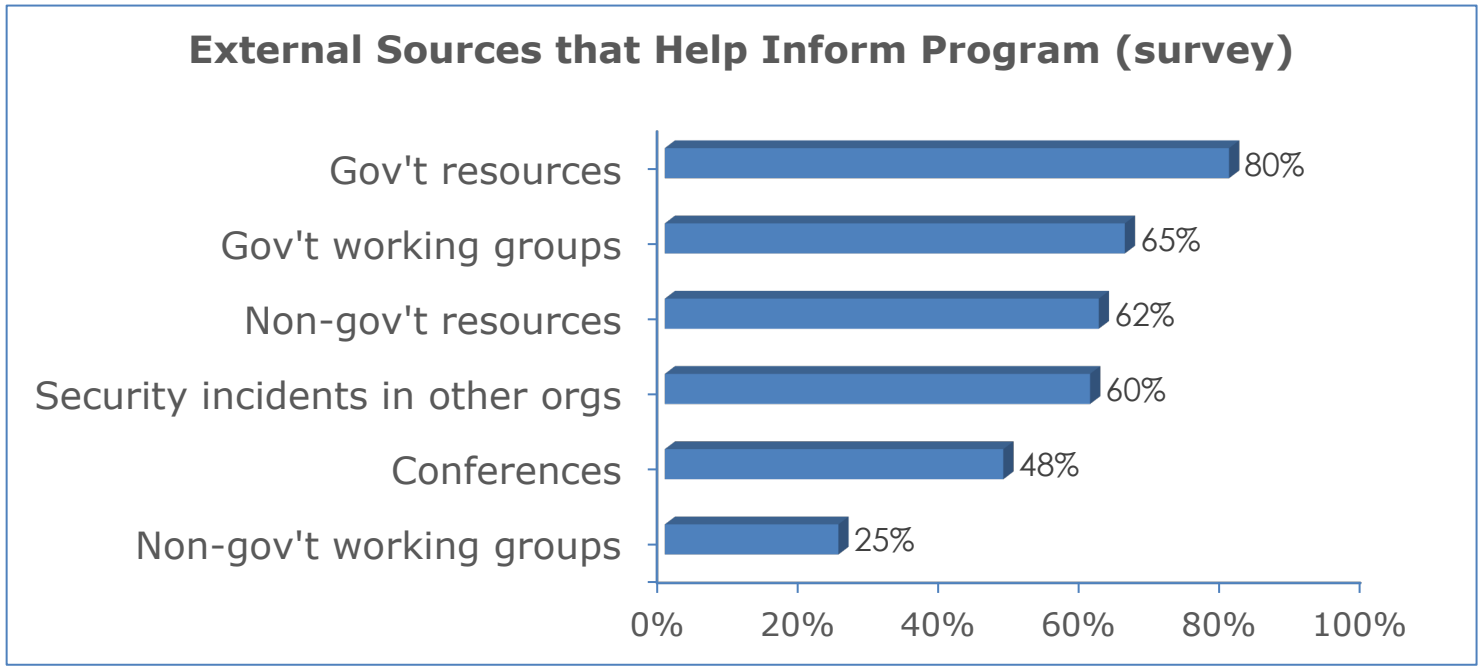
- 56% Providing information in an engaging way
- 47% Customizing for diverse workforce
- 29% Communicating to distributed workforce
- 40% Ensuring 508 compliance

"We're trying to reinforce the information, but we still want to have creative ways to present it so it doesn't feel like they're just taking the same thing over and over again and they're just clicking through without actually reading through the information." (N12)

Informing Content

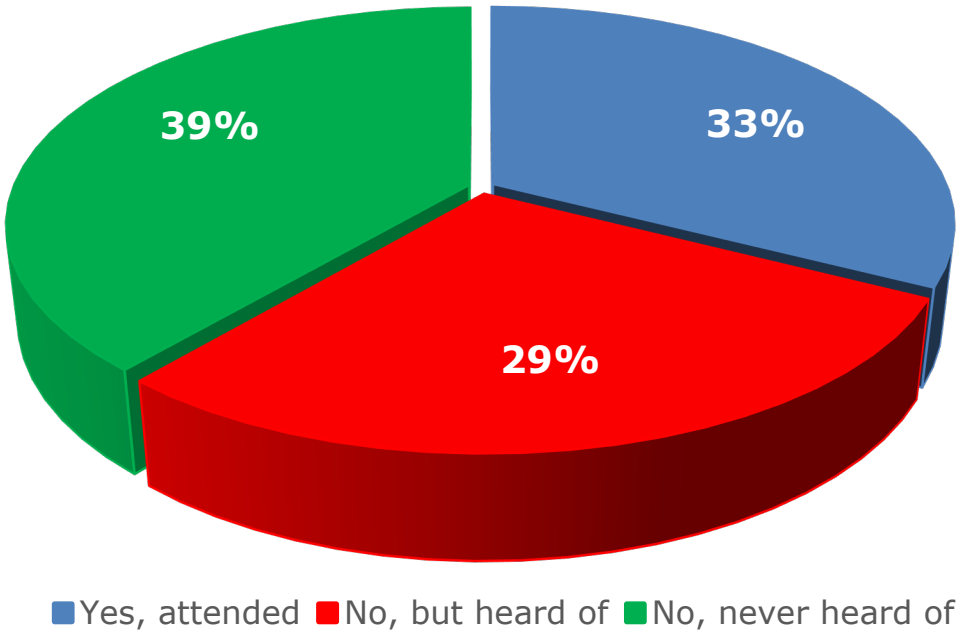
- Autonomy levels varied for program development and content customization
- Security awareness is a collaborative effort within the organization
- Internal and external sources informed content coverage and sources



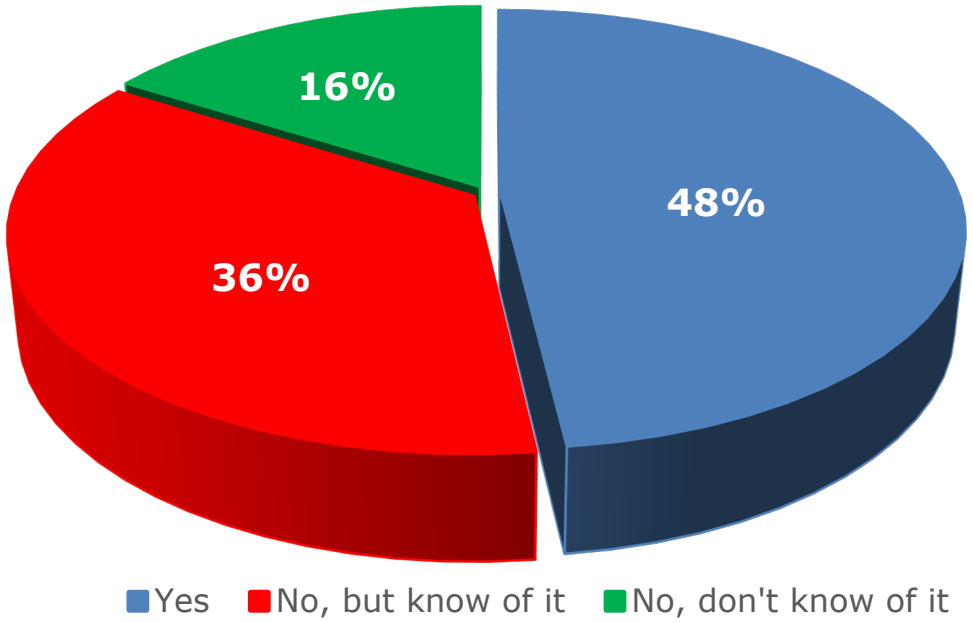


Awareness of FISSEA and NIST SP 800-50

Heard of FISSEA (survey)



Used NIST SP 800-50 "Building an IT Security Awareness and Training Program" (survey)



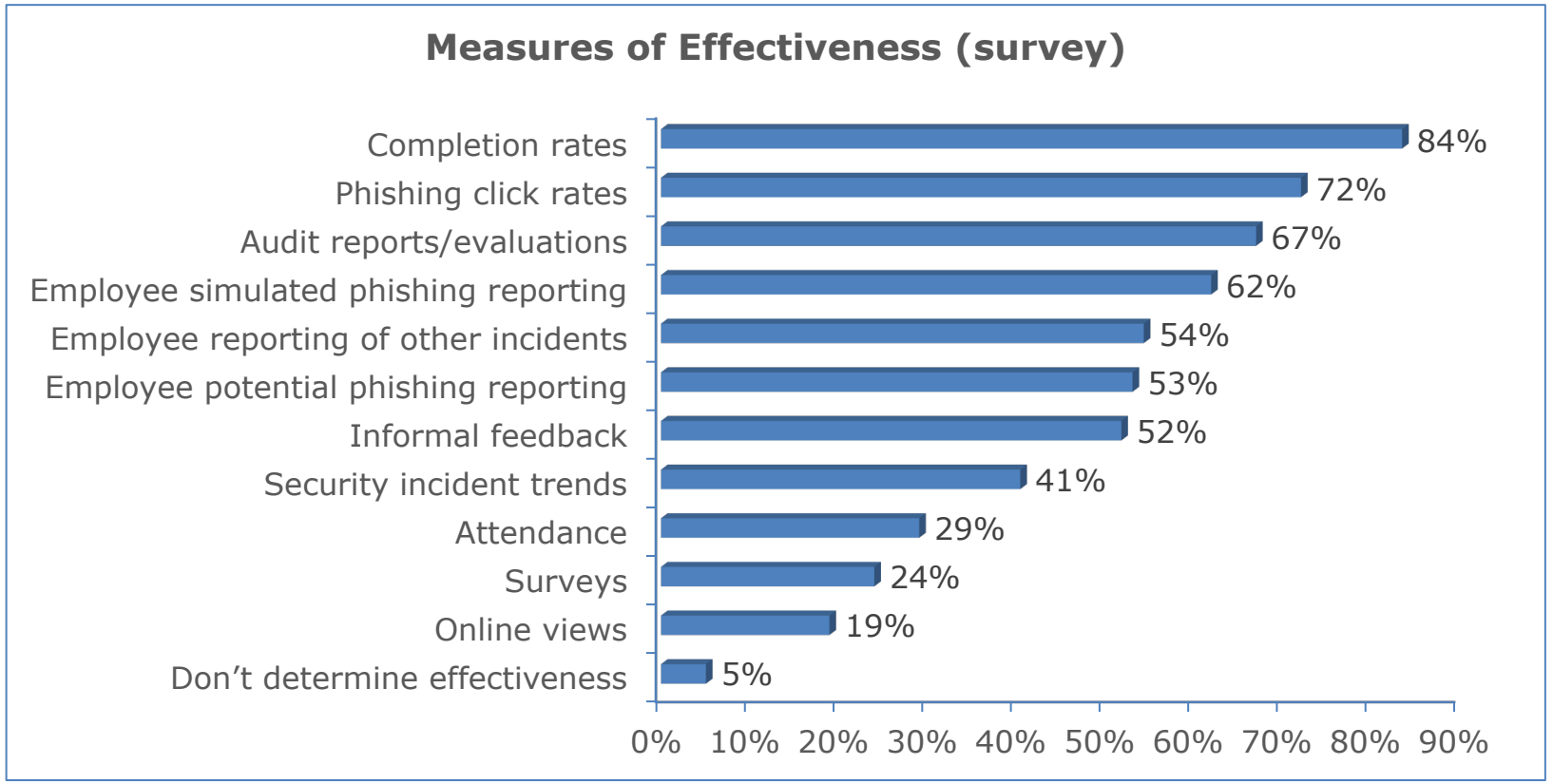
Informing Content Challenges

27% Collaborating with other federal security awareness professionals

33% Finding external sources of information relevant to organization

"There's a lot of resources out there to leverage. It's just the challenge is to be able to integrate it into your organization and not make it look like it's so out of place." (D05)

Measures of Effectiveness (MOEs)



- MOEs used for multiple reasons
  - **78%** - Demonstrate compliance
  - **71%** - Improve/inform program
  - **58%** - Show value of program to leadership
  - **42%** - Justify additional resources
- "Compliance is most important indicator of success"
  - Among leadership - **56%** Agree, 22% Disagree
  - Among respondents - **47%** Agree, 28% Disagree

Measures of Effectiveness Challenges

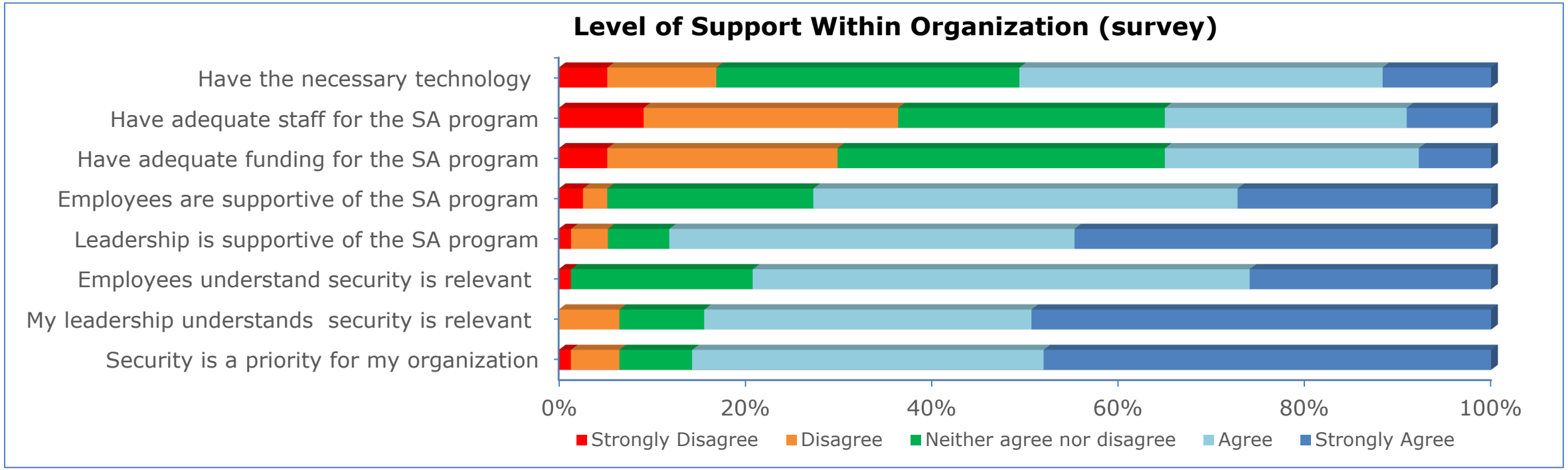
- 44% What/how to measure
- 37% Effectively presenting data to leadership
- 48% Integrating security awareness data with data from other groups
- 56% Benchmarking program against other federal organizations

Focus Groups:
Compliance vs. impact on behavior change

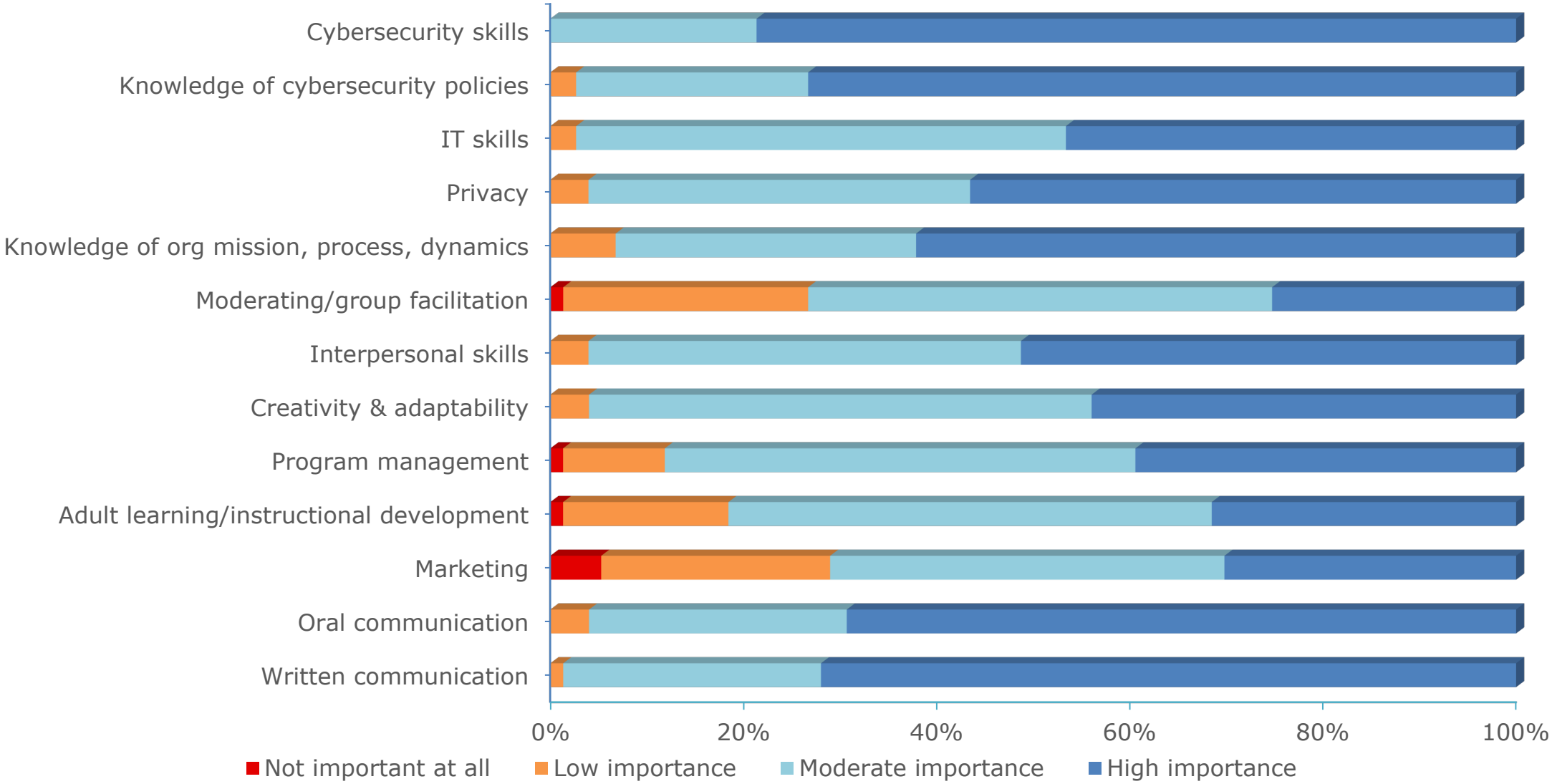
> "How do we determine whether or not it is effective? We have not come up with that solution yet…How are we making an impact? How are we making a difference when we educate our workforce?" (N04)

Program Support and Success

- **77%** of survey respondents think their program is moderately or very successful
- Varied views on level of support within the organization



Team Knowledge and Skills – Rating Importance



Mix of Skills/Knowledge

- **61%** of survey respondents think they have the right mix of skills/knowledge for their programs
- **Focus groups**:
  - Discipline diversity is beneficial
  - Programs often enlist help from other organizational groups (e.g., communications, HR) to augment their team

> "I have people who can design, are very artful, creative people. I have people who can run a learning management system… I have good project managers. I have cybersecurity professionals." (D01)

Advice from the Field

The Big Picture

Seek out management support & guidance	"Establish and maintain a good working relationship with senior management because their support can make or break your program." (N09)
First develop a strategy, then establish repeatable processes	"Assess your organization's need before you jump into things." (survey) "documenting the steps that you took…so that you would have a program that's repeatable." (N05)
Security awareness should not be "one-and-done"	"Have some other awareness campaigns that go on throughout the year just to try and keep it at the forefront of everybody's mind." (S01)

Approaches

Use a variety of communication channels and methods to deliver security information	"Interactive programs have proven much more effective than slide show-based programs." (survey) "try to make it fun." (N01)
Information should be relatable and tailored to the audience	"Use examples that the employees are likely to encounter in their daily work and personal experiences." (survey) "If you can't get that message across in a way that is understandable, you've lost." (D01)
Reward positive behaviors	"Focus less on bad behaviors and highlight good behaviors -- help employees learn from model employees, not through negative examples." (survey)

Security Awareness is a Team Effort

Use existing templates & guidance documents	"Really trying to make use of resources that are out there, …federal guidance that's been put out." (D03) "Borrow content from industry colleagues." (survey)
Participate in related fed information sharing groups	"If we…share the results, we can help each other build more efficient programs for our respective agencies." (D02)
Build a multi-disciplinary team or leverage other expertise	"You really got to have a team. There's no way one person can do it without a lot of backup." (D06) "Build relationships with offices within your organization." (survey)

Next Steps

Exploring Government-wide Solutions

Federal-level Training

- Alleviate challenge in finding/creating content
- Allow for customization for each organization

Collaborative Forums

- Real-time & interactive
- Share tips, content, ideas with other federal security awareness professionals

Federal Guidance

- Inform revision of NIST SP 800-50 & NICE Framework
- Impact-focused MOEs
- Lessons learned

Professional Development

- Gaining support
- Empowering the workforce
- Developing engaging materials
- Risk communication

Thank you!

Full report on study results targeted for late Fall

Julie Haney: julie.haney@nist.gov
Jody Jacobs: jody.jacobs@nist.gov
Susanne Furman: susanne.furman@nist.gov
Group Mailbox: usability@nist.gov

NIST Usable Cybersecurity Program:
https://csrc.nist.gov/usable-cybersecurity

Careers in Cybersecurity Awareness and Training

Davina Pruitt-Mentle
Moderator
NICE, Lead for Academic Engagement
National Institute of Standards and Technology

Panelists:

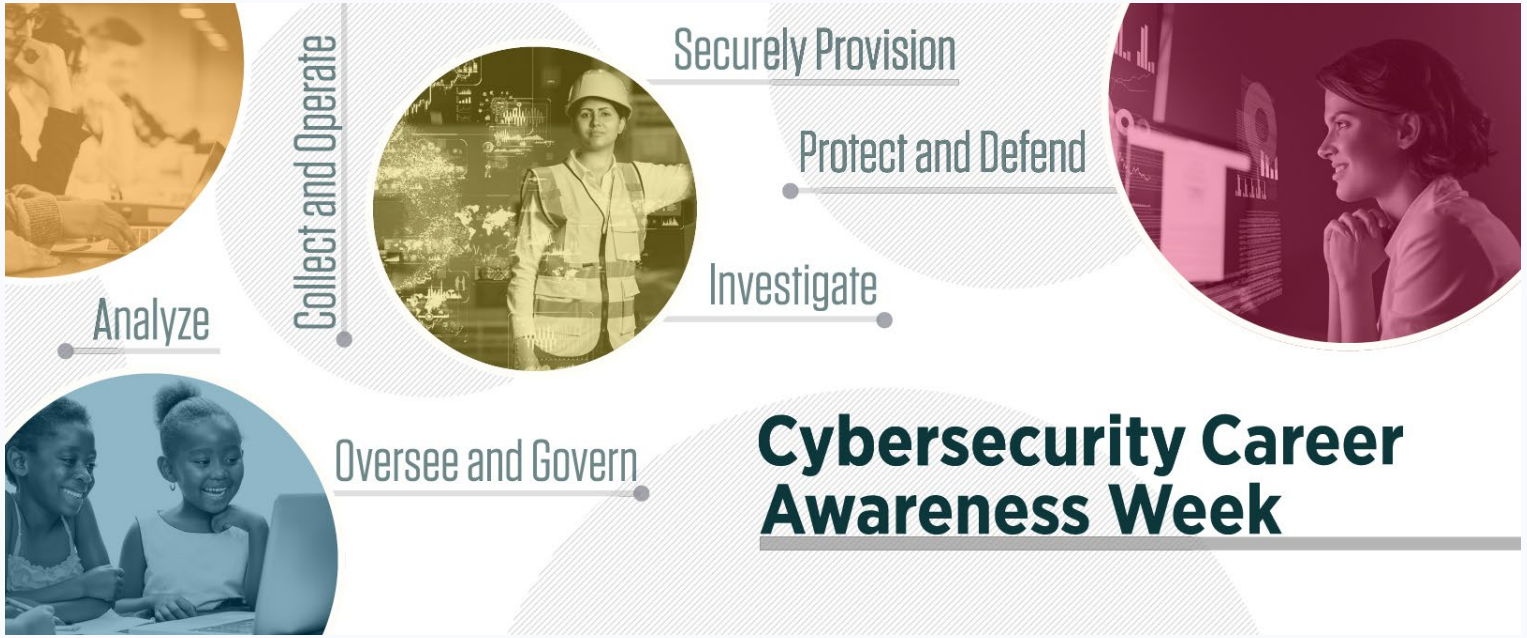
Fred Bisel
Training Lead
GSA, Data Center Optimization Initiative

Kimberly Hemby
Cybersecurity and Privacy Training Lead
Centers for Medicare and Medicaid Services, Health and Human Services

Fiona Gettinger
Cybersecurity Awareness Team Lead
Contractor, GDIT
Department of State
Diplomatic Security Service

Maureen Premo
Cybersecurity Awareness and Training Lead
Immigration and Customs Enforcement
Department of Homeland Security

SAVE THE DATE



SAVE THE DATE

October 18-23, 2021

nist.gov/nice/ccaw

Careers in Cybersecurity Awareness and Training

Davina Pruitt-Mentle
Moderator
NICE, Lead for Academic Engagement
National Institute of Standards and Technology

Panelists:

Fred Bisel
Training Lead
GSA, Data Center Optimization Initiative

Kimberly Hemby
Cybersecurity and Privacy Training Lead
Centers for Medicare and Medicaid Services, Health and Human Services

Fiona Gettinger
Cybersecurity Awareness Team Lead
Contractor, GDIT
Department of State
Diplomatic Security Service

Maureen Premo
Cybersecurity Awareness and Training Lead
Immigration and Customs Enforcement
Department of Homeland Security

Federal Information Security Educators (FISSEA) Fall Forum

BREAK

The Forum will resume at 3:00pm EDT

#FISSEA2021 | nist.gov/fissea

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

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

Security Awareness and Training Contest Recognition

Gretchen Morris

FISSEA Committee Contest Member

Technical Training Consultant, BQMI

FISSEA

Security Awareness, Training, and Education

Contest Winners

Gretchen Morris, CISSP
FISSEA Working Group Member
September 2021

Contest

Categories

- Blog
- Innovative Solutions
- Newsletter
- Podcast
- Poster
- Training
- Video
- Website

Judges

- Not affiliated with any of the groups that submitted entries
- From various positions and industries

Blog Entries (4)

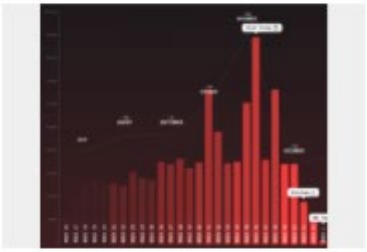
1. COFENSE
2. INDIAN HEALTH SERVICE
3. KNOWBE4
4. LIVING SECURITY

Security Blog Contest Winner!

KNOWBE4

KnowBe4
Human error. Conquered.

PRODUCTS & SERVICES ▾ FREE TOOLS ▾ PRICING ▾ RESOURCES ▾ ABOUT US ▾ CONTACT US ▾



[HEADS UP] Millions of malicious emails will slip past security filters in Q4

Sep 22, 2021 5:00:00 PM By Stu Sjouwerman

Researchers at Tessian have published a report looking at recent trends in spear phishing attacks. The researchers found that 45% of employees said that they clicked on a phishing email ...

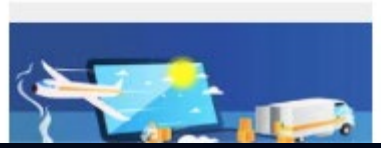
Continue Reading

Executives: Ransomware is the Greatest Threat Concern, But Few are Actually Prepared

Sep 22, 2021 4:04:30 PM By Stu Sjouwerman

A new poll from Deloitte shows organizations are all too aware of the problem of ransomware, but aren't ready to respond to the specific ransomware scenario given that the attackers have ...

Continue Reading



Travel-Related Phishing Scams and Websites Surge More Than 400%

Sep 22, 2021 4:04:22 PM By Stu Sjouwerman

Pent-up demand for traveling – both domestically and internationally – has driven

Search Our Blog

Search

Blog RSS Feed

Innovative Solution Entries (4)

1. CENTERS FOR MEDICARE & MEDICAID SERVICES
2. INDIAN HEALTH SERVICE
3. KNOWBE4
4. U.S. POSTAL SERVICE

Security Innovative Solutions Contest Winner!

INDIAN HEALTH SERVICE

COVID Vaccine Cybersecurity Awareness

Introduction | Scams | Phishing | Telework | Help & Tips

Introduction

The coronavirus vaccine is moving forward and is desperately anticipated by people hoping for a return to normal life. But criminals are waiting, too, ready to use that desperation to their advantage. Cybercriminals are seizing on coronavirus fears by using online scams to extract people's personal and financial information.

During these times of national hardship due to the coronavirus outbreak, bad actors increase their fraudulent activities. As such, the Indian Health Service (IHS) Office of Information Technology urges everyone to be extra vigilant against online scams such as phishing and malware.

These scams can be sent through email, phone, text or social media. They often appear to be from a legitimate organization or individual, including business associates or friends, and are using the COVID-19 pandemic to trick victims into clicking on links or downloading malicious software (malware) designed to spy on them or steal personal information.

Introduction | Scams | Phishing | Telework | Help & Tips

Newsletter Entries (7)

1. CENTERS FOR MEDICARE & MEDICAID SERVICES
2. COFENSE
3. HEALTH & HUMAN SERVICES
4. INDIAN HEALTH SERVICE
5. KNOWBE4
6. DEPT. OF VETERANS AFFAIRS
7. U.S. POSTAL SERVICE

Security Newsletter Contest Winner!

INDIAN HEALTH SERVICE

National Cybersecurity Awareness Month

National Cybersecurity Awareness Month

Office of Information Technology / Division of Information Security

OCTOBER 2020

WEEK 1

Cybersecurity - The Silent Threat

MYTH-BUSTERS

There are many cybersecurity myths that persist that can put our personal and IHS data at risk. This article attempts to dispel some cybersecurity myths you might encounter.

MYTH: IT staff have completely secured my computer and sensitive data. I am fully protected while at work and on my government issued computer.

IHS IT personnel do all they can to protect IHS data, computers, and employees. They have implemented technical security safeguards such as virus scanning, firewalls, automated patching, email/web filtering and much more; however, hackers continue to target individuals through social engineering, which can bypass existing IHS technical security controls. Social engineering is the act of tricking someone into divulging information or taking action, usually through technology. The idea behind social engineering is to take advantage of our natural tendencies to be helpful and our emotional reactions.

REALITY: While technical controls like anti-spam filters, intrusion detection/prevention systems, anti-virus software, and firewalls are good at keeping out some threats, they aren't designed to stop social engineering attacks. Here are some real world social engineering scams:

During tax season, phishing scams often impersonate tax software companies and government agencies.

Phishing emails frequently reference sporting events like the World Cup or the Olympics.

Spear phishers imitate loan providers or administrators to target university students and their parents.

Year after year, phishing scams exploit Black Friday and the holiday shopping season.

Podcast Entries (5)

1. Centers for Medicare & Medicaid Services
2. Cofense
3. KnowBe4
4. Dept. Veterans Affairs
5. National Security Corporation

Security Podcast Contest Winner(s)!

CENTERS FOR MEDICARE & MEDICAID SERVICES	NATIONAL SECURITY CORPORATION
Who says learning about audits has to be boring? In this innovative podcast, we personify the audit and let him tell us first-hand what he's about and why he's so important. The goal is to demystify the audit process and let listeners know that audits improve our cybersecurity – they don't just make more work.	CISO Tradecraft is a new production that offers a broad range of educational topics to empower the next generation of security leadership to achieve (or sustain) their career goal of serving as a Chief Information Security Officer. Never a "current events" format, each weekly episode offers a wealth of actionable information for government and civilian security professionals alike, covering technical knowledge, leadership mastery, and best practices.

Poster Entries (8)

1. CENTERS FOR MEDICARE & MEDICAID SERVICES
2. COFENSE
3. DEPT. OF STATE
4. DEPT. OF VETERANS AFFAIRS
5. HEALTH & HUMAN SERVICES
6. INDIAN HEALTH SERVICE
7. LIBRARY OF CONGRESS
8. U.S. POSTAL SERVICE

Security Poster Contest Winner!

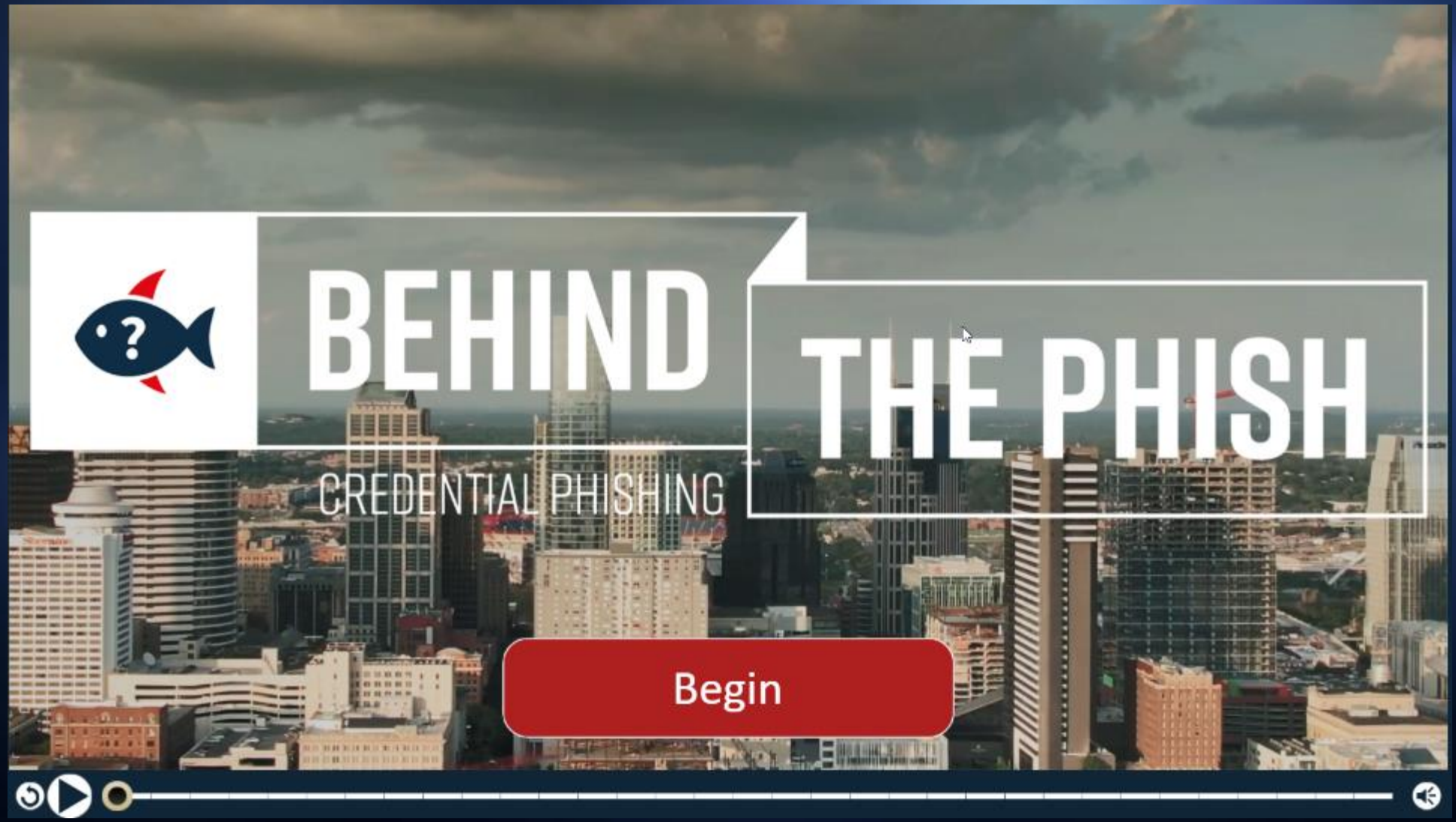
LIBRARY OF CONGRESS

Training Entries (5)

1. COFENSE
2. LAETARE CYBERSECURITY
3. HEALTH & HUMAN SERVICE
4. LIVING SECURITY
5. UNIVERSITY OF NEBRASKA

Security Training Contest Winner!

COFENSE

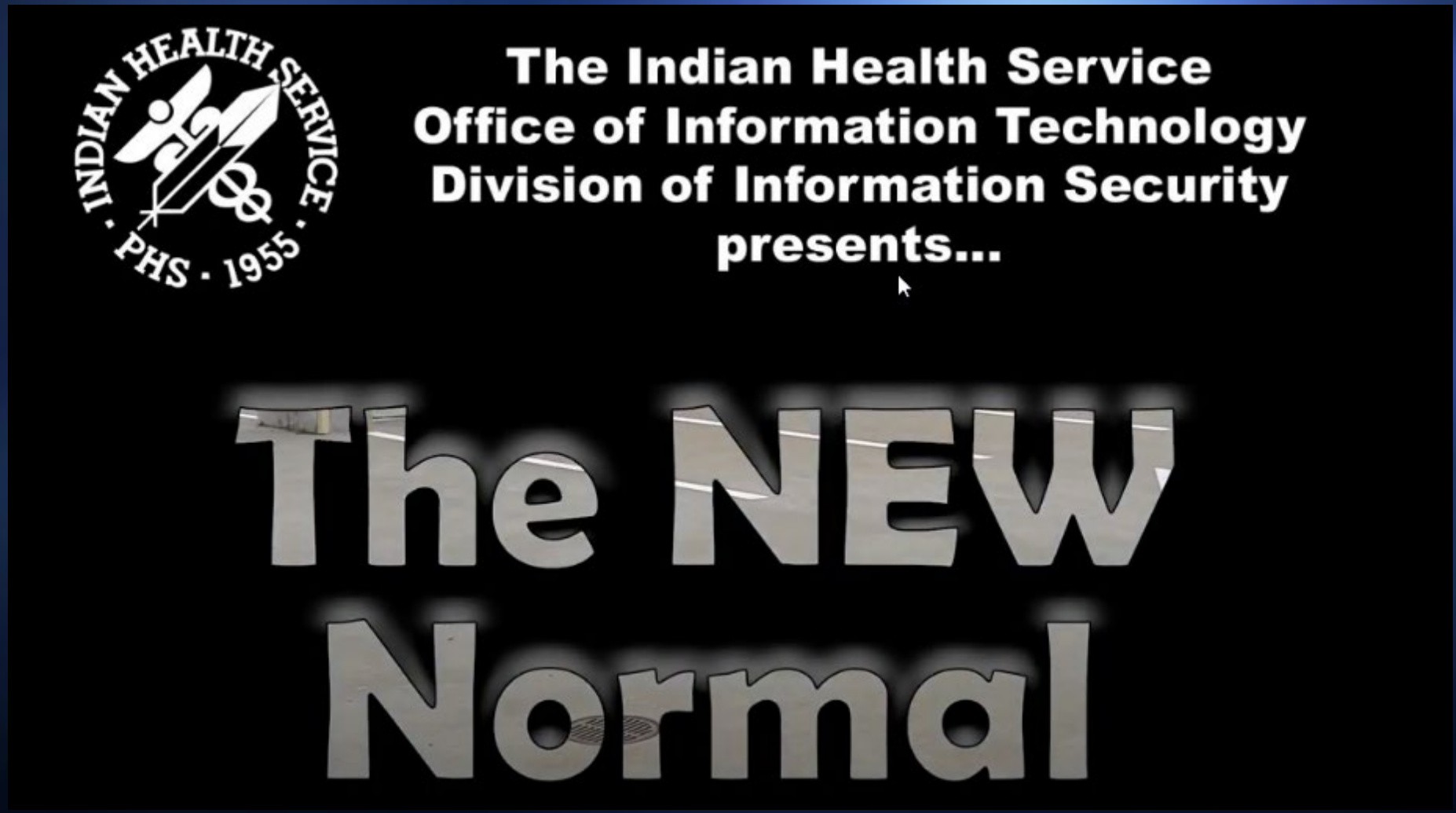


Video Entries (8)

1. CENTERS FOR MEDICARE & MEDICAID SERVICES
2. COFENSE
3. CYBER BENAB LIMITED
4. DEPT. OF HOMELAND SECURITY
5. HEALTH & HUMAN SERVICES
6. INDIAN HEALTH SERVICE
7. LIVING SECURITY
8. U.S. OFFICE OF PERSONNEL MGMT

Security Video Contest Winner!

INDIAN HEALTH SERVICE



Website Entries (6)

1. Centers for Medicare & Medicaid Services
2. COFENSE
3. Dept. of Homeland Security
4. Indian Health Service
5. Dept. of Veterans Affairs
6. U.S. Postal Service

Security Website Contest Winner!

INDIAN HEALTH SERVICE

U.S. Department of Health and Human Services

Indian Health Service
The Federal Health Program for American Indians and Alaska Natives

Search IHS

A to Z Index | Employee Resources | Feedback

The Indian Health Service continues to work closely with our tribal partners to coordinate a comprehensive public health response to COVID-19. Read the latest info.

About IHS | Locations | for Patients | for Providers | Community Health | Careers@IHS | Newsroom

Office of Information Technology (OIT) / IT Security / National Cybersecurity Awareness Month 2020 / Internet of Medical Things

Office of Information Technology (OIT)

- About Us
- Committees
- Enterprise Architecture
- IT Capital Planning & Budget
- Health Information Technology
- IT Operations
- IT Service Catalog
- **IT Security**
  - COVID Vaccine Cybersecurity Awareness
  - Incident Response
  - Information Systems Security Awareness
  - Information Technology Access Control

Internet of Medical Things

Today's internet-connected medical devices, known as the Internet of Medical Things, or IoMT, is a collection of medical devices and applications that can connect to and use healthcare information technology systems and networks.

The IoMT represents a great improvement in the ability to provide healthcare. A Deloitte report states that currently available are more than 500,000 medical technologies that are able to generate, collect, analyze or transmit health data or images and connect to healthcare provider networks, transmitting data to either a cloud repository or internal servers.

The IoMT allows doctors to monitor patients in real time, giving doctors more and more accurate information on which to make diagnoses. Real-time monitoring significantly decreases the need for patients to make in-person doctor visits and allows doctors to find issues in the early stages, possibly before noticeable symptoms appear, promoting proactive rather than reactive treatment. The earlier a health issue is caught, the better the patient's prognosis is, and the less expensive it is to treat.

IoMT also provides doctors with a much more effective and efficient method of managing drugs and medical equipment, saving costs. It allows patients to use devices in their own homes, and have consultations over the internet saving them and their doctors time and money. IoMT devices are poised to save the healthcare industry $300 billion annually, according to Goldman Sachs.

Thanks to all
who submitted entries!

Thanks to our judges!

Contest Winner Panel Discussion

Clarence Williams

Moderator
Senior Advisor, Cyber Workforce Management
Department of Veterans Affairs

Contest Winner Panel Discussion

Winning Categories

Awareness Video, Awareness Newsletter, Awareness Website, Innovative Solutions

Mike Ginn

Policy and Security Awareness Team Lead
Indian Health Services
Office of Information Technology
Division of Information Security

Ed Conley

IT Specialist
Indian Health Services
Office of Information Technology
Division of Information Security

Division of Information Security

FISSEA Fall Forum

Indian Health Service, Office of Information Technology, Division of Information Security

Mike Ginn & Ed Conley

9/28/2021

Cybersecurity Awareness Month

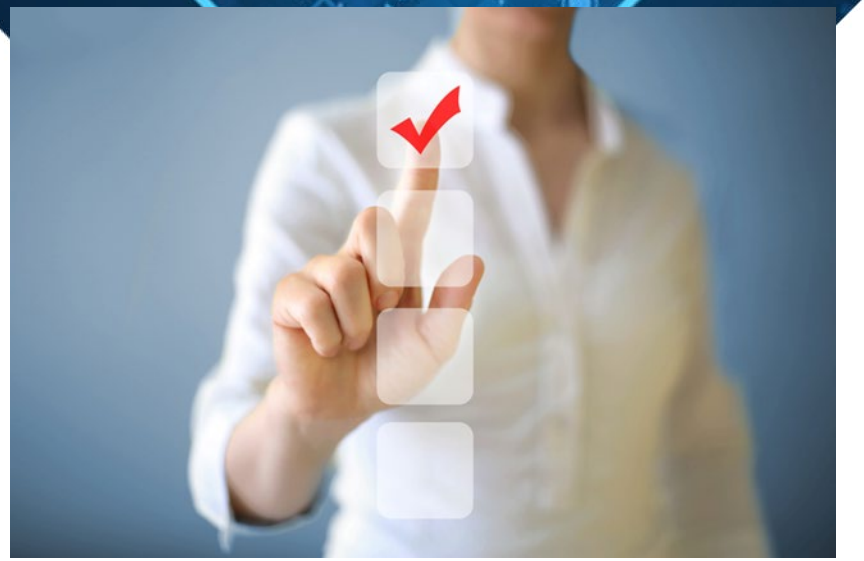
- All of our entries (except one) was created in support of Cybersecurity Awareness Month (October 2020).
- The IHS CIO sends out weekly awareness messages to the entire organization.
- Both the IHS CISO and IHS CIO support our work and give flexibility on content and the medium used.

Policy and Security Awareness Team

- Last year we had a Team of five (two Federal Employees and three Contractors).
- Each employee takes the lead for their awareness product.
- We are fortunate to have:
  - Technical writing expertise
  - Video/Graphics knowledge
  - 508 compliance knowledge
  - In-house web designer to avoid development queue.
  - Team members who recognize the importance of the IHS Mission
  - CISO support

Key Points

- Focus on the content or script before starting with graphics, video, audio, etc.
- Make sure all resources needed are available.
- Peer Review.
- Cite a source if you use it.
- Create templates for reuse.



Toolbox

- Powtoon
- Getty Images
- Adobe ColdFusion
- Adobe InDesign
- Adobe Premiere Pro
- Microsoft Publisher

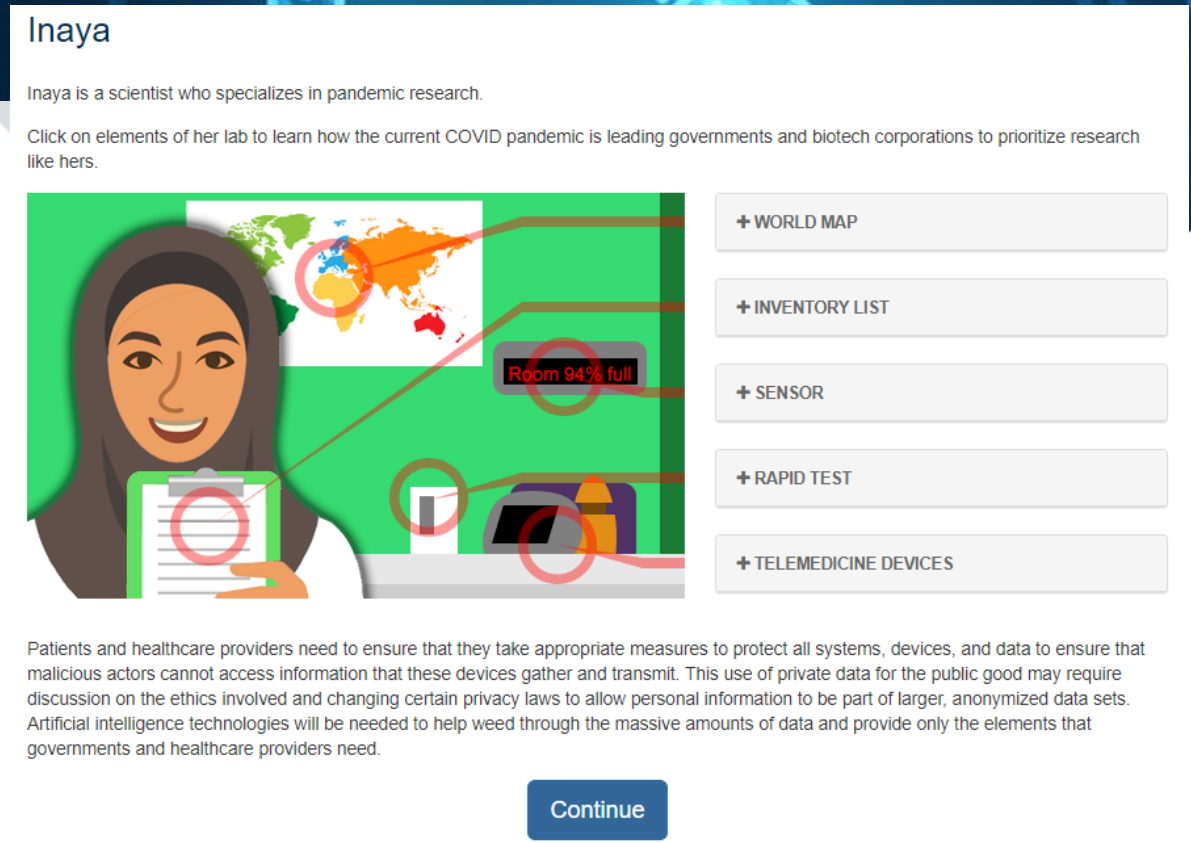
Security Website

Division of Information Security

The Internet of Medical Things

Adobe ColdFusion/ MURA CMS

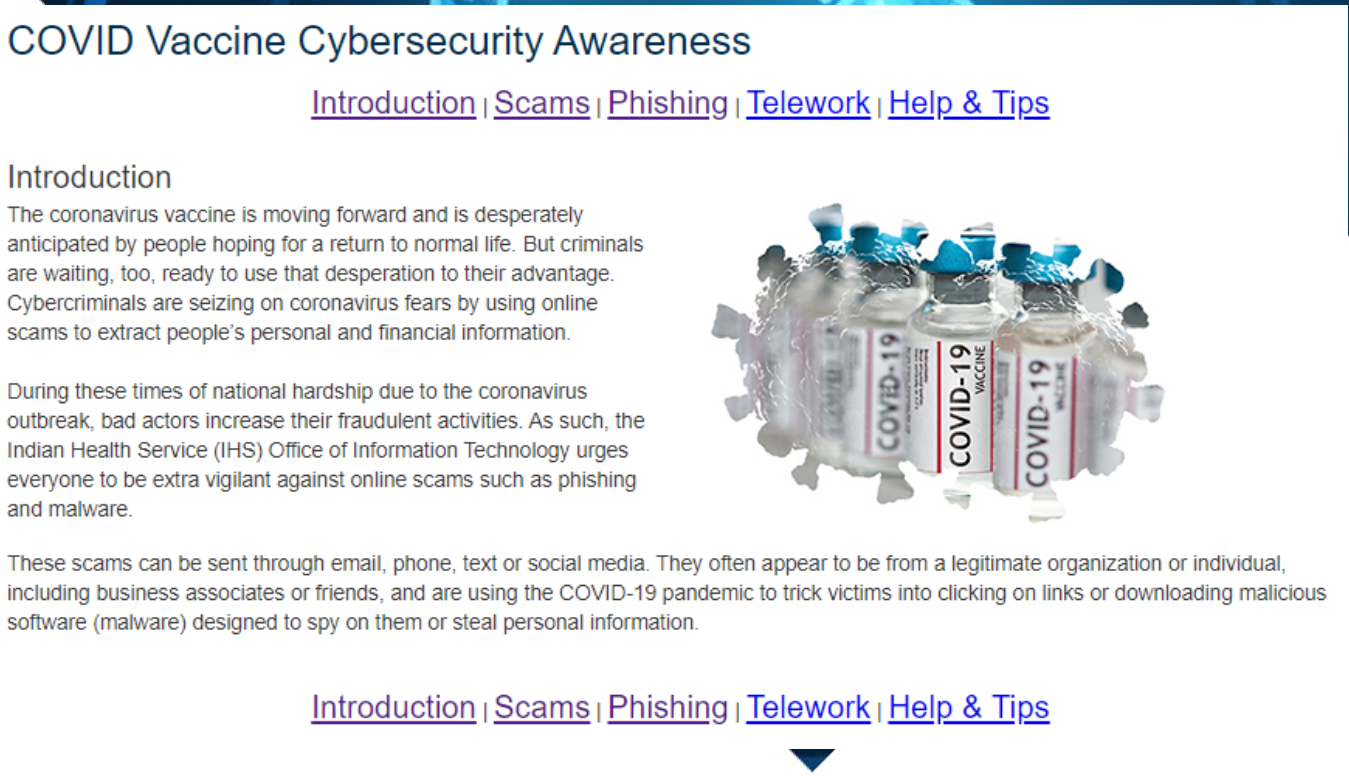
Interactive site allows users to explore the opportunities and dangers of Internet-connected medical devices.



COVID Vaccine Cybersecurity Awareness Site

Adobe ColdFusion/ MURA CMS

As the introduction of vaccines became imminent earlier in the year, IHS needed a quick way to get word out about potential phishing and other scams that might try to take advantage of a weary, desperate population.



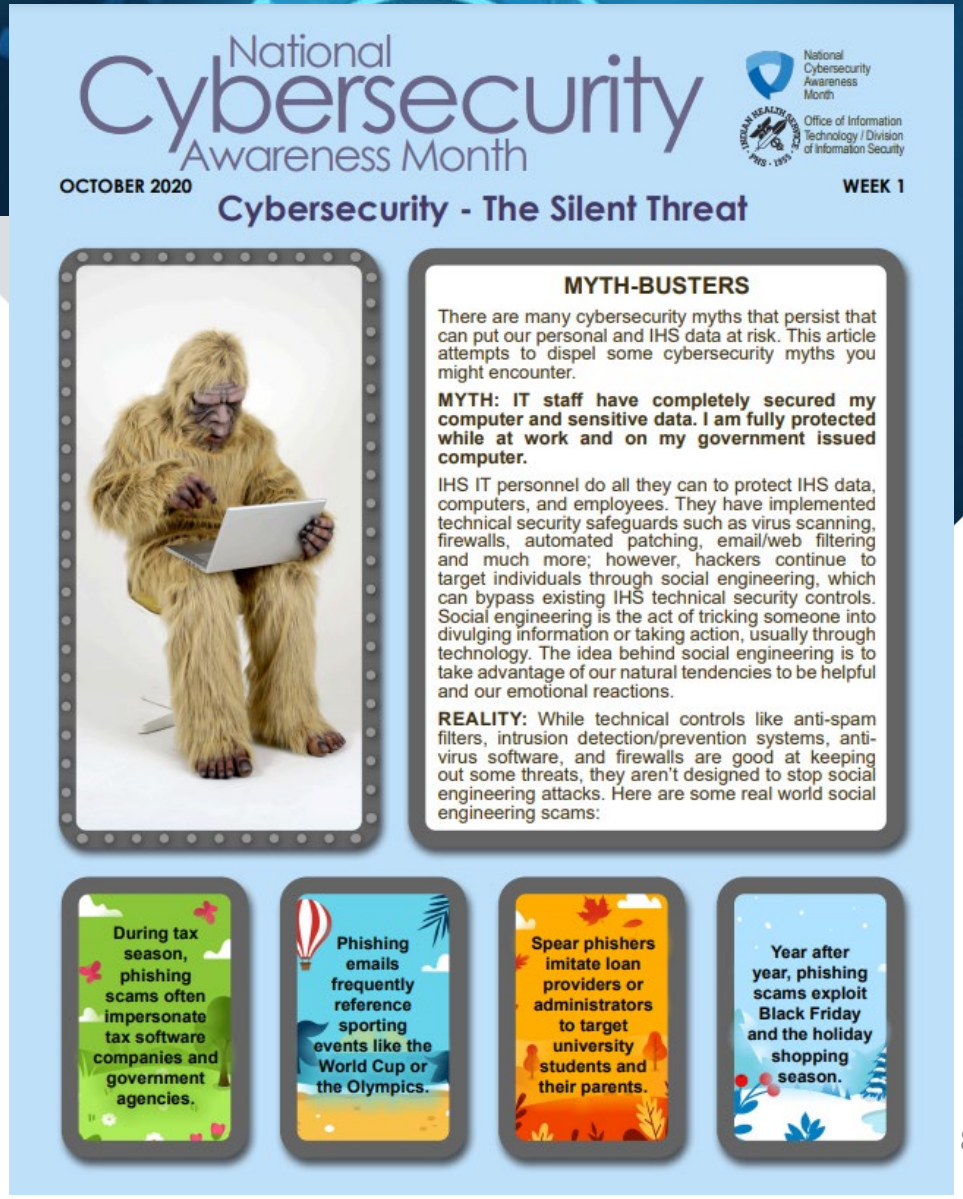
Security Newsletter

Division of Information Security

Cybersecurity: The Silent Threat

Adobe InDesign

A newsletter designed to dispel various myths surrounding such cybersecurity topics as phishing and passwords.



Security Video

Division of Information Security

“The New Normal”

Adobe Premiere Pro

Humorous video about the pitfalls of shadow listening devices in your new at-home telework environment.

Question/Answer

Division of Information Security

Mike Ginn Mike.Ginn@ihs.gov

Ed Conley Edward.Conley@ihs.gov

Cybersecurity@ihs.gov

Contest Winner Panel Discussion

Winning Category

Cybersecurity Podcast

Lee Martin

Director of Product Management – Content

Cofense

Behind the Phish

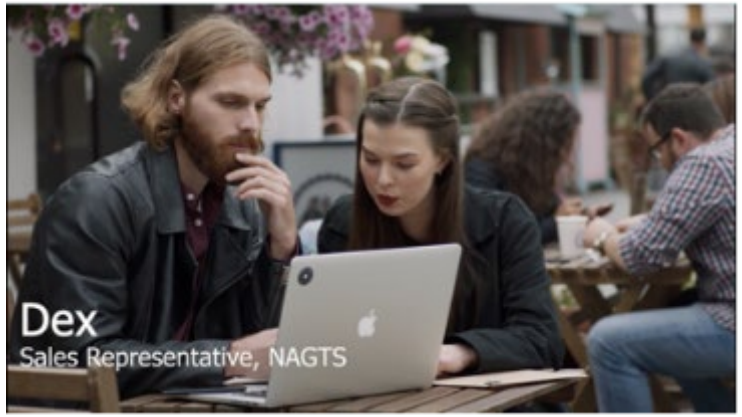
Original Docuseries

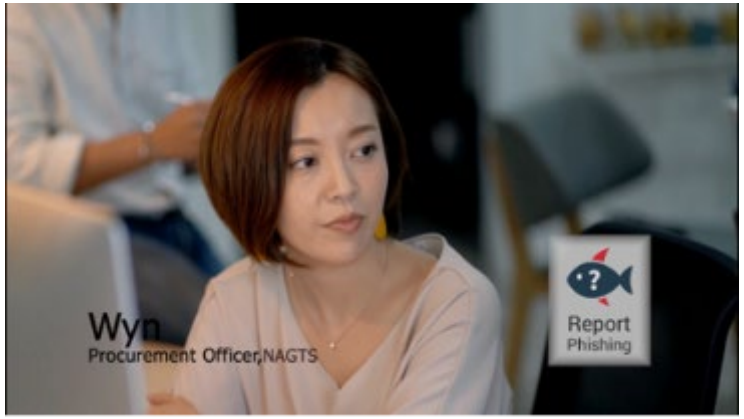
Behind The Phish

A Cofense Original Docuseries

Educates viewers on the dangers of credential phishing via:

- 3 CBTs/Videos
- 3 Phishing Simulation emails
- 2 quizzes





Key Features

- High fidelity to threat landscape (valuable data – converted into training)
- Lessons delivered in story form with narrator as learner proxy
- High production value
- Engaging to promote long-term memory and competency

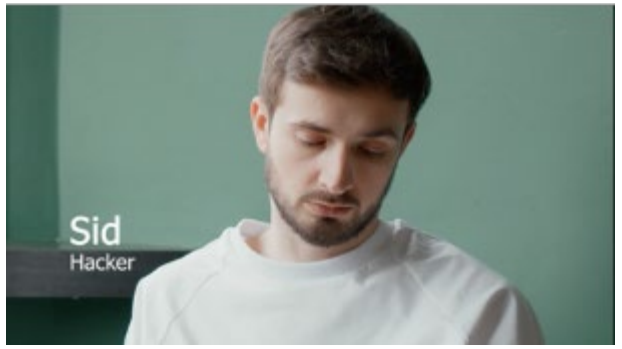
Behind the Phish

Small Team Built

1. Instructional Designer
2. Writer
3. Animator/Editor

Tools

1. Adobe Creative Cloud
2. Voice Talent
3. Online media sources



Inspiration

Originated from the intersection of the need to capture learner's attention and the popularity of docu-series on streaming platforms like Netflix.

Behind the Phish

Novel Delivery on Multiple Platforms

SCORM

LMS

PhishMe

Protect/Protect MSP

Contest Winner Panel Discussion

Winning Category

Cybersecurity Blog

Stu Sjouwerman

Founder and CEO

KnowBe4, Inc.

About Us

- Provider of the world's largest integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- Winner of numerous industry awards


855-KnowBe4
Blog
Support
Partners
Request A Demo
Account Login
KnowBe4
Human error. Conquered.
PRODUCTS & SERVICES
FREE TOOLS
PRICING
RESOURCES
ABOUT US
CONTACT US
Security Awareness Training Blog
Keeping You Informed. Keeping You Aware.
Stay on top of the latest in security including social engineering, ransomware and phishing attacks.
All Articles
Security Awareness Training
Phishing
Cybercrime
Social Engineering
Ransomware
KnowBe4
Social Media Quizzes May Be Data Scrapers Building Victim Profiles
Sep 21, 2021 3:58:01 PM
By Stu Sjouwerman
The seemingly benign quizzes asking personal details take advantage of individuals' willingness to share and could be used to establish passwords, password hints, and more.
Continue Reading
Kaspersky: Use of New QakBot Banking Trojan that Steals Emails Up 65%
Search Our Blog
Search
Blog RSS Feed
KnowBe4
Get Ready for

Thank You to FISSEA for Recognizing the KnowBe4 Blog as Best Cybersecurity Blog!

Contest Winner Panel Discussion

Winning Category
Cybersecurity Podcast

Kimberly Hemby

Cybersecurity and Privacy Training Lead
Centers of Medicare & Medicaid Services
Health and Human Services

Contest Winner Panel Discussion

Winning Category
Cybersecurity Podcast

G. Mark Hardy

President

National Security Corporation

CISO Tradecraft: A Podcast to Improve Cyber Security Leadership

G Mark Hardy
& Ross Young

Mission: Provide actionable intelligence to cybersecurity leaders by bridging the gap between pure technical podcasts and generic business podcasts

Tools used to Create CISO Tradecraft Podcast

- Fiverr - Custom Logos & Artwork
- Garage Band – Used to edit the podcast
- Google Docs – Create written scripts
- Microphone - Audio Technica 2008 USB
- Podbean - Podcast distribution
- PowerPoint – Used Smart Art capabilities to create Infographics
- Zencastr – Used to capture High Quality audio recordings

Podbean tool allows wide distribution of CISO Tradecraft podcast to match listener preferences

- Amazon Music
- Apple Podcasts
- Deezer
- Google Podcasts
- iHeartRadio
- Pandora
- Podbean
- Podcast Addict
- Spotify
- Stitcher
- TuneIn + Alexa
- YouTube

A Cyber Security Podcast for Executives that helps them understand:

Technical Topics

- Ransomware
- Zero Trust
- DevOps
- Identity and Access Management
- Introduction to the Cloud
- Securing the Cloud
- AI/ML
- Blockchain
- Cryptography
- Australian Signals Directorate The Essential 8
- NSA's Top 10 Cybersecurity Mitigation Strategies
- Global War on Email
- Modern Software Development

Executive Leadership Skills

- Principles of Persuasion
- How to Read Your Boss
- Change Management
- Crucial Conversations
- Executive Competencies
- Executive Presence
- Team Building
- First 90 Days as a CISO

Cyber Best Practices/Processes

- Asset Management
- Cyber Frameworks
- How to Compare Software
- IT Governance
- Setting up an AppSec Program
- Metrics that Matter
- Incident Response Playbooks
- EO on Improving the Nation's Security

Security Awareness and Training People's Choice Results

Gretchen Morris

FISSEA Committee Contest Member

Technical Training Consultant, BQMI

PEERS CHOICE AWARDS

CATEGORY (Votes)	WINNER (Top Percentage of Votes)
BLOG (92)	COFENSE (67.4)
INNOVATIVE SOLUTIONS (64)	Centers for Medicare & Medicaid Services (35.9%)
NEWSLETTER (108)	COFENSE (57.4%)
PODCAST (100)	COFENSE (61%)
POSTER (107)	COFENSE (57%)
TRAINING (89)	COFENSE (70.8%)
VIDEO (122)	COFENSE (48.4%)
WEBSITE (108)	COFENSE (54.6%)

Closing Remarks from FISSEA Chair

Susan Hansche

FISSEA Chair
Cybersecurity & Infrastructure Security Agency
Department of Homeland Security

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 Winter Forum

February 15, 2022

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