Federal Information Security Educators (FISSEA)

Fall Forum

November 14, 2023
1:00pm – 4:00pm ET

#FISSEA | nist.gov/fissea
Please Note...

This webinar and the engagement tools will be recorded.

An archive will be available on the event website.
Welcome and Opening Remarks

Marian Merritt
Deputy Director of NICE/FISSEA Lead
National Institute of Standards and Technology

Brooke Crisp
IT Cybersecurity Specialist/FISSEA Co-Chair
Social Security Administration

#FISSEA
Get Involved

Subscribe to the FISSEA Mailing List
FISSEAU Updates@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@list.nist.gov

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

#FISSEA
Opening Keynote

National Cyber Workforce and Education Strategy Overview

Seeyew Mo
Assistant Director
Office of the National Cyber Director

#FISSEA
From Compliance to Impact: Tracing the Transformation of an Organizational Security Awareness Program

Julie Haney
Computer Scientist
National Institute of Standards and Technology
From Compliance to Impact: Tracing the Transformation of an Organizational Security Awareness Program

Julie Haney\textsuperscript{1} and Wayne Lutters\textsuperscript{2}

\textsuperscript{1}National Institute of Standards and Technology, \textsuperscript{2}University of Maryland, College Park

November 2023
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.

All photos are Creative Commons licensed under CC BY-NC, CC BY-SA-NC, or CC BY-ND.
SECURITY AWARENESS
Program Failures
Measuring Effectiveness

versus
Research Goals

• Gain insight into how a security awareness team goes about developing, executing, and transforming their security awareness program
• Provide lessons learned useful to other programs
Case Study of “Agency Q”
Security Awareness Program

- Medium-sized government agency
- Security awareness team: government lead + 2 contractors
- Team responsible for:
  - Implementing and tracking mandatory, annual awareness training
  - Planning and executing initiatives to increase employee awareness
  - Managing role-based training
What We Did

- Interviewed:
  - Security awareness team
  - CISO and front-line supervisor
  - Employees

- Observed in-person events over the course of a year

- Analyzed historical reports, awareness materials, and results of post-event feedback surveys
Security Awareness Initiatives

- Drop-in lunchtime events
- Security days
- Security officer forums
- Campaigns
- Phishing simulation exercises
Challenges

- Lack of buy-in from some employees and leaders
- Compliance mentality
- Lack of resources
Challenges

People do it because they have to. You have the online training where it’s like “click, click, click, done”... rather than paying attention to the words they’re seeing on the screen ... Just because you’re compliant doesn’t mean that it’s an effective program.

program lead

- Lack of buy-in from some employees and leaders
- Compliance mentality
- Lack of resources
Engaging and Empowering the Workforce
Making Security Relatable

- Include topical information
  - Season of year
  - Recent security needs and threats
  - Workforce-suggested topics

- Address multiple contexts
  - Work-home connection
  - Physical and personnel security
Making Security Relatable

- Include topical information
  - Season of year
  - Recent security needs and threats
  - Workforce-suggested topics

- Address multiple contexts
  - Work-home connection
  - Physical and personnel security

"We want to secure the person, and we want everyone to think about all aspects in which they could secure themselves."

Chief Information Security Officer
Employing Engaging Communication Techniques

- Using a variety of communication methods throughout the year
- Implementing creative, memorable, and entertaining initiatives
- Trying new things even though not everything works
Providing Practical Recommendations

- Provide actionable steps to take
- Achievable given employee skills
- Described in understandable terms
- Accompanied by points of contact and resources for more information
Providing Practical Recommendations

“It’s beneficial] having the information presented in a manner where it’s not intimidating, ... in a way you can embrace it and take away information ... The more we know about it and the more we know people that we can reach out to that can help us if we have a question about it, I think that can make you feel more empowered and more comfortable in doing it the right way and protecting yourself as well.

employee
Event Attendance

I think we’re starting to make a difference. I can see that by the numbers of people who come to our events and look forward to it.

— program lead

- Increase in number of event attendees
- **Who** attends - how to reach groups that don’t typically attend
Employee Feedback

- Post-event surveys
  - Rating scales
  - Written feedback and suggestions
- Focus groups
- Personal feedback
Employee Feedback

- Post-event surveys
  - Rating scales
  - Written feedback and suggestions
- Focus groups
- Personal feedback

"You can get messages from the agency, and I go like, ‘Is this real?’ And I send it to the cybersecurity team to say, ‘Am I supposed to be answering this?’ So, basically, as a result of my training here, I am very, very suspicious of everything."

employee
Evidence of Leadership Support

“If we can get the leadership to look forward to what we’re doing and show some interest rather than just being another line on a report, I think that’s very good. I think we’re making some progress … Now I’ve got the CIO and the deputy CIO and the CISO and the deputy CISO sitting in the crowd and watching the whole [event] rather than just showing up to give their opening remarks and then leaving.”

program lead
User-Generated Incidents & Reporting

- Trends in employee-involved security incidents and reporting
- Contextualizing the trends
- Holistic approach to measuring effectiveness
User-Generated Incidents & Reporting

"We’re trying to...be able to tie in together the people who take their training to the people who get caught with phishing exercises, the people who are really getting caught with phishing exercises with people who are losing their badges to people who send out information they shouldn’t to see what’s the correlation here. Are these people just too busy? Are they not paying attention? Is there a training problem?"

program lead

- Trends in employee-involved security incidents and reporting
- Contextualizing the trends
- Holistic approach to measuring effectiveness
Takeaways
The Big Picture

- Emphasize impact, not compliance!
- Obtain leadership buy-in
- Security awareness should not be “one and done”
- Leverage diverse expertise
Approaches

- Use a variety of engaging communication channels and methods
- Information should be relatable, actionable, and tailored
- Reward positive behaviors
Measuring Effectiveness

- Measure program effectiveness by synthesizing data from multiple sources
  - Quantitative
  - Qualitative
- Provide evidence to leadership
THANK YOU!

human-cybersec@nist.gov

Q&A

Are There Any Questions?
Federal Information Security Educators (FISSEA) Fall Forum

BREAK

The Forum will resume at 2:30pm ET

#FISSEA | nist.gov/fissea
Welcome Back!

Marian Merritt
Deputy Director of NICE/FISSEA Lead
National Institute of Standards and Technology
Fireside Chat

Kristy Daphnis
Federal Workforce Branch Chief
Office of Management and Budget

Susan Hansche
CISA/CSD Training and Development
Department of Homeland Security

#FISSEA
Cybersecurity Awareness Month and More

Lisa Plaggemier
Executive Director
National Cybersecurity Alliance
Cybersecurity Awareness Month and More
Programs

Cybersecurity Awareness Month Overview

- 20th Cybersecurity Awareness Month
- Focus on four behaviors: phishing, MFA, software updates and passwords
- Launch of Secure Our World campaign
- "Oh Behave" Report on Cybersecurity Attitudes and Behaviors
- Kubikle Web Series
Results

- **4,080** Champions from 93 countries and all 50 states. Total est. reach approximately **102,277,394** individuals

- **765** people tuned into the Oct 4 campaign kick-off event

- **43,274** individuals posted about the campaign in **136,646** posts across social media platforms

Resulted in 651,263 total engagements and **1.8b** potential impressions
Results

US Media Reach 7.2B

Morningstar
Yahoo Finance
Marketwatch
60 Minutes
Fox
CBS
NBC
ABC
NPR
MSN
CNN
Time
New York Times
Economist
Wall Street Journal
Fortune
USAToday
Los Angeles Times
Washington Post
Cybersecurity Awareness Month

Speaking Engagements

- 9,500 individuals attended an NCA session or game show
- 135 companies reached

Logos of various companies and organizations, including CVS, State Farm, Costco Wholesale, Nasdaq, VISA, and Cisco, are displayed.
Programs

Oh Behave 2023

- Launched Oct 3, 2023
- 1,534 downloads to date
  - 42% increase compared to same period in 2022
- Coverage:
  - Fortune (UVM: 19M)
  - Beta News (UVM: 1M)
  - Dark Reading (UVM: 405K)
  - CyberWire (UVM: 32K)
Secure Our World

Simple ways to protect yourself, your family and your business from online threats.

Staying Safe Online is Easier Than You Think!

We're increasingly connected through digital tools and more of our sensitive information is online. This convenience...
Kubikle

Cybercrime is a scourge that rules lives. But who makes it? Other people, bad ones, with lives of their own. These are their stories. At least their stories in the online world. Welcome to Kubikle.
Online Holiday Shopping Campaign

- Social media campaign
- Toolkit – tips sheets, graphics, holiday cards
- Webinar with Trend Micro
- Media pitching
  - interview with BBC on Nov 24
Convene: Clearwater Beach Florida 2024
Sheraton Sand Key
January 17-18
Oh, Behave!
The Annual Cybersecurity Attitudes and Behaviors Report 2023
Security Behaviors

- ✔️ Password habits: password creation, password management, etc.
- 🚀 Using Multi-Factor Authentication (MFA)
- ⚠️ Installing the latest updates
- 🔍 Checking for signs of phishing
- 📁 Backing up data
Gen Z twice as likely to think cybersecurity isn't worth the effort
Prioritizing Cybersecurity

Question:
How do you feel about cybersecurity?

Statement:
“I feel that staying secure online is a priority”

[Diagram showing survey results]

- Strongly disagree: 1%
- Disagree: 3%
- Neither agree or disagree: 12%
- Agree: 30%
- Strongly agree: 54%
Security Behaviors

Question:
How do you feel about cybersecurity?

Statement:
“I feel that staying secure online is a priority”
Feelings

Question:
How do you feel about cybersecurity?

Statement:
“Staying secure online is under my control.”
Capability

Motivation

Opportunity

BEHAVIOR
Feelings

Question:
How do you feel about cybersecurity?

Statement:
“Staying secure online is under my control.”
43% of Gen Zs reported having lost data or money due to phishing.

39% of Gen Zs reported family members rely on them for online security.
Everyone’s afraid of the internet (and no one’s sure what to do about it)

Parents of Gen Z are especially worried when it comes to their children’s safety online

As parents of the first generation to grow up online, there’s genuine concern that Gen Z’s online activity could result in data breaches or identity theft. Parents agree: protecting their children’s data is a top priority.

- Protecting my child(ren) from having their personal information/data stolen is very important to me: 92%
- I worry that my child(ren) share online puts their safety at risk: 65%
- I worry that my child(ren)’s online behavior may lead to identity theft someday: 66%
- I worry that my child(ren)’s online behavior puts them at risk for getting their personal information stolen: 63%

Most Gen Zers are confident they know best how to stay safe, though only 1 in 3 parents agree

- Gen Z: 60% I know more about online safety and security than my parents do
- Parents of Gen Z: 36% My child(ren) know more about online safety and security than I do

Three in four parents feel they need better tools and education to keep kids safe online
Security Behavior

- I became better at recognizing and reporting phishing messages (e.g. emails, texts) - 50%
- I started using Multi-Factor (or Two-Factor) authentication (MFA/2FA) - 34%
- I started saving passwords using a password manager (e.g. in Browser, 1Password, Lastpass, iCloud Keychain) - 32%
- I started regularly installing the latest software and app updates - 28%
- I started using a strong and separate password(s) - 37%
- I started backing up my data - 22%
- I didn't change any of my online security behaviors - 6%
- I already do all these things, so I didn't change anything - 15%
ONLY 6% TOOK NO ACTION
Improving Training Effectiveness

- Design awareness and training for everyone
- More than once a year
- Train where the risk is
- Get people's attention
- Don't insult, judge or belittle
“The internet needs more helpers—people who will listen to others in need, answer simple tech questions without judgment...teaching every user along the way.”

- Oren Arar, VP of Consumer Privacy, Malwarebytes
perseverance

noun [U] • approving

us /ˈpɜːsrəvəns/  uk /ˈpɜːsərvəns/

Continued effort to do or achieve something, even when this is difficult or takes a long time
Stay safe online.

Website
StaySafeOnline.org

Twitter
@staysafeonline

Facebook
/staysafeonline

LinkedIn
/national-cyber-security-alliance

Email
info@staysafeonline.org
Q&A

Are There Any Questions?
An Ounce of Prevention Is Worth a Pound of Cure: How to Assess the Impact of Your Awareness Campaigns

Nadine Michaelides
Founder
Anima People
AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE- HOW TO ASSESS THE IMPACT OF YOUR AWARENESS CAMPAIGNS

Nadine Michaelides
Cyber Psychologist
Founder of Anima People
“An awareness campaign is crucial in that it is the vehicle for disseminating information that all users need”

(Bada, Sasse & Nurse, 2019)
Effective user security awareness campaigns can greatly enhance the information assurance posture of an organization.

User awareness represents a significant challenge in the security domain, with the human factor ultimately being the element that is exploited in a variety of attack scenarios.

Psychological theories of education, learning, environmental and healthcare behavioural change can be used to make information security awareness methods more effective (Khan et al. 2011).
HOW SUCCESSFUL ARE CAMPAIGNS?

Steen, Norris, Atha & Joinson (2020)

- Analysed 17 government-sponsored cybersecurity campaign materials

- Results were that security campaigns are often focused on education and increasing awareness, under the assumption that as long as citizens are aware of the risk, and are provided with information on how to improve their security behaviour, behaviour will change.
There is no evidence that merely increasing awareness leads to behavioural change.
ONE SIZE FITS ALL?!

• Upgrade the awareness campaigns so they focus on specific behaviours and threats

• Wherever possible try to avoid targeting the general public and target specific groups of users e.g. cyberbullying

• Avoid a ‘one size fits all’ approach

• Provide ‘coping skills’ in how to manage in certain situations
An awareness campaign is crucial in that it is the vehicle for disseminating information that all users need (Bada, Sasse & Nurse, 2019).

Match an individual’s self-guide or self-monitoring style.
PERSUASION...

Use ‘persuasion’ techniques as well as educational

Use techniques such as coercion and modelling, incentivization and enablement

Include cultural factors to encourage intrinsic motivation to security tapping into cognitive, affective or motivational characteristics

Make it personal and collective and relevant to the individual as well as the group.
PERCEPTIONS OF RISK...

Be aware and counter-in the varying perceptions of risk culturally between nations and states, or other groups of people.

There are four distinctive categories that distinguish country cultures; power distance, collectivism vs. individualism, femininity vs. masculinity and uncertainty avoidance.
FEAR...

• Refrain from using messages that are fear-provoking

• Not conducive to behaviour change

• Interventions based on theoretical knowledge such as social learning theory or the theory of self-efficacy, which takes into account cultural beliefs and attitudes, are more likely to succeed...

• especially when we take into account varying cultures.
REGULATORY FOCUS THEORY

Guided by a need for nurturance

And a need to align with the ideal self

Messages should be ‘promotion and prevention’ focused

And NOT instill fear…
Campaigns should use simple consistent rules of behaviour that people can follow, facilitating perceived control and better acceptance of the suggested behaviour.

"SIMPLICITY..."
Avoid monotonous advice from ‘security experts’ such as ‘change passwords’ which doesn’t take into account the responsibility and workload issues that may be present, acting as barriers to good cyber hygiene.
Include contact details which enable users to call a helpline or get help where possible.
<table>
<thead>
<tr>
<th>S/No.</th>
<th>Tool and technique</th>
<th>Component of knowledge</th>
<th>Component of attitude change</th>
<th>Component of subjective norms</th>
<th>Component of Intention</th>
<th>Change in behavior</th>
<th>Overall effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Education presentation</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>Email messaging</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Group discussion</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>Newsletters</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>Video games</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>CBT</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>Posters</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>2</td>
</tr>
</tbody>
</table>
FEEDBACK
WHAT DO WE NEED TO KNOW?

1. Whether the information has been received and by what means e.g. newsletter, social media, and this is where social media engagement metrics can be very useful, and...

1. Whether that information changes the perceptions, opinions and attitudes of those individuals, and

1. Whether those psychological processes translate to behaviour change, both for individuals and for communities.

“Understanding how people perceive risks is critical to creating effective awareness campaigns.”
EXAMPLES OF USEFUL METRICS...

85% Employees hate their job

52% Employees feel they get a positive experience

48% Say the biggest roadblock is ‘not enough time’

??% Time needed to adopt good hygiene
UNDERSTANDING PEOPLE'S MOTIVATION TOWARDS SECURITY.

Some people may not intentionally be malicious but still offer a threat to security. Despite the best training in the world, people must understand security's importance.

People can be your best asset and your biggest threat to security.
UNDERSTANDING PEOPLE’S MOTIVATION TOWARDS SECURITY.

Staff motivation towards security can change due to reasons that often go unrecognized or not considered important. Examples include:

- A promised pay review missed or ignored.
- A change of manager.
- Personal circumstances changing (divorce, bereavement, unexpected bill).
HOW...?

1. Investigate what’s happening behind the scenes
2. Get feedback direct from users
3. Implement the appropriate strategy
4. Create cyber-engaged communities
HOW TO MEASURE BEHAVIOR CHANGE?

Where possible campaigns could be distributed in small samples, controlling exposure to, and interaction with the materials to measure the direct effects of these campaigns on security behavior

- a combination of direct behavioral measures (e.g. number of people signing up for a training, or the percentage of people reporting a potential phishing email),
- intentions (e.g. questions on how an individual would act, if they find themselves in a potentially harmful situation),
- attitudes (e.g. attitudes towards the likelihood and severity of cyber threats such as ransomware) and
- awareness (e.g. reach of the campaign, whether people remember the message of the campaign materials) is needed.
**Figure 1.** Five step ladder model for measuring information security awareness.
Table 2. Information security awareness metrics.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security incident database</td>
<td>Incidents/6 months</td>
</tr>
<tr>
<td>Help desk calls</td>
<td>Calls/month</td>
</tr>
<tr>
<td>Phishing e-mails</td>
<td>E-mail/month</td>
</tr>
<tr>
<td>Number of accesses to intranet pages</td>
<td>Hits/month</td>
</tr>
<tr>
<td>Number of accesses to unauthorized pages</td>
<td>Attempts/month</td>
</tr>
<tr>
<td>Survey questionnaires based on knowledge</td>
<td>Average score of all employees</td>
</tr>
</tbody>
</table>
EXAMPLE QUESTIONS

The following are statements designed to determine attitudes towards negative cyber security behaviors (measured on a scale of perceived seriousness):

1. unacceptable use of email
2. inappropriate use of computer resources
3. unauthorized access to information systems
4. unacceptable use of information system passwords
5. unacceptable use of information systems

The study will also measure employee attitudes towards cyber security expectations from employers using the following statements to be answered according to level of agreement:

My employer’s expectations for cyber security are reasonable.
My employer expects me to spend a reasonable amount of time on cyber security.
My employer’s expectation of my knowledge of cyber security is reasonable.
My employer’s expectation for my level of responsibility for cyber security is reasonable. My employer expects a reasonable level of my attention for cyber security.
Fig. 6. GCS Evaluation Framework (GCS, 2015, p. 4).
Fig. 5. The DPRG/ICV Framework (DPRG & ICV, 2011b, p.13).
**Situation**
Social media accounts of users are at a higher risk of being hacked and it is thought that if we raise awareness of the issue then users will take more steps to secure their accounts.

**Inputs**
- Financial investment
- Staff
- Volunteers
- Materials
- Equipment
- Technology
- Partners

**Activities**
- **What we do**
  - Social media paid advertising
  - Digital events and workshops
  - Social media organic content
  - Blogs
  - Work with media
  - Develop and share tools
  - Share best
- **Reach**
  - General public – 13 to 30 y/o, both men and women
  - Emphasis on the 13-20 y/o public

**Outcomes**

<table>
<thead>
<tr>
<th></th>
<th>Short</th>
<th>Medium</th>
<th>Long term</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LEARNING</strong></td>
<td>ACTION</td>
<td></td>
<td>CONDITIONS</td>
</tr>
<tr>
<td>Knowledge</td>
<td>Behaviour</td>
<td></td>
<td>Social</td>
</tr>
<tr>
<td>Awareness</td>
<td>Practice</td>
<td></td>
<td>Economic</td>
</tr>
<tr>
<td>Attitudes</td>
<td>Decision-making</td>
<td></td>
<td>Civic</td>
</tr>
<tr>
<td>Skills</td>
<td>Policies</td>
<td></td>
<td>Environmental</td>
</tr>
<tr>
<td>Opinions</td>
<td>Social Action</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aspirations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motivations</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Assumptions:**
- 13-30 year olds use social media
- they are able to learn new skills through digital learning
- that they care about cybersecurity
- that they are use the channels included in the comms plan

**External factors**
- access to user data such as number of social media hacking incidents
- participation from Member States
- partnership/involvement of organisations
An effective cybersecurity awareness campaign can awaken fresh new habits that are conducive to protecting people and organizations. However, most campaigns focus solely on providing information rather than encouraging people to get involved or inspiring them to embrace change.

Behavior change stems from people's perceptions and attitudes, so individuals must be motivated to take action. Rather than assume people are interested in cybersecurity and motivated to improve security practices, campaigns should spawn from genuine reality, promoting long-term change.

Enter the Cybersecurity Awareness Campaign Process Model - developed to help organizations produce more effective campaigns by following step-by-step guidelines.
Key attributes of effective cybersecurity awareness campaigns

- **Disseminating knowledge** — Campaigns should help people become aware of cybersecurity by providing information and guidance.

- **Understanding motivation** — Campaigns need to be underpinned by psychological factors that motivate people to act in a more security-conscious way.

- **Engaging people in behaviour** — Campaigns should encourage people to engage in behaviour change.

- **Evaluating behaviour change** — Behaviour change resulting from the campaign should be evaluated for further development of policies and procedures.

- **Planning for the future** — By discovering exactly what motivates people to change their behaviour, future campaigns can be developed based on these factors.

Cybersecurity Awareness Campaign Process Model

- **Impact Evaluation**
  - Awareness

- **Proximal Impact I: Engagement**
  - Priming Steps

- **Proximal Impact II: Priming**

- **Distal Impact: Trialing Behaviour**

- **Outcome Evaluation**

Process for introducing a cybersecurity culture

<table>
<thead>
<tr>
<th>Unaware</th>
<th>Informed</th>
<th>Motivated</th>
<th>Active</th>
<th>Cyber Hygienic</th>
<th>Cyber Ambassadors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poorly trained or no guidance received for proper cybersecurity behaviours. This leads to a lack of awareness of cybersecurity. Organisations should design and develop effective cybersecurity awareness training and guidance for providing information and knowledge.</td>
<td>Trained but there is an obstacle to motivation (e.g. lack of commitment and trust in organisation)</td>
<td>Good intention and motivation exists but there is an obstacle to action (e.g. cybersecurity expectations are too unreasonable and take too much time)</td>
<td>Short-term behaviours in action — initially cyber-hygienic but over time they regress to their previous state (e.g. training is forgotten and security is not a priority)</td>
<td>While they have developed good cyber hygiene and long-term cybersecurity habits, they fail to educate and influence peers to adopt cyber hygiene (e.g. a tendency to work in silo, a lack of team spirit)</td>
<td>Initiators of culture change to create societal norms of cybersecurity. Once organisations reach this final stage, people will become initiators of culture change and create societal norms, resulting in a conducive cyber culture.</td>
</tr>
<tr>
<td>Poorly trained or no guidance received for proper cybersecurity behaviours. This leads to a lack of awareness of cybersecurity. Organisations should design and develop effective cybersecurity awareness training and guidance for providing information and knowledge.</td>
<td>Trained but there is an obstacle to motivation (e.g. lack of commitment and trust in organisation)</td>
<td>Good intention and motivation exists but there is an obstacle to action (e.g. cybersecurity expectations are too unreasonable and take too much time)</td>
<td>Short-term behaviours in action — initially cyber-hygienic but over time they regress to their previous state (e.g. training is forgotten and security is not a priority)</td>
<td>While they have developed good cyber hygiene and long-term cybersecurity habits, they fail to educate and influence peers to adopt cyber hygiene (e.g. a tendency to work in silo, a lack of team spirit)</td>
<td>Initiators of culture change to create societal norms of cybersecurity. Once organisations reach this final stage, people will become initiators of culture change and create societal norms, resulting in a conducive cyber culture.</td>
</tr>
</tbody>
</table>
# CYBERSECURITY AWARENESS CAMPAIGN MATRIX

This matrix details the sequence of steps from obtaining campaign information to changing behaviour, and explains the objectives of each step and how to evaluate its success.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Seen the campaign and perception of the campaign</td>
<td>Showing interest in the campaign or message by taking an action</td>
<td>Priming steps of behavioural change</td>
<td>Initial trialing behaviour and antecedents of behaviours</td>
<td>Desired behavioural change</td>
</tr>
</tbody>
</table>
| **Objectives** | • Disseminating information and knowledge  
• Increasing psychological factors motivating participants to perform security behaviour  
  - Self-efficacy  
  - Perceived severity/vulnerability  
  - Response costs/efficacy | • Tuning motivation into cybersecurity engagement  
• Encouraging people to pay attention to cybersecurity threats and issues | • Enhancing knowledge of cybersecurity  
• Increasing attitudes and intentions for cybersecurity behaviour  
• Building a cybersecurity culture | • Encouraging people to actively seek out more cybersecurity information | • Assessing actual cybersecurity behaviour  
• Evaluating behavioural change for future planning |
| **Evaluation Indicators** | • Emotional reaction to the campaign  
• Pre- and post-campaign questionnaires on cybersecurity awareness and practices  
  - Campaign effectiveness  
  - Hits to the campaign  
  - Calls to the information line  
  - Campaign feedback  
• Measurement of increase in psychological factors | • Digital engagement  
• Content analysis - cybersecurity related words  
• Information seeking behaviour  
  - Campaign website visits  
  - Corporate security police visits  
  - Security blog visits on the intranet  
• Email views - Cybersecurity news and announcements | • Knowledge (Assessment/Quiz)  
• Measurement of increase in psychological factors of priming steps  
• Attitudes/ Intentions towards cybersecurity behaviours  
• Normative beliefs - Security culture | • Awareness/ Security days (attendees’ reactions to attend noncompulsory security events)  
• Additional inquiries for cybersecurity related questions  
• Symptom recall/recognition (reporting symptoms that may have been infected by malicious activity) | • Simulation of phishing attempts  
• Audit/ Risk department reports  
• Security incidents  
• Personal activities when using corporate network  
• Social discourse (Conversation with colleagues about cybersecurity) |

© Anima People. All rights reserved.
THANK YOU
Q&A

Are There Any Questions?

#FISSEA
Closing Remarks

Marian Merritt
Deputy Director of NICE/FISSEA Lead
National Institute of Standards and Technology

#FISSEA
Get Involved

Subscribe to the FISSEA Mailing List
FISSEAU Updates@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 for 2023
Email fissea@list.nist.gov

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

#FISSEA
SAVE THE DATE

Federal Information Security Educators (FISSEA) Winter Forum
February 14, 2024

#FISSEA | nist.gov/fissea
THANK YOU

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

https://www.surveymonkey.com/r/2023FISSEAFallForum

#FISSEA | nist.gov/fissea