NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION

Identifying Best Practices for Federal Cybersecurity Awareness Training

Dr. Rex Min, Office of the Director of National Intelligence *with* Tom Walsh, SRA, Inc.

WWW.CSRC.NIST.GOV/NICE/ 09/14/11

About ODNI

- **Mission:**
  Lead Intelligence Integration
  Forge an Intelligence Community that delivers the most insightful Intelligence possible

- **Vision:** A Nation made more secure because of a fully integrated Intelligence Community

http://www.dni.gov/mission.htm

And Now, a Few Disclaimers...

- This is a conversation and work in progress. This is not an order, directive, policy, etc.

- We speak today as a part of the NICE community affiliated with the Office of the Director of National Intelligence (ODNI), ADNI for Human Capital. No further endorsements are implied.

Background

- **What: Codification of best practices for cybersecurity awareness training**

- Who: NICE Participants from the ODNI, Assistant DNI for Human Capital

- Why:
  - Congress asked us to
  - We support the NICE mission
  - People are the front line of cybersecurity

Today's Best Practices for Discussion

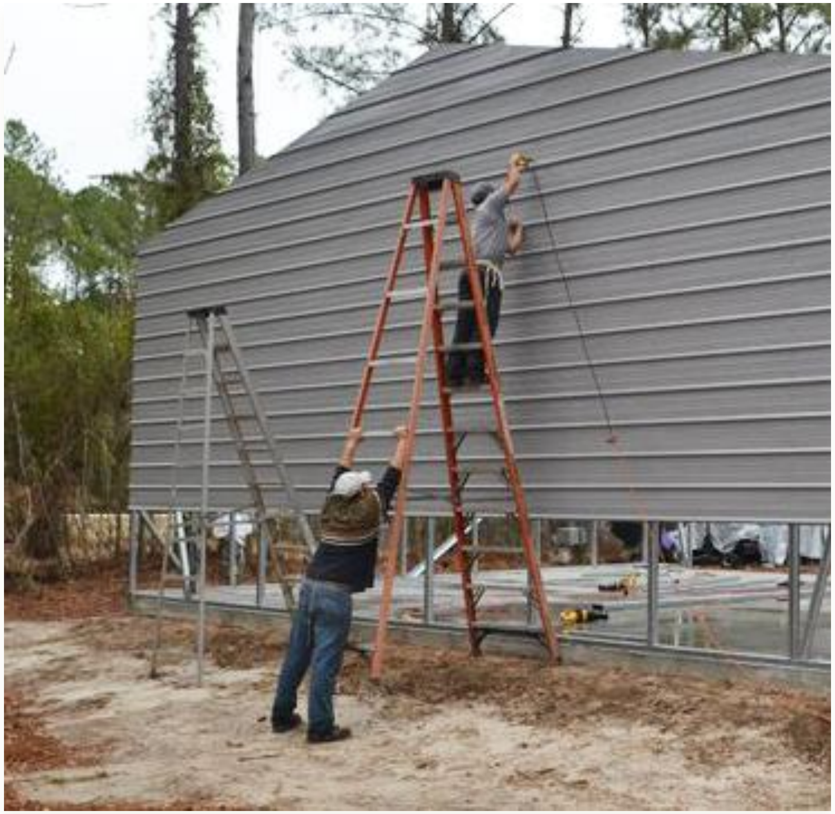
- Make training fun and relevant
- Use positive incentives
- Develop new metrics
- Involve all stakeholders

Make It Fun

- Do you require periodic awareness training? (You probably should)

- How do your users respond?
  - Can’t wait to do it! (genuine)
  - Ok, gotta do it.
  - Can’t wait to do it. (sarcasm)

Humor Works



http://www.public.navy.mil/navsafecen

#447: Helpful—and a Great Upper-Body Workout

Workers sometimes lack the time and energy to fit in an exercise session into their busy schedules. For those who can’t hit the gym on the way to work or go for a run at lunchtime, we offer this technique.

A variation is to slowly lower your arms, thereby tipping the guy with the drill away from the wall, allowing him to work on his balance skills.

Phishing Example

We need to verify your credit card number.
Don't take the bait. Protect your financial information.

(Federal Trade Commission, c. 2005)

Brainstorm: Making it Fun

- How can we turn a ritual exercise into something that users might actually look forward to?

Brainstorm: Making it Fun

- Social media
- Online videos
- Games (keep them short)
- User-generated content
- Users as teachers

- Leverage instructional best practices

Next, Make It Relevant

Athens, Greece. Twenty-six telecommunications vehicles, of the latest design, have arrived here to hasten the rehabilitation of Greece's telecommunications system, 60% destroyed during the occupation and guerrilla war. Two Greek workmen, carrying crude tools of their trade, inspect the fine alloy-steel blade on one of the new earth-boring trucks, 1948 - ca. 1955. USAID

Make it Relevant

- Cyber threats constantly evolve
- Organizations differ by...
  - Mission
  - Infrastructure
  - Security policy
- Individuals differ by...
  - Role
  - Responsibility
  - Experience
  - Level of public exposure

Make It Relevant

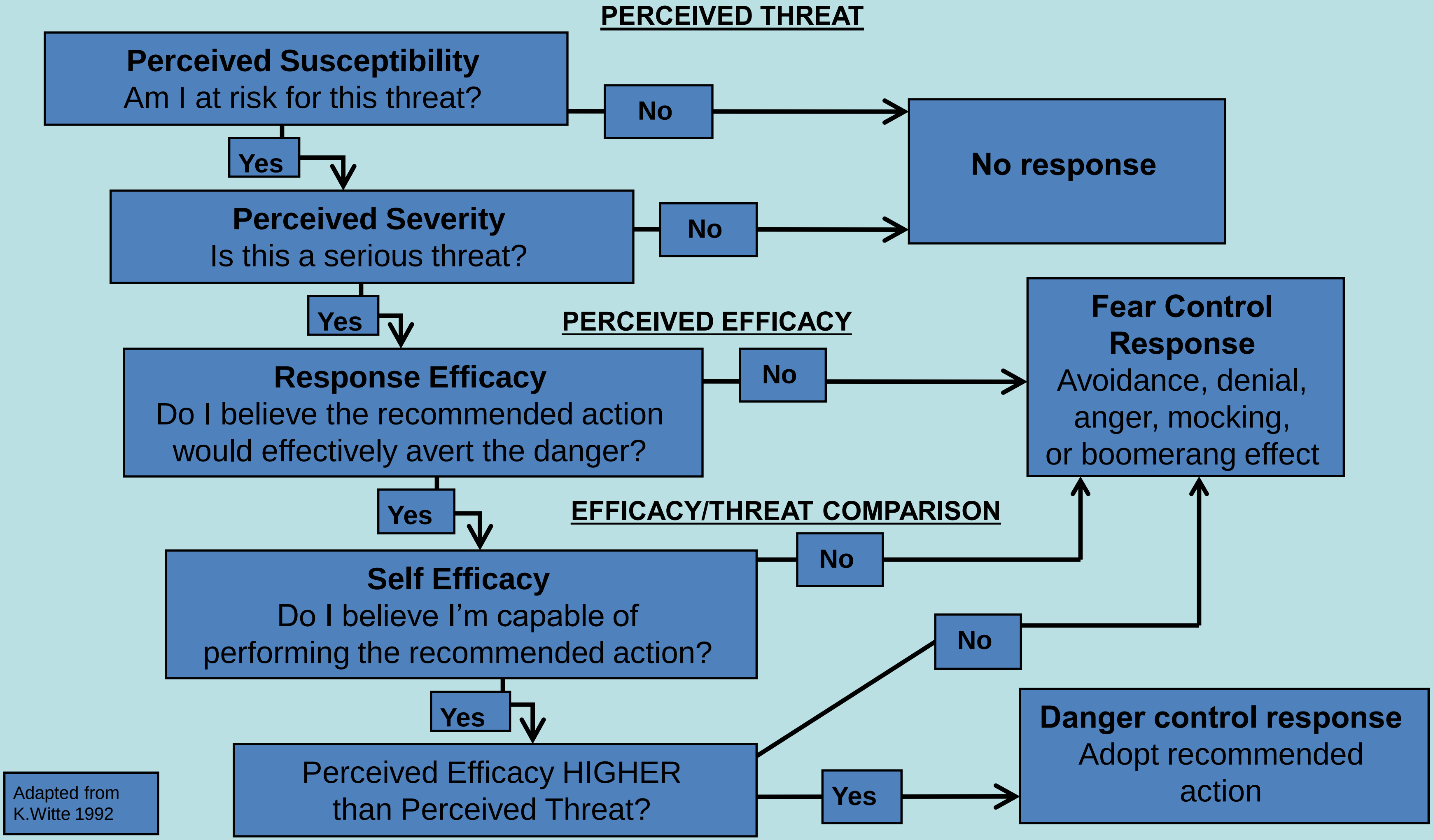
One size does not fit all

- Include material specific to your environment
- Review training objectives yearly
- Include the latest cyber threats
- Rotate course material

Use Positive Incentives

Does your organization use fear to encourage people to take awareness training?

Incoming message = **COMPLETE YOUR AWARENESS TRAINING OR ELSE!**



PERCEIVED THREAT

Perceived Susceptibility
Am I at risk for this threat?

No

Yes

No response

Perceived Severity
Is this a serious threat?

No

Yes

PERCEIVED EFFICACY

Fear Control Response
Avoidance, denial, anger, mocking, or boomerang effect

Response Efficacy
Do I believe the recommended action would effectively avert the danger?

No

Yes

EFFICACY/THREAT COMPARISON

Self Efficacy
Do I believe I'm capable of performing the recommended action?

No

No

Yes

Perceived Efficacy HIGHER than Perceived Threat?

Yes

Danger control response
Adopt recommended action

Adapted from
K.Witte 1992

Brainstorm: Positive Incentives

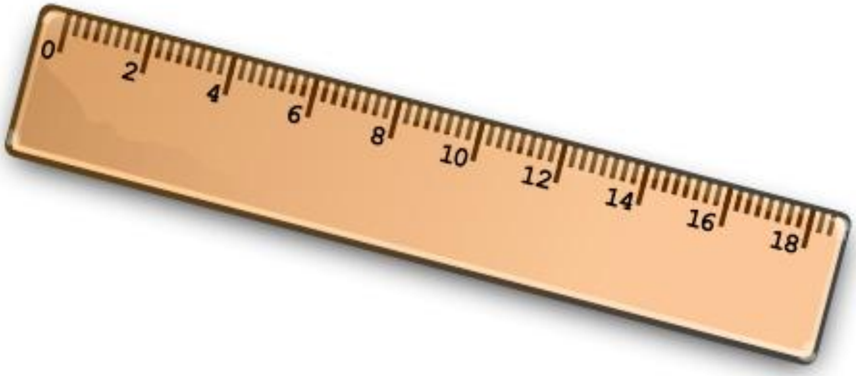
- People respond to incentives.
- Let’s brainstorm some.

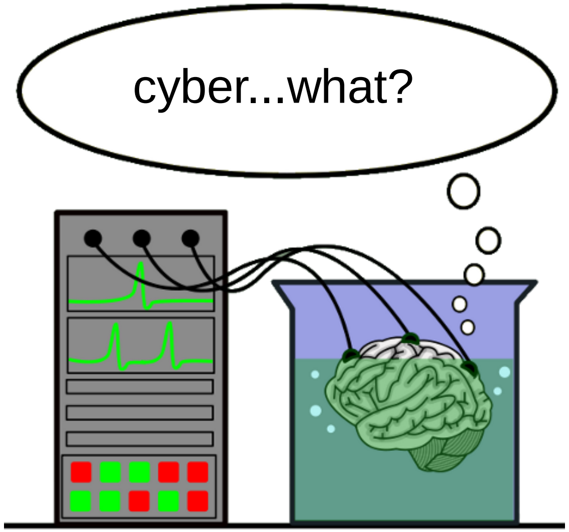
Brainstorm: Some Positive Incentives

- Provide “test-out” or expedited option upon demonstrated mastery
- Offer multiple ways to earn credit (e.g. external events)
- Credit advanced awareness training toward other training requirements
- Emphasize personal benefits of this knowledge
- Incentivize self-reporting of incidents
- Grant 59 minutes off for early completion

Develop New Metrics

- Does your organization track training completion rates? (It probably should.)
- But what does this really say about mastery and understanding?





Brainstorm: Metrics for Success

- Compliance doesn’t necessarily equal mastery
- With dwindling budgets, solid metrics are a must!
- Metrics to demonstrate competence...
  - Easier for traditional job training
  - Tougher for cybersecurity awareness

Brainstorm: Metrics

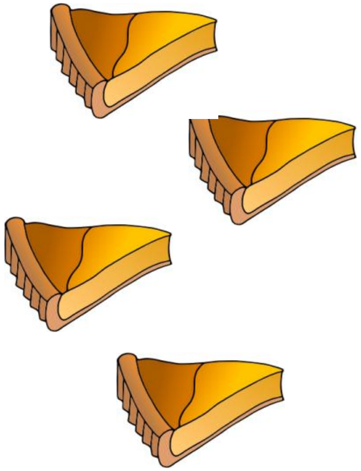
- How can we measure the effectiveness of cybersecurity awareness training?

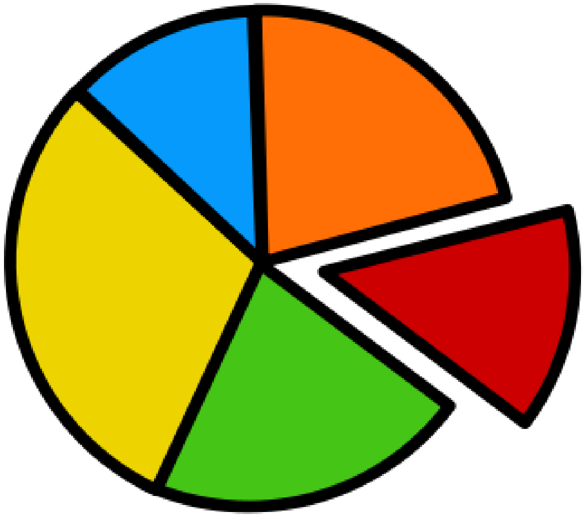
Brainstorm: Metrics

- Honestly, I don’t have the answer.
- That’s why I’m here.

Involve All Stakeholders

- Name the stakeholders in a cybersecurity awareness training program.





Potential Stakeholders

- Students/users
- Organizational managers
- Learning managers
- Training program coordinators
- Cybersecurity subject matter experts
- Security officers, incident responders, etc.

Stakeholder Communication

FROM:

TO:	1	2	3	4	5	6
1. Users						
2. Managers						
3. Learning Mgrs						
4. Training Coords.						
5. Cyber SMEs						
6. Security Officers						

Place an “X” in each box where significant collaboration is occurring. What information is being shared?

The Best Practice Generator Matrix

	TO:	1	2	3	4	5	6
FROM:	1. Users						X
	2. Managers	X					
	3. Learning Mgrs				X		
	4. Training Coords.			X			
	5. Cyber SMEs				X		
	6. Security Officers						

What information and feedback are being exchanged?

Is all communication two-way?

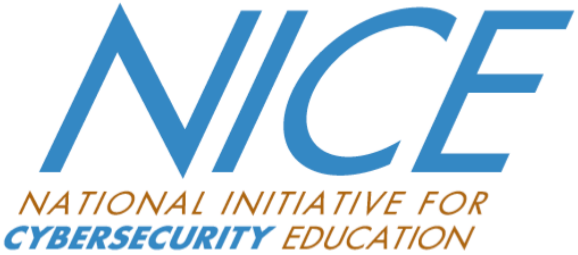
The Matrix Speaks…

- Are subject matter experts providing input to training program coordinators?
- Do program coordinators communicate needs to learning managers?
- Are front-line cybersecurity officers providing real-world stories to enrich course content?
- Do users receive feedback when they report incidents?

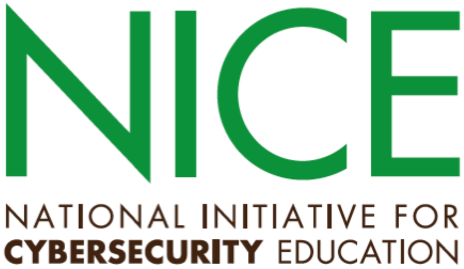
A Word about Branding

- Branding makes ideas “stick”
- Noticed all the NICE branding?

  (There’s even an official style guide...)



Do not distort or exaggerate the identity.



Do not change colors.

Potential Stakeholders

- Students/users
- Organizational managers
- Learning managers
- Training program coordinators
- Cybersecurity subject matter experts
- Security officers, incident responders, etc.
- **Graphic designers**

A Word about the NICE Community

- Have you seen...
  - The Stop-Think-Connect Campaign?
  - The Cybersecurity Workforce Framework?
  - The National Institute for Cybersecurity Studies?
  - The Cybersecurity Training Catalog?

- NICE resources are available to strengthen your cybersecurity awareness program

Potential Stakeholders

- Students/users
- Organizational managers
- Learning managers
- Training program coordinators
- Cybersecurity subject matter experts
- Security officers, incident responders, etc.
- Graphic designers
- **NICE Community**

A Word About this Presentation

- Original title was "**A Study of** Best Practices for Federal Cybersecurity Training"
- We actually conducted a study
- Finding the right POCs: *Tough*
- Getting everyone's permission to share the results: *Didn't happen*

A Call to Action

Collaborate! Connect!

Sharing our best practices (ideally through NICE) can only benefit us all

Potential Stakeholders

- Students/users
- Organizational managers
- Learning managers
- Training program coordinators
- Cybersecurity subject matter experts
- Security officers, incident responders, etc.
- Graphic designers
- NICE Community
- **Other agencies’ training programs**

A Word About Impact

“Our nation is at risk. The cybersecurity vulnerabilities in our government and critical infrastructure is a risk to national security, public safety, and economic prosperity.”

— NICE Strategic Plan, Draft, August 2011

Potential Stakeholders

- Students/users
- Organizational managers
- Learning managers
- Training program coordinators
- Cybersecurity subject matter experts
- Security officers, incident responders, etc.
- Graphic designers
- NICE Community
- Other awareness training programs
- **The United States of America.**

Conclusion

- Make training fun and relevant.
- Use positive incentives.
- Develop new metrics.
- Involve all stakeholders. *All of them.*