USSTRATCOM J7 Cyberspace Training Initiative(CTI) User Awareness Pilot Program

Liz Craven, Booz Allen Hamilton

Mr. Tim Kemper, DAFC

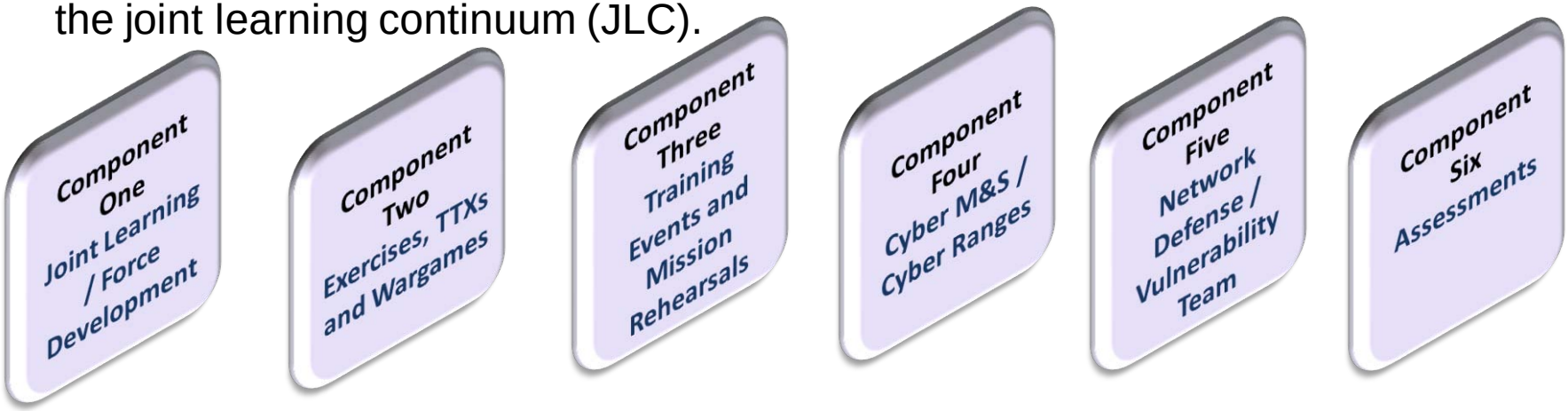
28 Mar 2012

This briefing is classified: UNCLASSIFIED

This slide is classified: UNCLASSIFIED

CTI Overview

- **Problem:** DoD lacks an integrated training approach that incorporates joint cyber education, training and exercises, as well as robust, timely and rapidly-developed cyber modeling and simulation capabilities to meet Joint Force Commanders' requirements to operate in and through cyberspace.
- **CTI Effort:** Provide an approach for educating, training, exercising, evaluating and assessing joint forces in conducting cyberspace operations by integrating and synchronizing training efforts with key stakeholders across the DoD.
- **Way Ahead:** Forces are trained through an integrated approach that incorporates joint cyber education, training, awareness and exercise methods using robust live, virtual and constructive mode and media capabilities across the joint learning continuum (JLC).



Joint Force Development: User Awareness Program

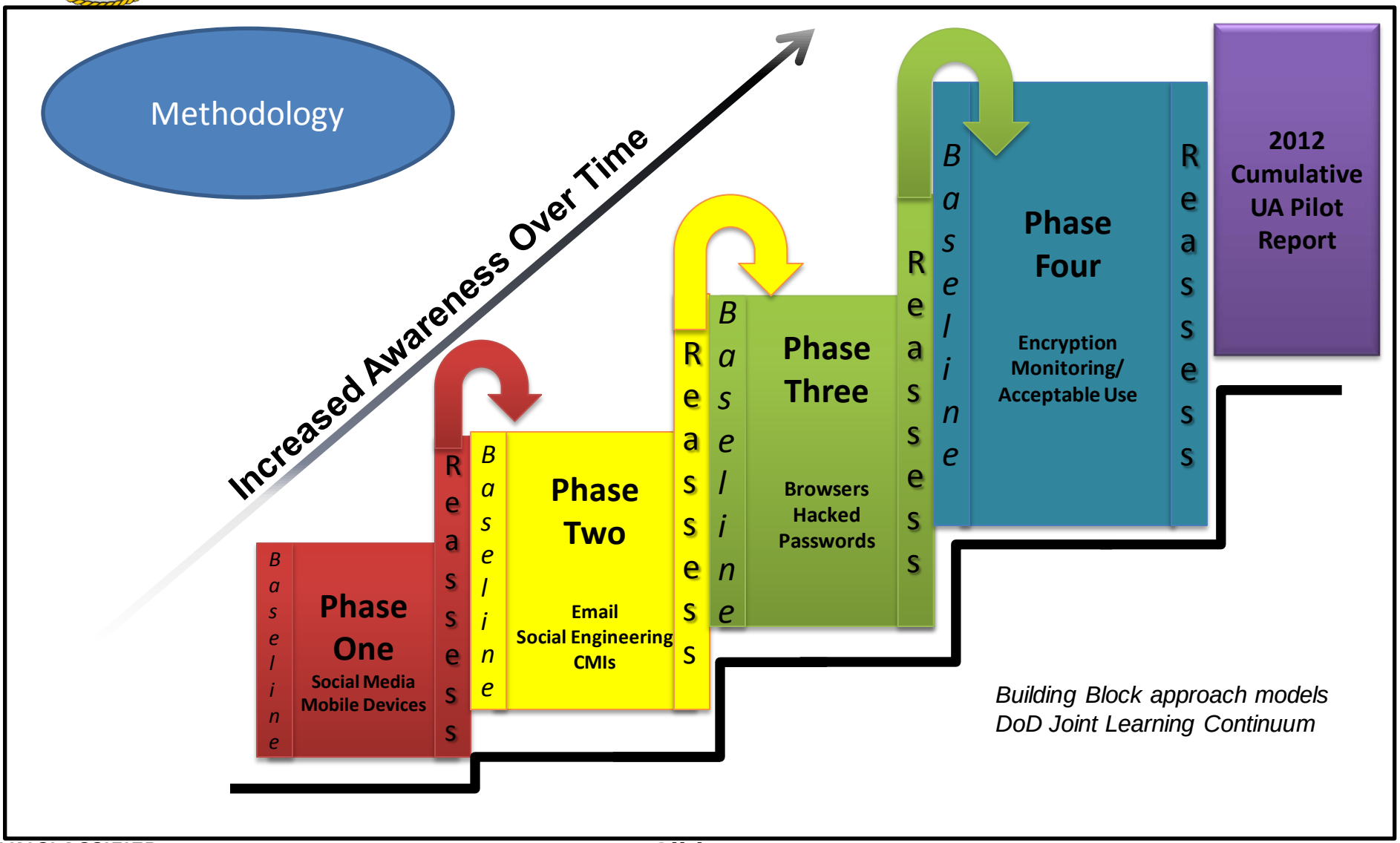
- **Problem:** The once annual Information Assurance training requirement is not sufficient for end users to practice cyber vigilance as a second nature behavior given the existing Advanced Persistent Threat (APT) landscape
  - End users ARE the greatest risk to any Automated Information System
  - Adversaries continue to gain a foothold through the actions of users, resulting in operational and financial impacts

- **Solution:** Pilot a results-based User Awareness Campaign to strengthen first line defenders by providing cybersecurity information on a recurring basis to determine if the Return on Investment (ROI) of such approach is sufficient to suggest for DoD-wide policy revision and/or implementation

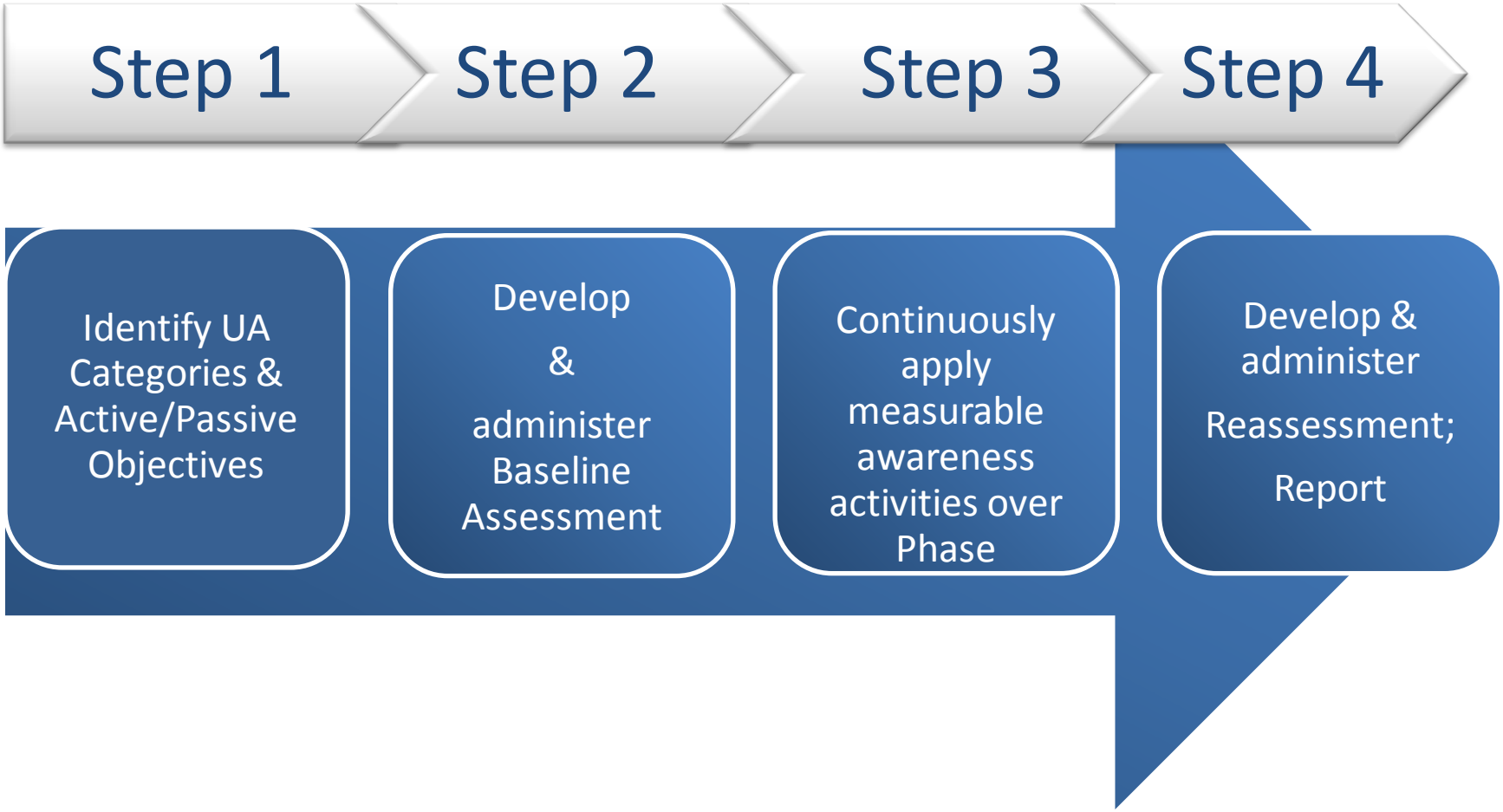
CTI User Awareness Pilot Program

- Focus is cybersecurity for all USSTRATCOM users at work, home and travel
- Utilizes a building block approach modeling the Joint Learning Continuum (JLC)
- The phased approach incorporates a blended learning experience and proven evaluation methods to continuously improve the state of cybersecurity awareness of the workforce over time
- Includes baseline and assessment metrics to measure success indicators on a cyclical continuous improvement model
- Enabling activities are consistent with the current state of cyber readiness based on assessments and include daily, monthly and quarterly events and/or products

2012 User Awareness Pilot Program



Phased Approach to User Awareness



Step One: Categories/Objectives

- Cybersecurity survey sent to cyber SMEs to determine where to apply user awareness
- Ten Categories, 100s of objectives, Four phases

User Awareness Categories

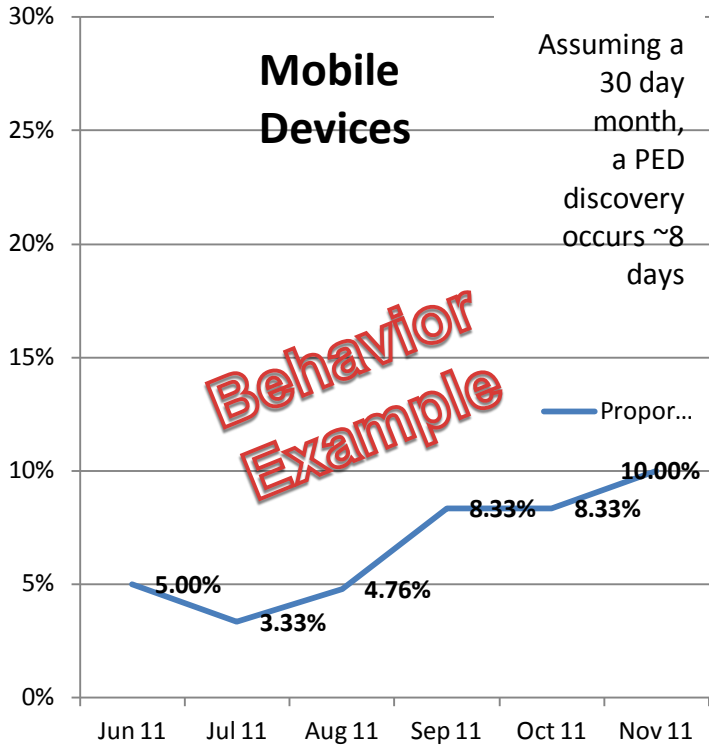
1. Social Media
2. Mobile Devices
3. Email/IM
4. Social Engineering
5. Classified Message Incidents
6. Browsers
7. Hacked
8. Passwords
9. Encryption
10. Monitoring/AUP

	CTI User Awareness Phase One Categories/Objectives
	At completion of Phase One User Awareness Campaign, first line defenders will:
CAT 1	Social Media
OBJ 1.1	Correctly define basic cybersecurity terms associated with social media
OBJ 1.2	State risks/vulnerabilities to USSTRATCOM associated with social media
OBJ 1.3	Recall personal risks/vulnerabilities associated with social media
OBJ 1.4	Recognize social media best practices for risk mitigation
OBJ 1.5	Apply knowledge of social media risks and risk mitigation in developing policy
OBJ 1.6	Participate in UA activities related to social media
OBJ 1.7	Interact with the social media material provided by CTI
OBJ 1.8	Endorse UA initiatives to increase cybersecurity awareness related to social media
OBJ 1.9	Placeholder: Recognize proper reporting procedures for social media policy violations
OBJ 1.10	Placeholder: Identify USSTRATCOM social media policies
OBJ 1.11	Placeholder: Apply knowledge of social media risks and risk mitigation to operations
OBJ 1.12	Placeholder: Demonstrate compliance with Command social media policies to protect personal and mission information

Example

Step Two: Baseline

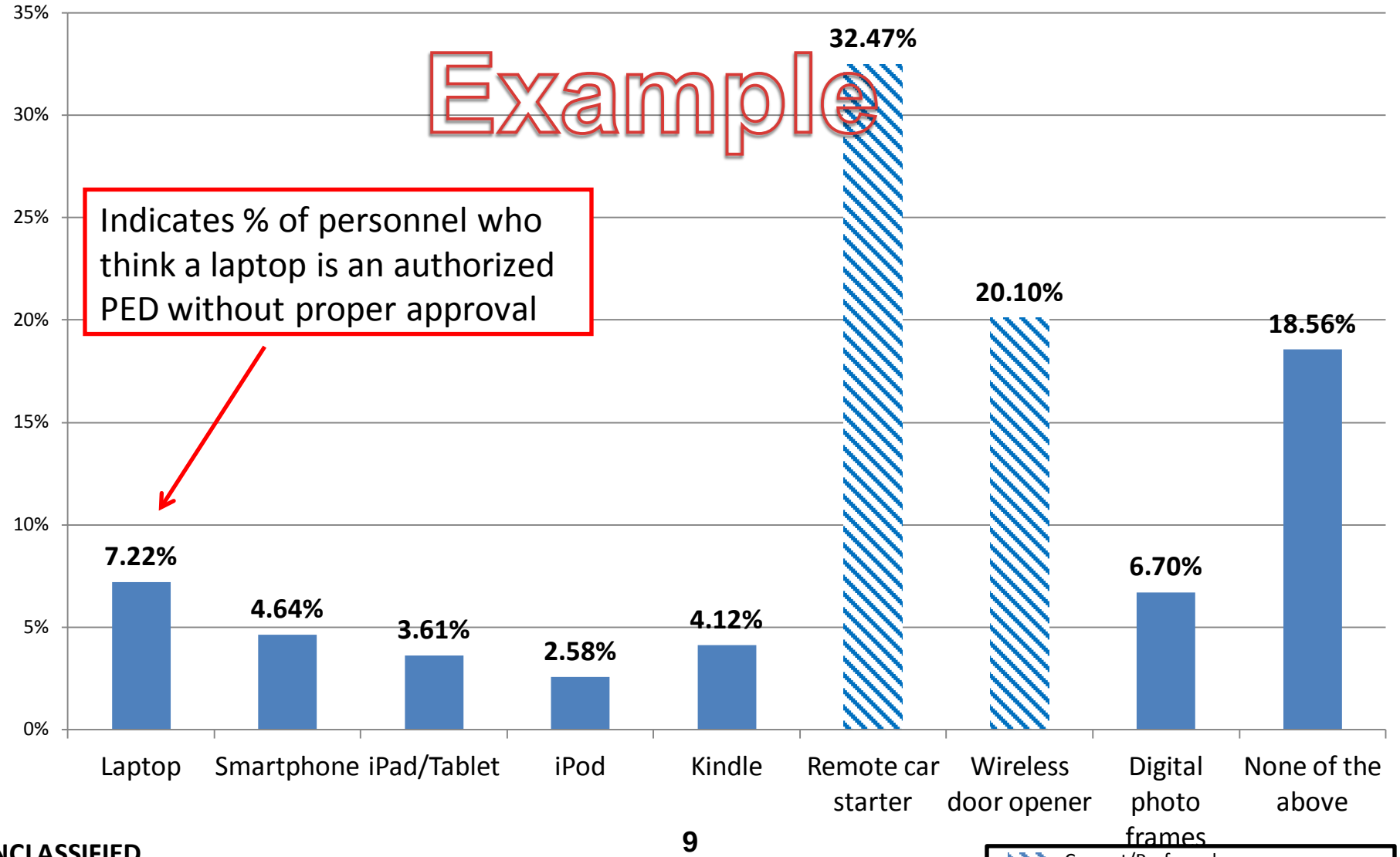
- **Collect baseline metrics prior to providing awareness**
- **Reassess at the completion of each phase to determine deltas**



Mobile Device Question	Correct Responses
What are some risks associated with Bluetooth use? (Select all that apply)	100%
Granting an application permission to your mobile device may allow it access to the following: (Select all that apply)	95
Which options increase the risk of introducing malware to your personal computer? (Select all that apply)	92%
What are some best practices for wireless settings on your mobile device? (Select all that apply)	95%
I am aware that I can install smartphone applications that _____. (Select all that apply)	80%
Can you introduce malware to a personal computer by plugging in an iPod?	71%
What is Near Field Communication (NFC)? (Select all that apply)	73%
Wi-Fi is short for _____.	85%
What actions have you taken to protect your mobile device from malware?	94%
What is the Strategic Instruction (SI) that governs mobile devices? (Select all that apply)	12%
In accordance with SI 301-6, which of these mobile devices ARE authorized for USSTRATCOM use without a Form 107? (Select all that apply)	22%
Have you checked/updated your mobile device(s) for operating system updates within the last 90 days?	46%
Have you changed your smartphone password/swipe pattern within the last 90 days?	31%
What is true about Bluetooth? (Select all that apply)	29%
How would you rate your level of knowledge of vulnerabilities associated with downloading applications to your mobile device?	2%

Knowledge Example

Baseline Result:
What mobile devices are authorized in this facility?



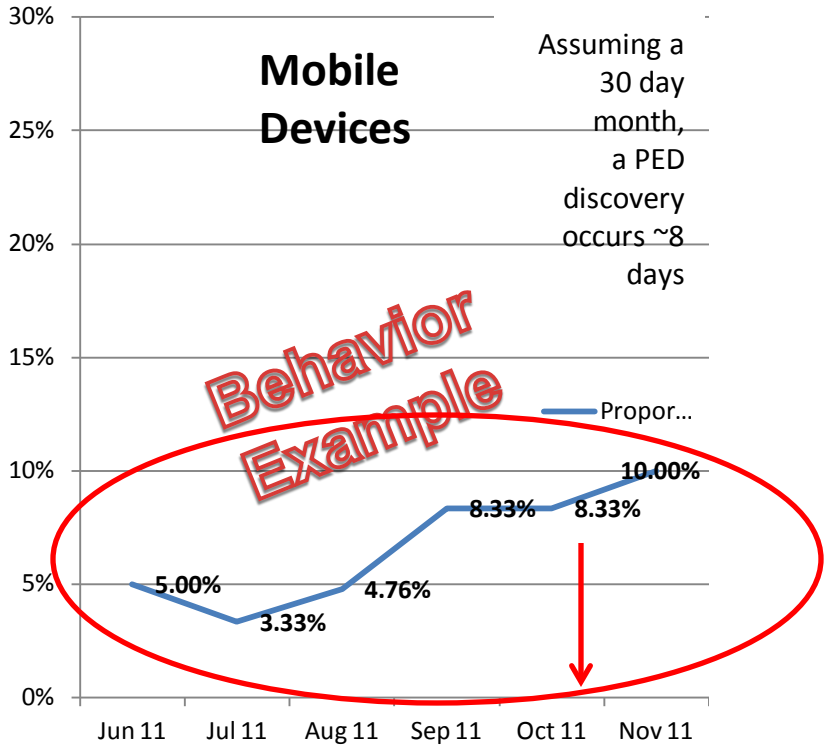
Step Three: Apply UA Activities

- **Use objectives to guide UA activities**
  - Cognitive
  - Psychomotor
  - Affective
- **Address user role**
  - General
  - Privileged
  - Sr Leader
- **Standing UA Activities**
  - Daily Cybersecurity update*
  - Monthly Cybersecurity Newsletter*
  - Bi-monthly Social Media cybersecurity update (Facebook/Twitter)*
  - Quarterly Cyber Speaker Series*

* Measurable

Step Four: Assess/Report

- **Reassess knowledge / performance activities**
- **Provide comprehensive report**



Mobile Device Question	Correct Responses
What are some risks associated with Bluetooth use? (Select all that apply)	100%
Granting an application permission to your mobile device may allow it access to the following: (Select all that apply)	95%
Which options increase the risk of introducing malware to your personal computer? (Select all that apply)	92%
What are some best practices for wireless settings on your mobile device? (Select all that apply)	95%
I am aware that I can install smartphone applications that _____. (Select all that apply)	80%
Can you introduce malware to a personal computer by plugging in an iPod?	71%
What is Near Field Communication (NFC)? (Select all that apply)	73%
Wi-Fi is short for _____	85%
What actions have you taken to protect your mobile device from malware?	94%
What is the Strategic Instruction (SI) that governs mobile devices? (Select all that apply)	12%
In accordance with SI 301-6, which of these mobile devices ARE authorized for USSTRATCOM use without a Form 107? (Select all that apply)	22%
Have you checked/updated your mobile device(s) for operating system updates within the last 90 days?	46%
Have you changed your smartphone password/swipe pattern within the last 90 days?	31%
What is true about Bluetooth? (Select all that apply)	29%
How would you rate your level of knowledge of vulnerabilities associated with downloading applications to your mobile device?	2%

Knowledge Example

Pilot Status Update

- **Four phased, four step approach**
  - Phase One concludes end of Mar
  - Phase Two baseline assessment underway
- **Pilot runs through 2012 calendar year**
  - Results shared with local STRATCOM leadership, DoD/CIO, DISA/IASE, OSD/P, & others

Questions?

Mr. Tim Kemper

kempert@stratcom.mil

cti@stratcom.mil

DSN: 272-5137

Comm.: (402) 232-5137