Assessing the Effectiveness of Security Awareness Training

Steve Kruse
Security Principal @ RSA
steve.kruse@rsa.com

Bill Pankey
Consultant @ Tunitas Group
bpankey@tunitas.com

State of Security Awareness Training

2010 Survey of Industry Security Awareness Training

Methods used to assess effectiveness:

- **Training completion / compliance rate: 100% [cost]**
  - **(User) Behavioral \ attitude measures: 13%**
  - **Correlation w/ security incident metrics: 7%**

High level of CISO / CIO satisfaction

⇒ Minimal expenditure on user awareness / training

Unsupported by empirical data

Assessment Problem

Prospective

Forecast user error / security violations

Useful

Support corrective action beyond merely ‘more training required’

Efficient & reliable

Summarize a lot of behavior & *context*

Security Awareness Calibration

How does the human fit into the security plan?

- As a threat … Then the actor must know enough and be motivated 'not to act' in a certain fashion
- As a counter-measure … Then the actor must know enough and be motivated 'to act' in a certain fashion

What are the capabilities of users?

- Compliance while completing work assignments
- Recognizing threats \ reporting
- Managing risk

Maturity Model

Provides a common scale for calibration

- Characterize security policy / plan expectations
- Characterize user awareness / likely behavior

Summarize to reduce complexity

- Baseline user awareness
- general relationship between user and systems
  - ⇒ Approach to motivation / awareness / etc

User Awareness Maturity Model

- Competent & Practiced
  - Expects to manage security risk (recognize and mitigate) when performing duties.
- Risk aware
  - Considers information security risk in performance of company duties, but
    - Unsure of appropriate action; sometime will report incidents

* Compliant
  - Aware of risks identified in company policy
    - Will take action identified in company security policy
- Consciously incompetent
  - Avoids behavior believed to 'risky', even if that results in some productivity loss
- Blissfully unaware
  - Uses *any* capability provided them … little recognition or acceptance of most information security threats
  - At this level, prevalent view is that information security is a property of IT systems and largely a matter of architecture and configuration. Security largely independent of user behavior.

* Typical target

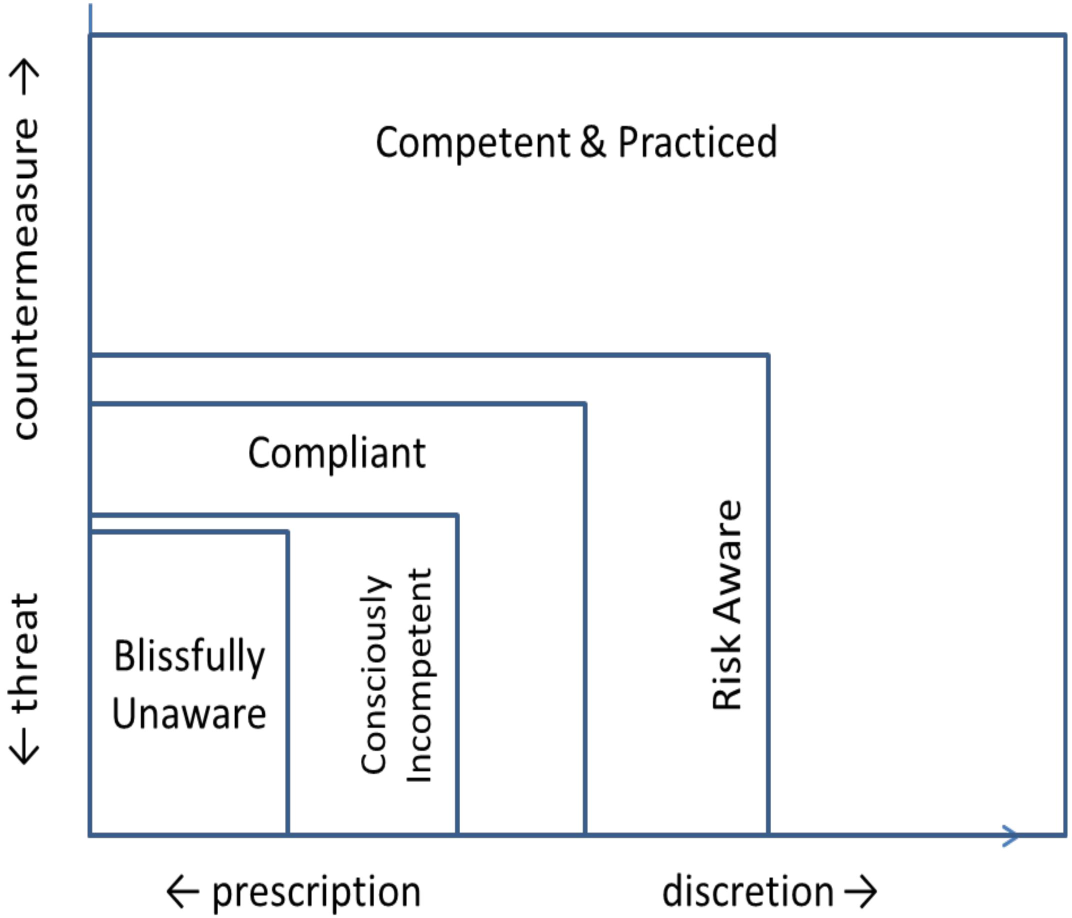
Underlying Maturity Factors

Discretion

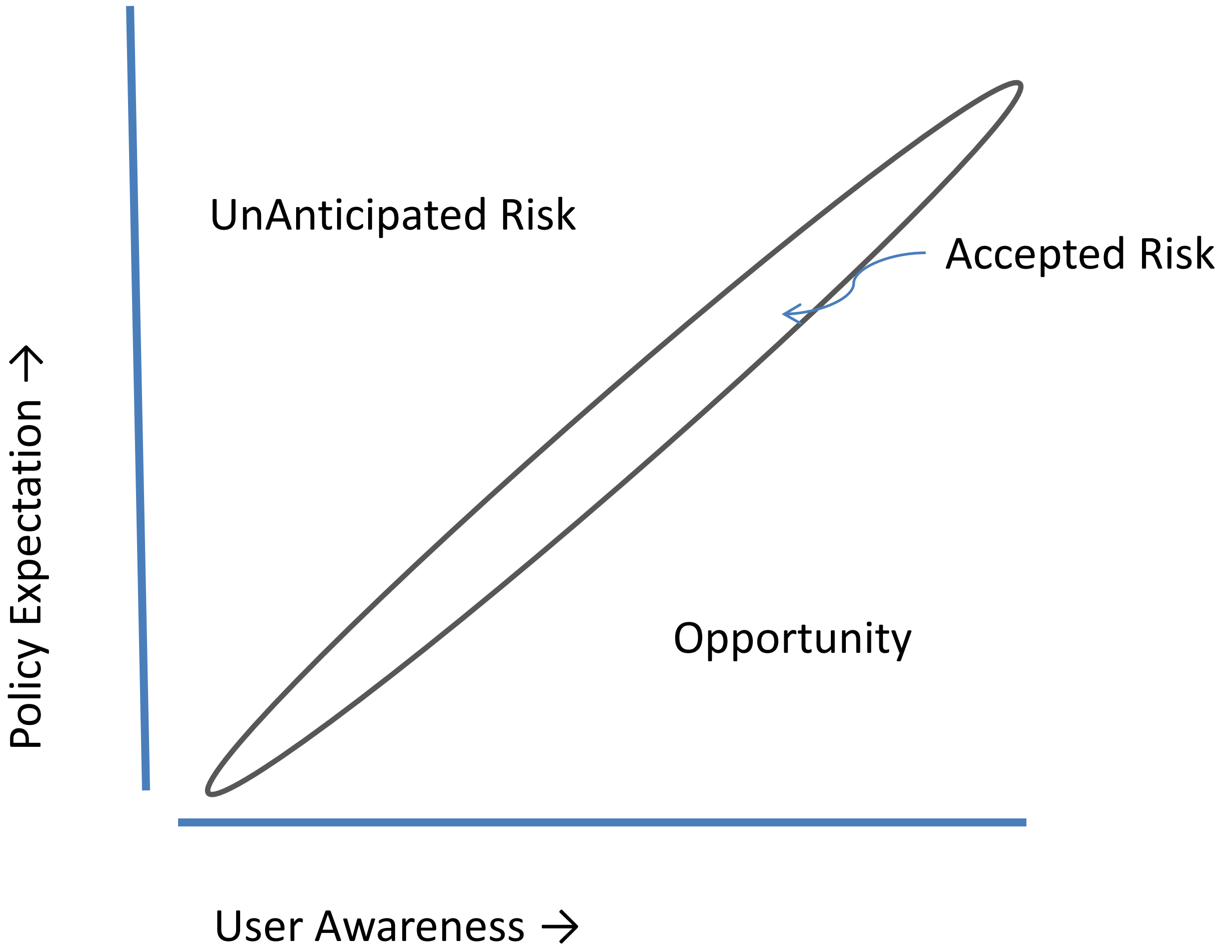
More flexibility allowed users as maturity increases

Participation

More risk management responsibility as maturity increases



Risk Map


UnAnticipated Risk
Accepted Risk
Opportunity
Policy Expectation →
User Awareness →

Example: A Teleworker Policy

Applied to 'at home' and 'alternate work location scenarios' - provisions at each maturity level

Blissfully Unaware

- *There will be no in-person client interviews or contact conducted at the telecommuters' home*.

Consciously Incompetent

- *Telecommuters are responsible for clarifying any questions regarding the applicability of rules, policies, practices and instructions through discussions with their supervisor.*

Compliant

- *Use of county equipment and supplies is limited to authorized persons for purposes relating to county business*.

Risk Aware

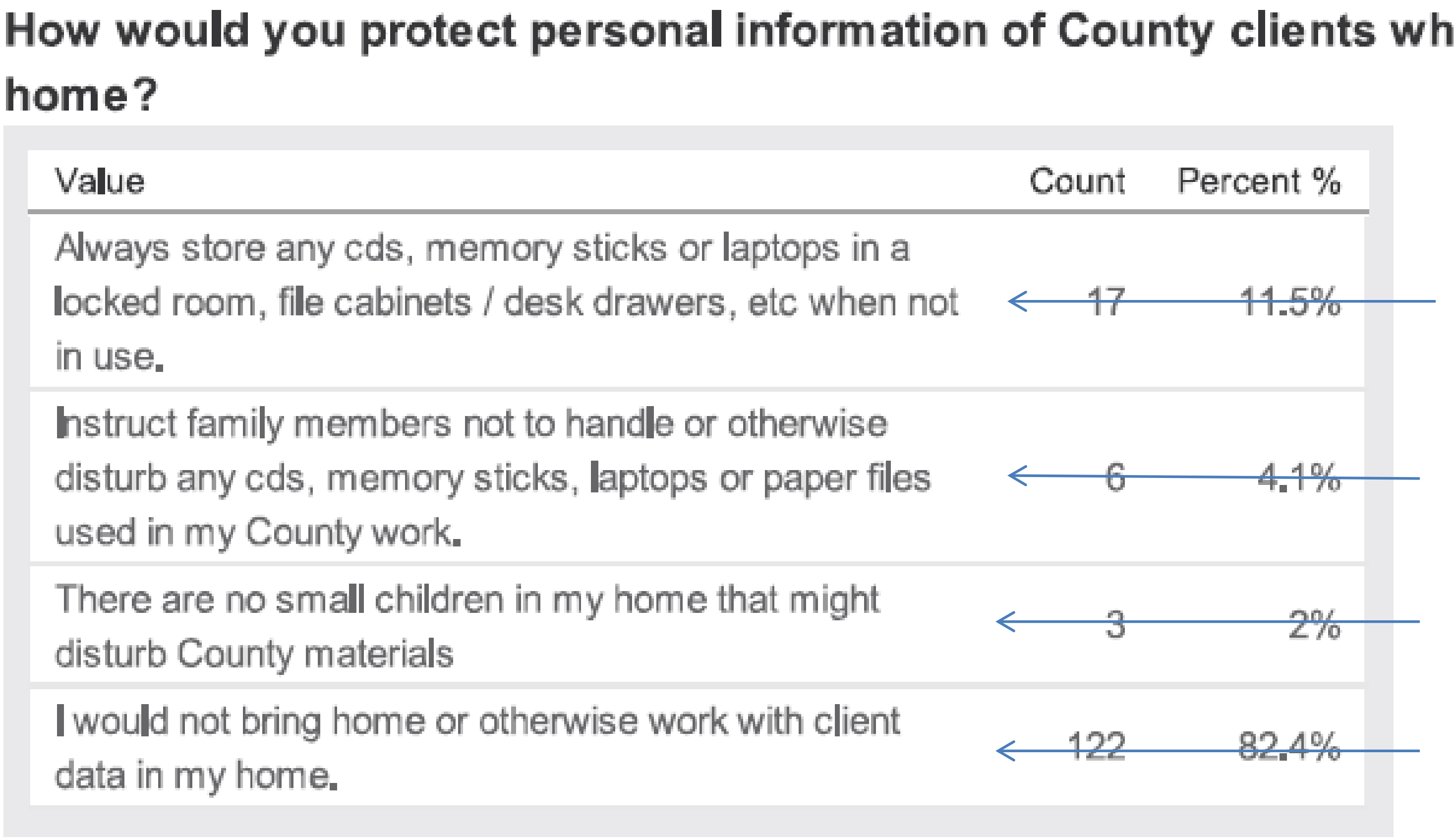
- *The employee must designate a workspace at home that is maintained in safe condition and free from hazards.*

Practiced and Competent

- *Telecommuters will take all precautions necessary to secure county information and equipment in their home, prevent unauthorized access to any county system or information*

Example: Behavioral Scoring

@ Company with the teleworker policy



How would you protect personal information of County clients when working at home?

Value	Count	Percent %
Always store any cds, memory sticks or laptops in a locked room, file cabinets / desk drawers, etc when not in use.	17	11.5%
Instruct family members not to handle or otherwise disturb any cds, memory sticks, laptops or paper files used in my County work.	6	4.1%
There are no small children in my home that might disturb County materials	3	2%
I would not bring home or otherwise work with client data in my home.	122	82.4%

Competent

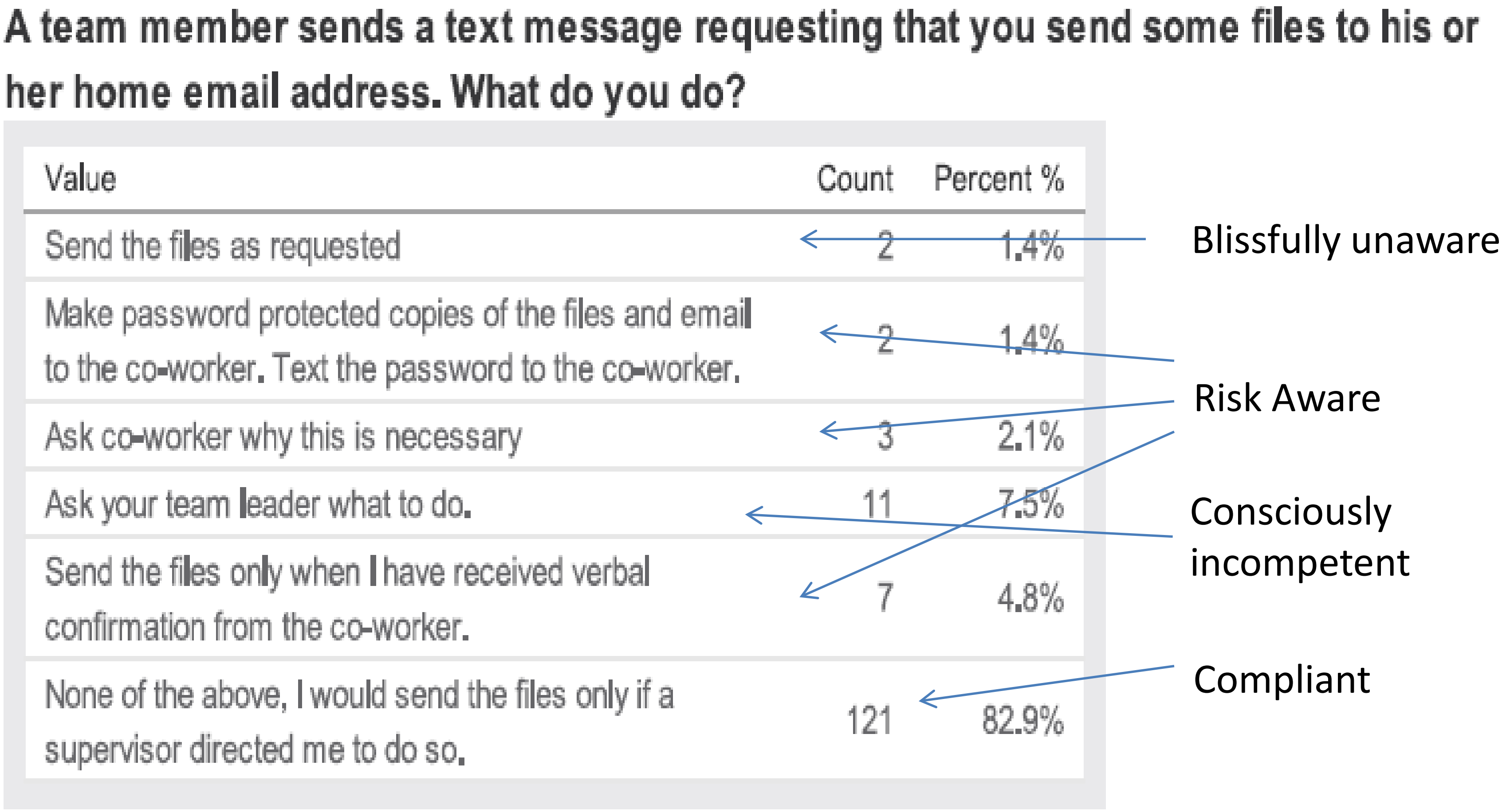
Risk Aware

Blissfully Unaware

Consciously Incompetent

Example: Behavioral Scoring

@ Company with the teleworker policy



A team member sends a text message requesting that you send some files to his or her home email address. What do you do?

Value	Count	Percent %
Send the files as requested	2	1.4%
Make password protected copies of the files and email to the co-worker. Text the password to the co-worker.	2	1.4%
Ask co-worker why this is necessary	3	2.1%
Ask your team leader what to do.	11	7.5%
Send the files only when I have received verbal confirmation from the co-worker.	7	4.8%
None of the above, I would send the files only if a supervisor directed me to do so.	121	82.9%

Blissfully unaware

Risk Aware

Consciously incompetent

Compliant

Example: Response

Illusory Policy assuming too much user maturity

> 10% of users making ‘incompetent’ choice when working w/ client confidential material at home

- Reconsidering teleworker policy

Increased technical safeguards to protect against the errors of the ‘blissfully unaware’

- VPN use of RDP (remote desktop protocol) / terminal services
- Restriction on accessing email attachments through OWA

Questions for Empirical Research

Does user capability at higher maturity level indicate capability at lower level? (i.e. form a ‘Guttmann scale’)

- Users making appropriate choices at one level of policy will make appropriate choices at lower levels of policy

Can user maturity be reliably measured with test scenarios?

- High whole / part test correlations

Does maturity modeling capture persistent aspects of user security understanding and capability?

- Insignificant correlation between responses after controlling for maturity level