Security Awareness & Training

Steve Kruse, Impruve

Bill Pankey, The Tunitas Group

Background

- Bill Pankey has been involved with information security issues for the past 12 years as a developer, architect, engineer, auditor and consultant. He is a Partner in the Tunitas Group, a healthcare-specific IT management consulting firm. He is a CISSP, CISA.
- Steve Kruse has been involved with information security since 1989. He has worked for security vendors and the last six years in consulting. He is a CISSP, CISA

Presenter(s) Bias(es)

- Bill believes the information security awareness discipline is primarily a marketing function and should be evaluated as such
- Steve believes people should be part of the solution, not part of the problem (similar to a quality initiative)
- Both believe risk issues lie beyond IT domains

A Paradox?

- Conventional wisdom: Non-malicious errors of the enterprise workforce (insiders) are responsible for as much as 80% of security breaches
  - Persistent view that has changed little over time
- Fact: 70% of companies spend less than 2% (48% < 1%) of security budget on activities that would increase the level of care on the part of ordinary users (2007 CSI computer crime survey)

2 Approaches to Resolution

- ‘Engineer around’ end users
  - Implement MAC and other constraints that limit the ability of end users to make infosec errors
  - Wrong side of the curve? Current business requirements is often to provide more information and more discretion to business users.
- “Train” end users to be part of infosec solution
  - Requires maturity in training management
  - Process goals, performance indicators and metrics

NIST 800-16/800-50

- **800-16 – Information Security Training Requirements – a Role and Performance-Based Model** revised March 20, 2009 (draft) – Emphasis on role-based training but topic-centric (as opposed to scenario based) and high level: “make sure material is appropriate for the audience”
- **800-50 – Building an Information Technology Security Awareness and Training Program** – more measures on delivering contents instead of content/program effectiveness. 800-50 is scheduled for revision in 2009

Are today’s metrics misdirected?

- Most UAT metrics are measures of *compliance* that focus on the delivery of training rather than training *effectiveness*
  - *% of staff not at optimal training level? (ITSM)*
  - *% of staff completing security awareness training? Refresher training per policy? (Jacquith)*
  - *% of employees in security roles receiving specialized security training (NIST 800-50)*
- Often support a training program designed to be proforma regulatory or other external requirement for ‘security awareness’ training; (e.g. HIPAA, FFIEC, PCI)

Do these metrics obscure the security objective?

- Implicitly assume the effectiveness of training
  - Relevance, credibility, appropriateness
- Anticipate change in end-user behavior

  “Why would we expect end-users to behave differently?”

  “What do we base that on?”
- Currently these measures are primarily *cost* metrics reflecting the scale of resource (end user time) consumption

On Going Survey

- Online Survey of security awareness training management practices
- Seek to identify ‘best practices’ re:
  - Management responsibilities
  - Selection of security objectives
  - Content
  - Measures of effectiveness

http://tinyurl.com/djdnlo

Questions

6. Has the Organization realized the expected benefits of the awareness program?

    No 60%

    Yes 40%

7. Who determines effectiveness of awareness?

    CSO/CISO 40%

    Director of Information Security 20%

    No one 40%

8. Would you expect increased benefits with further increase in security awareness training?

    Proportionate to time spent 60%

    Little or none 40%

53. The company's ordinary users can be and are relied upon to report threats to information security as they recognize them?

    No 60%

    Yes 40%

Survey Findings

- Little to no metrics for UAT effectiveness
- Simplistic training model – based on the entire community instead of role-based
- Training time for end users is not recognized in financial terms (5,000 end users spent 1 hour/year on class @ $50/hr = $250,000
- *yet*, Respondents are generally satisfied with their UAT program!?

User Awareness Maturity

- UAT metrics should be calibrated to security program’s <u>user maturity model</u> and expectations
  - – “blissfully unaware”
  - – “consciously incompetent”
  - – “compliant”
  - – “risk aware”
  - – “competent and practiced”
- Different goals and performance indicators at different maturity targets

Maturity Model

- Blissfully unaware
  - 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
- Consciously incompetent
  - Some recognition that there is a information security threat, but:
    - Poor risk assessment skill and intuition
    - Uncertain of action needed to protect company information assets will do nothing rather than create further harm
- Compliant
  - Aware of risks identified in company policy
    - Will take action identified in company security policy
- Risk aware
  - Considers information security risk in performance of company duties, but
    - Unsure of appropriate action; sometime will report incidents
- Competent & Practiced
  - Takes appropriate action within scope of role; otherwise reports incidents

Alternative Approach to UAT Metrics

- Identify specific security objective of training
  - E.g., avoid inappropriate disclosures | verify fax numbers before sending document
- Track incidents related to security objective
  - # of documents inappropriately faxed
- Correlate incidents with training (content and individual level)
  - # of incidents related to training objectives
  - # of incidents where individual deviated from training guidance

PDCA

- Appropriate metrics allow for management of the *security* objectives of UAT
- Determine the effectiveness of
  - Content
  - Delivery
  - Frequency and Timing
- Current UAT is typically guided by ‘instructional theory’
  - If that were enough the ‘paradox’ would not persist

Scenario

“You walk past an unlocked car in the parking lot, you notice a company laptop in the car. You should:”

a)Lock the car

b)Take the laptop into the company and give to the receptionist

c)Take the laptop and give to the help desk

d)Notify the facilities manager

Call to Action

- Looking for data to dispute assumptions
- Some companies devoting > 5% of budget on UAT, are they willing to be interviewed?
  - Evidence that the greater investments brings measurable results?
- Other parameters we should be tracking/measuring?