

Security Awareness



CSH5 Chapter 49

“Implementing a Security Awareness Program”

K Rudolph

1

Copyright © 2012 M. E. Kabay. All rights reserved.

Topics in CSH5 Ch 49



- Awareness a Survival Technique
- Critical Success Factors
- Approach
- Awareness Principles
- Content
- Techniques
- Tools
- Measurement and Evaluation
- Resources



2

Copyright © 2012 M. E. Kabay. All rights reserved.

Awareness as a Survival Technique



- Staff are countermeasure against security violations
- Staff first affected by security incidents
- Staff who are aware of security can prevent incidents and mitigate damage
- Awareness is prime factor in organization's successful security program



3

Copyright © 2012 M. E. Kabay. All rights reserved.

Critical Success Factors



- Information Security Policy
- Senior Level Management Support
- INFOSEC is a People-Problem



4

Copyright © 2012 M. E. Kabay. All rights reserved.

Information Security Policy



- Gives security program credibility
- Awareness policy should authorize and enforce
 - ❑ Everyone's participation
 - ❑ Sufficient time to participate in awareness activities
 - ❑ Responsibility of specific people for planning and carrying out activities
 - ❑ Methods for assessing outcomes



5

Copyright © 2012 M. E. Kabay. All rights reserved.

Senior Level Management Support



- Allocate budget for awareness activities
- Senior management participates fully
 - ❑ Employees naturally emulate “superiors”
 - ❑ If upper management show no interest in security and security awareness, neither will anyone else
- Backing security staff
 - ❑ Security is a pain in the ****
 - ❑ Need authority as well as responsibility to be able to shift corporate culture



6

Copyright © 2012 M. E. Kabay. All rights reserved.

Only YOU Can Ensure Security



- Information assurance depends on human support for technological methods
- Classic example: new card-access system
 - ❑ Violations not due to stupidity or hostility:
 - ❑ Conflict between politeness and security
- Need to establish new cultural norms in the organization
 - ❑ Hence “shifting corporate culture”



Copyright © 2012 M. E. Kabay. All rights reserved.

7

Goals of an Awareness Program



- Specific, realistic, measurable
- Reinforce employee awareness
- Develop “Think security” reflex in employees
 - ❑ Integrate importance of information security in all aspects of normal work
 - ❑ Consider consequences of security failures when evaluating business processes and decisions



Copyright © 2012 M. E. Kabay. All rights reserved.

8

Audience Profiles



- Needs of audience
 - ❑ What should they be able to do after the awareness program that they don't/can't do before the program?
- Roles and interests of audience
 - ❑ Who's in the audience?
 - ❑ What responsibilities do they have?
 - ❑ What authority do they have?
 - ❑ What do they know?
- Conduct research to answer these questions if necessary



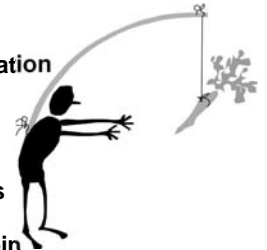
Copyright © 2012 M. E. Kabay. All rights reserved.

9

The Art of Motivation



- Recognize continuum of motivation
 - ❑ Beliefs
 - ❑ Attitudes
 - ❑ Behaviors
- Appeal to attitudes/preferences in your program
- Send message with positive spin
 - ❑ Encourage rather than punish
 - ❑ Amuse rather than frighten
- Don't bore people (duhhh)(snore)
- Don't overdo it – keep your sessions short



Copyright © 2012 M. E. Kabay. All rights reserved.

10

Approach



- Media campaign
 - ❑ Define program objectives
 - ❑ Identify primary, secondary audiences
 - ❑ Define information to be communicated
 - ❑ Describe benefits as perceived by audience
- Is a Plan Necessary? (Yes, can be short plan)
 - ❑ Status of company's current efforts
 - ❑ Program goals and objectives
 - ❑ Allows faster reaction; co-ordination behind a theme

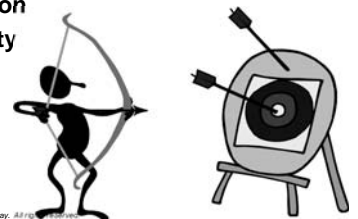
Copyright © 2012 M. E. Kabay. All rights reserved.

11

Awareness Principles



- Keep audience's attention
- Appeal to target audience
- Keep it simple and memorable
- Encourage feedback
- Reflect on current issues
- Give credible information
- Repeat and allow variety



Copyright © 2012 M. E. Kabay. All rights reserved.

12

Content

Address topics such as

- Risks “What does a threat look like”
 - ❑ Malware
 - ❑ Privacy issues
- Basic countermeasures
 - ❑ Procedures for secure computing
 - ❑ Information useful for protecting families
- Responsibilities
- Contact information for help or in case of trouble
 - ❑ Who, what, how, when



13

Copyright © 2012 M. E. Kabay. All rights reserved.

Communication Techniques (1)

Presentation is crucial

- Start with a bang – do NOT bore
- Use logos, themes, images
 - ❑ “What would happen if someone changes your data” - US Government courses
- Use stories and examples
 - ❑ Real people, real consequences
- Use failure as learning accelerator
- Ask questions and involve audience
- Be surprising



14

Copyright © 2012 M. E. Kabay. All rights reserved.

Communication Techniques (2)

- Address personality and learning types
 - ❑ Auditory, visual, kinesthetic
 - ❑ Use analogies, metaphors, similes
- Use relevant, *inoffensive* humor
- Take advantage of circumstances
 - ❑ Unplanned event like outsider visit
 - ❑ News programs on TV or radio (e.g., NPR)
 - ❑ Electronic newsletters with anecdotes
- User acknowledgement and sign-off
 - ❑ Positive: prizes, contests for successful exam score
 - ❑ Negative: withdraw system access if users fail awareness tests



15

Copyright © 2012 M. E. Kabay. All rights reserved.

Tools for Consciousness-Raising (1)

- Intranet/Internet/Extranet for
 - ❑ Online courses
 - ❑ Screen savers
- Posters
- Videos
- Trinkets and giveaways
- System login messages
- Important discussion:
 - ❑ Which tools are appropriate for *your* organization?
 - ❑ Which methods are
 - ✓ credible?
 - ✓ accessible?
 - ✓ feasible?



16

Copyright © 2012 M. E. Kabay. All rights reserved.

Tools for Consciousness-Raising (2)

- Publications
- Surveys, suggestion programs, contests
- Monitoring / Measuring
 - ❑ Security By Wandering Around (SBWA)
 - ❑ Inspections / Assessments
 - ❑ Audits (see next slide)
- Events
 - ❑ Conferences
 - ❑ Briefings
 - ❑ Presentations
 - ❑ Brown-bags



17

Copyright © 2012 M. E. Kabay. All rights reserved.

Evaluating Outcomes

- Audience satisfaction
 - ❑ Smiling faces, nods, few sleepers
 - ❑ Feedback
- Learning or teaching effectiveness
 - ❑ Pre- and post-tests
 - ❑ Preliminary survey and follow-up to measure improvement
- Skill transfer or audience performance
 - ❑ Follow-up interviews (open, fixed)
 - ❑ Monitor statistics on breaches before and after awareness program starts



18

Copyright © 2012 M. E. Kabay. All rights reserved.

Resources (1)



- Federal Information Systems Security Educators' Association (FISSEA)
<http://csrc.nist.gov/organizations/fissea/index.html>
- Computer Security Institute
 <http://gocsi.com>
- Videos
 <http://www.commonwealthfilms.com>
- Webcasts
 <http://siia.net/>
- Prof. Kabay's Web site©
 <http://www2.norwich.edu/mkabay>



M. E. Kabay. All rights reserved.

Resources (2)

- Native Intelligence
 - K Rudolph's Company
 - <http://nativeintelligence.com/>
- Vast array of posters and courses
- K is principal author of the chapter you are studying
- Co-author of *Cybersafety, 2nd Edition* with Prof. Kabay



20

Copyright © 2012 M. E. Kabay. All rights reserved.

Resources (3)



- Prof. Kabay's narrated PowerPoint lectures on how to teach effectively
 - Used in MSIA Program
- See
<http://www.mekabay.com/courses/academic/norwich/msia/index.htm>
or
<http://tinyurl.com/5tvm75>
- Use *Leadership* lectures
 - Part 3 (Presenting information effectively) (3.4 MB)
 - Part 4 (Presenting information -- cont'd) (3.4 MB)

21

Copyright © 2012 M. E. Kabay. All rights reserved.

Review Questions (1)



1. Why is security awareness important?
2. What are the necessary components of a security-awareness policy?
3. Why and how should senior management participate in security-awareness programs?
4. How is it that we can't ensure information security simply by implementing appropriate technology?
5. If a manager rages at employees who violate new security procedures, how can you calm her down using insights into the corporate-culture model of security compliance?
6. How would you summarize the practical goals of a security-awareness program?

22

Copyright © 2012 M. E. Kabay. All rights reserved.

Review Questions (2)



7. Why do the needs of your audience matter to you in a security awareness program? How would such factors influence your program?
8. Explain why security awareness programs work well by appealing to attitudes or preferences rather than to beliefs and behaviors.
9. Why should a security-awareness program be positive rather than negative?
10. Explain why it is valuable to define the benefits of security from the perspective of the audience rather than from the perspective of the organization.

23

Copyright © 2012 M. E. Kabay. All rights reserved.

Review Questions (3)



11. Analyze and explain each of the Awareness Principles enunciated in this chapter and these notes.
12. Why can it be useful to teach employees how to protect their families against computer dangers?
13. Why is it effective to involve employees as presenters in security-awareness programs?
14. What's the point of evaluating outcomes of security-awareness programs?

24

Copyright © 2012 M. E. Kabay. All rights reserved.