Information Security and Privacy
Awareness Materials Design and Development

Rebecca Herold, CISM, CISSP, CISA, FLMI

Educating with training is generally for those within the organization whose roles require special knowledge and following specific policies and procedures for addressing information security and privacy issues and events. Training is focused on providing knowledge, skills and abilities specific to a person's job responsibilities and roles. Training is a targeted, interactive event requiring the participant's full attention in order to benefit.

Educating with awareness methods is not training. In contrast to training, awareness can occur at the same time everywhere and on a continuous basis. Information security and privacy awareness activities promote ongoing compliance. Likewise, ongoing compliance helps ongoing awareness. As business models change so do compliance needs and awareness activities.

Awareness audiences are very broad; they include everyone within the organization and all those third parties who do work for, or on behalf of, the organization. The awareness audience has diverse experiences, backgrounds and job responsibilities. The awareness goal at the decision-making level is to convince the audience that information security and privacy risk reduction is achievable. Awareness goals at the end user level are to help them:

1. Understand information security and privacy risks and the actions to reduce them; and
2. Create a demand for risk reduction.

Awareness is typically the "what" component of your education strategy; training is typically the "how" component. To make awareness activities effective you must know your audience.

Awareness must not be boring. Fifteen ways to make awareness interesting:

1. Use analogies
2. Use recent, significant real-world examples and news events
3. Explain the importance of your message
4. Use scenarios and multifaceted situations (e.g., what would you do if?…)
5. Use graphics
6. Use photos and videos
7. Make it interactive
8. Make it memorable…use humor, shock, wit
9. Make it personal…show how it relates to your audience
10. Make it fresh…tie it to something current
11. Provide practical, "job-ready" information
12. Use known people in examples…celebrities, sports figures, etc.
13. Use animation
14. Recognize employees who have done an outstanding job
15. Use games and challenges

Awareness activities are different from training activities. The objectives for delivering information security and privacy awareness are similar to training options. However, there are some very important differences between training and awareness activities. The

© 2004 Rebecca Herold, CISM, CISSP, CISA, FLMI
All rights reserved

options and methods for awareness activities are typically much different than the more formal and structured training. Awareness activities should:

- Occur on an ongoing basis
- Use a wide range of delivery methods
- Catch the attention of the target audience
- Be less formal than training
- Take less time than training
- Be creative, memorable and fun
- Reinforce the lessons learned during formal training

An awareness program must remain current. As information security and privacy regulations change, and subsequently information security and privacy and security policies and procedures, personnel must be notified. Establish a method to deliver immediate information and updates when necessary. Perhaps new information is sent as the first alert item personnel see when logging into the network for the day. The awareness messages and methods must also be simple. The purpose is to get messages and ideas out to personnel quickly and easily. They cannot be confusing or convoluted so as to dissuade personnel from reading them, and eventually not paying attention at all to the messages. Make it easy for personnel to get information security and privacy and security information, and make the information easy to understand.

Think of positive, fun, exciting, and motivating methods that will give employees the message and keep the information security and privacy issues in their mind as they perform their daily job responsibilities. The success of an awareness program is the ability to reach all personnel using a variety of techniques. Examples of awareness materials and methods include the following (find approximately 60 more examples in addition to these within my book Managing an Information Security and Privacy Awareness and Training Program):

1. Invite guest speakers to give presentations and talks about information security and privacy topics
2. Obtain a celebrity endorsement of your organization's customer information security and privacy goals; use the endorsement internally and within marketing materials
3. Host information privacy and/or security awareness days
4. Create customer information security and privacy newsletters
5. Create employee information security and privacy newsletters
6. Write and publish articles in enterprise-wide newsletters and publications
7. Maintain Intranet web sites with security and privacy tips and guidance
8. Display information security and privacy posters: in parking lots, cafeterias, vending areas, meeting rooms, teams locations, restrooms, and so on. Some organizations have indicated increased awareness by posting on the inside of restroom stall doors.
9. Post information security and privacy banners over doorways
10. Include information security and privacy pamphlets within personnel paycheck envelopes
11. Send direct mailings of pamphlets or letters to personnel homes

© 2004 Rebecca Herold, CISM, CISSP, CISA, FLMI
All rights reserved

12. Hold staff and team meeting discussions during a set time each week, month or quarterly
13. Host team or department retreats to discuss security and privacy issues
14. Establish information security and privacy mascots
15. Establish information security and privacy taglines
16. Establish information security and privacy logos
17. Place attention-grabbing and recurring headlines on the intranet
18. Host information security and privacy lunch presentations
19. Hold departmental presentations
20. Hold organization-wide presentations
21. Post motivational or catchy slogans on screen savers, browser marquees, and so on
22. Display a random information security and privacy tip (see http://www.infostruct.net/sectips/ for example of this done with information security tips)
23. Make information security and privacy videotapes available in the corporate library
24. Hold showings of information security and privacy videotapes
25. Make computer-based awareness quizzes, game and so on available
26. Print and distribute brochures and fliers
27. Distribute pens, pencils, key chains, note pads, post-it notes and other types of promotional items with short information security and privacy messages.
28. Provide information security and privacy stickers for doors and bulletin boards
29. Publish cartoons and/or articles monthly or quarterly in in-house newsletter or specific department notices
30. Post an information security and privacy thought or advice of the day or week
31. Print and distribute special topical bulletins
32. Monthly email notices related to information security and privacy issues
33. Implement privacy and security banners or pre-logon messages that appear on the computer monitor
34. Distribute food items with awareness messages. For example, packages of chocolate that have attached labels with sayings like, "Maintaining Privacy is Sweet."
35. Provide a travel first aid kit with an information security and privacy slogan printed on the package, such as "Help ensure healthy information security and privacy "
36. Provide badge holders with an information security or privacy slogan, such as "Protect Privacy" or "Think Private Thoughts"
37. Distribute flashlights with a label similar to, "Spotlight information security and privacy"
38. Provide public information security and privacy law information to personnel
39. Send occasional messages to executives with security and privacy guidance
40. Provide links to Federal information security and privacy reports
41. Post an information security and privacy reading list
42. Post an information security and privacy Web-sites list
43. Post information security and privacy related templates
44. Post an information security and privacy glossary

45. Send pre-recorded voice mails with information security and privacy messages from executives to targeted groups and personnel
46. Send pre-recorded voice mails with information security and privacy messages from executives to all organizational members
47. Show movies related to and supporting information security and privacy. For example, the James Woods movie, "The Billion Dollar Bubble" is a good one to show the need for internal controls.
48. Browser pop-ups with information security and privacy messages
49. Post information security and privacy messages within the logon notification banner that change weekly or monthly
50. Observe International Computer Security Day activities (November 30)
51. Post instructions to users about how to backup their information from their personal devices
52. Post reminders about business continuity contacts for each department or team
53. Hold an information privacy and security poster contest
54. Host demonstrations of security and/or privacy software used by your organization
55. Pick a privacy or information security policy and publicize it each month, explaining why the policy is needed
56. Publicize recent news about information privacy and security on an intranet site
57. Place new information security or privacy tips each week or month within your network logon banner
58. Have a drawing and give the winners a copy of an information security and/or privacy book
59. Give an information privacy and security presentation at your organization's intern or children's schools
60. Recognize an employee each month as being outstanding for his or her information security and privacy practices
61. Host chat sessions to provide computer users with a basic understanding of computer security
62. Post an information security and privacy tip list in the computer operations room
63. Select a computer system on which to perform a risk analysis and communicate the results to the department personnel, indicating how they each can contribute to improve the outcome
64. Hold a discussion of ethics with computer users
65. Volunteer to speak about computer security or information privacy at a local computer club or school
66. Post information on your intranet site about how other organizations recognize International Computer Security Day
67. Participate in a local computer security or privacy meeting or seminar
68. Attend a national information security and privacy conference or seminar and report back to coworkers the highlights
69. Circulate email alerts to appropriate audiences when new information security and privacy laws are enacted

© 2004 Rebecca Herold, CISM, CISSP, CISA, FLMI
All rights reserved

70. Hold an information security and privacy organization-wide "Jeopardy" type of contest event
71. Hold monthly or quarterly drawings and give away security software to personnel to use on their home systems (for example, personal firewalls, anti-virus software, and so on)
72. Have an information security and privacy theme for your organization's cafeteria menu
73. Locate information security and privacy bulletin boards throughout the facilities
74. Provide laptop users with physical security locks (such as Kensington locks) to protect their device while traveling
75. Print and distribute cards to people with handheld computing devices giving tips on how to protect the devices from theft and loss
76. Implement information security and privacy screensavers
77. Make online information security and privacy slide presentations available to personnel
78. Provide personnel and business partners an information security checklist
79. Provide personnel and business partners an information privacy checklist
80. Provide an occasional information security or privacy announcement over the loud speaker
81. Provide mobile and home workers with surge protector strips and UPS devices
82. Incorporate information security and privacy practices into the job appraisal process
83. Provide personal privacy self-assessments on cards or posters for personnel
84. Create an information security and privacy suggestion "box" area on your intranet for ideas on how to improve
85. Award 4 or 8 hours of vacation time to personnel who are the first to notify the security or privacy area of a significant new security or privacy risk or threat

It is critical to remember that an awareness program never ends. An effective awareness program must repeat your message many times in many ways. The more important the message, the more often it should be repeated using multiple methods. Because it is an ongoing activity, it requires creativity and enthusiasm to maintain the interest of all audience members. Awareness messages must demonstrate that information security and privacy are important not only to your organization, but also to each employee, customer and business partner.

Rebecca Herold, CISSP, CISM, CISA, FLMI is an independent information security, privacy and compliance consultant, author and instructor. She can be reached at rebeccaherold@rebeccaherold.com or 515-491-1564. Rebecca has a B.S. in Math & Computer Science, an M.A. in Computer Science & Education, created "The Privacy Papers," co-authored "The Practical Guide to HIPAA Privacy and Security Compliance," and authored "Managing an Information Security and Privacy Awareness and Training Program" all published by Auerbach.

© 2004 Rebecca Herold, CISM, CISSP, CISA, FLMI
All rights reserved