

Managing an

**Information
Security**

and

**Privacy
Awareness
and Training
Program**

Rebecca Herold



Auerbach Publications
Taylor & Francis Group

Contents

1	Brief History of Corporate Information Security and Privacy Awareness and Training.....	1
	Once Upon a Time.....	1
	Welcome to the Information Age.....	3
	Information Security and Privacy Education	3
	Current Challenges Bring Changes in Professional Education	4
	Notes	4
2	Why Training and Awareness Are Important	5
	Regulatory Requirements Compliance.....	6
	Customer Trust and Satisfaction	7
	Compliance with Published Policies	8
	Due Diligence	8
	Corporate Reputation.....	13
	Accountability	15
	Notes	16
3	Legal and Regulatory Requirements for Training and Awareness	19
	Awareness and Training Needs	20
	Legal Considerations	21
	Copyright Considerations	23
	Specific Regulatory Education Requirements	23
	HIPAA.....	24
	21 CFR Part 11 (Electronic Records/Electronic Signatures).....	25
	Bank Protection Act: 12CFR Chapter V §568.....	25
	Computer Security Act.....	25
	CFAA.....	26
	Privacy Act (Applies to U.S. Government Agencies).....	26
	FOIA	27
	FISMA	27

OPM Security Awareness and Training Regulations (5 U.S.C. §930.301 for Federal Offices)	28
Appendix III to OMB Circular No. A-130	29
DMCA	30
GLBA	31
Department of Transportation DOT HM-232	31
SOX Act	31
Title IV Section 406 — Code of Ethics for Senior Financial Officers	32
1980 OECD Privacy Guidelines	32
PIPEDA	32
Notes	33
4 Incorporating Training and Awareness into Job Responsibilities and Appraisals	35
Motivation Factors	36
Motivation through Job Appraisals and Responsibilities	39
Methods of Security and Privacy Objectives Assessments	40
Performance against Specific Privacy and Security Objectives	41
Using Appraisal Results	43
Considering Security and Privacy within Job Performance as a Whole	43
Paying for Performance	46
Additional Percentage Element Added to Pay	47
Controlling the Amount and Distribution of the Awards	47
Applying Security and Privacy ARP to Certain Groups of Employees	49
Individual Security and Privacy Plans	50
Implementing the Individual Plan	51
Enforcing the Individual Plan	52
Challenges	53
Notes	53
5 Common Corporate Education Mistakes	55
Throwing Education Together Too Quickly	56
Not Fitting the Environment	56
Not Addressing Applicable Legal and Regulatory Requirements	57
No Leadership Support	57
Budget Mismanagement or No Budget	57
Using Unmodified Education Materials	57
Information Overload	57
No Consideration for the Learner	58
Poor Trainers	58
Information Dumping	58
No Motivation for Education	59
Inadequate Planning	59
Not Evaluating the Effectiveness of Education	59
Using Inappropriate or Politically Incorrect Language	59
Notes	60

6	Getting Started.....	61
	Determine Your Organization's Environment, Goals, and Mission	61
	Identify Key Contacts	62
	Review Current Training Activities	64
	Review Current Awareness Activities	64
	Conduct a Needs Assessment	65
	Create Your Road Map	70
	Sample Information Privacy and Security Awareness and Training Road Map	71
	Event and Situation Triggers	72
	Elements of an Effective Education Program	73
7	Establish a Baseline.....	75
	Hard Data	76
	Soft Data	76
	Benefits of a Baseline.....	76
8	Get Executive Support and Sponsorship	85
	Executive Security and Privacy Training and Awareness Strategy	
	Briefing	86
	Communicate Program Roles	88
	Education Program Success Indicators	89
	Demonstrate Importance	89
	Provide Examples of Security and Privacy Impacting Events.....	89
	Demonstrate How Security and Privacy Incidents Are Increasing.....	91
	Demonstrate How Information Security and Privacy Is a Core Business Issue	91
	Communicate the Increasing Security and Privacy Threats and Breaches.....	93
	Security and Privacy-Related Laws Impact Business.....	95
	The Financial Impact of Privacy on Business	96
	Communicate Leading Practices to Executives.....	98
	Note.....	99
9	Identify Training and Awareness Methods.....	101
	Adult Learning.....	101
	Readiness	102
	Sample Scenario	102
	Experience	102
	Sample Scenario	103
	Autonomy	103
	Sample Scenario	103
	Action	104
	Sample Scenario	104
	Training Delivery Methods.....	104
	General Lectures: Small- to Medium-Size Groups.....	105
	Auditorium Presentations to Large Groups	105
	Classroom.....	106
	CBT Modules	107

Entertaining.....	107
Subject Matter-Focused	112
Skills-Based	112
CBT Audiences.....	113
Remote Access Labs.....	113
Satellite or Fiber Optics Long-Distance Learning.....	114
Web-Based Interactive Training (such as Webinars).....	114
Audio Instruction	115
Video and DVD	115
Workbooks.....	116
On-the-Job (OTJ)	117
Conference Calls	118
Outsourced Training and Awareness with Professional Education Services	118
Education Provided by Professional Societies.....	119
Government-Sponsored Training.....	120
Awareness Methods	120
Notes.....	122
10 Awareness and Training Topics and Audiences.....	123
Target Groups	124
Topics.....	126
1. Information Security and Privacy Policies and Procedures	126
2. Information Security and Privacy Framework and Architecture	126
3. Security of Third-Party Access.....	126
4. Security and Privacy for Outsourced Services	127
5. Information Classification and Controls.....	127
6. Security and Privacy in Job Definitions and Performance Appraisals	127
7. Security and Privacy Incident Response.....	128
8. Physical Security	128
9. Computing Equipment Security.....	128
10. Work Area Security and Privacy.....	129
11. Operational Procedures and Responsibilities	129
12. Systems Planning and Acceptance	129
13. Protecting against Malicious Software.....	129
14. Backups and Logging.....	130
15. Network Security and Privacy Controls	130
16. Media Handling and Security	130
17. Exchanging Information and Software between Organizations	130
18. Business Requirements for Systems Access Control.....	131
19. IT User Access Management	131
20. Information and Systems User Responsibilities.....	131
21. Network Access Control.....	132
22. Operating Systems Access Control.....	132
23. Application Access Control.....	132
24. Monitoring Systems Access and Use.....	133
25. Mobile and Remote Computing	133

26. Security and Privacy Requirements of Systems.....	133
27. Security and Privacy in Application Systems	134
28. Cryptographic Controls.....	134
29. System Files Security	134
30. Security and Privacy in Development and Support Environments	135
31. Security for Outsourced Services	135
32. Business Continuity Planning	135
33. Information Security and Privacy Laws, Regulations, and Standards	136
34. Personal Information Privacy.....	136
35. Collection of Electronic Evidence	137
36. Security and Privacy Compliance Reviews and Audits	137
37. Systems Audit Controls and Tools	137
38. Security and Privacy Tools.....	137
39. Customer and Consumer Interactions (Customer Relationship Management).....	138
40. Asset Management Security and Privacy Issues.....	139
41. Electronic Commerce.....	139
42. Social Engineering	139
43. Data and Records Retention	139
44. Third Party and Partners	140
45. Transborder Data Flow	140
46. Due Diligence	140
47. PII, PHI, NPPI, and Other Information	140
48. E-Mail Security and Privacy	141
49. Identity Verification.....	141
50. Ethics.....	141
51. Policies.....	142
52. Procedures.....	142
53. Data Classification.....	142
54. Fraud Identification and Prevention	142
55. Incident Response.....	143
56. OECD Privacy Principles.....	143
57. Web Site Privacy Policies.....	144
58. Customer Privacy Communications.....	144
59. Exiting Personnel Security and Privacy	144
Mapping Topics to Roles and Target Groups	144
Standards and Principles	146
OECD	146
ISO/IEC 17799	148
NIST.....	149
COBIT	149
Draft 2004 The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Framework	150
Notes	151

11	Define Your Message.....	153
	Customer Privacy	154
	Laws and Regulations.....	156
	Access Controls.....	159
	Risk Management.....	163
12	Prepare Budget and Obtain Funding.....	167
	Obtain Traditional Funding if You Can	167
	Obtain Nontraditional Funding When Necessary.....	173
	Final Budget and Funding Thoughts	177
13	Training Design and Development.....	179
	Training Methods	179
	Design and Development	181
	Pitfalls to Avoid.....	181
	Design	182
	Development	182
	Choosing Content	184
	Core Content	185
	Targeted Content.....	185
	Job-Specific Content and Topics for Targeted Groups.....	187
	Learning Activities.....	192
	Training Design Objectives	194
	Note.....	194
14	Awareness Materials Design and Development	195
	Contrasting Awareness and Training.....	195
	Make Awareness Interesting	197
	Awareness Methods	197
	Awareness Is Ongoing.....	205
	Developing Awareness Activities and Messages	205
	Bimonthly Customer Privacy Newsletters	207
15	Communications	209
	1. Identify Where You Need to Improve, Update, or Create	
	Information Security and Privacy Training and Awareness	210
	2. Obtain Executive Sponsorship	210
	Launch Information Security and Privacy Education	
	Communications.....	211
	Executive Security and Privacy Training Announcement	212
	3. Communicate Information Security and Privacy	
	Program Overview	212
	4. Send Target Groups Communications Outlining the Information	
	Security and Privacy Training and Awareness Schedules and Their	
	Participation Expectations	212
	Plan and Establish Awareness and Training Deployment.....	213
	Deployment Timeline	213
	Presentation Slides	215

More Ideas.....	215
Communications Checklist	216
Sample Communication Plan Documents.....	216
16 Deliver In-Person Training.....	221
What to Avoid in Training	222
Multinational Training Considerations.....	223
Delivering Classroom Training.....	224
Tips for Trainers.....	226
Visual Aids.....	228
Training in Group Settings.....	229
Case Studies.....	232
Note.....	233
17 Launch Awareness Activities	235
1. Identify Areas in Which You Need to Improve, Update, or Create Awareness.....	236
2. Obtain Executive Sponsorship	237
3. Communicate the Information Security and Privacy Program Overview	237
4. Identify Trigger Events.....	237
5. Identify Target Groups.....	237
6. Identify Your Awareness Methods and Messages	239
7. Evaluate Changed Behavior	239
8. Update and Perform Ongoing Awareness	239
Plan for Specific Events.....	241
Sample Plan for Privacy Awareness Day	242
18 Evaluate Education Effectiveness	243
Evaluation Areas.....	244
Evaluation Methods.....	245
Evaluating Education Effectiveness: Intangible Benefits.....	246
Determining Intangible Benefits of Training and Awareness	278
Employees and Training Participants	278
Managers, Trainers, and HR.....	279
Evaluating the Effectiveness of Specific Awareness and Training Methods	280
Evaluating the Effectiveness of Computer-Based Training Modules ...	280
When Does CBT Training Make Sense?.....	281
Launching CBT Training.....	281
Managing CBT Participation.....	283
Effectiveness Evaluation Methods.....	287
Evaluating the Effectiveness of Awareness Newsletters	287
Sampling	287
Sampling Procedures	288
Sampling Approaches	288
Determining Sample Size	289
Surveys Composition	291

Survey Questions	292
Survey Administration.....	293
Education Effectiveness Evaluation Framework Activities Checklist	293
Notes	303

19 Leading Practices.....305

Consulting for a Federal Organization to Improve Its Training and Awareness Program	305
Data Collection.....	306
Analysis	308
Documenting Findings and Recommendations	308
Postimplementation.....	309
Case Study: 1200 Users, 11 Cities, in 7 Weeks ... and They <i>Wanted</i> to Come to Security Awareness Training.....	310
The Problem.....	311
Review Videos.....	311
Enter Creativity, Collaboration, and Conceptualization	311
Toys, Toys, and More Toys!.....	312
The Training Scenario.....	312
The One-Hour Agenda — Don't PowerPoint Them To Death.....	314
Logistics: Success Is in the Details	315
Pretraining Planning.....	315
Class Sizes and Scheduling	315
Session Planning for Each Location	316
99 Percent of Evaluations Returned	317
Makeup Sessions	317
Final Thoughts.....	318
Obtaining Executive Sponsorship for Awareness and Training.....	318
Recognizing Business Benefit	319
Security Metrics	320
Professional Delivery	321
Information Assurance Awareness Programs in Multinational Manufacturing Organizations	322
Introduction	322
The Approach.....	323
Steering Committee and Product Selection.....	324
The "Security Community" IAAP	324
Management Support.....	325
Test Panels and IAAP Introduction	326
IAAP Rollout.....	326
Lessons Learned	327
Conclusion	329
ISO 17799 Awareness for IT Managers Requires Security Mindset Changes: Putting the Cart before the Horse	329
The Challenge: Obtaining Buy-In and Support for Implementing ISO 17799-Based Policy and Standards	330
The Goal.....	330

The Process: Putting the Cart before the Horse	331
The Outcome	334
Education and Awareness for Security Personnel	334
Overview	335
The Basics	335
Security Administrator	336
Monitoring and Compliance	336
Designers and Architects	337
Security Consultant	338
Education and Awareness (E&A) Staff	338
In Conclusion	339
Security Awareness via E-Learning: A Case Study	339
What's the Speed of Dark? Enlightenment through Education	345
Aetna's Award-Winning Security Awareness Program	351
Aetna's Security Awareness Program	351
Four Basic Concepts	352
User Life Cycle and Delivery Mechanisms Expanded	356
1. Orientation	356
2. Retained Users	357
3. Exiting Users	365
Closing Comments	365
Addendum: How to Build a Custom Web-Based InfoSec Exam	366
Web-Based InfoSec Exam Development	367
Security Awareness Case Study	369
Security Awareness Framework	369
Security Awareness Techniques	370
A Complete Security Awareness Program	371
Conclusion	374

APPENDICES

A	Sample Executive Education Sponsorship Memo	375
B	Training Contact Training Data Collection Form	377
C	Effectiveness Evaluation Framework	379
D	Sample Privacy Roles Definitions	389
E	Suggested Customer Privacy Awareness and Training Strategy Announcement as Voice Mail Message	395
F	Security and Privacy Icon or Mascot	397
G	Sample Privacy Training Survey	405
H	Customer Privacy Sample Training Plans	409

I	Advocate and SME Interview Questions to Assist with Customer Privacy Training Development.....	413
J	Training and Awareness Inventory	419
K	Incorporating Training and Awareness into the Job Appraisal Process Interview/Questionnaire	423
L	Training Contact Data Collection and Evaluation Form	425
M	Sample Customer Privacy Awareness and Training Presentation	427
N	Designated Security and Privacy-Related Days.....	437
O	Education Costs Worksheet	441
P	Sample Pretraining/Awareness Questionnaire	447
Q	Security Awareness Quiz Questions	449
R	Consumer Privacy Pop Quiz	459
S	Information Security and Privacy Awareness and Training Checklist	467
T	Awareness and Training Resources.....	471
U	Awareness and Training Glossary	477
V	Sample Case Studies	493
	Index.....	499