

Contents

FOREWORDS	xi	
PREFACE	xv	
ABOUT THE AUTHORS.....	xvii	
ACKNOWLEDGMENTS	xix	
CHAPTER 1	What Is a Security Awareness Program?	1
	Introduction.....	1
	Policy Development.....	4
	Policy Enforcement	4
	Cost Savings	5
	Production Increases.....	5
	Management Buy-In	6
	Notes.....	7
CHAPTER 2	Threat	9
	The Motivations of Online Attackers.....	9
	Money.....	9
	Industrial Espionage/Trade Secrets	10
	Hactivism	10
	Cyber War	11
	Bragging Rights	12
	Notes.....	12
CHAPTER 3	Cost of a Data Breach.....	15
	Ponemon Institute	15
	HIPAA	15
	The Payment Card Industry Data Security Standard (PCI DSS).....	19
	State Breach Notification Laws.....	20
	Notes.....	23



CHAPTER 4	Most Attacks Are Targeted.....	25
	Targeted Attacks	25
	Recent Targeted Attacks	26
	Targeted Attacks Against Law Firms	26
	Operation Shady RAT.....	28
	Operation Aurora.....	29
	Night Dragon	30
	Watering Hole Attacks.....	30
	Common Attack Vectors: Common Results	31
	Notes.....	32
CHAPTER 5	Who Is Responsible for Security?	33
	Information Technology (IT) Staff	33
	The Security Team.....	34
	The Receptionist.....	34
	The CEO	34
	Accounting	35
	The Mailroom/Copy Center	35
	The Runner/Courier.....	35
	Everyone Is Responsible For Security	35
	Notes.....	37
CHAPTER 6	Why Current Programs Don't Work	39
	The Lecture Is Dead as a Teaching Tool.....	39
	Notes.....	43
CHAPTER 7	Social Engineering	45
	What is Social Engineering?.....	45
	Who are Social Engineers?	46
	Why Does It Work?	46
	How Does It Work?.....	46
	Information Gathering	47
	Attack Planning and Execution	49
	The Social Engineering Defensive Framework (SEDF)	52
	Where Can I Learn More About Social Engineering?.....	63
	Notes	63
CHAPTER 8	Physical Security.....	65
	What is Physical Security?	65
	Physical Security Layers	66
	Threats to Physical Security	67
	Why Physical Security is Important to an Awareness Program	67
	How Physical Attacks Work	68

	Minimizing the Risk of Physical Attacks.....	79
	Notes.....	80
CHAPTER 9	Types of Training	81
	Training Types	81
	Formal Training.....	81
	Informal Training.....	85
	Notes.....	87
CHAPTER 10	The Training Cycle	89
	The Training Cycle.....	89
	New Hire	89
	Quarterly.....	90
	Biannual.....	90
	Continual.....	90
	Point of Failure.....	91
	Targeted Training	91
	Sample Training Cycles.....	92
	Adjusting Your Training Cycle.....	93
	Notes.....	93
CHAPTER 11	Creating Simulated Phishing Attacks	95
	Simulated Phishing Attacks	95
	Understanding the Human Element.....	95
	Methodology.....	95
	Open-Source Tool, Commercial Tool, or Vendor Performed?	96
	Before You Begin	100
	Determine Attack Objective.....	101
	Select Recipients.....	102
	Select a Type of Phishing Attack	102
	Composing the E-mail.....	103
	Creating the Landing Page.....	104
	Sending the E-mail.....	105
	Tracking Results.....	106
	Post Assessment Follow-up	107
	Notes.....	107
CHAPTER 12	Bringing It All Together.....	109
	Create a Security Awareness Website.....	109
	Sample Plans.....	110
	Promoting Your Awareness Program.....	116
	Notes.....	117



CHAPTER 13	Measuring Effectiveness	119
	Measuring Effectiveness	119
	Measurements vs. Metrics	119
	Creating Metrics	119
	Additional Measurements	121
	Reporting Metrics	122
	Notes	124
CHAPTER 14	Stories from the Front Lines.....	125
	Phil Grimes	125
	Amanda Berlin	128
	Jimmy Vo.....	133
	Security Research at Large Information Security Company.....	135
	Harry Regan.....	137
	Tess Schrodinger.....	140
	Security Analyst at a Network Security Company.....	151
	Ernie Hayden	154
APPENDICES		159
INDEX		191