Contents at a Glance

Introduction 1

Part 1: Getting to Know Security Awareness 5

CHAPTER 1: Knowing How Security Awareness Programs Work 7

CHAPTER 2: Starting On the Right Foot: Avoiding What Doesn't Work 19

CHAPTER 3: Applying the Science Behind Human Behavior and Risk Management 33

Part 2: Building a Security Awareness Program 51

CHAPTER 4: Creating a Security Awareness Strategy 53

CHAPTER 5: Determining Culture and Business Drivers 61

CHAPTER 6: Choosing What to Tell The Users 75

CHAPTER 7: Choosing the Best Tools for the Job 89

CHAPTER 8: Measuring Performance 107

Part 3: Putting Your Security Awareness Program Into Action 119

CHAPTER 9: Assembling Your Security Awareness Program 121

CHAPTER 10: Running Your Security Awareness Program 143

CHAPTER 11: Implementing Gamification 165

CHAPTER 12: Running Phishing Simulation Campaigns 181

Part 4: The Part of Tens 207

CHAPTER 13: Ten Ways to Win Support for Your Awareness Program 209

CHAPTER 14: Ten Ways to Make Friends and Influence People 215

CHAPTER 15: Ten Fundamental Awareness Topics 221

CHAPTER 16: Ten Helpful Security Awareness Resources 227

Appendix: Sample Questionnaire 233

Index 253

COPYRIGHTED MATERIAL

Table of Contents

INTRODUCTION 1
About This Book 1
Foolish Assumptions 2
Icons Used in This Book 3
Beyond the Book 3
Where to Go from Here 4

PART 1: GETTING TO KNOW SECURITY AWARENESS 5

CHAPTER 1: Knowing How Security Awareness Programs Work 7
Understanding the Benefits of Security Awareness 8
Reducing losses from phishing attacks 8
Reducing losses by reducing risk 9
Grasping how users initiate loss 10
Knowing How Security Awareness Programs Work 11
Establishing and measuring goals 12
Showing users how to "do things right" 14
Recognizing the Role of Awareness within a Security Program 15
Disputing the Myth of the Human Firewall 16

CHAPTER 2: Starting On the Right Foot: Avoiding What Doesn't Work 19
Making a Case Beyond Compliance Standards 20
Treating Compliance as a Must 21
Motivating users to take action 22
Working within the compliance budget 22
Limiting the Popular Awareness Theories 23
Applying psychology to a diverse user base 23
Differentiating between marketing and awareness 24
Distinguishing Social Engineering from Security Awareness 26
Addressing Mental Models That Don't Work 27
Making Perfection the Stated Goal 28
Measuring from the Start 29
Prioritizing Program Over Product 29
Choosing Substance Over Style 30
Understanding the Role of Security Awareness 31

CHAPTER 3: **Applying the Science Behind Human Behavior and Risk Management** 33
Achieving Common Sense through Common Knowledge 34
Borrowing Ideas from Safety Science 35
Recognizing incidents as system failures 36
Responding to incidents 37
Applying Accounting Practices to Security Awareness 37
Applying the ABCs of Awareness 39
Benefiting from Group Psychology 40
The ABCs of behavioral science 41
The Fogg Behavior Model 42
Relating B:MAP to the ABCs of awareness and behavior 43
The Forgetting Curve 44
Remembering That It's All About Risk 45
Optimizing risk 46
The risk formula 46

PART 2: BUILDING A SECURITY AWARENESS PROGRAM 51

CHAPTER 4: **Creating a Security Awareness Strategy** 53
Identifying the Components of an Awareness Program 54
Choosing effective communications tools 55
Picking topics based on business drivers 56
Knowing when you're a success 57
Figuring Out How to Pay for It All 58

CHAPTER 5: **Determining Culture and Business Drivers** 61
Understanding Your Organization's Culture 62
Determining security culture 64
Recognizing how culture relates to business drivers 65
Identifying Subcultures 65
Interviewing Stakeholders 67
Requesting stakeholder interviews 67
Scheduling the interviews 70
Creating interview content 70
Taking names 72
Partnering with Other Departments 72

CHAPTER 6: **Choosing What to Tell The Users** 75
Basing Topics on Business Drivers 76
Incorporating Personal Awareness Topics 76
Motivating Users to Do Things "Right" 77
Common Topics Covered in Security Awareness Programs 79

Phishing 79
Social engineering 80
Texting and instant messaging security 80
Physical security 81
Malware 81
Ransomware 81
Password security 82
Cloud security 82
USB device security 82
Internet of Things 83
Travel security 83
Wi-Fi security 84
Mobile devices 84
Work from home 84
Basic computer security 85
Insider threat 85
Protecting children on the internet 85
Social media security 86
Moving security 86
Compliance topics 87

CHAPTER 7: **Choosing the Best Tools for the Job** 89
Identifying Security Ambassadors 90
Finding ambassadors 90
Maintaining an ambassador program 91
Knowing the Two Types of Communications Tools 92
Reminding users to take action 93
Requiring interaction from users 93
Exploring Your Communications Arsenal 95
Knowledgebase 95
Posters 96
Hardcopy newsletters 97
Monitor displays 97
Screen savers 98
Pamphlets 98
Desk drops 99
Table tents 99
Coffee cups or sleeves 99
Stickers 100
Mouse pads 100
Pens and other useful giveaways 100
Camera covers 101
Squishy toys and other fun giveaways 101
Active communications tools 101

CHAPTER 8: **Measuring Performance** 107
Knowing the Hidden Cost of Awareness Efforts 108
Meeting Compliance Requirements 109
Collecting Engagement Metrics 111
Attendance metrics 111
Likability metrics 112
Knowledge metrics 112
Measuring Improved Behavior 113
Tracking the number of incidents 113
Examining behavior with simulations 114
Tracking behavior with gamification 116
Demonstrating a Tangible Return on Investment 116
Recognizing Intangible Benefits of Security Awareness 117
Knowing Where You Started: Day 0 Metrics 118

PART 3: PUTTING YOUR SECURITY AWARENESS PROGRAM INTO ACTION 119

CHAPTER 9: **Assembling Your Security Awareness Program** . . . 121
Knowing Your Budget 122
Finding additional sources for funding 123
Allocating for your musts 125
Limiting your discretionary budget 126
Appreciating your team as your most valuable resource 126
Choosing to Implement One Program or Multiple Programs 127
Managing multiple programs 128
Beginning with one program 128
Gaining Support from Management 129
Devising a Quarterly Delivery Strategy 131
Ensuring that your message sticks 133
Distributing topics over three months 133
Deciding Whether to Include Phishing Simulations 136
Planning Which Metrics to Collect and When 137
Considering metrics versus topics 137
Choosing three behavioral metrics 138
Incorporating Day 0 metrics 138
Scheduling periodic updates 138
Biasing your metrics 139
Branding Your Security Awareness Program 139
Creating a theme 139
Maintaining brand consistency 140
Coming up with a catchphrase and logo 140
Promoting your program with a mascot 140

CHAPTER 10: **Running Your Security Awareness Program** 143
Nailing the Logistics 144
Determining sources or vendors 144
Scheduling resources and distribution 145
Contracting vendors 145
Recognizing the role of general project management 146
Getting All Required Approvals 146
Getting the Most from Day 0 Metrics 147
Creating Meaningful Reports 149
Presenting reports as a graphical dashboard 149
Adding index scores 152
Creating an awareness index 152
Reevaluating Your Program 153
Reconsidering your metrics 154
Evaluating your communications tools 155
Measuring behavioral changes 156
Redesigning Your Program 157
Anything stand out? 158
Adding subcultures 158
Adding, deleting, and continuing metrics 159
Adding and discontinuing communications tools 159
Revisiting awareness topics 160
Considering Breaking News and Incidents 161

CHAPTER 11: **Implementing Gamification** 165
Understanding Gamification 166
Identifying the Four Attributes of Gamification 168
Figuring Out Where to Gamify Awareness 169
Examining Some Tactical Gamification Examples 170
Phishing reporting 170
Clean desk drops 171
Tailgating exercises 172
USB drop reporting 173
Reporting security incidents 173
Ad hoc gamification 174
Putting Together a Gamification Program 175
Determining reward tiers 175
Offering valid rewards 177
Assigning points to behaviors 178
Tracking users and the points they earn 179
Promoting the Program 179

CHAPTER 12: **Running Phishing Simulation Campaigns** 181
Knowing Why Phishing Simulations Matter 182
Setting Goals for Your Phishing Program 183
Checking the box 183
Producing easy metrics 183
Benefiting from just-in-time training 184
Differentiating between risky and secure users 184
Planning a Phishing Program 185
Identifying the players 185
Obtaining permission and buy-in 186
Allocating enough time for phishing simulations 187
Choosing responsive tools 187
Choosing a Phishing Tool 188
Creating custom phishing tools 188
Choosing vendor options 189
Implementing a Phishing Simulation Program 192
Integrating Active Directory 192
Working with subcultures and geographies 193
Choosing languages 193
Registering phishing domains 194
Defining program goals 194
Collecting Day 0 metrics 194
Running a Phishing Simulation 195
Determining the targets 195
Preparing the lures 196
Creating landing pages 200
Addressing logistical concerns 201
Conducting a pilot test 203
Tracking Metrics and Identifying Trends 204
Dealing with Repeat Offenders 205
Management Reporting 206

PART 4: THE PART OF TENS 207

CHAPTER 13: **Ten Ways to Win Support for Your Awareness Program** 209
Finding Yourself a Champion 209
Setting the Right Expectations 210
Addressing Business Concerns 211
Creating an Executive Program 211
Starting Small and Simple 212
Finding a Problem to Solve 212
Establishing Credibility 213
Highlighting Actual Incidents 213

Being Responsive 213
Looking for Similar Programs 214

CHAPTER 14: **Ten Ways to Make Friends and Influence People** 215
Garnering Active Executive Support 215
Courting the Organization's Influencers 216
Supporting Another Project That Has Support 216
Choosing Topics Important to Individuals 217
Having Some Fun Events 218
Don't Promise Perfection 218
Don't Overdo the FUD Factor 218
Scoring an Early Win 219
Using Real Gamification 219
Integrating the Organization's Mission Statement 220

CHAPTER 15: **Ten Fundamental Awareness Topics** 221
Phishing 221
Business Email Compromise 222
Mobile Device Security 222
Home Network and Computer Security 223
Password Security 223
Social Media Security 223
Physical Security 224
Malware and Ransomware 224
Social Engineering 225
It Can Happen to You 225

CHAPTER 16: **Ten Helpful Security Awareness Resources** 227
Security Awareness Special Interest Group 228
CybSafe Research Library 228
Cybersecurity Culture Guidelines 229
RSA Conference Library 229
You Can Stop Stupid 229
The Work of Sydney Dekker 230
Human Factors Knowledge Area 230
People-Centric Security 230
Human Security Engineering Consortium 231
How to Run a Security Awareness Program Course 231

APPENDIX: SAMPLE QUESTIONNAIRE 233

INDEX 253