

# **Building an Information Security Awareness Program**

*Defending Against Social Engineering  
and Technical Threats*

**Bill Gardner  
Valerie Thomas**

AMSTERDAM • BOSTON • HEIDELBERG • LONDON  
NEWYORK • OXFORD • PARIS • SAN DIEGO  
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

**ELSEVIER**

Syngress is an Imprint of Elsevier

# Contents

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

# Contents

<b>CHAPTER 4</b>	<b>Most Attacks Are Targeted</b>	<b>25</b>
	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
<b>CHAPTER 5</b>	<b>Who Is Responsible for Security?</b>	<b>33</b>
	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
<b>CHAPTER 6-</b>	<b>Why Current Programs Don't Work</b>	<b>39</b>
	The Lecture Is Dead as a Teaching Tool	39
	Notes	43
<b>CHAPTER 7</b>	<b>Social Engineering</b>	<b>45</b>
	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
<b>CHAPTER 8</b>	<b>Physical Security</b>	<b>65</b>
	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
<b>CHAPTER 9</b>	Types of Training	81
	Training Types	81
	Formal Training	81
	Informal Training	85
	Notes	87
<b>CHAPTER 10</b>	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
<b>CHAPTER 11</b>	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
<b>CHAPTER 12</b>	Bringing It All Together	109
	Create a Security Awareness Website	109
	Sample Plans	110
	Promoting Your Awareness Program	116
	Notes	117

<b>CHAPTER 13</b>	<b>Measuring Effectiveness</b>	<b>119</b>
	Measuring Effectiveness	119
	Measurements vs. Metrics	119
	Creating Metrics	119
	Additional Measurements	121
	Reporting Metrics	122
	Notes	124
<b>CHAPTER 14</b>	<b>Stories from the Front Lines</b>	<b>125</b>
	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
<b>APPENDICES</b>		<b>159</b>
<b>INDEX</b>		<b>191</b>