

# Contents

Dedication .....	v
Author Biography .....	xiii
Preface.....	xv

## SECTION I UNDERSTANDING THE PROBLEM

---

<b>CHAPTER 1 The Changing Threat.....</b>	<b>3</b>
Introduction.....	3
The Current Landscape.....	4
Organizations View on Security.....	5
You will be Compromised .....	6
The Cyber ShopLifter .....	7
The New Defense in Depth.....	8
Proactive vs Reactive .....	10
Loss of Common Sense .....	11
It is All About Risk .....	12
What Was In Place? .....	13
Pain Killer Security.....	14
Reducing the Surface Space .....	14
HTML Embedded Email .....	15
Buffer Overflows .....	15
Macros in Office Documents .....	16
The Traditional Threat .....	16
Common Cold.....	17
Reactive Security .....	17
Automation .....	17
The Emerging Threat .....	18
APT—Cyber Cancer.....	19
Advanced Persistent Threat (APT) .....	19
APT—Stealthy, Targeted, and Data Focused.....	21
Characteristics of the APT .....	22
Defending Against the APT .....	23
APT vs Traditional Threat .....	24
Sample APT Attacks .....	25
APT Multi-Phased Approach.....	25
Summary .....	26

<b>CHAPTER 2</b>	<b>Why are Organizations Being Compromised?.....</b>	<b>27</b>
	Introduction.....	27
	Doing Good Things and Doing the Right Things.....	28
	Security is Not Helpless.....	29
	Beyond Good or Bad .....	31
	Attackers are in Your Network.....	31
	Proactive, Predictive, and Adaptive .....	34
	Example of How to Win .....	37
	Data Centric Security.....	39
	Money Does Not Equal Security .....	40
	The New Approach to APT.....	41
	Selling Security to Your Executives.....	42
	Top Security Trends .....	46
	Summary .....	49
<b>CHAPTER 3</b>	<b>How are Organizations Being Compromised?.....</b>	<b>51</b>
	Introduction.....	51
	What are Attackers After?.....	53
	Attacker Process .....	53
	Reconnaissance.....	54
	Scanning .....	56
	Exploitation.....	57
	Create Backdoors.....	58
	Cover Their Tracks .....	58
	Compromising a Server .....	59
	Compromising a Client.....	65
	Insider Threat.....	66
	Traditional Security .....	69
	Firewalls.....	69
	Dropped Packets .....	71
	InBound Prevention and OutBound Detection .....	73
	Intrusion Detection .....	74
	Summary.....	75
<b>CHAPTER 4</b>	<b>Risk-Based Approach to Security.....</b>	<b>77</b>
	Introduction.....	77
	Products vs. Solutions.....	78
	Learning from the Past.....	78
	What is Risk?.....	79
	Focused Security.....	80
	Formal Risk Model.....	84

Threat..... 85  
 Vulnerability ..... 88  
 Known and Unknown Vulnerabilities ..... 90  
 Putting the Pieces Back Together ..... 92  
 Insurance Model ..... 95  
 Calculating Risk..... 96  
 Summary ..... 96

**SECTION II EMERGING TRENDS**

**CHAPTER 5 Protecting Your Data..... 99**

Introduction..... 99  
 Data Discovery ..... 100  
 Protected Enclaves ..... 101  
 Everything Starts with Your Data ..... 104  
 CIA ..... 106  
 Data Classification ..... 107  
     Data Classification Mistake 1 ..... 108  
     Data Classification Rule 1 ..... 108  
     Data Classification Mistake 2 ..... 109  
     Data Classification Rule 2 ..... 109  
     Data Classification Mistake 3 ..... 109  
     Data Classification Rule 3 ..... 109  
 Encryption..... 111  
 Types of Encryption..... 113  
 Goals of Encryption ..... 114  
 Data at Rest..... 115  
 Data at Motion ..... 116  
 Encryption—More Than You Bargained For..... 117  
 Network Segmentation and De-Scoping..... 118  
 Encryption Free Zone ..... 119  
 Summary ..... 121

**CHAPTER 6 Prevention is Ideal but Detection is a Must..... 123**

Introduction..... 123  
 Inbound Prevention..... 125  
 Outbound Detection..... 131  
 Network vs. Host ..... 136  
 Making Hard Decisions ..... 138  
 Is AV/Host Protection Dead? ..... 142  
 Summary ..... 143

<b>CHAPTER 7</b>	<b>Incident Response: Respond and Recover .....</b>	<b>145</b>
	Introduction.....	145
	The New Rule .....	147
	Suicidal Mindset .....	149
	Incident Response .....	151
	Events/Audit Trails .....	154
	Sample Incidents.....	156
	6-Step Process.....	159
	Preparation .....	160
	Identification .....	162
	Containment.....	164
	Eradication .....	166
	Recovery .....	167
	Lesson Learned.....	167
	Forensic Overview .....	167
	Summary.....	171
<b>CHAPTER 8</b>	<b>Technologies for Success .....</b>	<b>173</b>
	Introduction.....	173
	Integrated Approach to APT .....	175
	How Bad is the Problem? .....	176
	Trying to Hit a Moving Target.....	179
	Finding the Needle in the Haystack.....	182
	Understand What You Have .....	188
	Identifying APT .....	189
	Assessment and Discovery .....	191
	Analysis and Remediation .....	196
	Program Review.....	198
	Minimizing the Problem.....	201
	End to End Solution for the APT.....	202
	Summary.....	204
<b>SECTION III THE FUTURE AND HOW TO WIN</b>		
<b>CHAPTER 9</b>	<b>The Changing Landscape: Cloud and Mobilization.....</b>	<b>209</b>
	Introduction.....	209
	You Cannot Fight the Cloud .....	212
	Is the Cloud Really New? .....	213
	What is the Cloud?.....	214
	Securing the Cloud .....	215
	Reducing Cloud Computing Risks .....	218

Mobilization—BYOD (Bring Your Own Device) .....	219
Dealing with Future Technologies .....	220
Summary .....	222
<b>CHAPTER 10 Proactive Security and Reputational Ranking .....</b>	<b>223</b>
Introduction.....	223
Facing Reality .....	225
Predicting Attacks to Become Proactive.....	226
Advanced .....	227
Persistent.....	228
Threat.....	229
Changing How You Think About Security .....	230
The Problem has Changed.....	233
The APT Defendable Network .....	234
Summary .....	240
<b>CHAPTER 11 Focusing in on the Right Security .....</b>	<b>243</b>
Introduction.....	243
What is the Problem That is Being Solved? .....	244
If the Offense Knows More Than the Defense You Will	
Loose.....	247
Enhancing User Awareness.....	250
Virtualized Sandboxing .....	250
Patching .....	252
White Listing .....	253
Summary .....	254
<b>CHAPTER 12 Implementing Adaptive Security .....</b>	<b>255</b>
Introduction.....	255
Focusing on the Human .....	257
Focusing on the Data .....	262
Game Plan.....	265
Prioritizing Risks .....	267
Key Emerging Technologies.....	272
The Critical Controls .....	275
Summary .....	280
<b>INDEX.....</b>	<b>283</b>