CONTENTS

Foreword xiii
Preface xvii
Acknowledgments xxiii

1.0 INTRODUCTION 1
  1.1 Defining Cybersecurity 1
  1.2 Cybersecurity is a Business Imperative 2
  1.3 Cybersecurity is an Executive-Level Concern 4
  1.4 Questions to Ask 4
  1.5 Views of Others 7
  1.6 Cybersecurity is a Full-Time Activity 7

2.0 WHY BE CONCERNED? 9
  2.1 A Classic Hack 9
  2.2 Who Wants Your Fortune? 12
  2.3 Nation-State Threats 13
    2.3.1 China 13
    2.3.2 Don’t Think that China is the Only One 17
  2.4 Cybercrime is Big Business 20
    2.4.1 Mercenary Hackers 20
    2.4.2 Hacktivists 25
    2.4.3 The Insider Threat 26
    2.4.4 Substandard Products and Services 29
  2.5 Summary 36

3.0 MANAGING RISK 37
  3.1 Who Owns Risk in Your Business? 37
  3.2 What Are Your Risks? 38
3.2.1 Threats to Your Intellectual Property and Trade Secrets 38
3.2.2 Technical Risks 42
3.2.3 Human Risks 47
3.3 Calculating Your Risk 54
  3.3.1 Quantitative Risk Assessment 55
  3.3.2 Qualitative Risk Assessment 63
  3.3.3 Risk Decisions 71
3.4 Communicating Risk 77
  3.4.1 Communicating Risk Internally 78
  3.4.2 Regulatory Communications 79
  3.4.3 Communicating with Shareholders 86
3.5 Organizing for Success 89
  3.5.1 Risk Management Committee 89
  3.5.2 Chief Risk Officers 90
3.6 Summary 91

4.0 BUILD YOUR STRATEGY 95
4.1 How Much “Cybersecurity” Do I Need? 95
4.2 The Mechanics of Building Your Strategy 97
  4.2.1 Where are We Now? 99
  4.2.2 What Do We Have to Work With? 103
  4.2.3 Where Do We Want to Be? 104
  4.2.4 How Do We Get There? 107
  4.2.5 Goals and Objectives 108
4.3 Avoiding Strategy Failure 111
  4.3.1 Poor Plans, Poor Execution 111
  4.3.2 Lack of Communication 113
  4.3.3 Resistance to Change 114
  4.3.4 Lack of Leadership and Oversight 117
4.4 Ways to Incorporate Cybersecurity into Your Strategy 118
  4.4.1 Identify the Information Critical to Your Business 119
  4.4.2 Make Cybersecurity Part of Your Culture 119
  4.4.3 Consider Cybersecurity Impacts in Your Decisions 119
  4.4.4 Measure Your Progress 120
4.5 Plan For Success 121
4.6 Summary 123
5.0 PLAN FOR SUCCESS

5.1 Turning Vision into Reality
   5.1.1 Planning for Excellence 127
   5.1.2 A Plan of Action 128
   5.1.3 Doing Things 131

5.2 Policies Complement Plans
   5.2.1 Great Cybersecurity Policies for Everyone 140
   5.2.2 Be Clear about Your Policies and Who Owns Them 188

5.3 Procedures Implement Plans 190

5.4 Exercise Your Plans 191

5.5 Legal Compliance Concerns 193

5.6 Auditing 195

5.7 Summary 196

6.0 CHANGE MANAGEMENT

6.1 Why Managing Change is Important 199

6.2 When to Change? 201

6.3 What is Impacted by Change? 205

6.4 Change Management and Internal Controls 209

6.5 Change Management as a Process 214
   6.5.1 The Touhill Change Management Process 215
   6.5.2 Following the Process 216
   6.5.3 Have a Plan B, Plan C, and maybe a Plan D 220

6.6 Best Practices in Change Management 220

6.7 Summary 224

7.0 PERSONNEL MANAGEMENT

7.1 Finding the Right Fit 227

7.2 Creating the Team 229
   7.2.1 Picking the Right Leaders 230
   7.2.2 Your Cybersecurity Leaders 233

7.3 Establishing Performance Standards 237

7.4 Organizational Considerations 240

7.5 Training for Success 242
   7.5.1 Information Every Employee Ought to Know 242
   7.5.2 Special Training for Executives 246
8.0 PERFORMANCE MEASURES 261
8.1 Why Measure? 261
8.2 What to Measure? 267
  8.2.1 Business Drivers 267
  8.2.2 Types of Metrics 271
8.3 Metrics and the C-Suite 272
  8.3.1 Considerations for the C-Suite 273
  8.3.2 Questions about Cybersecurity Executives Should Ask 275
8.4 The Executive Cybersecurity Dashboard 277
  8.4.1 How Vulnerable Are We? 277
  8.4.2 How Effective Are Our Systems and Processes? 282
  8.4.3 Do We Have the Right People, Are They Properly Trained, and Are They Following Proper Procedures? 286
  8.4.4 Am I Spending the Right Amount on Security? 287
  8.4.5 How Do We Compare to Others? 288
  8.4.6 Creating Your Executive Cybersecurity Dashboard 289
8.5 Summary 291

9.0 WHAT TO DO WHEN YOU GET HACKED 293
9.1 Hackers Already Have You Under Surveillance 293
9.2 Things to do Before it’s Too Late: Preparing for the Hack 295
  9.2.1 Back Up Your Information 296
  9.2.2 Baseline and Define What is Normal 296
  9.2.3 Protect Yourself with Insurance 297
  9.2.4 Create Your Disaster Recovery and Business Continuity Plan 298
9.3 What to do When Bad Things Happen: Implementing Your Plan 299
  9.3.1 Item 1: Don’t Panic 300
  9.3.2 Item 2: Make Sure You’ve Been Hacked 301
  9.3.3 Item 3: Gain Control 302
  9.3.4 Item 4: Reset All Passwords 303
  9.3.5 Item 5: Verify and Lock Down All Your External Links 304
  9.3.6 Item 6: Update and Scan 305
  9.3.7 Item 7: Assess the Damage 305
  9.3.8 Item 8: Make Appropriate Notifications 307
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.3.9 Item 9: Find Out Why It Happened and Who Did It</td>
<td>309</td>
</tr>
<tr>
<td>9.3.10 Item 10: Adjust Your Defenses</td>
<td>310</td>
</tr>
<tr>
<td>9.4 Foot Stompers</td>
<td>310</td>
</tr>
<tr>
<td>9.4.1 The Importance of Public Relations</td>
<td>310</td>
</tr>
<tr>
<td>9.4.2 Working with Law Enforcement</td>
<td>315</td>
</tr>
<tr>
<td>9.4.3 Addressing Liability</td>
<td>317</td>
</tr>
<tr>
<td>9.4.4 Legal Issues to Keep an Eye On</td>
<td>318</td>
</tr>
<tr>
<td>9.5 Fool Me Once</td>
<td>319</td>
</tr>
<tr>
<td>9.6 Summary</td>
<td>320</td>
</tr>
<tr>
<td><strong>10.0 BOARDROOM INTERACTIONS</strong></td>
<td>323</td>
</tr>
<tr>
<td>Appendix A: Policies</td>
<td>347</td>
</tr>
<tr>
<td>Appendix B: General Rules for Email Etiquette: Sample Training Handout</td>
<td>357</td>
</tr>
<tr>
<td>Glossary</td>
<td>361</td>
</tr>
<tr>
<td>Select Bibliography</td>
<td>371</td>
</tr>
<tr>
<td>Index</td>
<td>373</td>
</tr>
</tbody>
</table>