

# CONTENTS

<b>1</b>	<b>PREFACE</b>	<b>125</b>	<b>CHAPTER 9. COMPUTER CRIME</b>
<b>7</b>	<b>EXECUTIVE SUMMARY</b>	<b>130</b>	<b>CHAPTER 10. MOBILE RISK MANAGEMENT</b>
<hr/>			
<b>13</b>	<b>PART 1. INTRODUCTION</b>	<b>139</b>	<b>CHAPTER 11. BEST PRACTICES: BUILDING SECURITY CULTURE</b>
<b>14</b>	<b>CHAPTER 1. IT SECURITY IN THE DIGITAL AGE</b>	<b>144</b>	<b>CHAPTER 12. GENERAL RULES FOR COMPUTER USERS</b>
<hr/>			
<b>29</b>	<b>PART 2. SECURITY FOR INDIVIDUALS</b>	<b>150</b>	<b>CHAPTER 13. GLOBAL DIALOGUES ON SECURITY</b>
<b>30</b>	<b>CHAPTER 1. INTRODUCTION TO SECURITY FOR INDIVIDUALS</b>	<b>163</b>	<b>PART 4. INFORMATION SECURITY AND GOVERNMENT POLICIES</b>
<b>31</b>	<b>CHAPTER 2. UNDERSTANDING AND ADDRESSING SECURITY</b>	<b>164</b>	<b>CHAPTER 1. INTRODUCTION</b>
<b>35</b>	<b>CHAPTER 3. KEEPING YOUR COMPUTER AND DATA SECURE</b>	<b>167</b>	<b>CHAPTER 2. PROTECTING GOVERNMENT SYSTEMS</b>
<b>43</b>	<b>CHAPTER 4. KEEPING YOUR OPERATING SYSTEM AND APPLICATION SOFTWARE SECURE</b>	<b>174</b>	<b>CHAPTER 3. THE ROLE OF LAW AND GOVERNMENT POLICY VIS A VIS THE PRIVATE SECTOR</b>
<b>47</b>	<b>CHAPTER 5. MALICIOUS SOFTWARE</b>	<b>176</b>	<b>CHAPTER 4. GOVERNMENT CYBER-SECURITY POLICIES</b>
<b>53</b>	<b>CHAPTER 6. SECURING SERVICES OVER NETWORKS</b>	<hr/>	
<b>63</b>	<b>CHAPTER 7. TOOLS TO ENHANCE SECURITY</b>	<b>189</b>	<b>PART 5. IT SECURITY FOR TECHNICAL ADMINISTRATORS</b>
<b>68</b>	<b>CHAPTER 8. PLATFORM SPECIFIC ISSUES</b>	<b>190</b>	<b>CHAPTER 1. BACKGROUND</b>
<b>73</b>	<b>ADDENDUM 1. INTRODUCTION TO ENCODING AND ENCRYPTION</b>	<b>196</b>	<b>CHAPTER 2. SECURITY FOR ADMINISTRATORS</b>
<b>77</b>	<b>ADDENDUM 2. TCP/IP</b>	<b>209</b>	<b>CHAPTER 3. PHYSICAL SECURITY</b>
<b>79</b>	<b>ADDENDUM 3. MINI-GLOSSARY OF TECHNICAL TERMS</b>	<b>220</b>	<b>CHAPTER 4. INFORMATION SECURITY</b>
<hr/>			
<b>81</b>	<b>PART 3. SECURITY FOR ORGANIZATIONS</b>	<b>238</b>	<b>CHAPTER 5. IDENTIFICATION AND AUTHENTICATION</b>
<b>82</b>	<b>CHAPTER 1. INTRODUCTION</b>	<b>266</b>	<b>CHAPTER 6. SERVER SECURITY</b>
<b>86</b>	<b>CHAPTER 2. OVERVIEW OF E-SECURITY RISK MITIGATION</b>	<b>288</b>	<b>CHAPTER 7. NETWORK SECURITY</b>
<b>94</b>	<b>CHAPTER 3. RISK EVALUATION AND LOSS ANALYSIS</b>	<b>314</b>	<b>CHAPTER 8. ATTACKS AND DEFENSES</b>
<b>101</b>	<b>CHAPTER 4. PLANNING YOUR SECURITY NEEDS</b>	<b>326</b>	<b>CHAPTER 9. DETECTING AND MANAGING A BREAK-IN</b>
<b>105</b>	<b>CHAPTER 5. ORGANIZATIONAL SECURITY POLICY AND PREVENTION</b>	<b>341</b>	<b>CHAPTER 10. SYSTEM-SPECIFIC GUIDELINES</b>
<b>112</b>	<b>CHAPTER 6. PERSONNEL SECURITY</b>	<hr/>	
<b>117</b>	<b>CHAPTER 7. SECURITY OUTSOURCING</b>	<b>351</b>	<b>ANNEXES</b>
<b>122</b>	<b>CHAPTER 8. PRIVACY POLICIES LEGISLATION, AND GOVERNMENT REGULATION</b>	<b>352</b>	<b>ANNEX 1. GLOSSARY</b>
		<b>362</b>	<b>ANNEX 2. BIBLIOGRAPHY</b>
		<b>371</b>	<b>ANNEX 3. ELECTRONIC RESOURCES</b>
		<b>378</b>	<b>ANNEX 4. SECURITY ORGANIZATIONS</b>
		<b>384</b>	<b>ANNEX 5. PRINT RESOURCES</b>