

# Contents

<b>1.0</b>	<b>Introduction and Executive Overview .....</b>	<b>1</b>
1.1	Research Elements Used in This Report .....	2
1.1.1	Probabilities Defined .....	3
1.1.2	Type A, B and C Enterprises Defined .....	3
1.1.3	The Gartner Magic Quadrant .....	3
1.1.4	The Gartner Hype Cycle .....	5
1.2	Information Security — Establish a Strong Defense in Cyberspace .....	6
1.3	Understanding the Information Security Marketplace .....	8
1.4	Implementing Effective Antivirus Architectures .....	9
1.5	Managed Security Services — A Market in Transition .....	10
1.6	Organizational Structures for Information Security .....	11
1.7	How to Manage a Computer Incident Response Team .....	12
1.8	Enterprise Security Architecture for Web Services .....	13
1.9	Enterprise Security Strategies for Microsoft Windows .....	15
1.10	Public-Key Infrastructure and Digital Signatures .....	17
1.11	Intrusion Detection Gives Way to Intrusion Prevention .....	18
1.12	IT Security Management: Fighting Fires and False Alarms .....	19
1.13	Business Continuity and Disaster Recovery Planning .....	20
1.14	Implementing Wireless and Mobile Security .....	21
1.15	Cyberinsurance Policies — The Measure of Security .....	23
1.16	Measuring Information Security Effectiveness .....	24
<b>2.0</b>	<b>Information Security — Establish a Strong Defense in Cyberspace .....</b>	<b>27</b>
2.1	Assessing “Cyber-Threats” From the Enterprise Perspective .....	28
2.1.1	Securing the Enterprise From the Inside and Out .....	29
2.1.2	Establishing Security Management Governance .....	30
2.1.3	Creating a Security-Aware Enterprise Culture .....	31
2.1.4	Evolving an Enterprise’s Security Architecture .....	31
2.1.5	The Information Security Hype Cycle .....	32
2.2	Security Functionality via Network Security Platforms .....	32
2.2.1	Consolidating Business Tools .....	34
2.2.2	The “Good Enough” Information Security Solution .....	35
2.2.3	The Outsourcing Option and Evaluating Security Providers .....	35
2.3	The Role of Government in Fighting Cybercrime .....	36
2.4	The Business Value of Information Security .....	38
2.5	Security Is a Process, Not a State .....	38
2.6	Information Security Marketplace Summary .....	38
2.7	Recommendations .....	39

<b>3.0</b>	<b>Understanding the Information Security Marketplace .....</b>	<b>41</b>
3.1	Security Solutions and Enterprise Characteristics .....	42
3.2	The Changing Information Security Landscape .....	42
3.3	Terrorism's Impact on Security Attitudes .....	43
3.4	The Hype Cycle for Information Security .....	44
3.4.1	Technologies on the Rise .....	44
3.4.1.1	Quantum Cryptography .....	44
3.4.1.2	Network Security Platforms .....	45
3.4.1.3	Trusted Computing Platforms .....	45
3.4.1.4	Behavior Blocking .....	45
3.4.2	Technologies at the Peak of Inflated Expectations .....	45
3.4.2.1	Deep Packet Inspection Firewalls .....	45
3.4.2.2	Wi-Fi Protected Access Security .....	45
3.4.2.3	Instant Messaging Security .....	45
3.4.2.4	Anti-spam .....	46
3.4.3	Technologies Sliding Into the Trough .....	46
3.4.3.1	Federated Identity Management .....	46
3.4.3.2	Web Services Security Standards .....	46
3.4.3.3	Managed Security Service Providers .....	46
3.4.3.4	Biometrics .....	47
3.4.3.5	Advanced Encryption Standard .....	47
3.4.3.6	Intrusion Detection Systems .....	47
3.4.4	Technologies Climbing the Slope .....	47
3.4.4.1	Identity and Access Management .....	47
3.4.4.2	Enterprise Digital Rights Management .....	48
3.4.4.3	Public-Key Infrastructure .....	48
3.4.4.4	Tokens/Smart Cards .....	48
3.4.5	Technologies Entering the Plateau .....	48
3.4.5.1	Firewall Appliances .....	48
3.4.5.2	Secure Sockets Layer .....	48
3.5	The Evolution of Keeping the Bad Guys Out .....	49
3.5.1	Moving Toward Intrusion Prevention .....	49
3.5.2	Assessing the Firewall Vendor Arena .....	51
3.6	The Evolution of Letting the Good Guys In .....	51
3.6.1	The Public-Key Infrastructure Market .....	51
3.7	Security Appliances: It's All About Hardware Vendors .....	52
3.8	Factors That Slow Market Growth .....	53
3.8.1	Growth in Security Spending .....	55
3.9	Security Consulting Services .....	55
3.10	Managed Security Services .....	56
3.11	Homeland Security Initiatives .....	56
3.12	Cybersecurity Insurance .....	57
3.13	Conclusions .....	58
<b>4.0</b>	<b>Implementing Effective Antivirus Architectures .....</b>	<b>59</b>
4.1	The Malicious Code Management Hype Cycle .....	59
4.2	The Many Forms of Malicious Code .....	60
4.2.1	Multiheaded Worms .....	61
4.2.2	XML Worms .....	61
4.3	Holes in the Enterprise Firewall .....	61

4.4	<b>The Antivirus Market Landscape .....</b>	<b>62</b>
4.4.1	Turmoil in the Antivirus Market .....	62
4.4.2	Weaknesses in Enterprise Antivirus Offerings .....	62
4.4.3	Antivirus and Anti-Spam Vendors and Evaluation Criteria .....	63
4.4.4	Personal Firewalls .....	63
4.4.5	The Enterprise Antivirus Magic Quadrant .....	64
4.4.6	Microsoft's Antivirus Management Role .....	65
4.5	<b>Successful Management of Malicious Code Threats .....</b>	<b>66</b>
4.6	<b>Antivirus Management: Clout and Governance .....</b>	<b>66</b>
4.7	<b>Desktops Are the Key .....</b>	<b>66</b>
4.8	<b>Malicious Code Incident Response .....</b>	<b>68</b>
4.9	<b>Negotiating With Antivirus Vendors .....</b>	<b>69</b>
4.10	<b>Recommendations .....</b>	<b>69</b>
<b>5.0</b>	<b>Managed Security Services — A Market in Transition .....</b>	<b>71</b>
5.1	Managed Security Service Market Evolution .....	72
5.2	North American MSSP Magic Quadrant .....	72
5.3	Managed Security Market Drivers .....	74
5.4	Managed Security Service Market Size and Forecast .....	74
5.5	Enterprises' Security Priorities .....	75
5.6	Factors Influencing Selection of a Managed Security Service .....	75
5.7	Enterprises' Preferred Vendors for Managed Security Services .....	76
5.8	Service-Level Agreement Components for a Managed Security Service .....	76
5.9	Critical Factors for Managed Security Service Renewal .....	78
5.10	Should Your Enterprise Outsource Security Functions? .....	78
5.11	Managed Security Service Market Summary .....	79
5.11.1	Market Accelerators .....	79
5.11.1.1	Intrusion Detection as a Driver .....	79
5.11.2	Market Inhibitors .....	79
5.11.2.1	Security Expertise as an Inhibitor .....	80
5.12	Recommendations .....	80
<b>6.0</b>	<b>Organizational Structures for Information Security .....</b>	<b>81</b>
6.1	Align Security Controls and Architecture With Regulations .....	81
6.2	Risk Management Components .....	82
6.3	Organizing for Successful Information Security .....	82
6.3.1	The Chief Information Security Officer's Role .....	83
6.3.2	The CISO Organization .....	84
6.3.3	The CIRT Organization .....	85
6.4	Information Security Best Practices .....	86
6.4.1	Information Security Risk Management Cornerstones .....	86
6.4.2	Information Security Certifications .....	87
6.4.3	Creating an Effective Security Awareness Program .....	88
6.4.4	Measuring Information Security Expenditure Effectiveness .....	88
6.4.5	Information Security Metrics, Scorecards and Dashboards .....	89
6.5	Recommendations .....	90

<b>7.0</b>	<b>How to Manage a Computer Incident Response Team .....</b>	<b>91</b>
7.1	Internet Attacks: A Big Growth Area .....	92
7.2	What's Different Today That Is Driving Cyberattacks? .....	92
7.3	Building a Computer Incident Response Team .....	93
7.4	Establishing a CIRT Reporting Structure .....	94
7.5	The CIRT's Role .....	95
7.6	CIRT Staffing Requirements .....	95
7.7	Adapting the Incident Command System to the Corporate World .....	96
7.8	Creating an Investigation-Related Methodology .....	96
7.9	CIRT Tools and Resources .....	97
7.10	Maintaining the Chain of Evidence .....	98
7.11	Managed Security Services .....	99
7.12	Selecting an Incident Response Resource .....	100
7.13	Recommendations .....	100
<b>8.0</b>	<b>Enterprise Security Architecture for Web Services .....</b>	<b>101</b>
8.1	The Evolution of Web Services .....	102
8.1.1	Web Services Benefits and Pitfalls .....	102
8.1.2	Web Services Architecture Is Evolving .....	102
8.1.3	Deploying Web Services .....	103
8.2	The Hype Cycle for Web Services .....	104
8.2.1	Technologies on the Rise .....	105
8.2.1.1	Web Services Operations Managers .....	105
8.2.1.2	Web Services Brokers .....	106
8.2.1.3	Web Services Networks .....	106
8.2.1.4	External Web Services Deployments .....	106
8.2.1.5	Web Services for Remote Portals .....	106
8.2.1.6	Web Services for Business Process Management .....	106
8.2.2	Technologies at the Peak .....	106
8.2.2.1	Web Services Security Standards .....	106
8.2.2.2	Web Services for Supply Chain Management .....	107
8.2.2.3	Web-Services-Enabled Business Models .....	107
8.2.3	Technologies Sliding Into the Trough .....	107
8.2.3.1	Web Services for Customer Relationship Management .....	107
8.2.3.2	Secure Web Services .....	107
8.2.3.3	Portals as Web Services Consumers .....	107
8.2.4	Technologies Climbing the Slope .....	108
8.2.4.1	Universal Description, Discovery and Integration .....	108
8.2.4.2	XML Veneer Approach .....	108
8.2.4.3	Web Services Description Language .....	108
8.2.5	Technologies Entering the Plateau .....	108
8.2.5.1	Internal Web Services .....	108
8.2.5.2	Simple Object Access Protocol .....	108
8.2.5.3	XML Over HTTP .....	109
8.3	Maintaining Security at the Speed of E-Business .....	109
8.3.1	Web Services Security Drivers .....	109
8.3.2	Secure Sockets Layer and Digital Signatures .....	109
8.3.3	SAML: The Key to Authentication and Authorization .....	110
8.3.4	Investing in SSL Mechanisms .....	110

8.4	<b>Web Services' Security Challenges</b> .....	110
8.4.1	Many Security Challenges Ahead for Web Services .....	111
8.4.2	Implementing Application-Level Firewalls .....	111
8.4.3	Developing Web Services Security Standards .....	111
8.5	<b>Information Security Vendors</b> .....	113
8.6	<b>WS-Security: A Proposed Standard</b> .....	113
8.7	<b>Enterprise Web Services Security Architecture</b> .....	115
8.7.1	UDDI and Web Services .....	115
8.8	<b>Web Services Security: Best Practices</b> .....	116
8.9	<b>Recommendations</b> .....	117
<b>9.0</b>	<b>Enterprise Security Strategies for Microsoft Windows</b> .....	<b>119</b>
9.1	The Vulnerability of Windows .....	119
9.2	Decreasing Enterprise Exposure .....	120
9.3	Securing SQL Server .....	120
9.4	<b>Microsoft's Security-Related Efforts</b> .....	120
9.4.1	Microsoft Claims Security Is a Top Priority .....	121
9.4.2	Instituting a Culture Change .....	121
9.4.3	Looking Ahead at Microsoft's Security Efforts .....	121
9.5	Moving Beyond Windows 95 .....	122
9.6	<b>The Trusted Computing Platform Alliance and Palladium</b> .....	122
9.6.1	Next-Generation Secure Computing Base Overview .....	123
9.7	<b>Client-Side Security</b> .....	123
9.8	<b>Web Server Security</b> .....	124
9.9	<b>Heightening Internet Security</b> .....	124
9.10	<b>Web Services and Network Firewalls</b> .....	125
9.11	<b>Security Standards Under Construction</b> .....	126
9.12	<b>The Windows Security Life Cycle</b> .....	126
9.13	<b>Recommendations</b> .....	127
<b>10.0</b>	<b>Public-Key Infrastructure and Digital Signatures</b> .....	<b>129</b>
10.1	<b>Infrastructures</b> .....	130
10.2	<b>Public and Private Keys</b> .....	130
10.2.1	Emergence of Asymmetric Cryptography or PKC .....	131
10.2.2	The Use of Public and Private Keys .....	131
10.3	<b>Certification Authorities and Digital Certificates</b> .....	132
10.4	<b>Digital Signatures</b> .....	132
10.5	<b>The Value of PKI to the Enterprise</b> .....	132
10.5.1	Assessing the Risks of PKI .....	133
10.6	<b>Risk Mitigation Services</b> .....	134
10.7	<b>Banks: Digital Certificates and the Corporate Customer</b> .....	135
10.8	<b>The PKI Market: Software and Services</b> .....	137
10.9	<b>Electronic Signature Solutions</b> .....	137
10.10	<b>Case Study: The Transuranic Reporting and Inventory-Processing System</b> .....	138
10.11	<b>Electronic Signature Projects</b> .....	139

10.12	Advantages of PKI-Based Digital Signatures .....	139
10.13	Digital Signatures: Benefits and Challenges .....	139
10.14	PKI: Providing Trust in Web Services .....	141
10.15	Recommendations .....	141
<b>11.0</b>	<b>Intrusion Detection Gives Way to Intrusion Prevention .....</b>	<b>143</b>
11.1	The Role Intrusion Detection Has Played .....	143
11.1.1	Dynamics Affecting the Intrusion Detection Market .....	144
11.2	All About Intrusion Detection Systems .....	144
11.2.1	Problems With Intrusion Detection Technology .....	145
11.2.2	Active IDS .....	145
11.2.3	IDS Vendors .....	146
11.3	Moving Toward Intrusion Prevention .....	146
11.3.1	Mandatory Requirements for Intrusion Prevention .....	146
11.3.2	Host-Based Intrusion Prevention .....	147
11.3.3	Network-Based Intrusion Prevention .....	147
11.3.3.1	Characteristics and Benefits of Network Intrusion Prevention .....	148
11.3.4	Intrusion Prevention Summary .....	148
11.4	The DMZ Loses Validity .....	149
11.5	North American Managed Security Service Providers .....	150
11.6	Reaching Network Security Nirvana .....	150
11.7	Installing Network Agents .....	150
11.8	Content Switching .....	151
11.9	The Network Application Firewall Market .....	152
11.10	Firewall Evolution .....	152
11.11	Enterprise Firewall Vendors .....	153
11.11.1	Firewall Market Trends .....	153
11.11.2	Magic Quadrant Criteria .....	153
11.11.3	Leaders .....	154
11.11.4	Challengers .....	155
11.11.5	Visionaries .....	155
11.11.6	Niche Players .....	155
11.12	Recommendations .....	156
<b>12.0</b>	<b>IT Security Management: Fighting Fires and False Alarms .....</b>	<b>157</b>
12.1	Enterprise IT Security Management .....	157
12.2	Addressing the Top Security-Related Issues .....	158
12.3	Market Drivers and Inhibitors .....	158
12.4	Security Monitoring and Management in the Real-Time Enterprise .....	160
12.5	Systems and Security Management .....	160
12.6	Defining Enterprise IT Security Management .....	161
12.7	Security Management Vendors .....	162
12.7.1	Network and Systems Management Security Vendors .....	162
12.7.2	Broad-Scope Security Software Vendors .....	163
12.7.3	IT Security Management Point Solution Vendors .....	163
12.7.4	IT Security Management Magic Quadrant .....	164

12.8	Product Selection Considerations .....	167
12.9	Evolution of IT Security Management .....	167
12.10	Moving to Intrusion Prevention .....	167
12.11	The Impact of Web Services .....	168
12.12	Recommendations .....	169
<b>13.0</b>	<b>Business Continuity and Disaster Recovery Management .....</b>	<b>171</b>
13.1	The Basics of Business Continuity Management .....	171
13.2	The Evolution of Business Continuity .....	172
13.3	Business Continuity in the Real-Time Enterprise .....	173
13.4	The Impact of Business Continuity Regulations .....	174
13.5	Dealing in an Ailing Commercial Insurance Market .....	175
13.6	Business Continuity Management Trends .....	175
13.7	Creating a Successful Business Continuity Plan .....	176
13.8	Implementing Crisis Management .....	177
13.9	Performing a Business Impact Analysis .....	178
13.10	Assessing Recovery Capabilities: Two Case Studies .....	178
13.11	Developing a Disaster Recovery Classification Scheme .....	179
13.12	The Gartner Business Continuity Maturity Model .....	180
13.13	Emerging High-Availability Techniques .....	180
13.14	Multisite Architecture vs. Data Replication .....	183
13.15	The Outsourcing Decision .....	184
13.16	The North American Business Continuity Market .....	184
13.17	Recommendations .....	184
<b>14.0</b>	<b>Implementing Wireless and Mobile Security .....</b>	<b>187</b>
14.1	Creating Layers of Mobile Security .....	187
14.2	“Real” Mobile and Wireless Threats .....	188
14.3	WLAN Market Growth .....	188
14.4	Wireless Security Standards .....	189
14.5	Protecting E-mail Message Content .....	189
14.6	Wireless Security Architectures .....	190
14.7	Keeping the Bad Guys Out .....	190
14.8	Establishing Authenticated Access Control .....	191
14.9	Enhancing WLAN Security .....	191
14.10	Full Mobile VPN or SSL Portal? .....	191
14.11	Personal Firewalls: Protecting “Networks in Motion” .....	192
14.12	Encrypting Stored Data .....	192
14.12.1	Gartner’s Mobile Data Protection Magic Quadrant .....	193
14.13	Mobile PC Security: A Case Study .....	194

14.14	Managing Risk in the Mobilized Real-Time Enterprise .....	194
14.14.1	Classifying Mobile Risks for the RTE .....	194
14.14.1.1	Technology .....	195
14.14.1.2	Business Processes .....	196
14.14.1.3	Social and Personal Factors .....	196
14.14.1.4	Legal and Regulatory Risks .....	196
14.14.1.5	Ethical Factors .....	197
14.15	Recommendations .....	197
<b>15.0</b>	<b>Cyberinsurance Policies — The Measure of Security .....</b>	<b>199</b>
15.1	Defining Enterprise Risk .....	199
15.2	Improving Risk Management and Reporting .....	200
15.3	Regulatory and Legal Trends .....	201
15.4	Promoting Global Homeland Cybersecurity .....	202
15.5	Achieving a Balance .....	202
15.6	The Risk Management Process .....	202
15.7	Measuring Operational Risk .....	203
15.8	Risk Mitigation Practices .....	204
15.9	Defining Cyberinsurance .....	205
15.10	The Cyberinsurance Procurement Path .....	205
15.11	The Role of Self-Insurance .....	206
15.12	The Impact on Organizational Structure .....	206
15.13	A Lack of Detailed Security Standards .....	207
15.14	Selecting a Security Service Provider .....	208
15.15	Creating Security Contracts .....	209
15.16	Ensuring Quality Security Products .....	209
15.17	Recommendations .....	210
<b>16.0</b>	<b>Measuring Information Security Effectiveness .....</b>	<b>211</b>
16.1	Security Management Imperatives .....	211
16.2	Achieving Key Objectives .....	212

16.3	The Four Stages of IT Management .....	213
16.4	Assessing Effectiveness and Efficiency .....	213
16.5	Risk Assessment .....	214
16.6	Vulnerability Assessment .....	214
16.7	Spending Assessment .....	214
16.8	TCO Measurement .....	215
16.9	Security Metrics Assessment .....	215
16.10	Security Metrics .....	215
16.11	Best Practices Assessment .....	216
16.12	Examining Risk .....	217
16.13	Multifactor Justification .....	217
16.14	Recommendations .....	218
<b>Appendix A: All About Firewalls .....</b>		<b>219</b>
A.1	Firewall Policies and Rules .....	219
A.2	Firewall Technology .....	220
A.2.1	Types of Firewall Technology .....	220
A.2.2	Firewall Design .....	220
A.2.3	Firewall Technology Analysis .....	220
A.3	Firewalls in Business Use .....	222
A.4	Benefits and Risks Associated With Firewalls .....	223
A.5	Firewall Standards .....	223
A.6	Firewall Price Ranges .....	223
A.7	Firewall Selection Guidelines .....	224
A.8	Firewall Vendors and the Technology Leaders .....	224
A.9	The Critical Nature of Firewall Rule Sets .....	224
A.10	Firewall Best Practices .....	228
A.11	Conclusions .....	229
<b>Appendix B: Glossary .....</b>		<b>231</b>

# Figures

Figure 1-1: The Gartner Magic Quadrant .....	4
Figure 1-2: The Gartner Hype Cycle .....	5
Figure 2-1: Gartner's Cyber-Threat Hype Cycle .....	29
Figure 2-2: Multienterprise Security Is Only as Strong as Its Weakest Link .....	30
Figure 2-3: Security Governance Arrangement Matrix .....	31
Figure 2-4: Gartner's Information Security Hype Cycle .....	33
Figure 2-5: 'Best of Breed' Solutions Are Needed on Security Platforms .....	34
Figure 2-6: The Information Security Market Balancing Act .....	36
Figure 2-7: The Business Value of Information Security .....	37
Figure 3-1: Security Philosophy by Enterprise Type .....	43
Figure 3-2: Gartner's Information Security Hype Cycle .....	44
Figure 3-3: The Industry Is Moving Toward Intrusion Prevention .....	50
Figure 3-4: Security Is Just Application Plumbing .....	52
Figure 3-5: Security Is Becoming an Appliance World .....	53
Figure 3-6: Security Market Spending in 2001 and 2006 .....	54
Figure 3-7: IT Spending Trends .....	54
Figure 3-8: IT Security Spending Trends by Sector .....	55
Figure 3-9: Security Consulting: Now and Planned .....	56
Figure 3-10: Managed Security Services: Now and Planned .....	57
Figure 4-1: Malicious Code Management Hype Cycle .....	60
Figure 4-2: Antivirus and Anti-Spam for E-Mail: Technology Choices .....	64
Figure 4-3: Gartner's Antivirus Magic Quadrant .....	65
Figure 4-4: More Than Signature-Based Antivirus: Desktop, Server and Network Solutions .....	67
Figure 4-5: Antivirus Strategy Issues .....	67
Figure 4-6: Antivirus Architecture: Tiered Approach Useful, but Desktops Are Key .....	68
Figure 5-1: Managed Security Service Market Evolution .....	72
Figure 5-2: Gartner's North American MSSP Magic Quadrant .....	73
Figure 5-3: Worldwide Managed Security Service Market Size and Forecast (2002 to 2006) .....	74
Figure 5-4: Survey: The Top 10 Business Security Issues in 2003 .....	75
Figure 5-5: Survey: Reasons for Outsourcing Security .....	76
Figure 5-6: Survey: Preferred Type of Vendor for Managed Security Services .....	77
Figure 5-7: Survey: Most Important Elements of a Service-Level Agreement .....	77
Figure 5-8: Survey: Critical Factors for Managed Security Service Renewal .....	78
Figure 6-1: Risk Management Components .....	83
Figure 6-2: The Optimal Chief Information Security Officer Organization .....	85
Figure 6-3: Computer Incident Response Organization .....	86
Figure 6-4: Information Security Certifications .....	87
Figure 6-5: Security Awareness Program: Teach Your Employees Well .....	88

Figure 6-6: Information Security Risk Management Program: Use Scorecards and Dashboards .....	89
Figure 7-1: Cybercrime Trends .....	92
Figure 7-2: Internet Threats .....	93
Figure 7-3: CIRT Reporting Structure .....	94
Figure 7-4: CIRT Responsibilities .....	95
Figure 7-5: Incident Management .....	96
Figure 7-6: Investigative Decision Matrix .....	97
Figure 7-7: Forensic Analysis Tools .....	98
Figure 7-8: Other CIRT Tools and Resources .....	99
Figure 8-1: What Web Services Will Deliver .....	102
Figure 8-2: Web Services Architecture Evolution .....	103
Figure 8-3: Three Stages of Web Services Adoption .....	104
Figure 8-4: Gartner's Web Services Hype Cycle .....	105
Figure 8-5: Application-Specific Firewalls .....	112
Figure 8-6: Security Standards Still Developing .....	112
Figure 8-7: Public-Key Infrastructure and Extranet Access Management Magic Quadrants .....	114
Figure 8-8: Enterprise Architecture for Web Services .....	115
Figure 9-1: Windows Security Measures on Desktops .....	122
Figure 9-2: Server Security Elements .....	124
Figure 9-3: Microsoft.NET Firewalls .....	125
Figure 9-4: Windows Security Life Cycle .....	127
Figure 10-1: Symmetric Key (Secret Key) Cryptography .....	130
Figure 10-2: Asymmetric (Public Key) Cryptography .....	131
Figure 10-3: Digital Signatures Review: From Sender to Receiver .....	133
Figure 10-4: PKI Supports Cryptographic Digital Signature ... and More .....	134
Figure 10-5: Survey: Expected Providers of Risk Mitigation .....	135
Figure 10-6: Banks to Issue Digital Certificates to Corporate Customers .....	136
Figure 10-7: PKI Market Segmentation .....	136
Figure 10-8: Electronic Signature Vendors .....	138
Figure 10-9: PKI-Based Digital Signature Advantages .....	140
Figure 10-10: Digital Signatures: Benefits and Challenges .....	140
Figure 11-1: The Enterprise Protection Model .....	144
Figure 11-2: The DMZ Should Be Replaced by a Transaction Zone .....	149
Figure 11-3: Gartner's North American MSSP Magic Quadrant .....	151
Figure 11-4: Intrusion Detection Is Giving Way to Intrusion Prevention .....	152
Figure 11-5: Gartner's Enterprise Firewall Magic Quadrant .....	154
Figure 12-1: IT Security Management Is Highly Important .....	158
Figure 12-2: IT Security Management's Activities .....	159
Figure 12-3: Survey: Business Security Issues and IT Security Management .....	159

Figure 12-4: Intersection of Systems and Security Management .....	161
Figure 12-5: IT Security Management Layers .....	162
Figure 12-6: Security Management: Network and Systems Management Vendors .....	163
Figure 12-7: Security Management — Broad-Scope Security Vendors .....	164
Figure 12-8: Security Management — Point Solution Vendors .....	165
Figure 12-9: Gartner’s IT Security Management Magic Quadrant .....	166
Figure 12-10: Web Services Increases the Need for “Interior” Hardening .....	168
Figure 13-1: Business Continuity Components .....	172
Figure 13-2: Business Continuity Evolution Timeline .....	173
Figure 13-3: Business Continuity Regulations .....	174
Figure 13-4: Creating Business Continuity Plans .....	176
Figure 13-5: Crisis Management, Incident Response and Contingency Planning .....	177
Figure 13-6: What Is Your Cost of Downtime? .....	179
Figure 13-7: Classifying Business Process Service Levels in Project Life Cycle .....	180
Figure 13-8: The Business Continuity Management Maturity Model .....	181
Figure 13-9: How Technologies Reduce Disaster Recovery Time .....	182
Figure 13-10: Disaster Recovery Architecture .....	183
Figure 13-11: Disaster Recovery Strategies: Where Do Outsourcers Fit? .....	185
Figure 14-1: Wireless E-Mail: Understand the Risks .....	189
Figure 14-2: Mobile Data Protection Magic Quadrant .....	193
Figure 14-3: Examples of Classifying Mobile Technology Risks .....	195
Figure 15-1: Major Elements of Risk .....	200
Figure 15-2: Drivers of Enterprise Risk .....	201
Figure 15-3: The Risk Management Process .....	203
Figure 15-4: Risk Mitigation and Financing Dynamics .....	204
Figure 15-5: The Role of Cyberinsurance .....	206
Figure 15-6: Security Demands Will Affect the Organizational Structure .....	207
Figure 15-7: Mixing a Memorandum of Understanding With an Interconnection Agreement in a Security Contract .....	210
Figure 16-1: Measurement Is the Key .....	212
Figure 16-2: IT Management Progression .....	213
Figure 16-3: Security Metrics Assessment .....	216
Figure 16-4: Risk Relationships .....	218
Figure A-1: Three Main Types of Firewall Technology .....	221
Figure A-2: Three Categories of Firewalls .....	222
Figure A-3: Firewall Pricing .....	224
Figure A-4: Firewall Selection Criteria .....	225
Figure A-5: Firewall Vendors, Part 1 .....	226
Figure A-6: Firewall Vendors, Part 2 .....	227