

*This is the Table of Contents and list of Figures from a new report for 2005,
"Security: How to Protect Your IT Infrastructure and Spur Business Growth."
To order or to learn more about the Gartner Strategic Planning Series, go to www.gartnerpress.com/reports.*

Contents

1.0	Introduction and Executive Overview	1
1.1	Research Elements Used in This Report	2
1.1.1	Probabilities Defined	3
1.1.2	Type A, B and C Enterprises	3
1.1.3	The Gartner Magic Quadrant	3
1.1.4	The Gartner Hype Cycle	5
1.2	A Time of Reckoning for Information Security	5
1.3	Gartner's View of the Information Security Market	6
1.4	The State of Business Continuity Planning and Management	7
1.5	Best Practices for Continuous Application Availability	8
1.6	The Outlook for Malicious Code: A Long Battle Ahead	10
1.7	The Five Most Overhyped Security Threats	12
1.8	The Outlook for Strong Authentication	13
1.9	The Outlook for Authentication Repositories	14
1.10	Trends and Directions in Secure PCs, Servers and Operating Systems	16
1.11	Security, Privacy and Going Global	18
1.12	Vulnerability and Patch Management: Reducing the Risks	18
1.13	Gartner's Network Access Control Model	20
1.14	Information Security for Regulatory Compliance	21
1.15	Managing Mobile Devices Securely	22
1.16	Disaster Recovery and Data Replication Architectures	24
1.17	The Evolving Secure E-Mail Boundary	26
1.18	Business-Class Virtual Private Networks	27
1.19	Conquering Complexity Through Security Architectures	29
2.0	A Time of Reckoning for Information Security	31
2.1	Key Organizational Risk Management Issues	32
2.1.1	Most Important Problems Facing IT Organizations	32
2.2	The Security-Related Impact of New Technologies	33
2.2.1	Security Vulnerabilities in the Supply Chain	34
2.2.2	The Evolution of Cyber Threats	35
2.2.3	Regulatory Distraction: Regulations vs. Auditors	36
2.2.4	New Security, Privacy and Risk Technologies	37
2.3	The Business Value of Information Security	38
2.3.1	Key Security Industry Trends	38
2.3.2	Information Security Spending	38
2.3.3	Delivering a Security Service Level	39
2.3.4	The Role of Chief Information Security Officer	39
2.4	Most Effective Security Technologies	40
2.4.1	"Do Need" Security Technologies	40
2.4.2	"Don't Need" Security Technologies	40
2.5	Recommendations	41

- 3.0 Gartner's View of the Information Security Market 43**
 - 3.1 The Impact of Threats on the Information Security Marketplace 43**
 - 3.1.1 Top Enterprises' Security Activities 43
 - 3.1.2 Category Saturation Overview 44
 - 3.1.3 The Evolution of Cyber Threats 44
 - 3.2 Enterprise Information Security Spending 46**
 - 3.2.1 Enterprise Security Buying Centers 47
 - 3.2.2 Security Innovation 47
 - 3.2.3 The IT Heavyweights 48
 - 3.2.4 Managed Security Services Dynamics 48
 - 3.2.5 IT Budget Growth Rates 49
 - 3.2.6 Security Software Sector Revenue 50
 - 3.3 The Financial Market Perspective 51**
 - 3.3.1 Stock Market Messages 51
 - 3.4 Observations and Recommendations 52**
- 4.0 The State of Business Continuity Planning and Management 53**
 - 4.1 Mitigating the Risk of Business Process Downtime 53**
 - 4.1.1 Business Continuity Management Stakeholders and Their Expectations 53
 - 4.1.2 World Trade Center Response: Lessons Learned 54
 - 4.1.3 2004 Data Center Conference Survey Results: Room for Improvement 55
 - 4.1.4 BCM Maturity Model 55
 - 4.2 Key BCM Tools, Technologies and Processes 56**
 - 4.2.1 Plan Testing 56
 - 4.2.2 Measuring the Effectiveness of the BCM Program 56
 - 4.2.3 2004 Florida Hurricane Seasons: Lessons Learned 57
 - 4.2.4 High Availability and Disaster Recovery Spending 57
 - 4.2.5 Incident Management Communications 59
 - 4.2.6 E-Mail Recovery 59
 - 4.2.7 IT Service Management and BCM Interdependencies 59
 - 4.2.8 Data Center Strategies: No Single "Right" Answer 60
 - 4.3 The Evolution of the Business Continuity Market 60**
 - 4.3.1 Cost Comparison: Insourcing vs. Outsourcing Business Continuity Solutions 60
 - 4.3.2 North American Business Continuity Market 61
 - 4.3.3 Hot-Site Contract Negotiation 62
 - 4.4 Conclusions and Recommendations 63**
- 5.0 Best Practices for Continuous Application Availability 65**
 - 5.1 Defining and Measuring Continuous Availability 65**
 - 5.1.1 User-Defined Availability 66
 - 5.2 IT Service Availability Best Practices 67**
 - 5.2.1 Best Practice No. 1: Measure to the Users' View 67
 - 5.2.2 Best Practice No. 2: Determine SLAs Early in Life Cycle 67
 - 5.2.3 Best Practice No. 3: Know How Your IT Services Availability Metrics Stack Up 68
 - 5.2.4 Best Practice No. 4: Know Your Costs of Delivering Availability 69
 - 5.2.5 Best Practice No. 5: Invest in Service-Level Management and Architecture Standards 70
 - 5.2.6 Best Practice No. 6: Invest in Holistic, Resilient Application 70
and Infrastructure Architectures
 - 5.2.7 Best Practice No. 7: Invest in Multisite Architectures for Built-In Disaster Recovery 72
 - 5.2.8 Best Practice No. 8: Know Your IT Management Process Maturity Level 72
 - 5.2.9 Best Practice No. 9: Know Why Your IT Service Is Down 72

5.2.10	Best Practice No. 10: Get the Right Metrics for Downtime Analysis and Prevention ...	74
5.2.11	Best Practice No. 11: Get the Right Metrics for Downtime Analysis and Prevention ...	74
5.2.12	Best Practice No. 12: Invest in IT Change Management	75
5.2.13	Best Practice No. 13: Invest in Testing	76
5.2.14	Best Practice Case Study: UPS	76
5.2.15	Best Practice Case Study: EDS	76
5.3	Recommendations	77
6.0	The Outlook for Malicious Code: A Long Battle Ahead	79
6.1	The Evolution of the Malicious Code Market	79
6.1.1	Malicious Code Market Convergence	80
6.1.2	Endpoint Protection Market Progression	80
6.1.3	Personal Firewall Technology	82
6.1.4	The Microsoft Effect	83
6.1.5	Network Access Controls	83
6.2	Malicious Code Management Best Practices	85
6.2.1	Antivirus Product Selection Criteria	85
6.2.2	Multiple Technologies and Architectures	85
6.2.3	Firewall Placement	86
6.2.4	Multiple Antivirus Vendors	86
6.2.5	Spyware	87
6.2.6	End-User Security Policy	88
6.2.7	Vendor Pricing	88
6.3	Recommendations	89
7.0	The Five Most Overhyped Security Threats	91
7.1	Threat No. 1: IP Telephony is Unsafe	91
7.1.1	Eavesdropping	92
7.1.2	IP Telephony Security Priorities	92
7.2	Threat No. 2: Mobile Malware Will Cause Widespread Damage	93
7.2.1	Mobile Malware Threat Timeline	93
7.2.2	Malware Protection Best Practices	94
7.3	Threat No. 3: “Warhol Worms” Will Make the Internet Unreliable for Business Traffic and VPNs	95
7.3.1	VPN Deployment Drivers	95
7.3.2	VPN Deployment Best Practices	95
7.4	Threat No. 4: Regulatory Compliance Equals Security	96
7.4.1	Aligning Compliance and Security	97
7.4.2	Regulatory Best Practices	97
7.5	Threat No. 5: Wireless Hot Spot Threats	97
7.5.1	“Evil Twin” Attacks	98
7.5.2	Wireless Hot Spot Best Practices	98
7.6	Recommendations	98
8.0	The Outlook for Strong Authentication	99
8.1	Stronger Authentication: Business and Technology Drivers	100
8.1.1	“Stronger” Passwords Add Complexity	100
8.1.2	Passwords: Near Breaking Point	100
8.2	Online Banking Authentication Efforts	101
8.2.1	Online Banking	101
8.2.2	Online Banking Authentication Alternatives	102
8.2.3	Online Banking Case Studies	102

8.2.3.1	Skandinaviska Enskilda Banker AB	102
8.2.3.2	A German Bank	103
8.2.4	Identity Theft Attacks	103
8.3	Effective Use of Authentication	103
8.3.1	Determining Authentication Strength	103
8.3.2	Integration and Scalability Issues	104
8.3.3	Enterprise Single Sign-On	105
8.3.3.1	Strong Authentication and ESSO Case Study: A Swiss Bank	106
8.3.4	Mobile Authentication	106
8.4	Recommendations	106
9.0	The Outlook for Authentication Repositories	107
9.1	The Status of Directories	108
9.1.1	Common Directory Roles	108
9.1.2	Drivers for Separate NOS and Extranet Directories	108
9.1.3	Drivers for a Separate Application Directory	109
9.1.4	Beyond Directories	109
9.1.5	Moving Toward a Tiered User Repository	110
9.2	The Differences Between Authentication and Authorization Repositories	110
9.2.1	Different Tiers and Different Functions	110
9.2.2	Giving Up Control	111
9.2.3	Lack of Shared Definitions	112
9.3	Moving Toward Multiple Repository Management and Integration	112
9.3.1	The Classic Enterprise Directory	112
9.3.2	Metadirectories	112
9.3.3	Metadirectory vs. Provisioning	114
9.3.4	Single Sign-ON	115
9.3.5	Federation: The Next Wave of Single Sign-On	116
9.3.6	Identity and Access Management	117
9.4	Steps Toward Multiple Repository Management and Integration	118
9.5	Recommendations	119
10.0	Trends and Directions in Secure PCs, Servers and Operating Systems	121
10.1	The Evolution of Operating System Security Software	122
10.1.1	Security Platform Convergence	122
10.1.2	The Antivirus Market and the Gartner Magic Quadrant	122
10.1.3	A Personal Firewall on Every Desktop and Server?	123
10.1.4	Host-Based Intrusion Prevention	125
10.1.5	Is Linux More Secure Than Windows?	125
10.1.6	Microsoft's Operating System Security Road Map	126
10.2	The Evolution of Hardware to Support Security	127
10.2.1	Network Access Control	127
10.2.2	Cisco Systems' and Microsoft's Network Access Control	128
10.2.3	The NX Flag	129
10.2.4	The Trusted Platform Module	129
10.2.5	PC and Server Virtualization	130
10.2.6	Security as a Sub-Operating System Function	130
10.2.7	NSA Case Study	130
10.3	Security Best Practices and Total Cost of Ownership	131
10.4	Recommendations	132

11.0 Security, Privacy and Going Global.....	135
11.1 The Impact of Security and Privacy on Global Sourcing	135
11.1.1 International Data Transfer and Access	136
11.2 Global Industry Regulations and Legislation	137
11.2.1 Country Status of Risk	137
11.2.2 International Encryption Rule Compliance	138
11.2.3 Government-Mandated Access to Corporate and Personal Data	138
11.2.4 Private Sector Data Protection	138
11.2.4.1 National Confusion: European Privacy Rules	139
11.2.4.2 EU Data Transference Issues	140
11.2.5 Information Protection Requirements	140
11.3 Limiting Security- and Privacy-Related Risks	140
11.3.1 Create Detailed Standards	140
11.3.2 Develop an Architecture for Safety	141
11.3.3 Assess Outsourcer Security	142
11.3.4 Use Appropriate Levels of Security Tools and Techniques.....	142
11.3.5 Evaluate Security Contracts	142
11.3.6 Review Offshore Vendor's Procedures	143
11.4 Recommendations	144
12.0 Vulnerability and Patch Management: Reducing the Risks	145
12.1 Creating an Effective Vulnerability Management Program	146
12.1.1 Vulnerability Management Processes and Technologies	146
12.1.2 Audit and Regulatory Compliance	146
12.2 Managing a Vulnerability Assessment Effort	149
12.2.1 Network Vulnerability Assessment.....	149
12.2.2 Security Configuration Management	149
12.2.3 Broad-Scope Software	151
12.3 Vulnerability Management Best Practices.....	151
12.3.1 Vulnerability Management Activity Coordination	152
12.3.2 IT Security Risk Management Solution Selection	152
12.3.3 Shielding and Network Access Control Implementation	153
12.3.4 Using SIEM Technology	154
12.3.5 Areas of Convergence	154
12.3.6 Vulnerability Management Functional Requirements	155
12.4 Recommendations	156
13.0 Gartner's Network Access Control Model	157
13.1 The Elements of Gartner's NAC Model	158
13.1.1 Network Access Control Processes	158
13.1.2 NAC Access Control Functions	159
13.1.3 Baseline and Migration Technologies	160
13.1.4 Access Control Solutions	160
13.1.5 Monitoring and Containing	161
13.2 Leading NAC Vendors	162
13.2.1 Cisco Network Admission Control.....	162
13.2.2 Microsoft Network Access Protection	162
13.2.3 Host Security Software Vendors.....	163
13.2.4 Configuration Management Vendors	16
13.2.5 The NAC Vendor Landscape	164
13.3 Enforcing Corporate Policy	165
13.3.1 NAC Functional Requirements	165
13.3.2 NAC Deployment Issues	166

13.3.3	Technology Deployment Issues	166
13.3.4	Case Study: VPN Scan and Block	166
13.4	Recommendations	167
14.0	Information Security for Regulatory Compliance	169
14.1	Corporate Governance and IT Operations	170
14.1.1	Gartner's Hype Cycle for Global Regulations	170
14.2	IT Organization Support of Regulatory Compliance	171
14.2.1	Emergence of Best Practices	171
14.3	IT Organization's Handling of External Requirements	172
14.3.1	Regulations Are All the Same	172
14.4	The IT Organization's Role in Regulatory Compliance	173
14.4.1	Compliance Affects IT Primarily in Two Ways	173
14.5	Information Security's Role in Meeting Regulatory Requirements	174
14.5.1	Information Security Is Moving Toward the Strategic	174
14.5.2	Understanding and Enforcing Controls	174
14.5.3	Steps to Achieving Compliance	175
14.5.4	The Key Standards	176
14.5.5	Putting ISO 17799 to Work	176
14.5.6	Identity Management	176
14.5.7	Security Information Management Tools	178
14.5.8	Data-at-Rest Encryption	179
14.5.9	Detecting and Preventing Information Loss	180
14.6	Recommendations	181
15.0	Managing Mobile Devices Securely	183
15.1	Mobile Data Risks	184
15.2	Best Practices for Maintaining Mobile Device Security	184
15.2.1	Managing Mobile Device Protection	184
15.2.2	Protect Device Configuration With Lockdown	184
15.2.3	Protect Device Data With Encryption	185
15.2.4	Device Protection With Configuration Management	185
15.2.5	Protect Device Data With a Backup Plan	187
15.2.6	Protect Device Networking With Personal Firewalls	187
15.2.7	Protect Privacy by Blocking Spyware	188
15.2.8	Protect the Device Identification	188
15.2.9	Protect the User Identification	188
15.3	Aligning Security Needs and Application Issues	189
15.3.1	Three Mobile Protection Scenarios	189
15.3.2	Human Factors Issues	189
15.3.3	Be Flexible With Remote Authentication	190
15.3.4	VPN Alternative	190
15.3.5	On-Demand Protection	190
15.3.6	Get Creative With Portability	191
15.3.7	Act for the Company, Think Like the User	191
15.4	Recommendations	192
16.0	Disaster Recovery and Data Replication Architectures	193
16.1	DR and Continuous Application Availability Investments	194
16.1.1	Investing to Reduce Unplanned Downtime	194
16.1.2	The Business Impact Assessment	195
16.1.3	Defining Business Needs	195

16.2 Critical Technologies and Their Trade-Offs	195
16.2.1 Disaster Recovery Data Center Strategies	196
16.2.2 Data Recovery Architectures	196
16.2.3 Point-in-Time Copies	197
16.2.4 Data Replication Alternatives	197
16.2.4.1 Application- and Transaction-Level Replication	197
16.2.4.2 DBMS Log-Based and Journaling and Shadowing Replication	198
16.2.4.3 DBMS Log-Based Replication Case Study	199
16.2.4.4 Storage Controller Unit-Based Solutions	200
16.2.4.5 Synchronous Storage Controller Unit-Based Solutions	201
16.2.4.6 Asynchronous Storage Controller Unit-Based Solutions	202
16.2.4.7 File-Level and Volume Manager-Based Replication	203
16.2.5 Other Recovery Technologies	204
16.3 24x7 Availability and Disaster Recovery Best Practices	205
16.4 Recommendations	206
17.0 The Evolving Secure E-Mail Boundary	207
17.1 E-mail Security Best Practices	207
17.1.1 Minimizing Enterprise Spam	207
17.1.2 Architecture Evaluation	208
17.1.3 In-House or Outsource	209
17.1.4 The Regulation Effect	210
17.1.5 Enterprise Security Spending	210
17.1.6 E-mail Authentication Standards	210
17.1.7 E-mail Marketing	211
17.1.8 Compliance Outbound Filtering Issues	211
17.1.9 EU Content Filtering	212
17.2 Model and Vendor Selection	212
17.2.1 Multiple vs. Single Antivirus Vendor Selection	212
17.2.2 Enterprise Spam-Filtering Magic Quadrant	213
17.2.3 Microsoft and E-mail Security	214
17.2.4 Encrypted E-mail Methods	214
17.3 Recommendations	215
18.0 Business-Class Virtual Private Networks	217
18.1 VPN Architecture Development	217
18.1.1 Determining Long-Term Networking Solution Needs	218
18.1.2 Network Edge Access Methods	218
18.1.3 Remote User VPNs	218
18.1.4 In-LAN VPNs	219
18.2 Leading VPN Providers	220
18.2.1 Site VPN	221
18.2.2 Remote Access VPN	221
18.2.3 Encrypted VPN Gateway Products	223
18.2.4 MPLS Services	225
18.2.5 Managed Service Providers	225
18.2.6 VPN Case Studies	227
18.3 VPN Security Risks	227
18.3.1 Establishing Enterprise Encryption Levels	227
18.3.2 Understanding Privacy Exposure Points	229
18.3.3 Implementing Common Security Practices for VPN Extranets	229
18.3.4 Protecting Business Gateways	230
18.3.5 Using Authentication Credentials	230
18.4 Recommendations	230

19.0 Conquering Complexity Through Security Architectures	233
19.1 The Evolution of Security Architectures	234
19.1.1 Two Types of Security Architectures	234
19.2 Security Architecture Best Practices	234
19.2.1 Physical Security Infrastructure Architecture	234
19.2.2 Logical Security Infrastructure Architectures	236
19.2.3 Map Enterprise Security Architectures	236
19.2.4 Information Security Infrastructure Domains	236
19.2.5 The Security Systems Enumeration Process	237
19.2.6 Physical Architecture	238
19.2.7 Detailed Requirements Template	238
19.2.8 Logical Architecture	239
19.2.9 Project Architecture	240
19.2.10 Multiple Levels of Access	240
19.3 Managing New Security and Enterprise Technologies	241
19.3.1 Point-to-Point Dynamic Trust	241
19.3.2 Resources for Security Architects	241
19.4 Recommendations	242
Appendix A: Gartner's Hype Cycle for Information Security, 2004	243
A.1 The Hype Cycle for Information Security	243
A.2 On the Rise	243
A.2.1 Compliance Tools	243
A.2.2 Data-at-Rest Encryption Appliances	244
A.2.3 Security Platforms	245
A.2.4 Trusted Computing Group	245
A.2.5 Scan and Block	245
A.2.6 Vulnerability Management	245
A.2.7 Personal Intrusion Prevention	246
A.3 At the Peak	246
A.3.1 All-in-One Security Appliances	246
A.3.2 Deep Packet Inspection Firewalls	246
A.3.3 Instant Messaging Security	246
A.3.4 Spam Filtering	247
A.3.5 Patch Management	247
A.4 Sliding Into the Trough	247
A.4.1 Secure Sockets Layer VPNs	247
A.4.2 Web Services Security Standards	248
A.4.3 Federated Identity	248
A.4.4 Biometrics	248
A.4.5 Managed Security Service Providers	249
A.4.6 Intrusion Detection Systems	249
A.4.7 WPA Security	249
A.4.8 Digital Rights Management (enterprise)	249
A.5 Climbing the Slope	250
A.5.1 Public Key Operations/Soft Tokens	250
A.5.2 Reduced Sign-On	250
A.5.3 Identity Management	250
A.5.4 Security Smart Cards	251
A.5.5 Secure Sockets Layer/Trusted Link Security	251

A.6 Entering the Plateau	251
A.6.1 Hardware Tokens	251
A.7 Conclusions	251
Appendix B: Glossary	253

Figures

Figure 1-1: The Gartner Magic Quadrant	4
Figure 1-2: The Gartner Hype Cycle	5
Figure 2-1: Gartner Executive Survey: Top Technology Trends in 2005	32
Figure 2-2: Gartner Survey Results: Problems Facing IT Organizations	33
Figure 2-3: The Impact of Disruptive Innovation on Information Security	34
Figure 2-4: Business Relationships and Their Security Requirements	35
Figure 2-5: Gartner's Hype Cycle for Cyber Threats, 2005	36
Figure 2-6: Hype Cycle for Security Technology, 2005	37
Figure 3-1: Top Three Security Activities (January 2005-January 2006)	44
Figure 3-3: Gartner's Hype Cycle for Cyber Threats, 2005	45
Figure 3-2: Market Saturation of "Keep the Bad Guys Out" Technologies	45
Figure 3-4: General Observations on the Information Security Landscape	47
Figure 3-5: Location of Security Purchasing Authority	48
Figure 3-6: Security Product Innovation vs. Integration	49
Figure 3-7: Economic, Business and IT Growth in Selected Vertical Segments (2005 vs. 2004)	50
Figure 3-8: Security Software: New License Revenue Forecast, Worldwide	51
Figure 4-1: Crisis-Related Information Needs	54
Figure 4-2: Gartner's BCM Maturity Model	55
Figure 4-3: Business Continuity Plan Test Frequency	57
Figure 4-4: 2004 Florida Hurricane Season: Strategic Lessons Learned	58
Figure 4-5: 2004 Florida Hurricane Season: Tactical Lessons Learned	58
Figure 4-6: Outsourcing vs. Quick-Ship and Cold Site Solutions	61
Figure 5-1: Gartner Data Center Conference Availability Poll Results	66
Figure 5-2: Classification of IT Service Levels and Costs	68
Figure 5-3: End-to-End IT Service Availability Ranking	69
Figure 5-4: Availability Design and Development Costs	70
Figure 5-5: Availability SLAs and Architecture Standards	71
Figure 5-6: IT Maturity Levels	73
Figure 5-7: Unplanned vs. Planned Downtime	73
Figure 5-8: Multilevel Root Cause Coding	75
Figure 6-1: The Malicious Code Landscape	80
Figure 6-2: Endpoint Protection Market Progression Timeline	81
Figure 6-3: Personal Firewall Magic Quadrant	82
Figure 6-4: Microsoft Operating System Security Road Map	84
Figure 6-5: Microsoft Desktop Security Features 2005	84
Figure 6-6: Cisco and Microsoft Weigh In on Network Access Controls	85
Figure 6-7: Enterprise Spyware Decision Framework	87
Figure 6-8: Navigating Vendor Pricing Games	88

Figure 7-1: IP Telephony Threats	92
Figure 7-2: When Will Wireless Viruses Hit?	94
Figure 7-3: Anticipated VPN Adoption Benefits	96
Figure 8-1: Consumer Authentication: Passwords Aren't Good Enough	101
Figure 8-2: Authentication Strength vs. Complexity and Cost	104
Figure 8-3: Enterprise Single Sign-On	105
Figure 9-1: Identities Stored in Other Repositories	110
Figure 9-2: Moving Toward a Tiered User Repository	111
Figure 9-3: Application Behavior Must Change	113
Figure 9-4: Lack of Shared Definitions Complicate Sharing an Authorization Repository	113
Figure 9-5: The "Classic" Enterprise Directory	114
Figure 9-6: Metadirectory in the Middle	115
Figure 9-7: Single Sign-On	116
Figure 9-8: Federation: Authenticate Once, Trust Often	117
Figure 9-9: Identity and Access Management: The Bigger Picture	118
Figure 10-1: Security Platform Convergence Onto Host-Based Security Platforms	123
Figure 10-2: Personal Firewall Magic Quadrant	124
Figure 10-3: Host-Based Intrusion Prevention	125
Figure 10-4: Is Linux More Secure Than Windows?	126
Figure 10-5: Microsoft Operating System Security Road Map	127
Figure 10-6: Network Access Control: Scan and Block	128
Figure 10-7: NSA Case Study	131
Figure 10-8: Security Best Practices Impact on TCO	132
Figure 10-9: More About Security Best Practices Impact on TCO	133
Figure 11-1: The Evolution of Offshore Outsourcing	136
Figure 11-2: Overall Risk Climate by Country	137
Figure 11-3: Private-Sector Privacy Regulation (1998-2006)	139
Figure 11-4: Lines of Service and Related Information Protection Concerns	141
Figure 11.5: Review Offshore Vendor's Procedures	143
Figure 12-1: Steps in a Vulnerability Management Effort	147
Figure 12-2: IT Security Audit: Examples and Requirements	148
Figure 12-3: Regulatory Compliance: IT Security Operations Policy, Process and Function	148
Figure 12-4: Network Vulnerability Assessment Vendors	150
Figure 12-5: Security Configuration Management Vendors	150
Figure 12-6: Broad Scope Vendors	151
Figure 12-7: IT Security and Operation Group Responsibilities	153
Figure 12-8: Convergence in SIEM and Vulnerability Management	155
Figure 13-1: Network Access Control Processes	158
Figure 13-2: Network Access Control Functions	159
Figure 13-3: Monitoring and Containment	161
Figure 13-4: Cisco's Network Admission Control: Phase 2	162
Figure 13-5: Microsoft's Network Access Protection	163
Figure 13-6: Host Security Software Vendors	164

Figure 13-7: NAC Vendor Landscape: Integration Required	165
Figure 14-1: External Forces Are Changing the Agenda	170
Figure 14-2: Gartner’s Hype Cycle for Global Regulations	171
Figure 14-3: Real Requirements Only Emerge Over Time	172
Figure 14-4: Regulations Are All the Same	1734
Figure 14-5: Information Security Is Evolving Toward the Strategic	175
Figure 14-6: Three Key Standards	177
Figure 14-7: Putting ISO 17799 to Work	177
Figure 14-8: Identity Management and Separation of Duty	178
Figure 14-9: Security Information Management for Reporting	179
Figure 14-10: Preventing and Detecting Information Loss	180
Figure 15-1: Gartner’s Magic Quadrant for Mobile Data Protection	186
Figure 15-2: Mobile Support Is Being Pursued by Five Vendor Groups	186
Figure 16-1: Causes of Enterprise Unplanned Downtime	194
Figure 16-2: Criticality Ratings and Classification Systems	196
Figure 16-3: Application- and Transaction-Level Replication Pro and Cons	198
Figure 16-4: DBMS Log-Based Replication Pro and Cons	199
Figure 16-5: DBMS Data Replication Products, Strengths and Weaknesses	200
Figure 16-6: Storage Controller Unit-Based Solutions Pros and Cons	201
Figure 16-7: Synchronous Storage Controller Unit Replication Products, Strengths and Weaknesses ..	202
Figure 16-8: Asynchronous Storage Controller Unit Replication Products, Strengths and Weaknesses	203
Figure 16-9: File-Based and Volume Manager-Based Replication, Pros and Cons	204
Figure 16-10: File-Based and Volume Manager-Based Replication, Strengths and Weaknesses	205
Figure 16-11: Recovery Technology Vendor List	206
Figure 17-1: A Three-Step Approach to Minimize Enterprise Spam	208
Figure 17-2: Delivery Models: Volume Requires Tiers at the Edge, Not Internally	209
Figure 17-3: Keep In-House or Outsource	210
Figure 17-4: Gartner’s Spam-Filtering Magic Quadrant	213
Figure 18-1: The Three “Worlds” of Edge Access	219
Figure 18-2: In-LAN VPN Structure	220
Figure 18-3: Building a Reliable Network	221
Figure 18-4: Site VPN Alternatives	222
Figure 18-5: Site VPN Decision Framework	222
Figure 18-6: Remote Access VPN Decision Framework	223
Figure 18-7: Gartner’s IPsec VPN Magic Quadrant	224
Figure 18-8: Gartner’s SSL VPN Magic Quadrant	224
Figure 18-9: MPLS Services and Service Availability	225
Figure 18-10: Gartner’s North American Managed Service Providers Magic Quadrant	226
Figure 18-11: Gartner’s European Managed Service Providers Magic Quadrant	226
Figure 18-12: The Four Categories of VPN Security Risks	228
Figure 18-13: Time Required to Break Encryption	228
Figure 18-14: Three Site IP VPN Termination Points	229
Figure 19-1: Two Types of Security Architectures	235

Figure 19-2: Physical Security Infrastructure Architecture	235
Figure 19-3: Templates Based on Classification and Application	237
Figure 19-4: Physical Architecture Example	238
Figure 19-5: Detailed Requirements Template Example	239
Figure 19-6: Logical Architecture Example	240
Figure 19-7: Project Architecture Example	241
Figure A-1: Gartner's Hype Cycle for Information Security, 2004	244

