

Contents at a Glance

<i>Introduction</i>	1
<i>Part I: Building the Background</i>	7
Chapter 1: Defining Data Loss	9
Chapter 2: Examining Your Data Environment	29
Chapter 3: Governance, Risk, and Compliance	43
Chapter 4: Data Loss and You	67
Chapter 5: Calculating the Value of Your Data	87
Chapter 6: The Price of Your Data to Others	99
<i>Part II: Starting with the Endpoint</i>	107
Chapter 7: IT Security	109
Chapter 8: Protecting the Endpoint	119
Chapter 9 : USB Devices and Removable Media	137
Chapter 10: Mobile Phones and PDAs	153
Chapter 11: Geography	165
<i>Part III: Prevention at the Office</i>	177
Chapter 12: Keeping the Bad Stuff Out	179
Chapter 13: Keeping the Good Stuff In	195
Chapter 14: Protecting Your Data Center	217
Chapter 15: Authorization and Access Control	239
<i>Part IV: Applications</i>	249
Chapter 16: Backup and Archiving	251
Chapter 17: Protection through Web Applications	259
Chapter 18: Making Applications Safer	267
Chapter 19: Losses from the Unlikeliest Places	279
Chapter 20: Revisiting Policies	295
<i>Part V: More Preventative Measures</i>	305
Chapter 21: Technology Is Not a Silver Bullet	307
Chapter 22: Long-Term Prevention	325
Chapter 23: Partners and Suppliers	337

<i>Part VI: Dealing with the Inevitable</i>	347
Chapter 24: In the Event of Data Loss	349
Chapter 25: Preparing for the Future	359
<i>Part VII: The Part of Tens</i>	373
Chapter 26: Ten Tips to Prevent Data Loss Today.....	375
Chapter 27: Ten Common Mistakes.....	379
Chapter 28: Ten Tips to Protect Data at Home	383
<i>Index</i>	387

Table of Contents

.....

<i>Introduction</i>	1
Who Should Read This Book	1
Foolish Assumptions	2
How This Book Is Organized	3
Part I: Building the Background	3
Part II: Starting with the Endpoint	3
Part III: Prevention at the Office	3
Part IV: Applications	4
Part V: Additional Preventive Measures	4
Part VI: Dealing with the Inevitable	5
Part VII: The Part of Tens	5
Icons Used in This Book	5
Where to Go from Here	6
<i>Part I: Building the Background</i>	7
Chapter 1: Defining Data Loss	9
How the World of Data Has Changed	10
Economic growth — a barrage of gadgets	10
The messaging boom throws data everywhere	11
Technology gone wild; data gone missing	12
Where will we put it all?	14
Where will it all end?	15
Information and Communication: Risky Business	16
Web 2.0 and the dark side of progress	16
The business of cyber-crime	17
Target: your information	18
More connections, more risk	19
How IT Risk Affects Business Risk	20
IT risk — buckets of it	20
Electronic records — incoming!	23
Getting the Whole Picture	25
Knowing and controlling what you have	25
A one-size solution does not fit all	25
A mind map of data loss	26

Chapter 2: Examining Your Data Environment	29
Discovering the Types of Data at Risk	29
Data at rest	31
Data in motion	31
The most common at-risk data types.....	32
Where to Find Data at Risk.....	33
Discovering where your data hangs out	34
Telling the forest apart from the trees.....	35
Who Are We Protecting Against?.....	37
Bad things happening because of bad people	37
Bad things happening because of good people	39
The malicious insider	40
The Arms Race Continues	41
Chapter 3: Governance, Risk, and Compliance	43
Protecting Your Data — or Else.....	43
Data breaches, audits, and full disclosure	46
What can you really do about stolen data?	48
Regulations You Need to Know About.....	50
Existing full-disclosure legislation	50
Regulations in Europe and North America.....	55
How Good Governance Helps Compliance.....	58
Data classification to the rescue.....	59
The right technology for record retention and retrieval.....	59
Using data-loss prevention solutions	60
Balancing privacy and data protection.....	60
Creating Auditable Processes	61
Compliance technology requirements.....	62
Making your organization as strong its data.....	62
Which Regulations Are Relevant?	65
Chapter 4: Data Loss and You.	67
Risks and Consequences of Data Loss.....	67
Direct losses	67
Indirect losses	68
The total cost of data loss	70
Disclosure Laws and Cyber-Crime	71
New (cyber-) crime versus old habits.....	72
Treating Data Loss as a Disaster	77
Evaluating risk.....	78
Understanding the damage to reputation	79
Facing the prospect of fines	80
Protecting the data (or doing jail time)	80
Protecting information technology	81

Starting to Rethink Data Security	82
Looking at the basics of data security	82
Putting a monetary value on your data.....	83
Considering your options	85
Keeping an eye on the why.....	85
Chapter 5: Calculating the Value of Your Data	87
Modeling Information	87
Adding risk and consequences into the equation	89
Different perspectives for different devices	90
Different perspectives for different markets	91
Identifying Sensitive Data	91
Credit cards and bank details	92
Customer-loyalty cards.....	92
E-mail addresses	93
E-mail and other communication from customers.....	93
Health and welfare information	94
Sensitive corporate data.....	94
Other sources of sensitive data	95
The Elusive Total Cost.....	97
Chapter 6: The Price of Your Data to Others	99
How Much Is That Data Worth?.....	100
The most popular data for criminals to acquire.....	100
Pile 'em high, sell 'em cheap	101
Where to look for your data on the Web	102
The Value of Data Over Its Lifetime	104
 <i>Part II: Starting with the Endpoint</i>	 107
Chapter 7: IT Security	109
Surveying the Threat Landscape.....	109
The evolution of a script-kiddie to a cyber-criminal.....	112
Inside the mind of a data thief.....	113
The Basics of IT Security Threats	114
How anti-threat technology has evolved.....	114
Information is the cyber-criminal's priority.....	117
Chapter 8: Protecting the Endpoint	119
Why the Endpoint Is a Risk	119
Threats against the user and the endpoint	120
Wayward laptops	121

Dealing with Lost Laptops.....	122
Have laptop, will travel.....	122
Strategies for protecting laptops.....	123
Endpoint-Encryption Technologies.....	123
Full-disk encryption.....	124
File-based encryption.....	125
Enterprise digital rights management (eDRM).....	125
So many options . . . so little time.....	127
Here be dragons.....	127
Preventing Keyloggers and Rootkits.....	128
Defeating the keylogger.....	128
Defeating the rootkit.....	130
It's a war out there.....	131
Connecting Securely to the Corporate Network.....	131
Virtual private networks (VPNs).....	131
Thin-client solutions.....	132
Virtualizing the client.....	133
Which one for me?.....	134
Products to Protect the Endpoint.....	134

Chapter 9: USB Devices and Removable Media 137

Defeating USB Devices.....	139
Here comes a brave new (portable) world.....	139
Careless use of portable media.....	141
Strategies for Dealing with Removable Media.....	142
USB ports — limit or lock down?.....	144
More policies, more actions.....	144
Content-based encryption policies.....	145
Policies for Destroying Data on Removable Media.....	146
Three tips for destroying data.....	147
Storage-security policies.....	148
Locking Down a Laptop.....	149

Chapter 10: Mobile Phones and PDAs 153

Communicating the Risks and Benefits.....	154
Protecting Your Corporate Portal.....	155
Additional management challenges.....	156
Putting it all together.....	158
Controlling Functionality on Mobile Devices.....	158
Encryption strategies for mobile devices.....	159
Remote wipe and kill.....	160
The Dangers of Bluetooth.....	161
A simple solution for Bluetooth vulnerabilities.....	162
Bluejacking, bluesnarfing, backdooring and bluebugging.....	162
Protecting Data Against Mobile Phone and PDA Data Leaks.....	163

Chapter 11: Geography	165
Location-Based Access Control	165
Changing policies with geography.....	166
Merging logical and physical security.....	167
Risky Businesses.....	169
Conferences and exhibitions	170
Mergers and acquisitions	171
Internet Cafés	172
The evil twin	172
Holiday and vacation infections	173
You're a Stranger Around Here	174
Sweets from strangers.....	174
Protecting new hires	175
Working from home.....	175

Part III: Prevention at the Office..... **177**

Chapter 12: Keeping the Bad Stuff Out	179
The War Zone.....	179
The Threat from E-mail.....	181
The move from spam to phishing.....	182
Endpoint security	183
The Patience of Today's Criminals.....	186
Spear phishing.....	187
Big fish and little fish	189
Wireless Security to Prevent Data Loss.....	190
Scanning for wireless networks	190
Countering drive-by pharming.....	191
Locking down your wireless routers	191
Utilizing Hardware Appliances	193
Chapter 13: Keeping the Good Stuff In	195
Protecting Intellectual Property	196
Messaging systems.....	197
Protecting e-mail from accidental (or not-so-accidental) loss....	199
Web-based e-mail.....	200
Instant messaging	202
The wrong Dave	203
A better solution	205
Developing Consistent Data Classification	205
The meaning of life (-cycle management).....	206
Data classification and ILM as a business advantage	208
Consistency counts in classification	211

Recognizing Potential Security Holes	212
User-level security issues	212
Securing individual computers	213
Managerial security issues	214
Chapter 14: Protecting Your Data Center	217
The Curse of Unstructured Data Files.....	218
The content defines the value.....	220
Minimizing the number of copies	221
Data Availability for Good or Bad.....	224
Working 24/7.....	224
Intrusion detection	225
Protecting Server Infrastructure	226
Critical system protection	227
Servers, endpoints, and thin-client computing.....	228
Why centralized backup is a good idea	230
Denial-of-Service Attacks	231
Variations on the flooding attack.....	232
Poisoned DNS as a method of stealing data	232
Encryption in the Data Center	234
Why outright encryption might cause more problems than it solves.....	235
Content-based classification and protection	236
Managing digital rights across the enterprise	237
Chapter 15: Authorization and Access Control	239
Tightening Control over Access to Data.....	240
Reducing data access	241
What are the alternatives?.....	242
Network Access Control: What's In It	243
Data on the move.....	244
Data at rest	244
Comprehensive Remediation.....	245
Authorization strategies to reduce data access	246
Using NAC agents.....	247
Part IV: Applications	249
Chapter 16: Backup and Archiving	251
Backup: The Easiest Way to Lose Critical Data	251
Backup tapes . . . under lock and key?	252
Hardware encryption to protect offsite data	254

The Importance of an Archive	257
Identifying risk.....	257
Protecting the corporate memory.....	257
Chapter 17: Protection through Web Applications	259
Attacking Applications through the Web	259
SQL injection attacks.....	260
Preventing SQL injection attacks.....	261
The Dangers from the Internet Browser.....	261
Browser plug-ins	262
Cross-site scripting.....	262
Clickjacking.....	264
Session poisoning and hijacking.....	265
Chapter 18: Making Applications Safer	267
Data Corruption: Worse than Data Loss?	267
Guarding against data compromise	268
Taking the performance hit.....	269
Poor Code Results in a New Threat Vector.....	271
Open Source software	272
Developing data-loss testing	273
Putting it all together.....	274
Software as a Service: Who's Watching the Watchers?.....	275
Identifying threats in SaaS environments	276
Securing your data from tampering	276
Chapter 19: Losses from the Unlikeliest Places	279
Is That Your Data Walking Out the Door?	279
How to destroy electronic data	281
Disposing of old systems without losing data	283
Strategies for system repair	283
The Unseen Sources of Information.....	284
Local e-mail archives.....	284
SMS	285
The real deal on facsimiles (faxes).....	286
Printers and photocopiers.....	286
VoIP and answering machines	287
Digital cameras.....	288
Conference calls and Webcasts	288
Remote access.....	288
Miscellaneous attack vectors.....	289
Dealing with the Printed Word	290
Put up a sign	291
Cleaning up after meetings	292
Revisiting the document shredding policy.....	293
Pick a shredder, any shredder	294

Chapter 20: Revisiting Policies	295
The People Factor	295
Identifying broken processes	296
Interview techniques to identify data at risk	298
Common Policies That Put Data at Risk	300
Developing policies and procedures to prevent data loss	301
Correcting broken processes and policies	301
 Part V: More Preventative Measures	305
 Chapter 21: Technology Is Not a Silver Bullet	307
Social-Engineering Attacks	308
Piggybacking.....	308
Dumpster diving.....	309
Contractors.....	309
Impersonation	310
Controlling freebies	311
Eavesdropping	312
Processes and Procedures	313
The trouble with standards.....	314
Choosing a standard.....	319
Time to reevaluate.....	320
Ask the question	321
Treating Data Loss as a Disaster	321
The Importance of an Awareness Program.....	322
Security training for everybody	322
An ongoing program.....	323
Building a culture that protects data	324
 Chapter 22: Long-Term Prevention	325
Creating an Information-Protection Policy.....	325
Long-term strategy to handle data loss	326
Discovery — an ongoing effort.....	327
The importance of consistency	329
Moving on from discovery.....	329
Less data, less risk.....	331
Auditing for governance	332
Revisiting Decisions You've Made.....	333
Regulatory changes	333
Threat changes.....	334
Technology changes.....	334
 Chapter 23: Partners and Suppliers	337
Preventing Data Loss by Third Parties	337
Information-security audits	338
Outsiders inside your data center	339

Potential threats from Software as a Service (SaaS) providers ... 339
 Service Oriented Architectures and Data Loss 341
 Who can you trust? 342
 Fending off dangers in third-party data processing 342
 Questions to ask..... 343

Part VI: Dealing with the Inevitable 347

Chapter 24: In the Event of Data Loss 349

 Don't Panic 350
 Creating a plan 350
 Mobilizing the troops 352
 Dealing with the media..... 353
 The Ongoing Project 354
 Support desks and supporting your customers 355
 Minimizing customer impact..... 356
 Ensuring that it won't happen again 357

Chapter 25: Preparing for the Future 359

 The Decline of Implicit Trust 359
 Analyzing application access 361
 Analyzing user behavior 362
 Malicious data corruption 364
 Hiding Data You Don't Want Seen 365
 Information sensitivity and access..... 366
 Real-time redaction..... 367
 Social Networking and the Dangers of Data Loss..... 368
 Corporate phishing through private individuals..... 370
 Data loss in cyberspace 371

Part VII: The Part of Tens 373

Chapter 26: Ten Tips to Prevent Data Loss Today 375

 Identify what information you have that needs to be protected 375
 Identify where sensitive information resides 375
 Identify who has access to sensitive and confidential information..... 376
 Identify processes involving sensitive information 376
 Identify when and where data goes offsite..... 376
 Protect the endpoint 376
 Protect information in motion 377
 Revisit how reports and printouts are destroyed..... 377
 Revisit system disposal 377
 Start an education-and-awareness program 377

Chapter 27: Ten Common Mistakes	379
“It won’t happen to me”	379
Secrecy about data-loss threats	379
Mistaking ignorance for bliss	379
Trusting your partners blindly	380
Delaying finding out where your data was — especially after a breach	380
Assuming that it will be business as usual after an event	380
Assuming all data is equal	380
Giving data the same protection at all times	381
Assuming that people will do the right thing with the data	381
Assuming that your current processes won’t result in data loss	381
Chapter 28: Ten Tips to Protect Data at Home	383
Shred personal information	383
Understand what personal data you have on your laptop	383
When signing up for a service, consider which data is requested	384
Check the Web browser’s address bar	384
Lock down your home network	384
Keep your anti-virus and anti-malware software up to date	385
Install a pop-up blocker and Web-site checker	385
Educate your family	385
Run anti-spyware and anti-adware programs	386
Check browser plug-ins	386
Index	387