Index

• Numerics •

9/11 attacks, 302–304

• A •

ABCI (Associate of the Business Continuity Institute), 318
ABCP (Associate Business Continuity Professional), 315
absenteeism of employees, 11, 297–298
access control, 116, 118–119
access management, 156
Acrobat (Adobe), 99
Active Directory, 161
active/active server cluster mode, 168, 170
active/passive server cluster mode, 168, 170
Activity Accounting: An Activity-Based Costing Approach (Wiley), 63
Activity-Based Cost Management: An Executive’s Guide (Wiley), 63
Adobe
Acrobat, 99
Flash, 99
air sampling smoke detectors, 142
alternate processing facility
  hurricanes, 292
  identifying, 42–44
  tornados, 293
alternate work locations, 290
alternative site selection, 146–151
Andrew (hurricane), 291
anti-spam filters, 124
anti-virus software, 124, 282
APC InfraStruXure Express, 150
APIs (Application Programming Interfaces), 100
Apple Quicktime, 99
application architecture, 160–161
application clients, 104–108
application data. See data
application firewalls, 282
application interfaces, 189
Application Programming Interfaces (APIs), 100
application servers, 103–104
applications
  authentication, 187–188
  change management, 193
  client systems, 191–192
  configuration management, 193–194
  configuring, 186–187
  customizations, 189–190
  dependencies, 94, 190–191
  end users, 187–188
  external directory service, 187
  external users, 188–189
  fixes, 186
  inventory, 185–186
  local password database, 187
  networks, 192–193
  patches, 186
  roles, 188
  Single Sign On (SSO), 187
  versions, 186
Web browsers, 192
architectures
  application architectures, 160–161
distributed architectures, 159–160
network architectures, 170
server clusters, 170–171
Service-Oriented Architecture (SOA), 159, 166
Asian flu pandemic, 297
assembling response team, 37
assets, 55, 61
Associate Business Continuity Professional (ABCP), 315
Associate of the Business Continuity Institute (ABCI), 318
auditors, role in walkthrough test, 223
authentication
applications, 187–188
centralized, 161, 166
resets during a disaster, 117
workstation operating systems, 116–119
author’s e-mail address, 5
Avachinsky-Koryaksky volcano, 269
availability of IT systems, 334
avalanches
  disaster recovery plan, 295–297
  emergency power, 296
  emergency supplies, 296
  site selection, 269
  supplemental communications, 297
walkthrough test, 224

BCMI (Business Continuity Management Institute), 316–317
BCP Generator, 309
benefits of disaster recovery planning, 13, 331–338
BIA (Business Impact Analysis)
  assets, 55, 61
  conducting, 18–19, 54–55
  criticality ranking, 63
  employees, 55, 62, 71
  forms, 56–57
  IT systems, 55, 60–61, 70–71
  Maximum Tolerable Downtime (MTD), 19–20, 64, 72
  mitigation, 66
  org chart, 60
  process improvements, 333
  processes, 55, 58–60, 70–71
  purpose of, 52–53
  Recovery Point Objective (RPO), 20–22, 65–66, 73
  Recovery Time Objective (RTO), 19–20, 64–65, 72–73
  risk analysis, 66, 68–69
  statements of impact, 62–63
  suppliers, 55, 62, 71
  threat modeling, 66, 68
  worksheets, 56–57
BIA Professional, 308
biometric entry controls, 130, 134–136
Black Death pandemic, 297
blackouts, 140
Blocking Spam and Spyware For Dummies (Wiley), 124
bollards, 139
bottom-up view of IT systems, 80
break-ins, 280, 303–304
brownouts, 140
BS25999, 12
budget, 32, 53
building new servers, 157–158
bulletproof glass, 138
business applications
  authentication, 187–188
  change management, 193
client systems, 191–192
configuration management, 193–194
configuring, 186–187
customizations, 189–190
dependencies, 94, 190–191
end users, 187–188
external directory service, 187
external users, 188–189
fixes, 186
inventory, 78–79, 185–186
local password database, 187
networks, 192–193
patches, 186
roles, 188
Single Sign On (SSO), 187
versions, 186
Web browsers, 192
business changes, impact on disaster recovery plan, 243–245
Business Continuity Certified Expert (BCCE), 317
Business Continuity Certified Planner (BCCP), 316
Business Continuity Certified Specialist (BCCS), 317
Business Continuity Institute (BCI), 318–319
Business Continuity Management Institute (BCMI), 316–317
business continuity plan, 3
Business Impact Analysis (BIA)
assets, 55, 61
conducting, 18–19, 54–55
criticality ranking, 63
employees, 55, 62, 71
forms, 56–57
IT systems, 55, 60–61, 70–71
Maximum Tolerable Downtime (MTD), 19–20, 64, 72
mitigation, 66
org chart, 60
process improvements, 333
processes, 55, 58–60, 70–71
purpose of, 52–53
Recovery Point Objective (RPO), 20–22, 65–66, 73
Recovery Time Objective (RTO), 19–20, 64–65, 72–73
risk analysis, 66, 68–69
statements of impact, 62–63
suppliers, 55, 62, 71
threat modeling, 66, 68
worksheets, 56–57
business process engineering, 252–253
business process owner walkthrough test, 223
business processes
Business Impact Analysis (BIA), 55, 58–60, 70–71
Capability Maturity Model (CMM), 332
integration into disaster recovery plan, 328
mission-critical, 52–53, 65
opportunities for improvements, 332–333
risk analysis, 20
time-critical, 52–53, 65
business survival and role of disaster recovery plan, 12, 331

C

calculating
Maximum Tolerable Downtime (MTD), 72
Recovery Point Objective (RPO), 73
Recovery Time Objective (RTO), 72–73
cameras for video surveillance, 131
Camille (hurricane), 291
Cantor Fitzgerald, 304
Capability Maturity Model (CMM), 332
Carnegie Mellon University, 332
case study for multi-tiered disaster recovery standard, 254–256
CBCP (Certified Business Continuity Professional), 315
CDC (Centers for Disease Control), 297
cellular telephone communication standard, 166
Centers for Disease Control (CDC), 297
certificates, 118–119
<table>
<thead>
<tr>
<th>Certifications</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate Business Continuity Professional (ABCP)</td>
<td>315</td>
</tr>
<tr>
<td>Associate of the Business Continuity Institute (ABCI)</td>
<td>318</td>
</tr>
<tr>
<td>Business Continuity Certified Expert (BCCE)</td>
<td>317</td>
</tr>
<tr>
<td>Business Continuity Certified Planner (BCCP)</td>
<td>316</td>
</tr>
<tr>
<td>Business Continuity Certified Specialist (BCCS)</td>
<td>317</td>
</tr>
<tr>
<td>Business Continuity Institute (BCI), 318–319</td>
<td></td>
</tr>
<tr>
<td>Business Continuity Management Institute (BCMI), 316–317</td>
<td></td>
</tr>
<tr>
<td>Certified Business Continuity Professional (CBCP)</td>
<td>315</td>
</tr>
<tr>
<td>Certified Functional Continuity Professional (CFCP)</td>
<td>315</td>
</tr>
<tr>
<td>Disaster Recover Institute, 315–316</td>
<td></td>
</tr>
<tr>
<td>Disaster Recovery Certified Expert (DRCE)</td>
<td>317</td>
</tr>
<tr>
<td>Disaster Recovery Certified Specialist (DRCS)</td>
<td>316</td>
</tr>
<tr>
<td>Fellow of the Business Continuity Institute (FBCI)</td>
<td>319</td>
</tr>
<tr>
<td>Master Business Continuity Professional (MBCP)</td>
<td>315</td>
</tr>
<tr>
<td>Member of the Business Continuity Institute (MBCI)</td>
<td>319</td>
</tr>
<tr>
<td>Specialist of the Business Continuity Institute (SBCI)</td>
<td>318</td>
</tr>
<tr>
<td>Certified Business Continuity Professional (CBCP)</td>
<td>315</td>
</tr>
<tr>
<td>Certified Functional Continuity Professional (CFCP)</td>
<td>315</td>
</tr>
<tr>
<td>CFCP (Certified Functional Continuity Professional)</td>
<td>315</td>
</tr>
<tr>
<td>Change management</td>
<td></td>
</tr>
<tr>
<td>applications, 193</td>
<td></td>
</tr>
<tr>
<td>networks, 165</td>
<td></td>
</tr>
<tr>
<td>servers, 158</td>
<td></td>
</tr>
<tr>
<td>charter, 324–325</td>
<td></td>
</tr>
<tr>
<td>charter for disaster recovery plan, 17</td>
<td></td>
</tr>
<tr>
<td>checklist testing, 49</td>
<td></td>
</tr>
<tr>
<td>chemical hazards, 144–145</td>
<td></td>
</tr>
<tr>
<td>Cheops, 86</td>
<td></td>
</tr>
<tr>
<td>Chicagocrime.org, 100</td>
<td></td>
</tr>
<tr>
<td>civil disturbances</td>
<td></td>
</tr>
<tr>
<td>communication systems, 301</td>
<td></td>
</tr>
<tr>
<td>emergency power, 302</td>
<td></td>
</tr>
<tr>
<td>emergency supplies, 301</td>
<td></td>
</tr>
<tr>
<td>Los Angeles riots, 273</td>
<td></td>
</tr>
<tr>
<td>protection against, 273</td>
<td></td>
</tr>
<tr>
<td>transportation, 301</td>
<td></td>
</tr>
<tr>
<td>Class A–K fire extinguishers, 143</td>
<td></td>
</tr>
<tr>
<td>client software, 191</td>
<td></td>
</tr>
<tr>
<td>clocks, 164, 166</td>
<td></td>
</tr>
<tr>
<td>cluster architectures, 170–171</td>
<td></td>
</tr>
<tr>
<td>clustering and replication technologies and cutover tests, 235–236</td>
<td></td>
</tr>
<tr>
<td>clustering servers, 167–171</td>
<td></td>
</tr>
<tr>
<td>CMDB (configuration management database), 158</td>
<td></td>
</tr>
<tr>
<td>CMM (Capability Maturity Model), 332</td>
<td></td>
</tr>
<tr>
<td>COBRA (Consultative, Objective and Bi-functional Risk Analysis), 309</td>
<td></td>
</tr>
<tr>
<td>COBRA Risk Analysis, 308–309</td>
<td></td>
</tr>
<tr>
<td>cold sites, 147–149, 205–206</td>
<td></td>
</tr>
<tr>
<td>Colima volcano, 269</td>
<td></td>
</tr>
<tr>
<td>colocation facilities, 150–151</td>
<td></td>
</tr>
<tr>
<td>commercial media storage centers, 183</td>
<td></td>
</tr>
<tr>
<td>committed resources for disaster recovery plan, 325</td>
<td></td>
</tr>
<tr>
<td>communication systems. See also</td>
<td></td>
</tr>
<tr>
<td>supplemental communications</td>
<td></td>
</tr>
<tr>
<td>avalanches, 296–297</td>
<td></td>
</tr>
<tr>
<td>civil disturbances, 301</td>
<td></td>
</tr>
<tr>
<td>dependencies, 92–93</td>
<td></td>
</tr>
<tr>
<td>disruption of, 11</td>
<td></td>
</tr>
<tr>
<td>earthquakes, 286–287</td>
<td></td>
</tr>
<tr>
<td>e-mail communications, 121–125</td>
<td></td>
</tr>
<tr>
<td>fax machines, 125–126</td>
<td></td>
</tr>
<tr>
<td>floods, 289–290</td>
<td></td>
</tr>
<tr>
<td>hurricanes, 292</td>
<td></td>
</tr>
<tr>
<td>ice storms, 291</td>
<td></td>
</tr>
<tr>
<td>instant messaging, 126–127</td>
<td></td>
</tr>
<tr>
<td>landslides, 296–297</td>
<td></td>
</tr>
<tr>
<td>maintaining communications, 39–40</td>
<td></td>
</tr>
<tr>
<td>multiple communications paths, 31</td>
<td></td>
</tr>
<tr>
<td>pandemic, 298</td>
<td></td>
</tr>
<tr>
<td>teleconference bridge, 40</td>
<td></td>
</tr>
</tbody>
</table>
tornados, 293
tsunamis, 294–295
voice communications, 119–121
wildfires, 287–288
wind storms, 291
competitive advantage, 13, 338
Computer Viruses For Dummies (Wiley), 124
Computerworld Disaster Recovery Web site, 319
conducting Business Impact Analysis (BIA), 18–19, 54–55
conferences
DRJ World, 316
World Continuity Congress, 317
configuration management
applications, 193–194
networks, 165
servers, 157–158
configuration management database (CMDB), 158
configuring
applications, 186–187
e-mail gateways, 123
operating systems, 115, 118
consistency across multiple servers, 157–158
consolidating servers, 161–162
construction, 248
consultants, 33, 54
Consultative, Objective and Bi-functional Risk Analysis (COBRA), 309
contact lists and trees, 34, 47, 200–202
contacting the author, 5
contact-less proximity card reader, 133
Contingency Planning and Management Magazine, 11, 331
contracted facilities, 147
crash gates, 139
criticality ranking, 63
cross-training, 299
CSO Business Continuity and Disaster Recovery Web site, 320
CSO Magazine, 320
customizations of applications, 189–190
cutover test
clustering and replication technologies, 235–236
conducting, 230–234
defined, 327
leadership identification, 336
planning, 234–235
process improvements, 333
recommended frequency, 240
response team training, 261

damage assessment procedures, 203–205
data
data flow diagram, 80–84
data storage diagram, 80–84
disaster recovery plan, 23
high-level architectures, 23
latency, 159
protecting, 173–175, 184–185
recovering, 173–176
sensitive data, 162
transmitting, 184–185
data backups
electronic vaulting, 182–183
long-term archiving, 177, 179
managed backup services, 183
mirroring, 170, 180–182, 304
off-site storage strategy, 194–196
reciprocal processing site, 184
Redundant Array of Independent Drives (RAID), 179
removable hard drives, 176–179
replication, 170, 180–182, 304
storing, 178, 182–183
tape backups, 176–179
data centers. See also facilities
mobile data centers, 147, 150
security, 264–265
data circuits, 164
data replication, 170
data replication and mirroring, 278
data retention policy, 177
December 26, 2004 Indian Ocean tsunami, 267
deluge sprinkler systems, 143
demilitarized zone (DMZ) network segments, 165
Denial of Service (DoS) attacks
defined, 303
distributed Denial of Service (DDoS) defense, 303
prevention, 281, 303–304
Department of Homeland Security, 320
dependencies
applications, 190–191
business applications, 94
communication systems, 92–93
external, 95–96
identifying, 90–96
inter-system, 91–94
management service, 94
network service, 93
security, 94
system, 91–92
detecting
fire, 141–142, 271
intruders, 165
water/flooding, 145–146
diagrams
data flow, 80–84
data storage, 80–84
infrastructure, 84–90
digital certificates, 118–119
digital signatures, 124
direct damage of disasters, 10
dirty electricity, 140
disaster avoidance, 16
disaster declaration procedure, 34, 37–38, 198–200
Disaster Recover Institute, 315–316
Disaster Recovery Certified Expert (DRCE), 317
Disaster Recovery Certified Specialist (DRCS), 316
disaster recovery documents
distributing, 260
managing, 257–258
protecting, 257
publishing, 260
recordkeeping, 261
updating, 258–259
Disaster Recovery Journal, 310, 313, 316
disaster recovery plan. See also
interim plan
avalanches, 295–297
benefits of creating, 13, 331–338
budget, 32, 53
business changes, 243–245
charter, 17
civil disturbances, 301–302
committed resources, 325
competitive advantage, 338
damage assessment procedures, 203–205
data, 23
disaster declaration procedure, 34, 37–38, 198–200
document review procedure, 212
earthquakes, 285–287
emergency contact lists and trees, 200–202
end users, 23
executive sponsorship, 15–16, 32, 54, 323–324
experts, 325–326
external changes, 248–249
facilities, 23
floods, 289–290
hurricanes, 291–292
ice storms, 290–291
identifying basic recovery plan, 41–42
integration into other processes, 328–329
IT systems, 23, 333–335
landslides, 295–297
leaders, 202–203, 336
lifecycle commitment, 25, 218, 250–253, 327–328
luck, 329
market changes, 247–248
pandemic, 297–300
personnel changes, 245–247
preserving, 213
preventive measures, 24
process improvements, 333
project manager, 17–18, 32
project plan, 18, 53
project team, 53
recovery team, 209
requirements, 253–254
reviewing, 26
scope, 53, 324–325
security incidents, 303–304
sensitive data, 162
stakeholder support, 326–327
steering committee, 18
storing, 213
structure of, 210–212
subject matter experts, 32
survival, 331
system recovery and restart
   procedures, 205–207
technology changes, 242–243
terrorism, 302–303
test procedures, 220–221
test strategy, 219–220
time, 326
tornados, 292–293
transition to normal operations,
   207–209
tsunamis, 293–295
utility failures, 300–301
version control, 212
volcanoes, 288–289
war, 302–303
wildfires, 287–288
wind storms, 290–291
writing, 24
Disaster Recovery Plan Template,
   310–311
Disaster Recovery Planning.org Web site,
   317–318
Disaster Recovery World Web site, 317
Disaster Resource Guide, 319
Disaster-Resource.com Web site, 319
disasters. See man-made disasters;
   natural disasters
disruption
   of communication, 11
   of transportation, 10–11
distributed server architecture, 159–160
distributing
   documents, 260
   interim plan, 46–47
diverse power feeds, 141
DMZ (demilitarized zone) network
   segments, 165
DNS (domain name service), 164,
   166, 192
document review procedure (for disaster
   recovery plan), 212
document viewers, 99
document-level structure of disaster
   recovery plan, 211–212
documents
   distributing, 260
   managing, 257–258
   protecting, 257
   publishing, 260
   recordkeeping, 261
   updating, 258–259
domain name service (DNS), 164,
   166, 192
DoS (Denial of Service) attacks
   defined, 303–304
   distributed Denial of Service (DDoS)
   defense, 303
   prevention, 281, 303–304
DR plan. See disaster recovery plan
DRCE (Disaster Recovery Certified
   Expert), 317
DRCS (Disaster Recovery Certified
   Specialist), 316
DRI International, 315–316
DRI Professional Practices Kit, 310
DRJ World conference, 316
DRJ’s Toolbox, 313
dry pipe sprinkler systems, 143
due care, 16
due diligence, 16

• E •

earthquakes
   communications systems, 286–287
   disaster recovery plan, 285–287
   emergency power, 287
   emergency supplies, 286
   equipment protection, 138, 286
   IT systems, 285–287, 335
   power outages, 287
   replacement IT systems, 287
earthquakes (continued)
server clusters, 169
site selection, 267–268
supplemental communications, 287
transportation, 285–286
walkthrough test, 224
effects of disasters
communication disruption, 11
direct damage, 10
employee absenteeism, 11
evacuations, 11
inaccessibility, 10
transportation disruption, 10–11
utility outages, 10
on your organization, 30–31
electric generator, 141
electricity. See also emergency power
blackouts, 140
brownouts, 140
dirty electricity, 140
diverse power feeds, 141
electric generator, 141
IT equipment, 140–141
line conditioners, 141
Power Distribution Unit (PDU), 141
remote power controllers, 140–141
switching equipment, 141
Uninterruptible Power Supply (UPS), 141
electromagnetic shields, 138
electronic vaulting, 182–183
e-mail address for author, 5
e-mail clients, 122
e-mail communications, 121–125
e-mail gateways, 123
e-mail interfaces, 123
e-mail servers, 122–123
e-mail communications, 34
emergency communications, 34
emergency contact lists and trees, 34, 47, 200–202
Emergency Lifeline Corporation, 319
Emergency Management Guide For Business & Industry, 312–313, 320
Emergency Operations Center (EOC), 34, 48
emergency operations plan, 29, 33–34
emergency power
avalanches, 296
civil disturbances, 302
earthquakes, 287
floods, 290
hurricanes, 292
ice storms, 291
landslides, 296
as a preventive measure, 31
severe weather, 291–293
tornados, 293
tsunamis, 295
wind storms, 291
Emergency Response Team (ERT)
assembling, 37
contact lists and trees, 34, 47, 200–201
disaster declaration procedure, 38
maintaining communications, 39–40
training, 26–27, 48, 261–262
emergency supplies
avalanches, 296
civil disturbances, 301
earthquakes, 286
floods, 290
hurricanes, 292
ice storms, 291
landslides, 296
severe weather, 291–293
tornados, 293
tsunamis, 295
wildfires, 288
wind storms, 291
Emerging Threat Analysis: From Mischief to Malicious (Syngress), 69
employees
absenteeism, 11, 297–298
Business Impact Analysis (BIA), 55, 62, 71
home preparation for disasters, 283–284
interviewing, 55–57
org chart, 60
training, 262
enacting preventive measures, 44–46
encryption for e-mail messages, 124
encryption keys, 118–119
end users
    applications, 187–188
    disaster recovery plan, 23
e-mail communications, 121–125
fax machines, 125–126
instant messaging, 126–127
operating systems, 115
voice communications, 119–121
workstations, 98–99
enterprise-level structure of disaster recovery plan, 210–211
EOC (Emergency Operations Center), 34, 48
EPA (Environmental Protection Agency), 144–145
equipment protection
    earthquakes, 138, 286
equipment bracing, 138
equipment cages, 131, 139–140
ERT (Emergency Response Team) assembling, 37
    contact lists and trees, 34, 47, 200–201
disaster declaration procedure, 38
    maintaining communications, 39–40
training, 26–27, 48, 261–262
establishing requirements and standards, 253–254
evacuation
    as an effect of a disaster, 11
    fire, 142
executive sponsorship, 15–16, 32, 54, 323–324
experts (for implementing disaster recovery plan), 325–326
external changes, impact on disaster recovery plan, 248–249
external dependencies, 95–96
external directory service, 187
external users of applications, 188–189
extinguishing fire, 141, 143

• F •
face scan, 136
facilitator walkthrough test, 223
facilities
    alternative site selection, 146–151
    biometric entry controls, 130, 134–136
    cold sites, 147–149, 205–206
    colocation facilities, 150–151
    contracted facilities, 147
disaster recovery plan, 23
equipment cages, 131, 139–140
hardened facilities, 131, 138–139
hot sites, 147–149, 206–207
information processing facilities, 129–130
Internet Data Centers (IDCs), 264–265
key-card entry controls, 130, 133–135
locking storage cabinets, 131, 139
man traps, 130, 136–137
mobile sites, 147, 150
PIN pad, 134
PIN pad door locks, 134–135
prevention of facilities-related disasters, 264–269
reciprocal facilities, 147, 151
security guards, 131, 137–138
site selection, 265–269
video surveillance, 130–132, 283
warm sites, 147–149, 206
failure points, 160
Faraday cages, 138
fax machines, 125–126
FBCI (Fellow of the Business Continuity Institute), 319
Federal Emergency Management Agency (FEMA), 312–313, 320
Fellow of the Business Continuity Institute (FBCI), 319
FEMA (Federal Emergency Management Agency), 312–313, 320
fences, 138
file servers, 103
fingerprint reader, 136
fire. See also wildfires
detecting, 141–142, 271
evacuation, 142
extinguishing, 141, 143
fire alarms, 142, 271–272
gaseous fire suppression, 144
IT systems, 335
NFPA 1620, 12
prevention, 270–272
server clusters, 169
sprinkler systems, 143–144
suppressing, 142
firefighting equipment, 288
firewalls, 87, 165, 282
FIRMs (Flood Insurance Rate Maps), 266–267
fixed-focus cameras, 131
Flash (Adobe), 99
flood insurance, 320
Flood Insurance Rate Maps (FIRMs), 266–267
floods
alternate work locations, 290
communication systems, 289–290
disaster recovery plan, 289–290
emergency power, 290
emergency supplies, 290
hazard mapping, 320
IT systems, 290
replacement IT systems, 290
server clusters, 169
site selection, 266–267
supplemental communications, 290
transportation, 289
walkthrough test, 224
water/flooding detection, 145–146
foam and water sprinkler systems, 143
For Dummies Web site, 5
forms (for Business Impact Analysis), 56–57
FreeMap, 86–87
frequency
of disaster recovery plan testing, 26, 236–240
of disasters, 11–12, 17
function-based infrastructure diagram, 89–90

• G •
Galeras volcano, 269
gaseous fire suppression, 144
GD (geographically diverse) clusters, 169
geo-clusters, 169
geofically diverse (GD) clusters, 169
GSM cellular telephone communication standard, 166
guides
Disaster Resource Guide, 319
Emergency Management Guide For Business & Industry, 312–313, 320
Risk Management Guide for Information Technology Systems, 69

• H •
H5N1 avian flu, 297
hacking incidents, 280–282, 303–304
hand scan, 136
hardened facilities, 131, 138–139
hardware
failures, 168, 276–277
inventory, 78–79
hardware configuration of servers, 155
hardware encryption, 165
hardware platforms for workstations, 114–115
hazardous substances, 144–145
high-level architectures, 80
HIPAA (Health Insurance Portability and Accountability Act), 13, 337–338
hiring consultants, 33, 54
home preparation for disasters, 283–284
Hong Kong flu, 297
hot sites, 147–149, 206–207
hot swapping, 179–180
HousingMaps.com, 100–101
HP OpenView, 85
HTTP (HyperText Transfer Protocol), 166
humidity controls, 146
hurricanes
alternate processing facility, 292
communication systems, 292
disaster recovery plan, 291–292
emergency power, 292
emergency supplies, 292
Katrina, 295
server clusters, 169
site selection, 265–266
supplemental communications, 292
transportation, 291
walkthrough test, 224
HVAC failures, 145, 272
HyperText Transfer Protocol (HTTP), 166

IBM
NetView, 85
Tivoli Identity Manager, 161, 166

ice storms
disaster recovery plan, 290–291
emergency power, 291
emergency supplies, 291
supplemental communications, 291
walkthrough test, 224
IDCs (Internet Data Centers), 264–265
identifying
alternate processing facility, 42–44
basic recovery plan, 41–42
dependencies, 90–96
identity management, 116–119, 161, 166
IDS (intrusion detection system), 283
In Search of Clusters (Prentice Hall), 167
inaccessibility, 10
industrial hazards, 274–275
information processing facilities,
129–130
infrastructure diagrams, 84–90
installing operating systems, 118
instant messaging, 126–127
insurance
flood insurance, 320
Flood Insurance Rate Maps (FIRMs), 266–267
reducing premiums, 335
integration of disaster recovery plan into
other processes, 328–329
interfaces, 159, 161, 166
interim disaster recovery plan, 14–15
interim plan
alternative processing location, 42–44
disaster declaration procedure, 37–38
distributing, 46–47
documenting, 46
Emergency Response Team (ERT), 37
enacting preventive measures, 44–46
identifying basic recovery plans, 41–42
interim DR planners, 35
invoking, 39
maintaining communications, 39–40
storing, 46–47
testing, 48–50
writing, 30, 34–36
International Standards
Organization, 338
Internet Data Centers (IDCs), 264–265
inter-system dependencies, 91–94
interviewing
employees, 55–57
subject matter experts, 85
intrusion detection and prevention, 165
intrusion detection system (IDS), 283
intrusion prevention system (IPS), 283
inventories
applications, 185–186
business applications, 78–79
hardware, 78–79
infrastructure diagrams, 88
servers, 156–157
software, 78–79
invoking interim plan, 39
ionization smoke detectors, 142
IP addresses, 164–165
IPS (intrusion prevention system), 283
ISO 27001, 12, 337–338
IT equipment
electricity, 140–141
physical access controls, 130–140
IT systems. See also replacement
IT systems
availability of, 334
bottom-up view, 80
Business Impact Analysis (BIA), 55,
60–61, 70–71
dependencies, 90–96
IT systems (continued)
disaster recovery plan, 23, 333–335
earthquakes, 285–287, 335
fires, 335
floods, 290
high-level architectures, 80
infrastructure diagrams, 84–90
power outages, 335
power supply failure, 335
quality of, 334
reducing disruptive events, 334–335
security incidents, 303–304
top-down view, 80
tsunamis, 295
wildfires, 287

Java Virtual Machine (JVM), 100
journals and magazines
BCI Quarterly Journal, 318
Contingency Planning and Management Magazine, 11, 331
CSO Magazine, 320
Disaster Recovery Journal, 310, 313, 316

Katrina (hurricane), 291, 295
key-card entry controls, 130, 133–135

landsides
disaster recovery plan, 295–297
earthquakes, 296
emergency supplies, 296
site selection, 269
supplemental communications, 297
walkthrough test, 224
LANsurveyor, 86
latency, 159
LBL ContingencyPro Software, 312
LDAP (Lightweight Directory Access Protocol), 161, 166
LDRPS (Living Disaster Recovery Planning System), 307–308
leaders
disaster recovery plan, 202–203
identifying through testing, 336
lifecycle commitment for disaster recovery plan, 25, 218, 250–253, 327–328
lights-out data centers, 140–141, 299
Lightweight Directory Access Protocol (LDAP), 161, 166
line conditioners, 141
Living Disaster Recovery Planning System (LDRPS), 307–308
load balancers, 165
local computers, 108–113
local password database, 187
location-based infrastructure diagram, 89–90
location-sensitive business, 43
locking storage cabinets, 131, 139
long lead time items, 164
long-term archiving, 177, 179
Los Angeles riots, 273
luck, role in disaster recovery planning, 329

magazines and journals
BCI Quarterly Journal, 318
Contingency Planning and Management Magazine, 11, 331
CSO Magazine, 320
Disaster Recovery Journal, 310, 313, 316
magnetic stripe reader, 133
magtape, 176
maintaining communications, 39–40
malware outbreaks, 281, 303–304
man traps, 130, 136–137
managed backup services, 183
management service dependencies, 94
managing
documents, 257–258
networks, 165
operating systems, 115
workstations, 98–99
man-made disasters
civil disturbances, 301–302
security incidents, 303–304
terrorism, 302–303
utility failures, 300–301
walkthrough tests, 225
war, 302–303
manual stations for fire detection, 142
MAOT (Maximum Acceptable Outage Time), 38
market changes, impact on disaster recovery plan, 247–248
mashups, 100–101
Master Business Continuity Professional (MBCP), 315
Mauna Loa volcano, 269
Maximum Acceptable Outage Time (MAOT), 38
Maximum Tolerable Downtime (MTD), 19–20, 64, 72
MBCI (Member of the Business Continuity Institute), 319
MBCP (Master Business Continuity Professional), 315
media players, 99
media storage centers, 183
Member of the Business Continuity Institute (MBCI), 319
metadata, 57
Microsoft
  Active Directory, 161
  Identity Integration Server, 166
mirroring, 170, 180–182, 304
mission-critical processes, 52–53, 65
mitigating steps, 20
mitigation, 66
mobile data centers, 147, 150
mobile platforms, 114
monitors, 131
monoculture, 277–278
Mount Etna volcano, 269
Mount Merapi volcano, 269
Mount Nyiragongo volcano, 269
Mount Rainier volcano, 269
Mount St. Helens volcanic eruption, 267–268
Mount Unzen volcano, 269
MTD (Maximum Tolerable Downtime), 19–20, 64, 72
multiple communications paths, 31
multi-tiered disaster recovery standard case study, 254–256

\section*{N}

NAS (Network Attached Storage), 170, 180
National Institute for Standards and Technology, 69
natural disasters
  avalanches, 295–297
  earthquakes, 285–287
  floods, 289–290
  hurricanes, 291–292
  ice storms, 290–291
  landslides, 295–297
  pandemic, 297–300
  tornados, 292–293
  tsunamis, 293–295
  volcanoes, 288–289
  wildfires, 287–288
  wind storms, 290–291
netViz, 86
network architectures, 170
Network Attached Storage (NAS), 170, 180
Network Magic, 86
network mapping tools, 85–87
network services
  defined, 163
  dependencies, 93
  server configuration, 156
Network Time Protocol (NTP), 164, 166
networks
  access control, 116, 118–119
  addressing, 165
  applications, 192–193
  change management, 165
  configuration management, 165
  connectivity, 116, 119
networks (continued)
defined, 163
DMZ (demilitarized zone) network
segments, 165
failures, 168
firewalls, 165
hardware encryption, 165
intrusion detection and prevention, 165
IP addresses, 164–165
load balancers, 165
managing, 165
recovering, 163–166
routing, 165
security, 165
server configuration, 156
spam filters, 165
voice networks, 164
Web proxies and filters, 165
NFPA 1620, 12
9/11 attacks, 302–304
Novell Identity Manager, 166
NTP (Network Time Protocol), 164, 166

○ Oblix, 161
Occupational Health and Safety
Administration (OSHA), 144–145
off-site storage strategy, 194–196
open standards, 166
operating systems
configuring, 115, 118
derender-user capabilities, 115
installing, 118
managing, 115
patches, 115, 118
servers, 155–156
supported versions, 115
updates, 115, 118
workstations, 113–119
opportunities
for process improvements, 332–333
as a result of disasters, 329
Oracle Identity Management, 166
org chart, 60
OSHA (Occupational Health and Safety
Administration), 144–145

○ Pandemic
Asian flu, 297
Black Death, 297
characteristics of, 297–298
communication systems, 298
disaster recovery plan, 297–300
H5N1 avian flu, 297
Hong Kong flu, 297
SARS (Severe Acute Respiratory
Syndrome), 297
Spanish flu, 297
transportation, 298
walkthrough test, 224
pan/tilt/zoom cameras, 131
paper test
conducting, 221–222
defined, 222, 327
recommended frequency, 237
response team training, 261
parallel test
conducting, 227–229
defined, 327
leadership identification, 336
planning, 234–235
process improvements, 333
recommended frequency, 239–240
response team training, 261
password database, 187
patches for operating systems, 115, 118
Payment Card Industry Data Security
Standard (PCI DSS), 12, 336–338
PBX trunks, 164
PCI DSS (Payment Card Industry Data
Security Standard), 12, 336–338
PDU (Power Distribution Unit), 141
people-related disasters, 279–280
personnel changes, impact on disaster
recovery plan, 245–247
photoelectric smoke detectors, 142
physical access controls for IT
equipment
biometric entry controls, 130, 134–136
equipment cages, 131, 139–140
hardened facilities, 131, 138–139
key-card entry controls, 130, 133–135
locking storage cabinets, 131, 139
man traps, 130, 136–137
security guards, 131, 137–138
video surveillance, 130–132
PIN pad, 134
PIN pad door locks, 134–135
plan. See disaster recovery plan
planning
  emergency operations, 33–34
  resources, 32
  role of, 31–32
plug-ins, 100
political events, 249
Power Distribution Unit (PDU), 141
power failures, 272–273
power feeds, 141
power management. See electricity
power outages
  earthquakes, 287
  IT systems, 335
power supplies. See also emergency
  power
  failures, 335
  redundant, 180
pre-action sprinkler systems, 143
pre-detonation screens, 138
preserving the disaster recovery
  plan, 213
prevention
  enacting preventive measures, 44–46
  facilities-related disasters, 264–269
  fire, 270–272
  HVAC failures, 145, 272
  industrial hazards, 274–275
  people-related disasters, 279–280
  power failures, 272–273
  role of, 31
  security incidents, 280–283
  technology-related disasters, 275–278
preventive measures, 24
print servers, 103
privacy
  backup media, 178
  sensitive data, 162
  probability of occurrence, 20
procedures
  damage assessment procedures,
  203–205
  disaster declaration procedure, 34,
  37–38, 198–200
  document review procedure, 212
  recovery procedures, 22
  system recovery and restart
    procedures, 205–207
  test procedures, 220–221
  transition to normal operations,
  207–209
  walkthrough test procedures, 223–224
process engineering, 252
processes
  Business Impact Analysis (BIA), 55,
  58–60, 70–71
  Capability Maturity Model (CMM), 332
  integration into disaster recovery
  plan, 328
  mission-critical, 52–53, 65
  opportunities for improvements,
  332–333
  risk analysis, 20
  time-critical, 52–53, 65
professional certifications
  Associate Business Continuity
    Professional (ABCP), 315
  Associate of the Business Continuity
    Institute (ABCI), 318
  Business Continuity Certified Expert
    (BCCE), 317
  Business Continuity Certified Planner
    (BCCP), 316
  Business Continuity Certified Specialist
    (BCCS), 317
  Business Continuity Institute (BCI),
  318–319
  Business Continuity Management
    Institute (BCMI), 316–317
  Certified Business Continuity
    Professional (CBCP), 315
  Certified Functional Continuity
    Professional (CFCP), 315
  Disaster Recove Institute, 315–316
  Disaster Recovery Certified Expert
    (DRCE), 317
professional certifications (continued)
Disaster Recovery Certified Specialist (DRCS), 316
Fellow of the Business Continuity Institute (FBCI), 319
Master Business Continuity Professional (MBCP), 315
Member of the Business Continuity Institute (MBCI), 319
Specialist of the Business Continuity Institute (SBCI), 318
Project Management For Dummies (Wiley), 18
project manager, 17–18, 32
project plan, 53
project plan for disaster recovery plan, 18
project team, 53
protecting
  data, 173–175, 184–185
documents, 257
protection
  against civil disturbances, 273–274
  against war, 273–274
publishing documents, 260
purpose of Business Impact Analysis (BIA), 52–53

• Q •

quality of IT systems, 334
Qualys FreeMap, 86–87
Quicktime (Apple), 99

• R •

RAID (Redundant Array of Independent Drives), 179
reciprocal facilities, 147, 151
reciprocal processing site, 184
recordkeeping
  backup media, 178
disaster recovery plan, 261
recovering
  data, 173–176
mobile platforms, 114
networks, 163–166
workstations, 98–99
Recovery Point Objective (RPO), 20–22, 65–66, 73
recovery procedures, 22
recovery server, 157–158
recovery team members
  disaster recovery plan, 209
  instant messaging, 126–127
  walkthrough test, 223
Recovery Time Objective (RTO), 19–22, 64–65, 72–73
reducing disruptive events within IT systems, 334–335
reducing insurance premiums, 335
redundancy of servers, 154
Redundant Array of Independent Drives (RAID), 179
regulations
  BS25999, 12
  HIPAA (Health Insurance Portability and Accountability Act), 13, 337–338
  impact on disaster recovery plan, 249
  ISO27001, 12, 337–338
  NFPA 1620, 12
  PCI DSS (Payment Card Industry Data Security Standard), 12, 336–338
remote access, 116, 119
remote power controllers, 140–141
removable hard drives, 176–179
replacement IT systems
  earthquakes, 287
  floods, 290
tsunamis, 295
replication, 170, 181–182, 304
requirements, establishing, 253–254
resilient architecture, 278
resilient storage, 179–180
resource configuration of servers, 156
resources for planning, 32
response team
  assembling, 37
  contact lists and trees, 34, 47, 200–202
disaster declaration procedure, 38
  maintaining communications, 39–40
  training, 26–27, 48, 261–262
retina scan, 136
reviewing disaster recovery plan, 26
risk analysis
   Business Impact Analysis (BIA), 66, 68–69
disaster scenarios, 20
mitigating steps, 20
probability of occurrence, 20
process improvements, 333
processes, 20
vulnerabilities, 20
Risk Management Guide for Information Technology Systems guide, 69
role
   of planning, 31–32
   of prevention, 31
roles, 188
Rothstein Associates Inc., 321
routing, 165
RPO (Recovery Point Objective), 20–22, 65–66, 73
RTO (Recovery Time Objective), 19–22, 64–65, 73

● S ●
SaaS (Software as a Service), 83
sabotage, 169
Sakurajima volcano, 269
SAN (Storage Area Network), 170, 180
Santa Maria volcano, 269
Santiaguito volcano, 269
Santorini volcano, 269
SARS (Severe Acute Respiratory Syndrome), 297
satellite phones, 287
SBCI (Specialist of the Business Continuity Institute), 318
scenarios, 67–68
scope of disaster recovery plan, 53, 324–325
scribe, role in walkthrough test, 223
secondary effects of disasters, 67
security
data centers, 264–265
dependencies, 94
e-mail, 123–124
networks, 165
workstation operating systems, 117–119
security configuration of servers, 156
security guards, 131, 137–138
security incidents, 280–283, 303–304
security patches, 282
senior management walkthrough test, 223
sensitive data, 162
server access workstations, 102–104
server clustering, 278
servers
   access management, 156
   application servers, 103–104
   building new servers, 157–158
   change management, 158
   clustering, 167–171
   configuration management, 157–158
   consistency across multiple servers, 157–158
   consolidation, 161
   distributed server architecture, 159–160
e-mail servers, 122–123
file servers, 103
hardware configuration, 155
inventories, 156–157
network configuration, 156
network services configuration, 156
Network Time Protocol (NTP), 164, 166
operating systems, 155–156
print servers, 103
recovery server, 157–158
redundancy, 154
redundant server connections, 180
resource configuration, 156
security configuration, 156
system readiness, 154–155
system-level components, 156
Web servers, 103
Service Level Agreements (SLAs), 311–312
Service-Oriented Architecture (SOA), 159, 166
Severe Acute Respiratory Syndrome (SARS), 297
severe weather. See also hurricanes; ice storms; tornados; wind storms
emergency power, 291–293
emergency supplies, 291–293
supplemental communications, 291–293
walkthrough test, 224
Shockwave, 99
Simple Mail Transfer Protocol (SMTP), 166
Simple Network Management Protocol (SNMP), 166
simulation test
carried out, 226–227
defined, 327
interim plan, 49–50
leadership identification, 336
process improvements, 333
Single Sign On (SSO), 187
site selection, 265–269
Skype, 127
SLA Toolkit, 311–312
SLAs (Service Level Agreements),
311–312
smart card reader, 133
smoke detectors, 142
SMTP (Simple Mail Transfer
Protocol), 166
SNMP (Simple Network Management
Protocol), 166
SOA (Service-Oriented Architecture),
159, 166
social engineering, 281
software. See also applications; tools
failures, 168, 276–277
inventory, 78–79
SaaS (Software as a Service), 83
spam filters, 124, 165
Spanish flu pandemic, 297
Specialist of the Business Continuity
Institute (SBCI), 318
sprinkler systems, 143–144
SSO (Single Sign On), 187
stakeholder support for disaster
recovery plan, 326–327
standards
BS25999, 12
case study, 254–256
establishing, 253–254
GSM cellular telephone communication
standard, 166
HIPAA (Health Insurance Portability
and Accountability Act), 13, 337–338
ISO27001, 12, 337–338
NFPA 1620, 12
open standards, 166
PCI DSS (Payment Card Industry Data
Security Standard), 12, 336–338
statements of impact, 62–63
steering committee, 18
storage architecture, 170
Storage Area Network (SAN), 170, 180
storing
data backups, 178, 182–183
disaster recovery plan, 213
interim plan, 46–47
storms. See ice storms; tornados; wind storms
Strohl Systems
BIA Professional, 308
Living Disaster Recovery Planning
System (LDRPS), 307–308
structure of disaster recovery plan
document-level, 211–212
enterprise-level, 210–211
subject matter experts
disaster recovery plan, 32
interviewing, 85
walkthrough test, 223
Sun Java System Identity Manager, 166
Sun Microsystems Project Blackbox, 150
Sun Solstice Enterprise Manager, 86
SunGard mobile data center, 150
supplemental communications
avalanches, 297
earthquakes, 287
floods, 290
hurricanes, 292
ice storms, 291
landslides, 297
severe weather, 291–293
tornadoes, 293
tsunamis, 295
wildfires, 288
wind storms, 291
suppliers, 55, 62, 71
suppressing fire, 142
surveillance, 130–132, 283
survival of businesses and role of disaster recovery plan, 12, 331
switching equipment, 141
system clocks, 164, 166
system dependencies, 91–92
system failures, 276
system readiness, 154–155
system recovery and restart procedures, 205–207
system-level components of servers, 156
systems and services acquisition, 250–252
systems development, 251

T

Taal Volcano volcano, 269
tape backups, 176–179
TCP/IP, 166
technology. See IT systems technology changes, impact on disaster recovery plan, 242–243
technology-related disasters, 275–278
Teide volcano, 269
teleconference bridge, 40
telephone service, 164
telework, 246–247
temperature fire detectors, 142
TEMPEST (Transient Electromagnetic Pulse Emanation Standard), 138
terminal emulators, 192
terminals, 99–102
terrorism, 169, 302–303
testing
checklist testing, 49
cutover test, 230–236, 327, 333, 336
frequency of, 26, 236–240
importance of, 24–25, 217–219
interim plan, 48–50
paper test, 221–222, 327
parallel test, 227–229, 234–236, 327, 333, 336
simulation test, 49–50, 226–227, 327, 333, 336
test procedures, 220–221
test strategy, 219–220
walkthrough test, 49–50, 222–226, 327, 333
threat modeling, 66, 68
time for developing disaster recovery plan, 326
time-critical processes, 52–53, 65
tools
BCP Generator, 309
BIA Professional, 308
Cheops, 86
COBRA Risk Analysis, 308–309
Disaster Recovery Plan Template, 310–311
DRI Professional Practices Kit, 310
DRJ's Toolbox, 313
Emergency Management Guide For Business & Industry, 312
FreeMap, 86
HP OpenView, 85
IBM NetView, 85
LANSurveyor, 86
LBL ContingencyPro Software, 312
Living Disaster Recovery Planning System (LDRPS), 307–308
netViz, 86
Network Magic, 86
network mapping tools, 85–87
SLA Toolkit, 311–312
Sun Solstice Enterprise Manager, 86
top-down view of IT systems, 80
tornados
alternate processing facility, 293
communication systems, 293
disaster recovery plan, 292–293
emergency power, 293
emergency supplies, 293
server clusters, 169
site selection, 265–266
supplemental communications, 293
transmission, 293
walkthrough test, 224
training
employees, 262
response team, 26–27, 48, 261–262

Transitional Electromagnetic Pulse
Emanation Standard (TEMPEST), 138
transition to normal operations, 207–209
transmitting data, 184–185

transportation
avalanches, 295
civil disturbances, 301
disruption of, 10–11
earthquakes, 285–286
floods, 289
hurricanes, 291
ice storms, 290–291
landslides, 295
pandemic, 298
tornados, 293
tsunamis, 294
volcanic eruptions, 288–289
volcanoes, 288–289
wildfires, 287
wind storms, 290–291
trunks, 164

vandalism, 169
vehicle barriers, 139
version control (for disaster recovery
plan), 212
Vesuvius volcano, 269
video recording equipment, 131
video surveillance, 130–132, 283
viewing monitors, 131
virtual networks (VLANs), 165
Virtual Private Network (VPN), 116
virtualization, 180
VLANs (virtual networks), 165
voice communications, 119–121
voice networks, 164
volcanic eruptions
\( \cdot U \cdot \)
Ulawun volcano, 269
Uninterruptible Power Supply (UPS), 141
updates for operating systems, 115, 118
upgrading documents, 258–259
UPS (Uninterruptible Power Supply), 141
U.S. Department of Homeland
Security, 320
U.S. National Institute for Standards and
Technology, 69
users. See end users
utility changes, 248
utility failures
\( \cdot V \cdot \)
utility outages, 10
vandalism, 169
vehicle barriers, 139
version control (for disaster recovery
plan), 212
Vesuvius volcano, 269
video recording equipment, 131
video surveillance, 130–132, 283
viewing monitors, 131
virtual networks (VLANs), 165
Virtual Private Network (VPN), 116
virtualization, 180
VLANs (virtual networks), 165
voice communications, 119–121
voice networks, 164
volcanic eruptions
\( \cdot U \cdot \)
Ulawun volcano, 269
Uninterruptible Power Supply (UPS), 141
updates for operating systems, 115, 118
upgrading documents, 258–259
UPS (Uninterruptible Power Supply), 141
U.S. Department of Homeland
Security, 320
U.S. National Institute for Standards and
Technology, 69
users. See end users
utility changes, 248
utility failures
\( \cdot V \cdot \)
utility outages, 10
vandalism, 169
vehicle barriers, 139
version control (for disaster recovery
plan), 212
Vesuvius volcano, 269
video recording equipment, 131
video surveillance, 130–132, 283
viewing monitors, 131
virtual networks (VLANs), 165
Virtual Private Network (VPN), 116
virtualization, 180
VLANs (virtual networks), 165
voice communications, 119–121
voice networks, 164
volcanic eruptions
\( \cdot U \cdot \)
Ulawun volcano, 269
Uninterruptible Power Supply (UPS), 141
updates for operating systems, 115, 118
upgrading documents, 258–259
UPS (Uninterruptible Power Supply), 141
U.S. Department of Homeland
Security, 320
U.S. National Institute for Standards and
Technology, 69
users. See end users
utility changes, 248
utility failures
\( \cdot V \cdot \)
utility outages, 10
vandalism, 169
vehicle barriers, 139
version control (for disaster recovery
plan), 212
Vesuvius volcano, 269
video recording equipment, 131
video surveillance, 130–132, 283
viewing monitors, 131
virtual networks (VLANs), 165
Virtual Private Network (VPN), 116
virtualization, 180
VLANs (virtual networks), 165
voice communications, 119–121
voice networks, 164
volcanic eruptions
\( \cdot U \cdot \)
Ulawun volcano, 269
Uninterruptible Power Supply (UPS), 141
updates for operating systems, 115, 118
upgrading documents, 258–259
UPS (Uninterruptible Power Supply), 141
U.S. Department of Homeland
Security, 320
U.S. National Institute for Standards and
Technology, 69
users. See end users
utility changes, 248
utility failures
\( \cdot V \cdot \)
utility outages, 10
vandalism, 169
vehicle barriers, 139
version control (for disaster recovery
plan), 212
Vesuvius volcano, 269
video recording equipment, 131
video surveillance, 130–132, 283
viewing monitors, 131
virtual networks (VLANs), 165
Virtual Private Network (VPN), 116
virtualization, 180
VLANs (virtual networks), 165
voice communications, 119–121
voice networks, 164
volcanic eruptions
\( \cdot U \cdot \)
Ulawun volcano, 269
Uninterruptible Power Supply (UPS), 141
updates for operating systems, 115, 118
upgrading documents, 258–259
UPS (Uninterruptible Power Supply), 141
U.S. Department of Homeland
Security, 320
U.S. National Institute for Standards and
Technology, 69
users. See end users
utility changes, 248
utility failures
\( \cdot V \cdot \)
utility outages, 10
vandalism, 169
vehicle barriers, 139
version control (for disaster recovery
plan), 212
Vesuvius volcano, 269
video recording equipment, 131
video surveillance, 130–132, 283
viewing monitors, 131
virtual networks (VLANs), 165
Virtual Private Network (VPN), 116
virtualization, 180
VLANs (virtual networks), 165
voice communications, 119–121
voice networks, 164
volcanic eruptions
\( \cdot U \cdot \)
Ulawun volcano, 269
Uninterruptible Power Supply (UPS), 141
updates for operating systems, 115, 118
upgrading documents, 258–259
UPS (Uninterruptible Power Supply), 141
U.S. Department of Homeland
Security, 320
U.S. National Institute for Standards and
Technology, 69
users. See end users
utility changes, 248
utility failures
\( \cdot V \cdot \)
utility outages, 10
vandalism, 169
vehicle barriers, 139
version control (for disaster recovery
plan), 212
Vesuvius volcano, 269
video recording equipment, 131
video surveillance, 130–132, 283
viewing monitors, 131
virtual networks (VLANs), 165
Virtual Private Network (VPN), 116
virtualization, 180
VLANs (virtual networks), 165
voice communications, 119–121
voice networks, 164
volcanic eruptions
walkthrough test
conducting, 222–226
defined, 327
interim plan, 49–50
process improvements, 333
recommended frequency, 238–239
response team training, 261
war, 273–274, 302–303
warm sites, 147–149, 206
water/flooding detection, 145–146
Web applications, 99–100
Web browsers, 192
Web proxies and filters, 165
Web servers, 103
Web sites
APC InfraStruXure Express, 150
BCP Generator, 309
Business Continuity Institute (BCI), 318–319
Business Continuity Management Institute (BCMI), 316–317
Capability Maturity Model (CMM), 332
Cheops, 86
Computerworld Disaster Recovery, 319
CSO Business Continuity and Disaster Recovery, 320
Disaster Recovery Journal, 310, 313, 316
Disaster Recovery Plan Template, 310–311
Disaster Recovery Planning.org, 317–318
Disaster Recovery World, 317
Disaster-Resource.com, 319
DRI International, 315–316
DRI Professional Practices Kit, 310
Federal Emergency Management Agency (FEMA), 320
For Dummies, 5
FreeMap, 86
HIPAA (Health Insurance Portability and Accountability Act), 338
HP OpenView, 85
IBM NetView, 85
International Standards Organization, 338
LANsurveyor, 86
LBL ContingencyPro Software, 312
National Institute for Standards and Technology, 69
netViz, 86
Network Magic, 86
Payment Card Industry Data Security Standard (PCI DSS), 338
Rothstein Associates Inc., 321
SLA Toolkit, 311
Strohl Systems, 307–308
Sun Microsystems Project Blackbox, 150
Sun Solstice Enterprise Manager, 86
SunGard, 150
Web terminals, 99–102
wet pipe sprinkler systems, 143
WHO (World Health Organization), 297
wildfires
communications systems, 287–288
disaster recovery plan, 287–288
emergency supplies, 288
firefighting equipment, 288
IT systems, 287
site selection, 269
supplemental communications, 288
transportation, 287
wind storms
disaster recovery plan, 290–291
emergency power, 291
emergency supplies, 291
supplemental communications, 291
walkthrough test, 224
window coating, 139
Windows Media Player, 99
worksheets (for Business Impact Analysis), 56–57
workstations
application clients, 104–108
hardware platforms, 114–115
local computers, 108–113
workstations (continued)
managing, 98–99
Network Time Protocol (NTP), 164, 166
operating systems, 113–119
recovering, 98–99
server access, 102–104
terminals, use as, 99–102

World Continuity Congress, 317
World Health Organization (WHO), 297
World Wide Web, 166
writing
disaster recovery plan, 24
interim plan, 35–36