

INDEX

- Ad hoc responses, 7, 42. *See also* Unprepared organizations
- Airline crisis, 185–87, 188, 189
- Airport traffic control crisis, 172–73
- AT&T, 172–73
- Audits. *See* Crisis audits
- Backup activities, 53–54
- Breaks. *See* Equipment/plant malfunction
- Business recovery, 53–54
- crisis audits and, 76, 77, 79–80
- industrial disaster example and, 169–70, 178–79
- in overall picture of crisis management, 10, 17–18
- Causal factors, types of, 48–50.
See also Types of crises
- Challenger disaster, 47, 76, 78
- Chemical industry crisis, 37–39
- CM. *See* Crisis management
- CMT. *See* Crisis management team
- Communications. *See also*
- Initial information phase;
- Injuries, response to;
- Media; Responsibility for crisis, assumption of;
- Systemic factors
- blocking of, 47, 49
- crisis management team and, 104
- key customers and, 53, 54
- notification of senior officers and, 32–33
- in overall picture of crisis management, 10, 18–19
- public perception and, 175–76, 177, 187–89
- systemic crisis involving, 106–11
- Community, surrounding, 181.
See also Communications; Media; Public perception

- Contaminant leak, and crisis
 management process, 159–82
 crisis scenario for, 160–71
 goals of crisis management in, 161–62
 overview of crisis
 management and, 171–82
 warning signal detection and, 162–64
- Corporate Communications (CC) division, 87, 104
- Credibility of information
 sources, 28–30, 124, 186–87
- Criminal attack, 46, 73. *See also*
 Product tampering; Types of crises
- Crisis. *See also* Precipitating crisis; Secondary crisis; Types of crises
 capabilities needed to handle, 7
 checklist on preparedness for, 20–24
 definition of, 7–8
 importance of preparation for, 6, 40–42
 inevitability of, 5–7
 matched *vs.* experienced, in CrMgt, 145–46
 Crisis audits, 59–97. *See also*
 Postcrisis audit; Precrisis audit
 CrMgt software package and, 129, 139–42
 development of crisis
 management capabilities and, 85–94
 example of, 95–96
 importance of, 97
 main factors of crisis
 management and, 71–85
 postcrisis audit and, 69–71
 precrisis audit and, 60–68
 Crisis diagnosis phase, 42–50
 causes of crisis and, 48–50
 early warning signs and, 47
 types of crises and, 42–47
 Crisis management (CM). *See also*
 Phases of crisis management; Preparedness
 characteristics of effective
 approach to, 116–17
 contaminant leak example and, 159–82
 criteria for crisis response, 38–39, 40
 detailed guide to, 27–55
 development of capabilities for, 85–94
 goals of, in industrial disaster, 161–62
 ideal manual for, 190–92
 main factors in, 71–85
 overview of, 8–19, 171–80
 postcrisis audit and, 69–71
 precrisis audit and, 60–68
 as systematic, 19–20, 75, 115–17
 Crisis management (CM)
 profile, 66–68, 123–26, 127, 136, 152–55
 Crisis management team (CMT)
 activation of, 31–32, 163–64, 174, 175

- business resumption and, 169–70
 composition of, 12–13, 87
 early actions of, 35
 information on, in CrMgt software package, 146, 151, 152
 in overall picture of crisis management, 10, 12–13
 responsibilities on, 101–4
 role of facilitator on, 89, 101
 simulation example and, 91, 92–94
 systems thinking and, 104–11
 training of, 13, 87, 89–96
 Crisis portfolio, 72
 Crisis-prone organizations, 49, 78, 80, 82–83, 85. *See also*
 Unprepared organizations
 Critical systems thinking
 crisis management
 effectiveness and, 117
 as function of crisis
 management team, 104–6
 importance of, 106–11
 selling crisis management and, 115–16
 CrMgt software package, 121–42
 “Audit” button, 134, 139
 button colors in, 128
 Capability Score in, 146–52
 “Clear All” button, 130
 “Clear” buttons (third card), 139
 “Click Here to Continue” button, 133–34, 139
 “Click here to start” button, 124
 “CM PROFILES” button, 152–55
 “Conduct Interdisciplinary Risk Analyses” box, 152, 154
 crisis management profile and, 66–68, 123–26, 127, 136
 damage containment strategies and, 80–82
 “Dial” button, 152
 entering information into, 128, 130
 first (main control) card in, 127, 128–29, 139, 155
 fourth card in, 139–42
 “Hide all” button, 128, 134
 “II PHASES” button, 146
 information on crisis management team in, 146, 151, 152
 “I Types” button (fourth card), 139–42
 moving between screens in, 128, 129, 130
 Performance Score in, 144–46
 Plan Score in, 142, 143
 quitting, 128, 129
 “Return” button, 130, 142
 scoring in, 142, 144–52
 second card in, 129–34, 135
 “Show all” button, 128, 134
 starting up, 122–23, 128
 “Systems Causes Known?” button, 134

- CrMgt software package
(*continued*)
third card in, 134, 136, 137
"Type/Nature of Crisis
Known?" button, 130-33,
134, 142
- Damage containment, 50-52
crisis audits and, 76, 77, 79
CrMgt software package and,
137-39
industrial disaster example
and, 167-69
in overall picture of crisis
management, 10, 17-18
strategies for, by type of
crisis, 80-82
- Decisionmaking
assumption of responsibility
and, 33-35
checklist in CrMgt software
package, 123-29
crisis diagnosis and, 42-50
determination of preparedness
and, 31
determination of
responsibility and, 35-39
information sources and, 28-
30
non-proactive response and,
35-39
proactive response and, 31-33
seriousness of crisis and, 35-
39
- Development of capabilities,
85-94
audits and, 85, 87
- crisis management team and,
87, 89
CrMgt software package and,
146-52, 154
simulations and, 89-94
- Early warning signals, blocking
of, 47, 96. *See also* Signal
detection
- Economic attack, 46, 73. *See
also* Types of crises
- Emotional trauma, 176-78
- Equipment/plant malfunction,
46, 73. *See also* Systemic
factors; Types of crises
- Evacuation, 52-53, 175-76,
179-80
- Exxon Valdez oil spill, 14-15,
79
- Food industry crisis, 37-39
Fortune magazine, 14-15
- GM products crisis, 30
- Governmental authorities. *See
also* Regulatory crisis;
Stakeholders
in overall picture of crisis
management, 10, 18-19
treatment phase of crisis and,
52-53, 179
- Health and Safety division, 87,
103-4
- Health crisis, 46, 74. *See also*
Types of crises
- Honda, 106

- Human factors, as cause of
crisis, 48, 172-73. *See also*
Systemic factors
- Human resources crisis, 46,
74. *See also* Types of
crises
- IBM PC type computers, and
CrMgt software package,
121-22
- Ideal crisis manual, 190-92
- Industrial disaster, 46, 73. *See
also* Types of crises
contaminant leak example,
159-82
- Information sources
industrial disaster example
and, 167-69
power and credibility of, 28-
30, 124, 186-87
- Initial information phase
assumption of responsibility
and, 33-35
CrMgt software package and,
123-29
determination of
responsibility and, 38-39
determination of seriousness
and, 35-39
effect of delayed response
and, 40-42
nature of source of
information and, 28-30
prepared *vs.* unprepared
organizations and, 172-74
proactivity decision and, 31-
33
- Injuries, response to. *See also*
Seriousness of crisis
assumption of responsibility
and, 33-35
crisis diagnosis and, 45
as first priority, 10, 13-16
treatment of injured persons,
178
- Isolation, as containment
option, 50, 52
- Johnson & Johnson, 33, 187-88
- Key customers, 53, 54. *See also*
Stakeholders
- Larousse encyclopedia crisis,
75-76
- Learning, 80, 170-71. *See also*
"No-fault learning"; Phases
of crisis management;
Postcrisis audit
- Legal counsel, role on crisis
management team, 87,
101-2
- Legal crisis, 46, 74. *See also*
Types of crises
- Macintosh computers, and
CrMgt software package,
121
- Management audit guide, 62-
64
- Media. *See also* Information
sources; Stakeholders
in crisis management process,
9, 10, 11-12, 18-19

- Media (*continued*)
 crisis management team and, 104
 as initial source of information, 29–30
 organizational credibility with, 165–66, 187–88
 prototype messages and, 177
 Monitoring, 28–30, 36, 169
- NASA, 104, 106, 113. *See also* *Challenger* disaster
 Natural disaster, 46, 73. *See also* *Types of crises*
 “No-fault learning,” 70–71, 76, 77, 80, 170–71
- Object-oriented programming, 124
- Occupational crisis. *See* Human resources crisis
- Operations division. *See* Quality assurance division
- Organizational crisis. *See* Crisis
- Organizational culture. *See also* Systemic factors
 as cause of crisis, 48–49, 104–11
 crisis audits and, 82–83
 crisis awareness exercises and, 111–14
 precrisis surveys and, 181–82
 selling crisis management and, 115–16
- Organizational structure
 as cause of crisis, 48–49
 crisis audits and, 70, 82
- PA. *See* Public affairs division
- Phases of crisis management
 components of, 76–82
 crisis audits and, 66, 69–71, 96
 crisis diagnosis phase, 42–50
 CrMgt software package and, 146, 147
 initial information and action phase, 28–42
 preparedness and, 76–82
 treatment phase, 50–54
- Postcrisis audit, 59, 61, 68–71
 causal factors and, 69–71
 CrMgt software package and, 129, 144–46
 goal of, 68
 “no-fault learning” and, 70–71, 80
- Power of information sources, 28–30, 124, 186–87
 definition of power and, 30
- Precipitating crisis
 decision to monitor, 28–30
 identification of, 10, 16–17
 in overall picture of crisis management, 9, 10
- Precrisis audit, 60–68, 129
 scoring types in CrMgt software package and, 142, 143
- Preparedness
 checklist, 20–24
 crisis audits and, 76, 77, 78–79
 determination of, during crisis, 31–32

- development of crisis
 awareness and, 111–13
 development of crisis
 management capabilities and, 85–94
 importance of, 6, 55, 180
 in industrial disaster example, 164–66
 issues associated with main factors and, 71–85
 notification of senior officers about crisis and, 32–33
 precrisis activities and, 180–82
 precrisis audit and, 60–68
 scoring for, in CrMgt software package, 142, 143
- Prevention. *See* Preparedness
- Proactivity, 31–33
 activities following non-proactive decision, 35–39
- Probing. *See* Preparedness
- Product tampering, 75–76. *See also* Criminal attack
- Proprietary information, loss of, 46, 73. *See also* *Types of crises*
- Public affairs (PA) division, 87, 104
- Public perception. *See also* *Types of crises*
 crisis communication and, 175–76, 181, 187–89
 organization as villain, hero, or victim and, 10, 19
 as type of crisis, 46, 74
- Quality assurance (QA) division, 87, 103
- Rawl, Lawrence, 14–15
- Recovery. *See* Business recovery
- Regulatory crisis, 46, 74. *See also* *Types of crises*
- Removal, as containment option, 50, 52
- Responsibility for crisis
 assumption of, 33–35, 37–39
 determination of, 35–39
- Resumption of business. *See* Business recovery
- Reward system. *See* Organizational structure
- Scrolling field, 132
- Sears, financial crisis at, 104–5, 113
- Secondary crisis, 10, 19, 40
- Security division, 87, 102–3
- Senior officers. *See* Top management
- Seriousness of crisis, 35–39
- Signal detection, 76, 77, 78, 96, 162–64. *See also* Early warning signals
- Simulation exercises, 89–94
 example of, 91, 92–94
- Stakeholders. *See also* Governmental authorities; Media
 crisis audits and, 66, 69–71, 83–85, 86, 96
 CrMgt software package and, 146, 149, 150

- Stakeholders (*continued*)
 external, 70, 88, 150
 internal, 86, 149, 151
- Stand-alone applications,
 122
- Storage sites, hot *vs.* cold, 53–
 54
- SuperCard software system,
 122, 123–25
- Systemic factors. *See also*
 Critical systems thinking
 crisis audits and, 66, 69–71,
 82–83, 84, 96
 CrMgt software package and,
 146, 148
 nature of crisis management
 and, 19–20, 115–17
- Technology, as cause of crisis,
 48. *See also* Systemic
 factors
- Temporary facilities, 53–
 54
- Top management. *See also*
 Crisis management team;
 Systemic factors
 crisis management team and,
 87
 development of crisis
 awareness and, 111–13
 notification about crisis, 32–
 33
 postcrisis audit and, 70
 precrisis audit interviews and,
 60–65
 psychology of, as cause of
 crisis, 49, 82–83
 response of, in non-prepared
 organization, 34, 35, 42
 trauma treatment and, 177–
 78
- Total quality management
 (TQM), 75
- Training
 assassin-team exercise and,
 113–14
 crisis management team and,
 13, 87, 98–96
 development of crisis
 awareness and, 111–13
 industrial disaster example
 and, 166
- Treatment phase, 50–54, 178–
 80. *See also* Business
 recovery; Damage
 containment; Evacuation
- Tylenol poisonings, 33, 187–88
- Types of crises
 crisis audits and, 66, 69–71,
 95–96
 crisis diagnosis and, 42–47
 CrMgt software package
 and, 129–34, 135, 141,
 142, 143
 damage containment
 strategies and, 80–82
 preparedness and, 71–76
- Union Carbide explosion in
 India, 79
- Unprepared organizations. *See*
also Crisis-prone
 organizations
 ad hoc responses and, 7, 42

- communications and, 32–33
 crisis diagnosis and, 45–47
 example of systemic crisis
 and, 106–11
 impact of delayed response
 and, 40–42
 organizational culture and,
 82–83
 performance scoring in CrMgt
 and, 144
 USAir crisis, 185–87, 188–89
 Utilities industry, audit example
 for, 95–96
 Witnesses, and trauma
 treatment, 177–78

IIM (IAN I. MITROFF) LICENSE AGREEMENT

This is a legal agreement between you (either an individual or an entity), the end user, and IIM. If you do not agree to the terms of this Agreement, promptly return the disk to Oxford University Press, 198 Madison Ave., New York, New York 10016-4314.

IIM SOFTWARE LICENSE

(1) GRANT OF LICENSE. This IIM (Ian I. Mitroff) License Agreement ("License") permits you to use one copy of the specified version of the IIM software product identified below ("SOFTWARE") on any single computer provided SOFTWARE is in use on only one computer at any time unless you have express written permission from IIM, the author/developer of the SOFTWARE. The SOFTWARE is "in use" on a computer when it is loaded into the tem-

porary memory (i.e., RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that computer, except that a copy installed on a network server for the sole purpose of distribution to other computers is not "in use." If the anticipated number of users of the SOFTWARE will exceed the number of applicable Licenses, then you must have a reasonable mechanism or process in place to assure that the number of persons using the SOFTWARE concurrently does not exceed the number of Licenses. If the SOFTWARE is permanently installed on the hard disk or other storage device of the computer (other than a network server) and one person uses that computer more than eighty percent of the time it is in use, then that person may also use the SOFTWARE on a portable or home computer.

(2) **COPYRIGHT.** The SOFTWARE is owned by IIM and is protected by United States copyright laws in international treaty provisions. Therefore, you must treat the SOFTWARE like any other copyrighted material, e.g., a book or a musical recording, except that you may either (a) make one copy of the software solely for back up or archival purposes, or (b) transfer the SOFTWARE to a single hard disk provided you keep the original solely for back-up or archival purposes. You may not copy the written materials accompanying the SOFTWARE.

(3) **OTHER RESTRICTIONS.** This IIM License Agreement is your proof of license to exercise the rights granted herein and must be retained by you. You may not rent, lease, or transfer the SOFTWARE to other persons except that you transfer to another person on a permanent basis provided that you retain no copies and the recipient agrees to the terms of this license. You may not reverse engineer, decompile, or disassemble the SOFTWARE.

(4) **LIMITED WARRANTY.** IIM warrants that (a) the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt; and (b) any hardware accompanying the SOFTWARE will be free from defects in materials and workmanship under normal use and service for a period of one (1) year from the date of receipt. Any implied warranties on the SOFTWARE and hardware are limited to ninety (90) days and one (1) year, respectively.

(5) **NO OTHER WARRANTIES.** IIM disclaims all other warranties, either expressed or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose, with respect to the SOFTWARE, the accompanying written materials, and any accompanying hardware.

(6) *NO LIABILITY FOR CONSEQUENTIAL DAMAGES.* In no event shall IIM, Oxford University Press, or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use this IIM product, even if IIM has been advised of the possibility of such damages.

(7) The SOFTWARE was created on SuperCard. SuperCard is a registered trademark of the Allegiant Technology Corporation, Inc., copyright 1989–1991, 1994.