

Harris Interactive Online survey reviews crisis planning in US companies

Highlights top worries and the crisis management plans in place to deal with incidents that occur.

Topping the list of crisis situations that worry corporate executives is compromise of corporate information systems, cited by 61 percent as a major worry or one of their top worries. Terrorism (55 percent) and corporate malfeasance (40 percent) round out the top-three potential crisis situations that worry these business leaders most.

These are among the results of an Internet-based survey of 197 senior executives of large corporations (US\$1 billion+ in revenue) conducted in September by Harris Interactive. The results have only just been published.

"No business can survive without customer trust," said Mike Dabadie, division president of the company's Brand and Strategic Consulting practice. "In today's computerized economy, customers trust companies with a lot of sensitive personal and financial information. Any breach of data security that would compromise that trust can have a devastating impact on the company's reputation."

Commenting on the 55 percent who named terrorism as a major worry, Dabadie said, "The fact that, more than five years after 9/11, more than half of business leaders are still worried about terrorism is a significant finding."

To view the complete December 2006 issue of The Harris Report that elaborates these data and offers advice to business leaders on principles of effective crisis management, go to <http://www.harrisinteractive.com/news/harrisreport.asp>

The following tables show questions and responses from the survey:

TABLE1
CRISIS SITUATIONS AND EXTENT OF WORRY

Question:

"Now we'll present a list of situations that others have mentioned. Please indicate whether that is one of your top worries, a major worry, a minor worry or not a worry at all."

Base: All respondents

	Total Top/Major Worry (NET)* %	One of my top worries %	A major worry %	A minor worry %	Not a worry at all %
Compromise of corporate information systems	61	24	37	30	9
Terrorism	55	13	42	31	14
Corporate malfeasance	40	14	26	38	22
Environmental mishaps	32	8	25	39	29
Negative claims about product health or safety	30	7	23	35	35
Internet rumors and					

misinformation	29	6	23	48	23
Industrial accidents	24	4	21	43	33
Product contamination or tampering	23	5	18	33	44
Product recalls	21	4	18	32	47
Workforce violence	19	2	17	46	36

*Net includes: "One of my top worries" + "A major worry."

Note: Percentages may not add up to exactly 100% due to rounding.

TABLE 2
BUSINESS-RELATED CRISIS SITUATIONS AND EXTENT OF WORRY

"Now consider just a few more situations that may be a more normal part of the business environment. Again, please indicate the extent to which each worries you."

Base: All respondents

	Total Top/Major Worry (NET)* %	One of my top worries %	A major worry %	A minor worry %	Not a worry at all %
Negative financial news about the company	45	12	34	43	12
Litigation against the company	40	8	32	47	13
Negative news about workplace or business practices	39	9	30	50	11
Unexpected corporate leadership changes	31	7	24	53	16
Strikes or work stoppages	16	2	14	31	53

*Net includes: "One of my top worries" + "A major worry."

Note: Percentages may not add up to exactly 100% due to rounding.

TABLE 3
CRISIS MANAGEMENT PLAN IN PLACE

"Does your company have a crisis management plan in place for situations like those mentioned previously?"

Base: All respondents

	Total %
Yes	74
No	26

TABLE 4
MAJOR COMPONENTS OF CRISIS MANAGEMENT PLAN

"What are the major components of this crisis management plan?"

Base: Has crisis management plan (n=146 respondents)

	Total
	%
Advance procedures (Net)	32
Communication	18
Setup of specific guidelines	8
Recovery plan	8
Training	2
Proactive response	2
Risk management program	1
Contact HR	1
Data/Security (Net)	18
Business continuity planning	10
Alternate/Backup locations	5
Redundant/Backup data sources	3
Safety/Security contingencies	2
Tested backup plans	2
Disaster preparedness	1
Team/Leadership/People (Net)	18
Team setup	7
Leadership/Decision makers	5
Subject matter experts	3
Staff involvement	3
Succession planning	2
Response responsibility	1
Legal/PR/Media response (Net)	9
Public relations	5
Legal response	3
Media contact	3
No answer given (Net)	23
Confidential material	15
Not part of that process	5
Too extensive to explain	4
Other	11
Don't know	14
Decline to answer	10

Note: Multiple-response question.

TABLE 5
USE OF CRISIS MANAGEMENT PLAN COMPONENTS

"Have you ever had to use any component of this crisis management plan?"

Base: Has crisis management plan (n=146 respondents)

	Total
	%
Yes	40
No	60

TABLE 6
SATISFACTION WITH PERFORMANCE OF PLAN

"And, how satisfied were you with the way this plan performed?"

Base: Used crisis management plan (n=59 respondents)

	Total %
Total satisfied (Net)	85
Very satisfied	37
Somewhat satisfied	47

Total dissatisfied (Net) 15

Somewhat dissatisfied 12

Very dissatisfied 3

Note: Percentages may not add up to exactly 100% due to rounding.

TABLE 7
MONITORING OF BLOGS OR WEBSITES

"Does your company monitor blogs or websites for information pertaining to
your line of business?"

Base: All respondents

	Total %
Yes	53
No	47

TABLE 8
EFFECTIVENESS OF MONITORING TO MANAGE POTENTIAL CRISIS

"How effective is this monitoring in your efforts to help manage potential
crises?"

Base: Company monitors blogs (n=105 respondents)

	Total %
Total effective (Net)	70
Very effective	10
Somewhat effective	60
Total ineffective (Net)	30
Somewhat ineffective	26
Very ineffective	5

Note: Percentages may not add up to exactly 100% due to rounding.

TABLE 9
ACTIVITIES TO MINIMIZE RISKS

"More generally, what kind of activities are you or other senior executives working on to minimize various risks to which your company could be exposed?"

Base: All respondents

	Total %
Advance procedures (Net)	27
Communication	9
Training	8
Risk management program	5
Better planning	5
Setup of specific guidelines	4
Recovery plan	3
Crisis management	1
Proactive response	1
Data/Security (Net)	24
Safety/Security contingencies	8
Improving privacy breaches/Internet security	8
Business contingency planning	5
Redundant/Backup data sources	3
Alternate/Backup location	1
Disaster preparedness	1
Pandemic preparedness	1
Improved systems	1
Company audits/monitoring (Net)	19
Monitoring	7
Quality control	4
Compliance policies/teams	4
Company audits	3
Being ethical	3
Complying with Sarbanes-Oxley	3
Legal/PR/Media response (Net)	5
Public relations	2
Media contact	2
Legal response	2
Team/Leadership/People (Net)	5
Team setup	2
Staff involvement	1
Staff hiring process	1
Leadership/decision makers	1
No answer given (Net)	12
Confidential material	6
Not part of the process	5
Too extensive to explain	1
Other	14
None/Nothing	4
Don't know	6
Decline to answer	14

Note: Multiple-response question.