

How to Respond to War in Iraq

Rich Mogull, Dan Miklovic

The outbreak of war in Iraq places stress on enterprises in a number of ways. Enterprises should focus on the basics, such as keeping workers safe and supply chains running.

NEWS ANALYSIS

Event

On 19 March 2003, a U.S.-led coalition attacked Iraq to remove the regime of President Saddam Hussein and disarm the country.

Analysis

Times of crisis call for enterprises and IT managers to remain cool-headed and to attend to basics. Implement crisis management plans but do not make sudden changes in direction or do anything drastic unless it's been thought out. For the present, Gartner reiterates the following advice:

- *Don't panic and don't succumb to media hype.* If you hear media reports about a situation that may require action, confirm them first with government officials, IT security groups, industry groups or peers within your industry.
- *Address workforce and workplace issues.* Focus first on the health and safety of workers — keep in touch with traveling employees and secure workplaces that could be targeted by protests or attacks. Expect that workers will need to remain in close touch with family. Accommodate workers who are reservists, civic volunteers or emergency workers. Plan for additional call-ups.
- *Set up a separate database to allow workers to discuss the war.* Gently remind workers they should not clog company e-mail with such discussion and should above all refrain from national or religious slurs.
- *Ensure the continuity of supply chains and outsourcing.* Communicate closely with suppliers, customers and partners. Develop redundancies — for example, line up alternative suppliers and have outsourcing vendors back up code, data and critical project information on site.
- *Put disaster recovery teams on alert* (for example, cancel vacations). Engage your crisis management facility. Gather the latest contact information for all staff and document travel plans for all employees.
- *Prepare for increased "hactivism"* as people use cyberattacks to express political views. Establish mechanisms for reporting suspicious activities.
- *Enterprises involved with government, critical infrastructure or brands emblematic of the United States or its allies* (such as Coca-Cola) will more likely be targeted by physical or cyberattacks; they should take conservative security measures.

For up-to-the-minute discussion of war-related developments and recommendations, follow "Conflict in Iraq: Key Issues for Business and IT" (<http://weblog.gartner.com/weblog/index.php?blogid=4>).

Analytical Sources: Rich Mogull and Daniel Miklovic, Gartner Research

Recommended Reading and Related Research

- "The Emerging Storm: Preparing for the Next Gulf War" — What is the "emerging storm"? It's a metaphor for the confusion, conflict, and sometimes-violent clashes of interests and ideologies in a globalized world. **By French Caldwell**

- "CIOs, HR Executives: Prepare Your Workforce for War" — Enterprises should ensure workers are safe and feel connected to the company and their families. **By Diane Morello**

(You may need to sign in or be a Gartner client to access all of this content.)

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509