

## **COLD CRISIS LEADERS and HOT SITES in the DISPERSED MODE**

Enhancing Virtual Crisis Management Environments

by

Jim Truscott & Robert Kilsby

The expression Virtual Crisis Management Environment (VCME) is increasingly being used to describe virtual preparedness for crises. Organizations use VCME to optimise crisis communications and information systems through various combinations of:

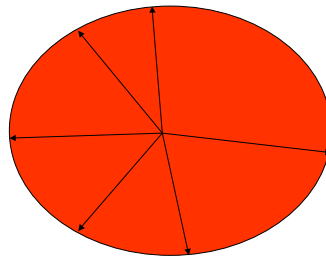
- Virtual private networks.
- Crisis portals to inform traveling crisis team members.
- Same time and same place collaborative software for geographically separated Business Support Teams.
- 1800 numbers for public hotlines on particular crisis issues.
- Switchboards, which allow for a cascading system of answering multiple calls by internal Call Centres to overcome log jams in telephone communications.
- Fixed email addressees for Business Support Team to allow 24/7 communications.
- Dark websites, which can be quickly activated to replace normal sites for media releases and fast facts.
- Organizations with prepared business continuity plans may also integrate a Disaster Recovery Centre (DRC) into their VCME for a fast transition to interim operations. Cold site DRCs require the user to bring their information with them; warm sites already store some of the organization's information; while hot sites contain updated information through constant replication.

Despite all of this technology, and with such systems approach and virtual networking allowing organizations to fight above their weight, VCME can be manpower intensive, and organizations must always be prepared to go back to basics in crisis situations. For example, the crisis benchmark for posting media releases is one hour; a near impossible task without pre-programmed email and facsimile addressees.

In adopting various VCME practices, computers in the crisis room can fascinate executives, but VCME are no substitute for the mental wetware required to develop strategy and implement crisis leadership under pressure. Crisis teams and their chiefs of staff need to guard against these fascination devices, which optimise software and hardware, but which do not generate the bold and creative second and third-stage thought required to control and transform from crisis situations.

Furthermore current global security threats are increasingly challenging the networked security of VCME. As a consequence organizations must be prepared to manage and lead crises from cold site DRCs. So is there another option for defeating internal and external information attacks? How can business harden its bunkers in the terrorist and criminal environment while still competitively engaging the market?

It takes a network to beat a network...we say DRCs will also operate in a dispersed mode. In the old sense of industrial sabotage and guerrilla warfare, the DRC simply represents the fire station or spare parts warehouse for which saboteurs and operatives would give equal attention as high value targets for destruction. In the new sense of information attacks against critical infrastructure, digital terrorists and criminal hackers with expertise in nodal analysis and network-centric warfare will give equal attention to DRCs, as much as other information exchange nodes. So what comes after the DRC? Quite clearly like guerrillas, DRCs must also disperse to remain an effective option. This is cost-effective self-insurance, especially for small to medium enterprises, which require a do it yourself or lean and mean approach to business crises.



**Hot Site Disaster Recovery Centre operating  
in a Dispersed Mode**

2

V1.1

Simplistically, employees with the ability to operate from home already offer an in-situ DRC. It makes sense to optimise this in-house bid as it represents a discretionary service at internal rates, or a Claytons hot site if you cannot afford a hot site. For just several hundred dollars, a company can give some hardware and software to each employee to take home. For only a few more hundred dollars these employees can be networked by high-speed links.

Just as Chief Continuity Officers are replacing Chief Information Officers and Knowledge Managers, there is no doubt that hot site DRCs operating in the dispersed mode will become the mainstay of VCME. Using people as a dispersed hot site offers an economical solution to man-induced risks for which the likelihood is low, but the consequences are high. Companies should use this security imperative to revisit the concept of employees having the option to work from home.