



A Material World

by: Andy Hagg

Pages: 6; November, 2001

文章简介：本文讨论了“911”事件给信息时代的应急计划工作带来的启示，即人们在制定应急计划过程中应该考虑到多方面的威胁，其中不仅包括高科技手段的威胁，也包括传统手段的威胁。



[华安信达](http://ChinaCISSP.com)

Just a few weeks ago, it was e-this and e-that. Cyber-here and cyber-there. We were discussing all sorts of vulnerabilities in the new, global, digital economy. Then along came September 11 and changed our conversation. A group of terrorists invited us back to the Industrial Age, and in some cases the Stone Age.



The prevailing talk of cyberwarfare and of the complexities involved in outsmarting high-tech hackers has been overshadowed by talk of a slow and deliberate campaign to drag individuals out of caves in third-world countries. Concern over security has shifted from topics like e-mail virus threats to topics like physical mail and the physiological threat of anthrax-laced packages. The public presently is less concerned about firewalls than they are about reinforced cabin doors. The privacy issue, which had been heating up intensely last summer, is now less a concern over government spying on our personal information and more a desire to have government protecting our persons.

In all these ways, the presence of terrorism in our country has made us remember that, despite the tremendously exciting Information Age we've been enjoying, we still live in a physical world, with physical dangers.

This same shift is reflected in the BCP field. For instance, before last September, what contingency planner gave much serious thought to records management? And yet, while companies' data was being recovered via sophisticated information systems moments after the World Trade Center was struck, millions of critical paper documents were floating to the ground throughout lower Manhattan, never to be recovered. Or, what contingency planner would consider such print-to-mail failures as could occur by an entire post office being shut

down for a week because of an anthrax scare? And yet, while e-mail flows through cyberspace unabated, employees aren't getting their paychecks, customers aren't getting their bills, and companies aren't getting their messages out through direct-mail marketing pieces. Finally, who would have thought that the gray-haired World War II veteran in the security booth outside your corporate campus would be more important to you than the 28-year-old techie manning your data center?

This is not to say that these new threats should take your attention away from other, much more likely, vulnerabilities that businesses face. They certainly should not. In fact, even with all the focus on terrorism, power failure, communications failure, hardware and software failure, human error, and natural disasters remain the most likely causes of business disruption. Effectively mitigating them should remain a priority in your business continuity program.

But if we've learned anything from the horrendous events of the past few weeks, it is that we live in a big, big world; a world of vast information and highly sophisticated technology, but also a material world. A threat can come from any angle, from cyberspace or from a dusty village. It can target the U.S. Senate or the business next door. It's your job to have a broad enough business continuity program for you to mitigate it, whatever "it" is.

For years this publication has been saying that business continuity is not just about IT. This is what we mean.

A handwritten signature in black ink, appearing to read "Andy Hagg". The signature is fluid and cursive, with a large initial "A" and "H".

Andy Hagg

Editorial Director