



## A Tangled Web

*by: Andy Hagg*

***Pages: 6; March, 2002***

文章简介: 本文讨论了应急计划制定者在分析各种中断威胁时所面临的问题, 信息时代的威胁来自多个方面, 高技术和传统威胁交织在一起对应急计划的制定提出了新的挑战。



[华安信达](http://ChinaCISSP.com)

Some interesting observations came out of a panel discussion I was privileged to participate in last month at the United Nations. The panel was part of the AIT Global-coordinated Global E-Commerce 2002 conference and centered on physical and electronic security threats that organizations commonly face, and how proper disaster management can effectively address those threats.



As the panel moderator, I had a great opportunity to draw upon a wide range of expert panelists. One panelist, a professor at a university's school of medicine, brought to the discussion issues surrounding the use of electronic systems to manage information in the health care field. Another was an expert in assessing corporations' and governments' susceptibility to physical and electronic terrorist threats. There was an authority on biometric and authentication technologies for countering identity fraud, and still another who specialized in video surveillance for facility security. There was even a representative from the United Nations Development Program who works to prevent computer theft, looting, and bombing of UNDP Country Offices.

Before September, I don't think there could have been a very cohesive discussion involving individuals with such a wide array of experiences, issues, and concerns. After all, what does a doctor's ability to carry a palm device with patients' medical records have to do with whether or not a U.S. Customs Official can identify a perpetrator of identity theft? Or, what's the common denominator between a hacker's activities on the Web and a bomb going off in a foreign embassy? What's the relationship between a parking lot surveillance system and anti-virus software?

And more importantly, what does any of this have to do with business

continuity?

The one underlying theme of the discussion that struck a chord with the participants and the audience alike is that, in today's climate of new and global threats, vulnerabilities in the physical realm and in the "cyber" realm are very often intertwined in a complex web. Criminals, for instance, can and do infiltrate computer networks to gain physical access to facilities, and once inside cause damage to facilities and destroy intellectual assets. Disgruntled employees can and do manipulate both their network security authentication devices and their facility security passes to get to files they don't belong in, and floors they don't belong on. And there is a real threat of terrorists targeting a combination of physical and electronic assets to inflict the most damage on their enemies, be they businesses or governments. Just imagine if al Qaeda had managed to hack into and shut down the computer and communication networks that run air traffic control.

So often in the past, we've thought of an information security problem being the IT department's problem, and a facility security breach being a facility manager's problem. Even to this day, it is doubtful that very many companies have considered the possibility of a significant business disruption resulting from a simultaneous intrusion on both fronts.

When was the last time your facility security personnel sat down and talked with your information security personnel about all known vulnerabilities and how to address them? As a business continuity manager charged with ensuring the survival of your company's operations, that's a question you may want to address.

A handwritten signature in black ink, appearing to read "Andy Hagg". The signature is fluid and cursive, with the first name "Andy" and the last name "Hagg" clearly distinguishable.

Andy Hagg

Editorial Director

