Financial giants plan to unveil new security auditing group

AIG, Ernst & Young, KPMG, Deloitte Touche Tohmatsu and PriceWaterhouseCoopers are collaborating on "Global Security Consortium"

A new group comprised of the **AIG Insurance Company,** four giant U.S. audit firms, and other technology, investment and services companies, is developing a new *quantitative* method to assess the physical and IT security of large organizations. AIG might be more willing to write insurance policies covering cyber and physical security risks if large organizations were to adopt widely agreed-upon auditing standards.

The organization, likely to be called the Global Security Consortium, is keeping its full membership, timetable and methodologies close to its chest, but its executive director, Martin Ross, acknowledged to *GSN* that his organization will probably debut in the Spring or Summer of 2004.

The new organization has been acting in what one IT industry observer called "stealthy mode" for several months. That may be the case because the consortium's organizers have not yet nailed down all of its key corporate members or the precise role that the federal government might play in its future.

Industry sources suggest that AIG insurance and four of the nation's largest accounting firms, **Ernst & Young, PricewaterhouseCoopers,**

Deloitte Touche Tohmatsu and **KPMG,** all based in New York City, are planning to participate in the Global Security Consortium. Ross declined to confirm the participation of these specific companies, but did say that additional companies in the technology, investment and services sectors will also play roles in the new consortium.

Ever since 9/11, government agencies and large corporations have attempted to enhance the security of their personnel, property and IT systems, but many have been hampered by the absence of agreed-upon standards, or "metrics," by which the status of both their existing security arrangements and their future performance can be measured. "Given that we know that in both the public sector and the private sector there is a need for greater security," said Ross, "the first step for any organiza-

MARK KAPLAN

tion is to know where its security is at."

In its preliminary work, the consortium has been developing what its calls its information security Risk Preparedness Index (RPI), a quantitative approach to measuring the security of an organization's computer network and its physical property. Such a *quantitative* approach, if the chosen algorithms and category weightings are accurate, could result in a clearer assessment of a company's vulnerabilities than a purely *qualitative* view of the same situation, industry observers say.

The consortium is also vague on its current relationship with the Department of Homeland Security beyond indicating that its organizers have met with key DHS officials. The consortium may be hoping that the federal government will eventually bless its approach to standardizing the measurement of IT and physical security

or, better yet, that the government will require large corporations to use the consortium's risk-assessment tools.

The Security Forum, part of an IT organization called The Open Group, has been briefed by an organizer of the new consortium on its goals and methodology. "The initial goal for the [Risk Preparedness Index] is to provide a risk measurement model and tool that has the support of the big four audit firms, to demonstrate due diligence in performing best practice in the insurance industry," said The Open Group on its Web site. With such a tool in place, AIG insurance and, perhaps, other insurance carriers, may be more willing to offer insurance policies that cover a variety of cyber and physical security risks for commercial customers. AIG declined to be interviewed on the consortium's plans.

Thus far, The Security Forum has critiqued the consortium's proposed RPI methodology, but is adopting a wait-and-see attitude toward the new group itself. "There is a solid trend developing around assessing risks, taking a business management approach to those risks, and then moving on," Mike Jerbic, an IT consultant and chair of The Security Forum, told *GSN.* ∎