

WEIS 2008

Workshop on the
Economics of
Information Security

CISO Perspective – Evaluating and Communicating Information Risk

Russ Pierce, Chief Security Architect, CVS Caremark

Phil Venables, Managing Director and Chief Information Risk Officer, Goldman Sachs

Kavitha Venkita, Practice Manager, IT Practice, Corporate Executive Board

Eric Johnson, Dartmouth College (moderator)

While security professionals have long talked about risk, moving an organization from a “security” mindset to one that thoughtfully considers information risk is a challenge. Managing information risk means building risk analysis into every business decision. In this panel, we will discuss how CISOs are working to move the conversation from security towards information risk. In particular, we will address questions about risk categorization, communication, and measurement such as:

- How does your organization view risk to information? What is the difference between “security management” and “risk management”?
- While there is an endless parade of new threats, what are the risks within your organization that worry you the most?
- How do you build a process to evaluate and rank the evolving risk? Can these risks be measured in way that the organization understands?
- How do you communicate risk throughout the organization? What has worked and what has failed?