Security in knowledge

Risk Management: How to Put Theory into Practice

Moderator

Eric Chabrow

Information Security
Media Group

Panelists

Ron Ross

National Institute of Standards and
Technology

John Streufert

Department of Homeland Security

Justin Somaini

Former CISO at Yahoo, Symantec

RSA®CONFERENCE2013

Session ID: GRC-W22

Session Classification: Intermediate

Topics to be Addressed

- Provide leadership
- Assess risk in a volatile environment
- Mitigate conflicting approaches
- Define roles of CISO, other leaders
- Keep stakeholders informed
- Determine how culture affects risk
- Decide what to do if resources are lacking

Goals of Leading IRM Implementation

- Search for, find, fix and report on the worst cyber-risks first in near real time.
- Automate best practice defense to keep pace with threats, to leave time for what only humans can do.
- As a team, engineer security into systems sooner and more comprehensively than ever before for the best return on investment.

Assessing Risk in Volatile Times

- Inventory organizational data to determine its criticality (using the FIPS 199 security categorization standard).
- Establish ‘worst case mission/business impact’ if such information is comprised.
- Understand threat space, vulnerabilities built into IT enterprise architecture.
- Bring together threat, vulnerability, impact data to develop current risk assessments.

Handling Conflicts Among Stakeholders

- Establish a split reporting chain of risk reporting.
- Have your framework be flexible and standards based.
- Facilitate a discussion.

The Conversation Continues

- Define roles of CISO, other leaders
- Keep stakeholders informed
- Determine how culture affects risk
- Decide what to do if resources are lacking

It’s Your Turn

- What questions do you have for our panelists?