Discussion Guide

Security through Information Risk Management

October 5, 2007

As information security risks continue to evolve, many organizations are moving from a traditional security mindset to a risk management mindset. Effectively evaluating the risks, both internal and external, requires understanding the motivation of the attackers. While shielding the organization from the latest automated online 'noise', such as worms or viruses, may consume many security resources, the most serious threats to any business come from attackers with economic motivation. Increasingly, organizations are faced with threats from professionals with very specific intentions. Some of these motivations are obvious and immediately recognizable. Others are more subtle with lasting impact. For example, protecting against intellectual property leakage may be one of the most difficult assignments for CISOs since the losses are often not immediately observed and the impact may not be felt for years. Protecting against these economically-driven threats requires much more than technology. It requires building security into the culture of an organization so that everyone can recognize and evaluate the risks. Like total quality management, total security management means security at the source—every employee, manager, and executive.

In this workshop, CISOs/directors of information security will discuss how companies are managing their information security risk and building secure organizations in the face of more sophisticated attacks. Using a moderated roundtable format with panel discussions and structured breakouts, we will explore the following topics.

Senior Executive Panel – Business Risk and Information Risk (*A panel of executives will discuss the following questions. Come prepared to dialog with them*). Does your firm think about information risk in terms of overall business risk?

- Firms face many types of risks. How do line-of-business executives within your firm think about information risk as compared with other business risks?
- How are information risks identified and prioritized within your organization? How does this differ from other business risks?
- How do you move the conversation from "protect us from a breach" to "help us make economically driven decisions about information risk and reward"?
- Information security has been on the top of many IT executives' agenda for the past few years. What is the difference between an organizational mindset of managing information risk vs. managing information security?
- What role do the board and senior management play in focusing the organization on information risk?
- When your firm discusses risk management, is information risk an important part of the discussion?
- How are the information risks your firm faces changing? Are risks associated with the loss of intellectual property gaining in prominence?

- The increasing usability and sophistication of communication/collaboration technology coupled with Web 2.0 services means business users more than ever have the ability to innovate in developing and procuring their own information systems and services—what impact will this have on information risk?
- Much is discussed on the impact of Generation Y/Millennials entering the work force—will this have a positive or negative impact?
- Does business resilience (business continuity) have a synergy or a conflict with information protection?

CISO Moderated Roundtable #1 – Information Risk in Your Organization (*Please come prepared to share your biggest challenges in helping your organization think about information risk.*) Does you organization see a distinction between information risk and information security?

- On a scale of 1-10, where do you think your firm is and why?
    - 1 – CISO should simply make us secure and call us when it is done.
    - 10 – Everyone is involved in information risk decisions, making economic and risk trade-offs, and information risk is part of every business discussion.
- Does the senior leadership get it?
- What are the least understood information risks your firm faces? How do you see those risks evolving in the next 12-18 months?
- How are risks to intellectual property different than the risks to mountains of business data you are charged to protect?
- How do you manage information risks arising in your partner organizations? What risks are they taking that don't align with your risk posture?

Breakout: Security Transformation Café
In a series of three breakouts, we will push deeper to understand effective methods of ranking, communicating, and measuring risk. Our goal is to go beyond understanding best practice to developing an action plan to move forward in the next 12-18 months. *Come prepared to share your approach to ranking threats, one lesson in communicating risk, and one metric that has been particularly effective in your organization. In the breakouts, we will consider the following questions:*

Ranking the Information Threats: What are some of the largest threats to your business? How do you prioritize those threats? What is your process for discovering new threats and communicating those threats to the organization? Is the government helpful in identifying and ranking threats? Are you confident that you have the necessary information to accurately rank threats? Is the motivation of threat actors relevant to your ranking?

Communicating the Information Threats: How do you help the organization understand and recognize economically driven threats? How does the organization embed these risks into its overall risk management? How do you jointly educate and manage the threats within your supplier and partner organizations?

Measuring Progress: How do you know if information risk practices are making a difference? Is the organization making progress? How should we measure improvement? What tools and methodologies do you use to do this?

CISO Moderated Roundtable #2 – Preparing the Organization to Protect Itself (*Based on the outcome of the breakouts, we will identify and discuss key lessons in building information risk into the organization's DNA.*)

- At the level of the individual employee, how do you reduce the risk of information leakage?
- Privileging and access open doors to information. Can you measure the risk of access?
- Would better privileging and provisioning processes substantially reduce risk in your organization?
- How do you build teams that recognize and manage information risk within the group?
- Where are the largest risk sources and how do you address them?
- What would "security at the source" look like in your organization?