Embedding Information Security Risk Management into the Extended Enterprise

A Workshop on Developing a Secure Organization

Washington Duke Inn
Durham, NC

Discussion Guide

The risks of serious information security failures are all around us. Managing these risks is a balancing game between maintaining security without inhibiting the business. In today's outsourced enterprises, effective risk management is quickly becoming a source of competitive advantage. Consequently, the role of the CISO is becoming more strategic. Yet moving the needle on information security is a team activity, requiring participation by everyone. The technology community has made much progress in the past five years improving the technical aspects of security. The hardest remaining issues involve people and organizations. In this workshop, we will discuss how companies are managing their information security risk and working to build secure organizations. We will explore how firms are creating secure cultures and embedding information risk management into their overall enterprise risk strategy. Using a panel discussion, moderated roundtables, and structured breakouts, we will discuss:

Senior Executive Panel – Business Drivers for Security (*A panel of IT executives will discuss the following questions. Come prepared to dialog with them*). How is security embedded into the business?

- What are the business drivers for information security within your organization?
- How successfully do you feel the security issues have been communicated at the executive level?
- Are security managers able to contribute to the executive dialog on business strategy or is security an afterthought?
- What do you find is the most successful way to communicate security risk and investment requirements to other executives and general managers?
- What are the organizational barriers to information security?
- How do you see the different groups within your organization (CIO, CSO, CISO, physical security, risk management, loss prevention, finance compliance (SOX), board audit committee) coordinating to arrive at a rational risk management process?

CISO Moderated Roundtable #1 – Organizing for Security (*Please come prepared to share insight into the organizational structure for security within your firm and describe a current organizational challenge you face.*) How does organizational design impact the success of security initiatives?

- How is information security currently organized and funded in your firm?
- What are your biggest security concerns for the next 12-18 months?
- How are these concerns reflected in your current or planned security organization?
- What elements of organizational structure really matter: reporting relationships, sponsorship, funding, or responsibility (governance vs. deployment)?
- How do you manage business risks stemming from partner organizations?
- How is securing intellectual property different than protecting systems against attacks?

Breakout: Security Transformation Café
In a series of three breakouts, we will push deeper to understand the role of culture, measurement, and investment on security. 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 one cultural, one measurement, and one investment challenge you face. In the breakouts, we will consider the following questions:*

Culture:

- What does a secure culture mean in a global organization?
- How do you "inculcate" information security?
- What is the role of executives throughout the organization regarding information security?
- What are the top issues the CISO must face in the next 12-18 months in preparing the organizational culture?

Measurement – risk and security:

- How do you know if security initiatives and awareness are making a difference?
- How should metrics cascade throughout the organization?
- How can risk and security metrics be more closely tied to tactical and strategic decision making?
- What types of metrics should CISOs champion in the next year?

Investment Decisions:

- Who needs to be involved in information security investments?
- What funding models have been most successful?
- How do you incorporate everyone into a process that balances risk and rewards?
- What critical changes do you see in the way CISOs address security funding?

CISO Moderated Roundtable #2 – Imperatives to Building a Secure Organization (*Based on the outcome of the breakouts, we will identify and discuss key imperatives for secure organizations.*)

- What are key aspects of secure organizations?
- What are the most important items CISOs should address in the next 12-18 months?
- What action steps will you take back to your organization?