Discussion Guide

Assessing Risk in Turbulent Times

July 14, 2009

We are all facing some of the biggest changes of our working lifetime. Well before the current downturn, enterprise information technology and business itself was changing. Security executives in every industry were already struggling with the consumerization of technology, globality, and the challenges of securing information across far-flung employees, partners, and customers. The explosion of communication capabilities has empowered a new generation of employees who are operating in new, more virtual world. These steady changes continue to rock traditional operating models, transforming the character of work, shifting the nature of the employer-employee relationship, and changing the boundaries of the firm.

The downturn has moved the rate of change to an entirely new level. Deepening cost pressures and organizational transition have opened new risks and made everyone's job more challenging. With downsizing comes process disruption and organizational gaps. Business partners, squeezed by the same forces, are themselves growing risks. And the downturn seems to have also increased innovation among economically motivated criminals.

In this workshop, CISOs/directors of information security will discuss how companies are assessing and managing these new risks. Using a moderated roundtable, panel discussions, and structured breakouts, we will explore how we are assessing, rating, and managing the evolving threats, new internal risks, and risks outside our enterprise.

Risks and Opportunities in China (Optional Monday Afternoon Session) (*A special guest, courtesy of General Dynamics and Pamir Consulting, will brief the group on risks stemming from China. Bring a question about China from your own business*).

- How does China really view Western businesses, from a business, economic, technology and political perspective? Pamir representatives—unique experts on China with decades of on-ground experience in that country—will deliver an abbreviated presentation highlighting some of China's complex goals and aspirations for engaging international conglomerates at home in China, and abroad. Bring an open mind and use this opportunity to ask that one question of a true insider that you have always wanted to ask.

Roundtable Session #1 – The Perfect Storm: New Internal Risks (*Please come prepared to share how the downturn has impacted security in your organization and the resulting new internal risks you see*).

- Almost every organization is facing in new levels of transition and turmoil. With organizational changes come new risks. Shifting roles often open gaps in process execution and erode policy compliance. Employees leaving the firm exit with intellectual

property. Those who remain are stretched ever more, making it harder to ensure good security hygiene. How do you evaluate and manage these risks?

- Has your senior leadership been able to maintain a security focus or have the pressures of cost cutting overwhelmed them? What implicit or explicit tradeoffs do you see being made?
- How do you manage the tension between cost effectiveness and the changing security landscape?
- The usability and sophistication of communication/collaboration technologies have led to an explosion of Web 2.0 services—what impact is this having on information risk?

CISO Moderated Roundtable #2 – Evolving External Risks (*Please come prepared to share a new evolving external risk for your organization.*)

- How do you manage information risks arising in your partner organizations?
- Cost pressures have pushed many organizations to increase off-shoring. How do you assess the new information risks posed by these vendors?
- What risks are your vendors taking that don't align with your risk posture?
- As partners face economic turmoil, how do you update your assessment of their risk?
- Many firms have noticed a rise in attacks and new innovation among cyberthieves. Is this real and should we expect more? How do you assess these new risks and prepare your organization?
- How are you handling the growing needs for e-Discovery?
- What are the least understood new external information risks your firm faces? How do you see those risks evolving in the next 12-18 months?

Breakout: Risk Assessment Breakouts

In a series of three breakouts, we will push deeper to understand effective methods of assessing risk. Our goal is to go beyond understanding best practice, painting a vision for the next 12–18 months. *Come prepared to share your approach to rating and ranking risks. In the breakouts, we will consider the following questions:*

Building Internal Capability: How do you evaluate the risk posture of different parts of your business? How do you rate, score, and prioritize risk? What is your process for discovering new threats and communicating those threats to the organization?

Risk Assessment Services: Do you use outside services to evaluate risk? What types of risk ratings are most useful? Could an assessment services become a major factor in your industry?

Industry Initiatives for Shared Assessment: How useful are the risk evaluation efforts of your industry? What industry-led programs are in place and how effective are they? What could make these programs more effective? Should we invest more effort in developing shared assessment?

CISO Moderated Roundtable #3 – Managing and Reducing Risk (*Based on the outcome of the breakouts, we will discuss key lessons in risk assessment and approaches to managing risks*)

- Business partners often represent one of the greatest unknowns. What are the most important risks? How do you access and rate the risk of suppliers, vendors, and partners.
- What is the way forward? New risk rating methodologies? Building internal capability or developing shared services and approaches?
- How do you maintain an appropriate security culture during a time of change?
- If security is a losing game, can we design business processes that operate in a world without security?