"Security and Privacy: At Odds with Speed and Collaboration?"

Thought Leadership Summit on Digital Strategies
May 25, 2004 – Hanover, NH

Discussion Guide

Topic Statement

Economic growth and prosperity rely on healthy business communications. Whether this is between corporations, with customers, or with governments the ability to quickly and reliably share information is key to the long-term success of any venture. But wrestling with the potential tradeoffs between speed and collaboration vs. risk and exposure is not a simple matter. The customer information that must be kept private is also an essential ingredient to product design, marketing and relationship management. The financial information that is confidential needs to be communicated rapidly and transparently to investors at the appropriate time. Similar issues exist in most processes of today's extended enterprise. All of this takes place in an increasingly complex regulatory environment. Information security is no longer a discussion just about firewalls and encryption. It must include the people who gather and use the information, the defined processes for using the information, and the technology to secure it when in transit, storage or use. This summit will explore this complex set of interactions and living with the tradeoffs and organizational issues they imply.

Flow of the Day – Questions to Consider

Session 1: Defining and Exploring the Security Issues

What are the chief issues in corporate information security today? What are the best practices for dealing with them?

- Is there an inherent tradeoff between collaboration and speed on the one hand and security and privacy on the other? How have companies wrestled with determining providing the right level of security while minimizing the business friction?
    - What business processes are most impacted by security processes or concerns?
    - How much friction is there and how do you mitigate it? For instance, how do you balance keeping customer information confidential while allowing this information to be available to mining for inclusion in areas such as product design, marketing, efficient customer service and relationship management?
    - What are the organizational implications?
- How much does security hold back extended enterprise efforts? How do you work with business partners (customers and suppliers) to ensure consistent, un-obtrusive security across an extended enterprise?
- How do you organize information security on a global scale and manage the inherent security challenges this scale brings?
    - How do global corporations with worldwide partner, alliance, employee, and customer bases balance the need for open communications with the need for the

controls and security that lead to the protection of intellectual property, other important data, and privacy?
    - How do they deal with the different cultures and views inherent in operating in various points around the world?
    - How do you wrestle with the notion that you are as vulnerable as your weakest point?
- What are the best practices you have seen in each of these areas?

Session 2: Examining Organizational Responsibility, Sarbanes-Oxley and Privacy

In this session, we will examine three separate but related questions in more depth: Where does responsibility for information security lie? What effect does Sarbanes-Oxley have on dealing with security? What's the interaction between security and privacy?

- What are the current organizational structures and processes in place to ensure information security?
    - Is a chief security officer needed?
    - If so, should this person have responsibility for information and physical security? Who should he/she report to?
- What is/should be IT/business unit leader's role in educating the company and business partners about security (both about risks and opportunities)?
- What's the interplay between Sarbanes-Oxley / other regulation / external audit requirements and information security policy, procedures and reporting?
    - Is Sarbanes-Oxley merely pushing us to do things we should be anyway? Is it a help or a nuisance?
    - Do all the reporting processes have to be automated to be "effective"? What are the key decisions to be made on this and the best emerging guidelines for making them?
    - What concerns exist about greater government involvement in setting security regulations or privacy requirements?
- What's the interaction between security and privacy? Are they really separate issues, flip sides of the same coin, or integrally intertwined?
    - For consumer privacy?
    - For employee privacy?

Breakout: Privacy and Security – Where Do They Meet?

Session 3: Elaborating the Positive Reasons for Security

We've all heard the "or else", "chicken little", or regulatory demand reasons for increased information security, but is there a positive reason to drive for high security?

- Are there opportunities created by the need for increased security?
- Can good security create real competitive advantage? Can good security be a potential asset for the future (i.e., make partners more likely to do business with or invest in a company because they are leaders in security/privacy)?
- Is there even a positive business case for security (i.e. positive operational reasons for information visibility investments that can also be used to enhance security)?
- Which business processes or areas are most likely to benefit from better information security? Marketing? Supply chain? Internal processes and accountability?

- What will drive greater investment in, and attention to, security issues: Market dynamics? Shareholder pressure? Government pressure? Customer pressure?

Session 4: Summary and Further Research

We will identify as a group the takeaways, the key "portable" learnings from the day for each participant and the group (following focus areas suggested):

- Best practices
- Organizational impact
- Metrics, incentives and productivity
- Digital strategies opportunities
- Value chain collaboration opportunities

We will also take a look at the future: What do you view as the most significant security/privacy issues for the near-term and long-term? How do IT and business differ in their thinking? What research could be done to help move these issues forward?