Center for Information Systems Research
Sloan School of Management
Massachusetts Institute of Technology

RESEARCH BRIEFING

Volume V *Number 3B* *December 2005*

WHAT MAKES AN IT RISK MANAGEMENT PROCESS EFFECTIVE?

George Westerman, *Research Scientist*
MIT Center for Information Systems Research

The causes and effects of IT risk are complex, especially in large organizations. Only a well-defined risk management process can make sense of the complexity. According to Novartis CIO James Barrington:

> *"The organization is so complex—we've grown to 75,000 PCs with thousands of servers, all sorts of security issues—there's not a physical way to manage all of the risk associated with such a large environment in a perfect way. So, we've taken the approach that if you can't eliminate the risk, better try and understand it and manage it.*
>
> *So, we have started trying to understand the risk in each of these areas. And once we know the risk, then we try and manage the solution or the effort in direct relation to the size of the risk… That's very helpful for us… we get a much better leverage on our resources."*

The IT Risk Management Process

The IT Risk Management process is simultaneously distributed and centralized (Figure 1). Experts in each part of the enterprise identify and assess risks in their areas. These local risk managers address each risk they control, and escalate large risks (or risks that require action by other people) to managers with broader authority.

The process provides a global view of all risks in a domain (see Figure 2) so managers can make tradeoffs and prioritize limited resources to shape an acceptable risk profile. Managers can choose to address each risk in one of four ways:

- *Avoid* the risk, by either stopping an activity or deciding not to undertake a risky activity.
- *Transfer* the risk, such as by outsourcing a process or buying insurance.
- *Reduce* the risk, by taking action to improve a risky condition.
- *Accept* the risk, either because the risk is small or because it cannot be addressed given current conditions and resources.

Effective Practices for the Risk Management Process

Using survey data from more than 130 enterprises around the world, and interviews with more than 30, we have identified a set of practices that form the core of an effective IT risk management process.[1] Organizations with effective IT risk management:

1. Create the environment for risk management using:

   Risk Policies: Policies describe acceptable standards and unacceptable behaviors in all risk-relevant processes. Examples include infrastructure standards, e-mail retention policies, vendor management rules and information privacy protections. Clear, well-publicized policies help risk managers in each area identify risky conditions, and help employees throughout the enterprise avoid inappropriate behaviors or decisions.

   Best Practices: Industry "best practices," such as recommended software configurations, daily virus updates and standard internal controls, are often available from industry specialists and trade associations. Best practices enable risk managers to reliably implement a baseline of "good enough" risk protection in standard areas. Then, effective risk managers can focus on unique processes that need more attention.

2. Ensure a consistent view across multiple units and functions using:

   Formal Risk Categories: A small but comprehensive set of well-defined categories for IT risks and risk factors improves the risk management process in two ways. First, the categories

[1] Organizations using each of these practices reported mitigating statistically significantly more risk in at least three of four enterprise IT risks: availability, access, accuracy, and agility. For more information on these four risk categories, see *Understanding the Enterprise's IT Risk Profile*, MIT Sloan CISR Research Briefing Vol IV, No 1C, March 2004.

and their definitions serve as a checklist to help local experts identify and assess risks. Second, they help higher levels of the organization prioritize and monitor risks by grouping similar risks across the enterprise.

Risk Register: An IT risk register records and tracks all IT risks. At a minimum the risk register identifies the name and description of the risk, category, risk owner and the risk's impact and likelihood. The register also tracks what action is planned, and whether progress is being made.

Quantified Risk Assessments: Quantified assessments of risk impact and likelihood improve the firm's ability to globally compare and prioritize risks. Because of its newness and complexity, IT risk does not have the detailed actuarial information that insurance companies use to price other types of risk— IT risk managers must use less precise methods to assess IT risk. Some assess each risk's impact and likelihood broadly, using well-defined thresholds for high, medium and low. Others use more detailed scoring sheets to generate relative impact and likelihood scores based on heuristics and best practices.

3. Provide the correct resources for the process, including:

Single person in charge of process: The chief IT risk manager designs and runs the risk management process but does not manage particular risks. The process enables local experts to identify and address IT risks, and higher-level managers to monitor and prioritize important ones. By making a single person accountable for the process, effective firms gain a clear focus on IT risk management and a mechanism for continuous improvement.

Risk committee: An IT risk committee, consisting of senior IT and business executives, makes decisions on how to address the most important IT risks facing the enterprise. The committee also considers changes such as adding new IT risk categories, conducting audits or threat assessments or adjusting the firm's acceptable risk profile.

Improving the Process Over Time

The risk management process typically requires 12–18 months to reach a baseline level of effectiveness. During this learning period, the process can be difficult. People throughout the organization learn how to identify and assess risks, and become comfortable sharing risk information. Additionally, the chief risk manager continuously monitors and improves the process to meet business needs without being overly burdensome. For example, the first cycle of the IT risk management process in one financial services firm identified more than 300 risks—too many to meaningfully prioritize or monitor. Through an iterative process of discussion and policy improvement, the firm reduced the number of active IT risks to around 30.

Risk managers monitor risk trends—using charts like Figure 3 or regular updates to a risk map as shown in Figure 2—to ensure that the organization is focused on the correct risks and that new risks are being addressed effectively. In time, instead of repeatedly conducting detailed assessments of all risks, firms can shift to incremental status updates on existing risks coupled with targeted new risk assessments. In addition, many new risks can be identified by embedding risk management into other IT processes. For example, several firms have embedded risk-related reviews into IT project initiation and review processes, so that risks are identified or avoided as part of the normal demand management process.

Benefits of an Effective IT Risk Management Process

Upon accepting the new CIO position at financial services provider PFPC, Michael Harte decided to make IT risk management a key pillar of his transformation program.[2] He and his staff developed an IT risk management process to guide key IT governance decisions and improve the firm's IT risk profile. Harte now participates in sales calls in order to showcase the firm's IT risk management capabilities to potential clients.

Although not all CIOs would gain similar customer attention for their IT risk management processes, the other benefits are clear. Firms using the practices listed above report statistically significantly lower risk, higher confidence in their risk management capabilities and less likelihood that the enterprise is missing important IT risks. The benefits also go beyond risk avoidance. Discussing IT decisions in terms of specific risk/return tradeoffs puts technical decisions into language that business executives are comfortable with. This transparency improves the relationship between IT and business by making risk-related decisions easier and clarifying the importance of key IT governance processes.

[2] See MIT Sloan CISR Working Paper No. 352, *PFPC: Building an IT Risk Management Competency* by George Westerman and Robert Walpole, April 2005.

Figure 1: The IT Risk Management Process Balances Local Expertise with Central Oversight

Figure 2: The IT Risk Map Provides a Global View for Prioritization and Monitoring

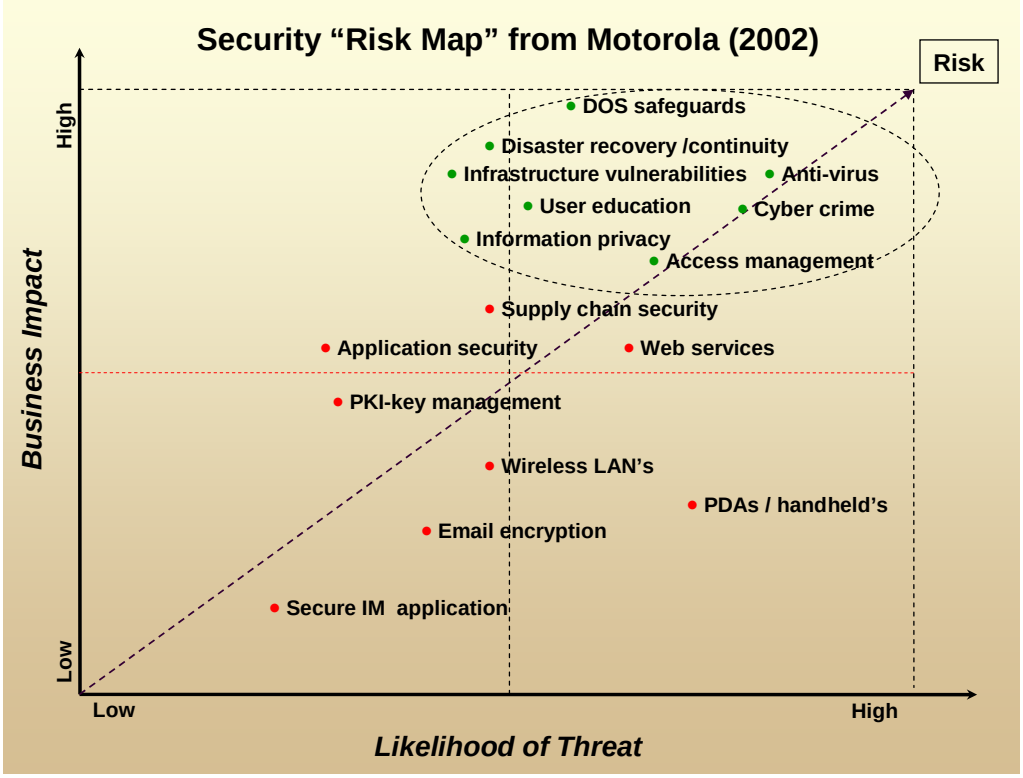
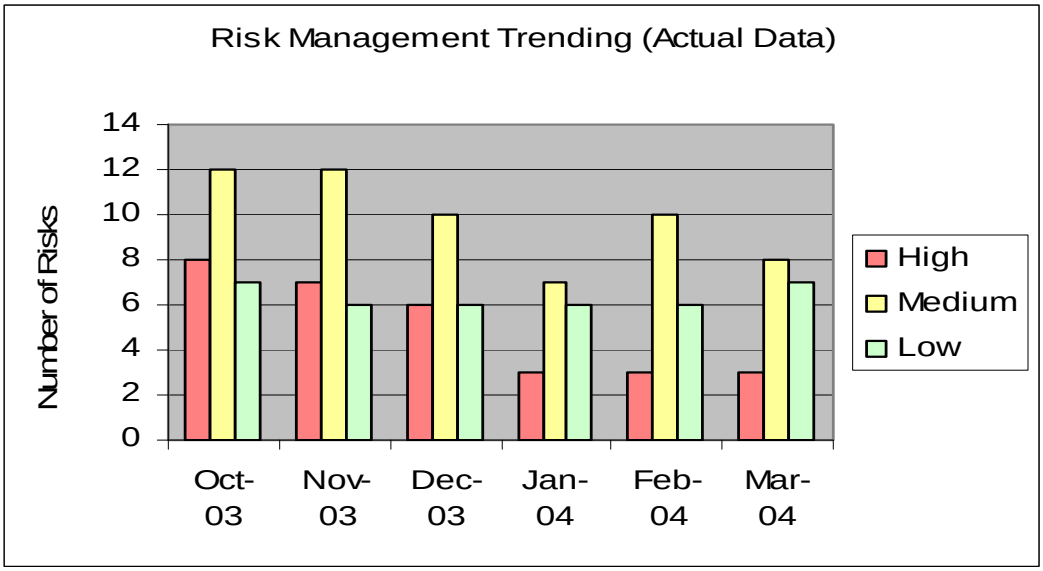


Figure 3: Regular Monitoring Ensures that the Most Important Risks Are Being Addressed First



MIT SLOAN CISR MISSION

MIT CISR was founded in 1974 and has a strong track record of practice-based research on the management of information technology. MIT CISR's mission is to perform practical empirical research on how firms generate business value from IT. MIT CISR disseminates this research via electronic research briefings, working papers, research workshops and executive education. Our research portfolio includes but is not limited to the following topics:

- IT Governance
- Enterprise Architecture
- IT-Related Risk Management
- IT Portfolios and IT Savvy
- Operating Model
- IT Management Oversight
- Business Models
- IT-Enabled Change
- IT Innovation
- Business Agility
- The IT Engagement Models

In July of 2008, Jeanne W. Ross succeeded Peter Weill as the director of CISR. Peter Weill became chairman of CISR, with a focus on globalizing MIT CISR research and delivery. Drs. George Westerman, Stephanie L. Woerner, and Anne Quaadgras are full time CISR research scientists. MIT CISR is co-located with MIT Sloan's Center for Digital Business and Center for Collective Intelligence to facilitate collaboration between faculty and researchers.

MIT CISR is funded by Research Patrons and Sponsors and we gratefully acknowledge the support and contributions of its current Research Patrons and Sponsors.

CONTACT INFORMATION

Center for Information Systems Research
MIT Sloan School of Management
5 Cambridge Center, NE25, 7th Floor
Cambridge, MA 02142
Telephone: 617-253-2348
Facsimile: 617-253-4424
Email: cisr@mit.edu
http://mitsloan.mit.edu/cisr

CISR RESEARCH PATRONS

Boston Consulting Group, Inc., The
BT Group
DiamondCluster International, Inc.
Gartner
Hewlett-Packard Company
Microsoft Corporation
Tata Consultancy Services – America

CISR SPONSORS

Aetna Inc.
Allstate Insurance Company
American Express Corporation
AstraZeneca Pharmaceuticals, LP
Biogen Idec
Campbell Soup Company
CareFirst Blue Cross Blue Shield
Care USA
Celanese
Chevron Corporation
Det Norske Veritas (Norway)
Direct Energy
eFunds Corporation
EMC Corporation
Guardian Life Insurance Company of America
ING Groep N.V.
Intel Corporation
International Finance Corporation
Merrill Lynch & Co., Inc.
MetLife
Mohegan Sun
Motorola, Inc.
Nomura Research Institute, Ltd.
Pasco County, Florida
PepsiAmericas, Inc.
Pfizer, Inc.
PFPC, Inc.
Raytheon Company
State Street Corporation
TD Banknorth
Telenor ASA
Trinity Health
TRW Automotive, Inc.
United Nations – DESA
US Federal Aviation Administration

Mission and Contact Information as of August 1, 2009.