



BILL MAYER

Five Steps to **IT RISK** Management Best Practices

by Greg Hughes

As individuals, corporations, and our economy grow increasingly dependent on the Internet and IT systems, the risks in these systems become far more visible and significant. Breaches or failures of information systems cause serious business crises, including reputation damage caused by identity theft, business losses stemming from system failures and regulatory restrictions arising from compliance issues.

The rate of recovery from these events is a contributing factor in the severity of the business crises. A recent study by Oxford Executive Research found that companies that recovered quickly from major operational disasters increased their share price by 5% on average versus the market. Companies that struggled to regain their operations took a 20% drop in relative value. From this research, it appears that investors factor a company's resilience to adversity into its stock price.

It is clear to see why corporate executives in boardrooms around the world want answers to the IT risk question: How do we dramatically mitigate the risk and improve the return on investments in information systems?

The answer to these questions lies in treating information technology risk within the integrated framework of business risk management. IT risks need to be identified, measured and managed as part of a single view of all risks in the corporation, with oversight by senior management to understand and guide the appropriate risk/reward tradeoffs to achieve the goal of increasing return on IT investments. The name for this approach to managing and balancing information risk and reward is IT risk management.

The Reality of IT Risk Management

Most companies have a poor awareness of their IT risk exposure. Few are fully exploiting the breadth of tools available to manage these risks,

and many have not begun to build the knowledge and processes required to manage their IT risks successfully.

Companies have struggled partly because IT risk management is a newly emerging field where traditional risk management does not always apply. For example, the ability to transfer risk is a fundamental concept in financial risks. However, since liquid markets do not yet exist for buying and selling IT risks, companies must build the internal competence to manage these risks on their own.

Another example of the difference is that IT risks are more challenging to quantify. In IT, the kind of well developed statistical or actuarial models that assess financial risk and give it a reasonable level of preci-



Most companies have not begun to build the knowledge and processes required to manage their IT risks successfully.

sion do not yet exist. However, "roughly right" approaches based on heuristics and experience still yield accurate, valuable and usable measures of IT risk.

Going from current to best-practice IT risk assurance could yield substantial improvements to shareholder value. To do this, business leaders should: 1) develop an awareness of the nature of the different IT risks to the business; 2) quantify the impact to their business resulting from the loss of information or access to applications; 3) understand the range of tools available to manage IT risks; 4) align the costs of IT risk management to the business value; and 5) build a systematic, corporate capability to manage security risk.

Developing Awareness

Information technology risks either concern the potential loss of information and its recovery, or they concern

the ongoing usage of information. They fall into the following six major categories.

Security. Risk that information is altered or used by nonauthorized people. This includes computer crimes, internal breaches and cyberterrorism.

Availability. Risk that data is not accessible, such as after a system failure, due to human error, configuration changes, lack of redundancy in architectures or other causes.

Recoverability. The risk that necessary information cannot be recovered in sufficient time after a security or availability incident such as hardware and/or software failure, external threats or natural disasters.

Performance. The risk that information is not provided when it is needed thanks to distributed architectures, peak demand and heterogeneity in the IT landscape.

Scalability. The risk that business growth, provisioning bottlenecks and siloed architectures make it impossible to handle major new applications and businesses cost effectively.

Compliance. Risk that the management or usage of information violates regulatory requirements. The culprits here include government regulations, corporate governance guidelines and internal policies.

Understanding the Impact

It is essential to understand risks in terms of the probability of an event that would trigger the risk, and how this relates to the time value of the exposure should such risk occur. Furthermore, the risks need to be quantified for each critical business application. Knowing these two parameters allows the decision maker to plot the values on a simple two-dimensional graph and assign mitigation/remediation priorities to different applications. Moreover, a policy to deal with different and/or multiple categories of risks can be defined and applied effectively and consistently throughout the enterprise.

Looking more broadly across mul-

multiple categories and correlating risks across these categories will better quantify the business impact. For example, an exploited security vulnerability may contribute to a recoverability risk. An application performance issue that prevents data access may provide an opening for a security risk or result in a compliance risk. The business impact may be direct or indirect, including financial, legal, customer loss and operational dependencies. Each of these may, in turn, have downstream implications.

Businesses find diligence in this area hard to justify, and there is often denial that risks exist or that their impact can be effectively measured. While challenges are real, quantifying the business impact gets to the core issue of being able to manage the risk equation.

Managing IT Risks

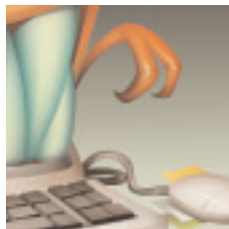
IT risks have different root causes and thus different approaches are required to manage and mitigate them. Broadly speaking, these approaches require a combination of process, people, technology and information.

First, processes for running data center and IT operations are going through a similar period of rapid evolution, as the best run IT organizations are moving from a haphazard, “job shop” model to more rigorously designed, executed and measured systematic approach. IT Infrastructure Library (ITIL), International Organization for Standardization (ISO), and other standards are emerging to describe “best of breed” IT operational processes.

Second, companies are paying more attention to the way they employ their people in the battle to reduce risk. Companies are experimenting with a wide range of techniques, including awareness-building, identity or role specific authority, new divisions of labor, new roles and specialists, and enhancing risk mitigation capabilities at all levels.

Third, new software is emerging from vendors who are responding to the demand for improved IT risk management. Rapid advances have created an arsenal of software in areas such as long-distance replication, clustering, content, intrusion and phishing detection, data protection and backup, vulnerability assessment, and policy management. Importantly, these tools are being integrated to offer workflow-driven solutions designed to follow customized processes and regulatory requirements. Event-driven automation is increasingly taking the place of onerous manual analysis and remediation.

Finally, information sources are available that provide insight into emerging as well as known threats and vulnerabilities, which can be



IT risks have different root causes and thus, different approaches are required to manage and mitigate them.

assessed against companies’ internal security environment (e.g., security risks, virus signatures and databases, operating system patches and configurations) to identify exposures and develop mitigation plans. Considering the speed with which new attacks propagate across networks, such early warning intelligence is essential to proactive and successful defense.

Aligning the Costs

Investments in process, people technology and information are required to mitigate risks. However, since IT budgets are constrained (and feeling continued downward pressure), leading companies need to make sure they are not over-investing or under-investing in risk management. How do companies manage their IT risk management investments effectively and efficiently?

Utility computing has emerged over the past few years as the most promising approach to align the costs

of IT to the business value. In utility computing, the role of IT with respect to the business evolves from a “cost center” to a “service center.” As it evolves under the utility computing approach, the IT organization masters four primary activities: 1) providing IT as a collection of well-defined services, developed and managed by a “service management” group that interfaces with the business; 2) exposing these services to the business through “service level agreements” and charge-backs to the business; 3) building and maintaining a shared, heterogeneous infrastructure to improve capital utilization and reduce costs, rather than building custom systems for each business application; and 4) running IT operations in an automated fashion to increase labor efficiency and reduce costs.

A number of leading companies are first applying the utility computing concept by building “storage utilities” that hold data for business application usage through different service classes, such as “platinum” (very high performance, availability, recoverability and security), “gold” (moderate service) and “bronze” (low service).

The costs of these different storage services are exposed to the business. Platinum is typically 10 times more costly than bronze service—aligning the risk requirements of the business and overall usage to the spending on IT.

Mastering the activities of utility computing is a journey for IT organizations. The first step they take is to discover the IT assets—servers and storage, for example—and ideally tie these assets to critical business processes. Second, they redesign and consolidate the environment to gain efficiencies in administrator productivity and resource utilization. Third, they start to standardize—classifying applications and agreeing upon specific vendors for storage and server hardware, while managing the environment through a standard set of

software tools. Fourth, they automate, driving down the time and labor required to request, provision and manage the environment. Fifth, they move to a true service provider model by equating service level delivery with costs by allocating or charging-back to the business units.

Building Institutional Capability

Leading corporations are building an institutional capability to understand, act on and control IT risks with the same level of scrutiny and urgency as financial risks. Using insight from a variety of sources they develop a risk “heat map” showing the potential impact and likelihood of the six IT risks on their lines of business, core business processes or major applications. Then, they create a prioritized program to remediate these risks and deploy the tools of software, people, process improvements and information. Finally, they control the risks by continuous measurement and improvement. In these corporations, IT risk management is fundamentally affecting IT governance and risk governance approaches.

As companies build IT risk management into an institutional capabili-

ty, they should do so with a core set of questions in mind.

- How does our IT strategy need to evolve or change to maintain an acceptable risk posture?
- Should we have new or expanding leadership roles to address IT risk, such as an IT risk manager?
- How do we monitor performance?
- Must we create governance to oversee and approve IT risk decisions?
- How do we educate our IT staff, and build skills for cultural awareness and understanding of risk throughout the employee base?
- What steps should be taken to make our planning and testing processes more rigorous and to make our systems impenetrable?

Improving IT risk management should be on the agenda of nearly every senior executive of a large corporation. Those executives, who are aware of their IT risks, understand the tools to manage these risks, and build the institutional capability to control them should be in a fundamentally better position to improve the risk and return of information investments. ■

Greg Hughes is executive vice president, worldwide services and support, managing Symantec’s consulting, education, and technical support operations, and ensuring that customers gain lasting and substantial value from the adoption and use of Symantec technology.

Hughes joined Symantec through the company’s merger with VERITAS Software. At VERITAS, Hughes was executive vice president of global services, managing services, consulting, support and education. Hughes joined VERITAS from McKinsey & Co., where he was a partner. During his 10-year career at McKinsey, Hughes founded and led the North American Software Industry practice. Hughes also advised senior executives of Fortune 500 companies in manufacturing, communications, retail, and aerospace on information technology-related issues. Prior to McKinsey, Hughes was the founder and CEO of Granite Microsystems, an industrial computer company.

Hughes holds a Master of Business Administration degree from the Stanford Graduate School of Business, and a bachelor’s degree in electrical engineering and a master’s degree in electrical engineering and computer science from Massachusetts Institute of Technology.

