

Focus on IT Risk Management

JOHN JACKSON

While many of us find ourselves focused on business continuity and disaster recovery, IT and operational risk management are becoming critically important functions in every company. This is a result of increasing vulnerability and threat activity as well as the legal, regulatory, and business exposures tied to those threats.

Organizations have struggled for decades to get a firm handle on risk, in order to shift from a model of “experience and react” to one of “anticipate and adjust.” Technology is at the core of both the problem and the solution.

As the visibility of risk has risen within the organization, management structures have undergone a transformation as well. Once disparate activities related to disaster recovery, business continuity, security, production high availability, and operational risk are now converging under the domain of the chief risk officer. Some companies have extended this scope to include physical security and are embracing the term “enterprise risk management.” These managers often come from audit, legal, or insurance risk management backgrounds and don’t have the tools or experiences to handle the diversity of risk under their purview.

Additionally, due to a lack of business context, companies are challenged to set priorities, make informed decisions, and build roadmaps and budgets. Organizations lack the metrics to facilitate decision-making, provide management reporting, and ensure accountability.

Reality suggests that organizations must understand the full spectrum of risks and then decide on a course of action for each. Unfortunately, until now, there have been no automated tools to help executives manage risk holistically, while providing a context to determine how important each issue is in relation to the others. Additionally, organizations tend to address risk one project at a time and lose the leverage that can be gained by addressing risk systemically. The result is a risk management program that is often ineffective, inefficient, and too expensive.

Does your organization know which risks are mission critical and which may be deferrable? In businesses where everything is considered important to someone, it is a challenge to determine what is most important and, conversely, what is not! Risk management usually means making difficult decisions, such as having to accept some

risks because there are simply not enough funds to appropriately dispose of all of them. Effective, efficient, and economical programs require a consolidated decision framework that clearly identifies the appropriate disposition of risk.

There are five viable choices for managing risk. They are: protect, eliminate, accept, assign, and mitigate. The criteria for deciding on the best disposition strategy for a given risk is usually based on probability and severity analysis, coupled with an assessment of the gap between the current state, the desired state, and the investment required to close that gap.

Protect: Protection, or avoidance, is a common form of risk management that is rarely as effective as some would like to believe. Some level of protection is applied to virtually everything of value. Most people lock their doors at night, and others add another layer with an alarm system. But the reality is that protection is never fool-proof. And protection is simply an approach used to reduce the probability of a risk becoming a reality.

Eliminate: Not the panacea that it may sound like, risk elimination usually means not engaging in a specific business activity or not deploying a given technology or business application because the risk offsets the value derived. More commonly deployed in risk-reward decisions surrounding large investments like mergers and acquisitions, risk elimination is increasingly becoming a consideration in more mundane situations where there is just too much risk in relation to the upside benefits and costs to manage that risk.

Accept: While some might refer to this as the “do-nothing” alternative, accepting risk must be a conscious decision. Some risks are acceptable. Risks with low probability and low severity may not merit investment. For example, it doesn’t make sense to implement a million dollar solution to protect or mitigate a thousand dollar exposure. Experience suggests that acceptance of risk is a reasonable and prudent strategy for some risks. The challenge is determining the right ones! Increasingly, auditors and regulators are requiring organizations to demonstrate the business logic used to conclude that a given risk is acceptable.

Assign: Some risk can be assigned or transferred, in whole or in part, by offloading the risk to another party.

Realistically, assignment is most practically implemented in response to financial losses. Insurance is the most common technique for assigning risk and serves only to mitigate the financial impact. Steps to protect or mitigate are still necessary in dealing with most risks and may affect insurance rates or even insurability. Outsourcing is not a valid “assignment” in that the risk is still born by the organization if the outsourcer fails.

Mitigate: When all else fails, risk mitigation becomes the strategy of choice. There are two options for risk mitigation. The first is proactive, anticipatory mitigation. In this case, actions are planned, and the plan is put into action. To be effective, planned activities require some ongoing support to keep them vital and utilize resources that are reserved for that purpose. The other option for mitigation is reactive. In this model, little more than casual thought has been applied in advance and a mad scramble ensues to cover the bases and put things back together. Such reactive strategies are relatively inexpensive until they are exercised, and then they become costly and unreliable.

Most organizations employ a combination of these five approaches to their overall risk management program in pursuit of the new ideal, defined as having the innate ability to defend, protect and recover, so that the business operations continue even in the face of severe adversity.

The result is a loose confederation of “solutions” that often overlap in some areas and leave gaps in others. And the organization is left with undetected risk, excess effort and investment, and unrealistic expectations. The move towards the ideal highlights the need to view risk holistically in order to make sound business decisions on what tools to deploy in which situations, and at what cost. **CI**

John Jackson is a co-founder of Fusion Risk Management and a member of the Continuity Insights Editorial Advisory Board. He is an expert in the fields of business continuity, disaster recovery, and high availability. His 30 years of experience includes running all aspects of IBM, HP, and Comdisco’s disaster recovery businesses and participating in over 500 actual recoveries for client companies. He can be contacted via e-mail at JJ@FusionRiskMgmt.com.

AmeriVault Delivers Advanced Business Continuity & Disaster Recovery for the SME



AmeriVault delivers advanced D2D backup services that seamlessly protect your data.

- ★ **Secure Online Backup**
Automated, offsite and tape-free.
- ★ **Real-Time Replication**
Continuous data backup or high availability.
- ★ **Digital Archiving**
Compliant online records preservation & discovery.
- ★ **Comprehensive Recovery Solutions**
From mobile disk devices for large data recoveries to mobile recovery units for people and infrastructure.

Visit our site today to learn how AmeriVault can tailor affordable solutions that greatly improve backup and ensure recovery when you need it.

AmeriVault
Excellence in Data Protection Solutions

www.AmeriVault.com