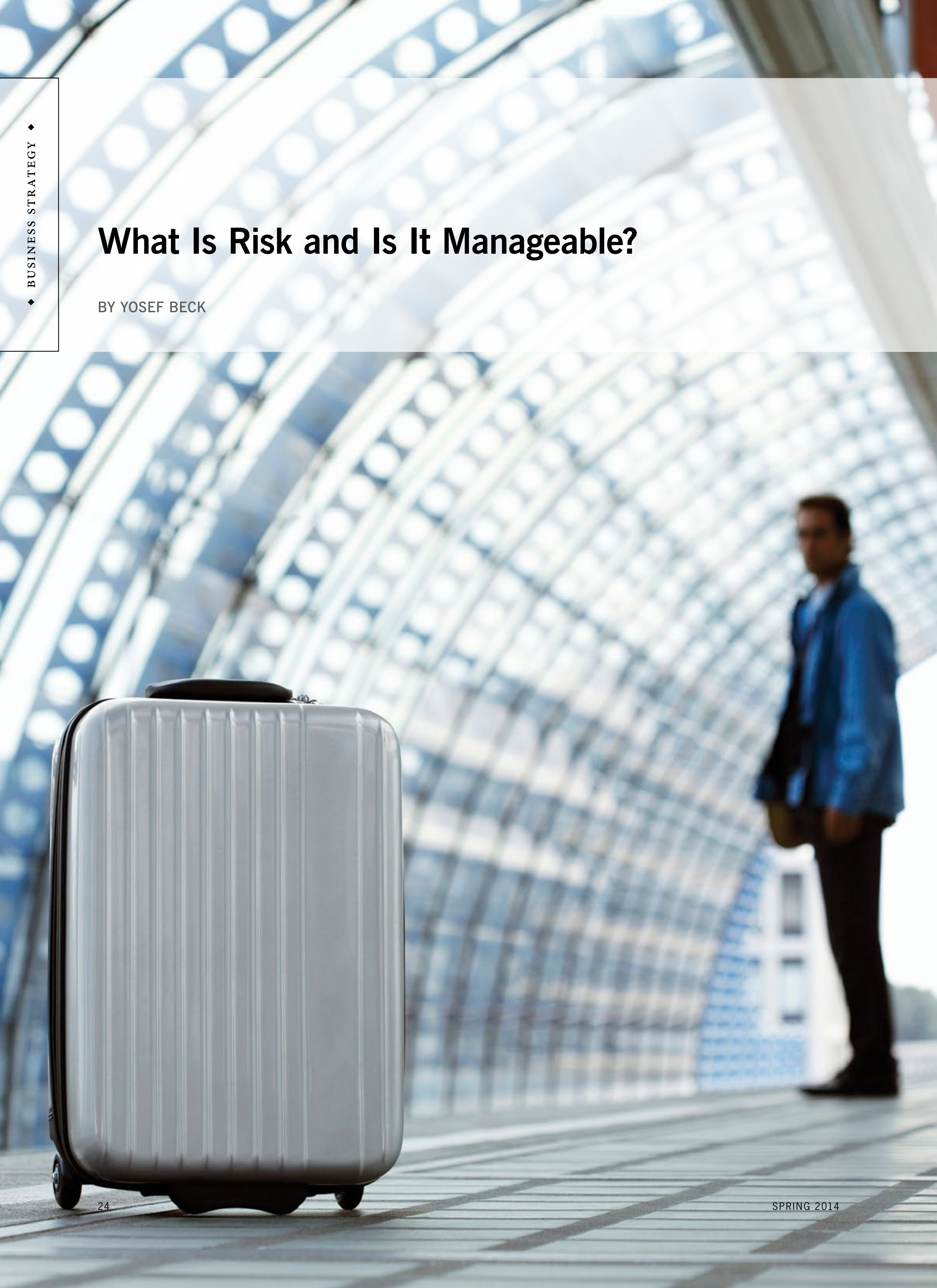
What Is Risk and Is It Manageable?

BY YOSEF BECK



High-profile database breaches, worldwide crime, terrorist activities, legislation such as Sarbanes-Oxley, and other security challenges are forcing companies to have to continuously monitor and update their risk management practices. In doing so, are companies simply responding to external stimuli, or are they truly able to manage their risk to an acceptable level while continuing to maximize their ROI?

IDENTIFYING:

Before discussing the management of risk, an organization needs to identify and define what it considers a risk. Although used interchangeably, risk and threat mean different things. Defined by Bruce Schneier (internationally renowned security technologist), a threat is a potential danger posed to an organization. A risk takes into account the probability of a threat as well as the seriousness of its impact on the organization.

An employee stealing intellectual property (IP) and an atom bomb are both "threats" to an organization. However, there is a much higher risk that an employee would steal IP than that an atom bomb would disrupt the business, and the probability of IP theft is increasing yearly.

Defining the risks to the organization should include identifying:

- The organization's accepted level of risk
- The organization's definition of success (in limiting liability)
- Potential problems and threatening entities (whether they are human, animal, or computer)
- Available tools (people, money, electronics, etc.)

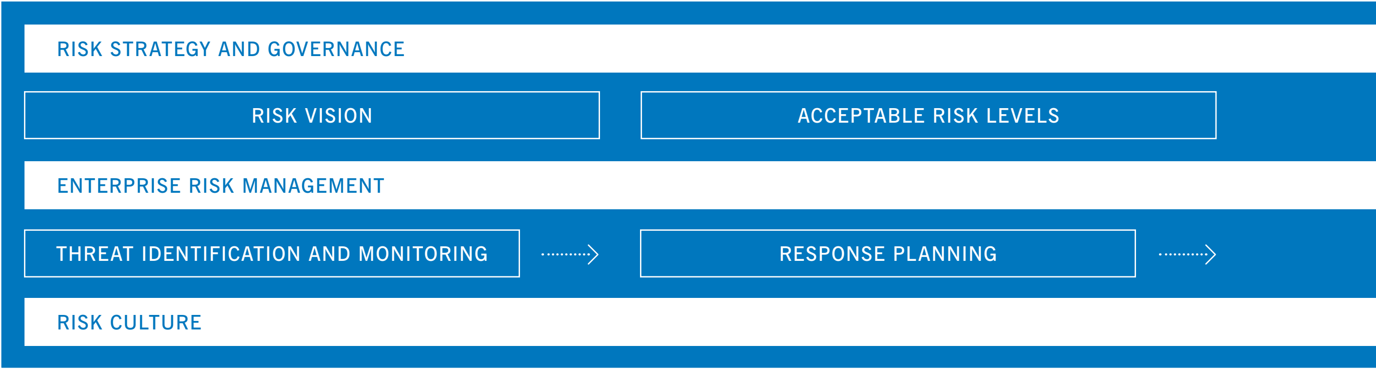
QUALIFYING:

Once an organization has defined risk as it applies to itself, the organization should then quantify the value of risk management. Reducing the probability of threats brings value to an organization. Examples include: decreasing the risk of employee productivity loss, reducing rework and legal fees, and reducing the loss of business from security incidents (e.g., damage to brand).

When is risk management specifically called for? One could argue that an organization is always managing risk. Even if it makes a conscious decision to do nothing, that is also a risk management approach. However, to ensure consistent and comprehensive application to the entire organization, a risk management framework may be necessary. Examples of such situations include when an organization is engaging in behavior outside the accepted level of risk, or if priority levels are unclear or shifting too often. Other applications calling for risk management include when an organization inherently changes its accepted level of risk, such as when it is pursuing transformational objectives like an HR reorganization.

Alternatively, a prime candidate for applying a risk management framework is an organization that does not know what its current liability exposure is and needs help determining what levels are acceptable. Perhaps the worst-case scenario is when business leaders are disengaged from strategic, risk-minimizing decision-making

Figure 1: Risk Management Framework



RISK STRATEGY AND GOVERNANCE

RISK VISION

ACCEPTABLE RISK LEVELS

ENTERPRISE RISK MANAGEMENT

THREAT IDENTIFICATION AND MONITORING

RESPONSE PLANNING

RISK CULTURE

ALIGNING:

A framework helps an organization align its risk strategy to its overall business strategy, as well as functionally integrating its approach to limiting liability into all aspects of the organization. All too often, organizations put their primary focus on their IT liabilities. A framework can help an organization take a holistic view of all potential liabilities and focus on its human resources as well as its physical and soft assets (see Figure 1).

IMPLEMENTING:

Risk Strategy and Governance

Risk strategy and governance provide direction and ensure that the necessary processes are in place to empower required resources to monitor and respond to risk. In addition, they provide structure for ensuring that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions.

Risk strategy and governance should incorporate the definition of risk as defined in the first stage of identifying risk as the organization's risk vision. What does the organization consider acceptable levels of risk? What is the current level of risk management maturity and where does it need to be? Finally, governance of risk includes setting risk policy, disseminating that policy, and upholding it throughout the organization.

Enterprise Risk Management

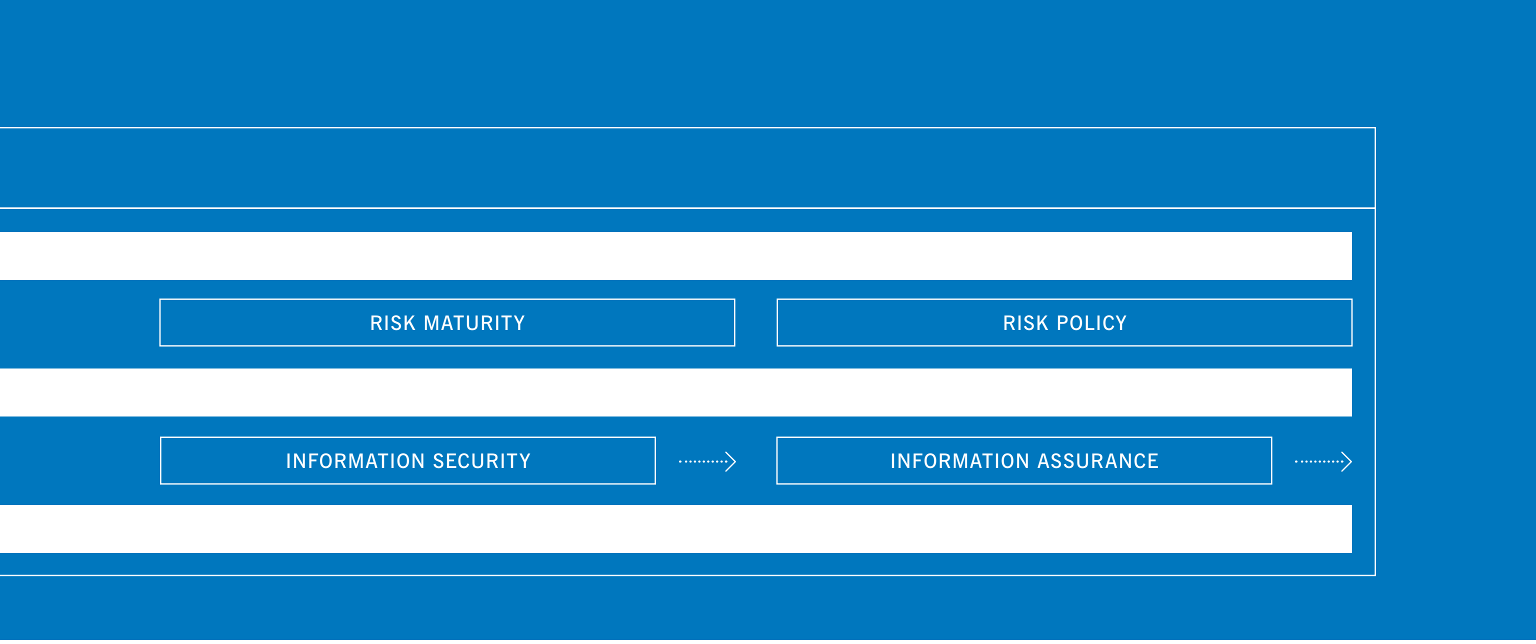
Enterprise risk management provides the required business functions to enable an organization to manage its liabilities to an acceptable level while maximizing its ROI. It should provide the following comprehensive business functions in a holistic approach across the human element, hard assets, and soft assets of an organization:

Step 1: Threat Identification and Monitoring

Although the original phrase is "the first blow is half the battle," when it comes to risk management, it is best to go with GI Joe's version: "knowing is half the battle." Threat identification and monitoring helps identify potential threats and avenues of approach. This allows an organization to increase its window of warning of a threat and includes everything from monitored security cameras to sophisticated fraud detection software.

Step 2: Response Planning

From the probable to the improbable, response planning helps break down all the possibilities in order to plan accordingly. What happens if the database administrator of your HR department dies tomorrow? Will you know how to administer payroll without him? How will you respond if another Hurricane Katrina wipes out your supply chain for months? Will you still be able to fulfill your customers' orders? Daunting from the outset, and too often ignored until it is too late, planning for business continuity is a necessity.



Step 3: Information Security

Information security protects information and information systems from unauthorized access, use, recording, modification, etc., by ensuring that only authorized people have access to information or locations. This includes conducting background checks on new employees, having physical checkpoints or locks, password protection and firewalls, authorizing viewing of personal or secure information, and restricting system and database usage.

Step 4: Information Assurance

Knowing that information has been compromised is as important as stopping the compromising activities in the first place. Information assurance is any action taken to know if compromising of information has occurred. This includes the use of tools such as personnel access logs, tamper-evident tape, server logs, etc.

RISK CULTURE

Ultimately, risk management is dependent upon a strong risk culture, which enables an organization's people to make the right decisions in an informed manner. Education and monitoring are key to building a strong risk culture, and legislation such as Sarbanes-Oxley has been one step forward in improving security for investors to build a stronger risk culture.

MONITORING:

In 2011, a Harvard Business Review Analytic Services survey found that "42% of companies with 10,000 or more employees reported that they had a chief risk officer, compared with only 11% three years ago." However, at the same time, the survey found that "barely one-third of all respondents felt they were doing well at any of the six risk management capabilities [as defined in the survey] they most often cited as critical to organizational performance."

Risk management, recognized as a continuous need of any organization, is enhanced by using a risk management framework. Applied consistently across the organization, risk management does not have to be an unwieldy beast or an overly broad function. By continuously monitoring its application, an organization ensures that it delivers value, that the organization is aligned to its accepted level of risk, and that threats and capabilities are updated on an ongoing basis.

© 2014 JABIAN, LLC. ALL RIGHTS RESERVED.

YOSEF BECK
yosef.beck@jabian.com

Yosef is a Manager and applies his expertise in systems analysis to his passion of security optimization