

synnovation



Vol. 1 Issue 3

Beating the Odds

Leading an organization through a risk-laden environment is often a game of chance. But enterprise risk management can help your odds.

EDS

Unwelcome Surprises

By Al Decker

Towers Perrin

Coming of Age

By Prakash Shimpi

Microsoft

Defending the Crown Jewels

By Ron Markezich

Oracle

Protect, Detect, Deploy

By Vipin Samar

Dell

Super Power

By Dr. Reza Rooholamini

Sun Microsystems

Tapping Tag Power

By Jim Del Rossi

Xerox

For the Record

By Charles P. Brett

EMC

Reaching Out

By Gregg Therkalsen

Cisco Systems

A Matter of Self Defense

By Bob Gleichauf

EDS

Conversations

With Ron Rittenmeyer

Microsoft

Up Close and Personal

With Ron Markezich

Risk Takers

From Meltdowns to Management Strategies, the Way We Handle Risk is Changing

By Rebecca Whitener, EDS

At its simplest definition, *risk* is the idea that something “bad” might happen. But perhaps a more thorough explanation is the following: Enterprise risk is the possibility of losses or other negative consequences caused by an event, or a chain of events, that can adversely affect the achievement of an organization’s objectives.

Within that simple idea are some important questions to consider: What are the chances that this bad event will happen? What will be the consequences if it does happen? Generally, when thinking about risk, we walk through a range of alarming scenarios, focusing on those events with the potential to generate the most impact. It may sound rather simplistic, but in reality, managing enterprise risk is a complex undertaking.

Over the last 10 years, we’ve witnessed some highly visible meltdowns of major established companies with *presumably* sound risk management strategies. Over the same time period, we’ve also seen enormous growth and financial gains experienced by start-up companies with no formal risk management processes in place. This phenomenon raises the question of whether risk management as a discipline is no more than a combination of luck—being in the right place at the right time—and the ability of certain leaders to navigate changing conditions and the vast unknown.

Because risk refers to the possibility of some future event, in many ways risk management can be described as a game of chance. That doesn’t mean an enterprise can prepare for future precarious scenarios without effective risk planning processes. It does mean, however, that even with deep-rooted risk management processes in place, luck often plays a role in the eventual outcome.

Fortunately, prudent organizations today aren’t



willing to bet their business viability on good luck. They’re investing in technology and processes to enhance their ability to explore the future for risky events and to create workable solutions to reduce the likelihood and impact of these events. Enterprises are looking ahead and seeking to improve the outcome of negative future scenarios by implementing what’s being referred to as an enterprise risk management framework—complete with policies, standards, and governance models.

We see a heightened focus on this activity not because it’s the solution for all potential destructive forces, but because executives, regulators, investors, and other stakeholders want more clarity on how well prepared organizations are for these future uncertainties. A company that can define

and document in an auditable framework the activities in place to scan the horizon for opportunities and threats, and then map these identified risk events back to existing plans and processes, is considered better prepared for potential threats than those companies that claim to be managing risk but are doing so by primarily hoping for the best. And then relying on destiny.

Enterprise risk management is aided by a number of innovative tools developed to help business leaders. Diverse risk scenarios and their impacts can be created from a range of converging events and illustrated through visualization technologies, which then lead to more informed risk mitigation planning. Executive-level risk dashboards are being developed to inform leaders of any significant risk event that's close to, or has exceeded, risk threshold tolerances. New reporting mechanisms are helping chief risk officers collect cross-functional data and correlate risk identification and assessment results across the enterprise so that duplication of effort is minimized and decision-makers are better informed.

If silo-based risk management was the trend of the past, it's now becoming a reminder of how organizations have been blindsided by surprises. It's becoming increasingly more evident that elevating key risk identification, assessment, evaluation, and mitigation activities to a cross-functional enterprise level helps shed light on the most serious risk issues and leads to better, more risk-informed decisions. Today's enterprise risks are global, complex, multidimensional, and interrelated. A systematic approach to examining and managing these risks helps ensure that the majority of the "what can go wrong scenarios" have been considered, and that mitigation plans have been put into place for the most significant possibilities.

Clearly, the function of enterprise risk management is maturing and shows a lot of promise for the future. As known and unknown risks continually invade our ever-changing ecosystems, it's time to get more offensive in our approach to risk and uncertainty. Technology will continue to serve as the catalyst for that plan. [s]

About the Author: **Rebecca Whitener** is EDS' CRO and an EDS fellow. An authority in security and privacy solutions, Whitener was appointed to the U.S. Federal Trade Commission Advisory Committee for Online Access and Security.

Where's ERM Headed?

Take a look at what could be some of the new weapons in your enterprise risk management arsenal in the near future.

Real-Time Enterprise Dashboards—Tomorrow's dashboards will truly be capable of measuring real-time activity, allowing decision-makers to have today's information today for real-time action. Additionally, data will be moved out of organizational silos and up to the enterprise level for a relational view of the enterprise.

Visualization & Scenario Planning—Much in the same way they play, Generation X and Generation Y workers will manage with visualization, which allows them to actually see how various scenarios play out as a result of different decisions. Imagine "seeing" the probability of an acquisition succeeding or the operational impact of a hurricane or pandemic flu.

Encryption—In the near future, all data will be encrypted, so when devices and records are stolen—and they will be—the data will not be readily useable. As with all security measures, there will be counter measures, and encryptions will be broken. Clearly, encryption will be a security measure that will need to keep one step ahead of the "bad guys."

Embedded Security—Today we attempt to protect the device, the network, the platform, the application, or the system. Tomorrow we'll protect the data by embedding the appropriate level of security file into the data itself. The protection will follow the data rather than the device.

Zero Latency Security—In the past, there has been a reluctance to deploy security measures because controls often slow performance and thus impact business and revenues. In the future, zero latency technologies embedded with data will significantly reduce that lag on performance and the "friction" inherent with security, allowing for free-flow, transparent security.

Immune Systems—Similar to how our body's immune system fights off viruses, tomorrow's information systems will use knowledge and experience to learn how viruses invade and mutate in order to build defenses and "antibodies" to counteract viruses and threats.