

18 – 22 October 2009 Orlando, Florida

TRIP REPORT

Security & Risk Management Community

This year's Gartner Symposium/ITxpo was organized around the theme of balancing cost, risk and growth. This report offers an overview of what was on attendees' minds and what they learned from Gartner analysts and each other.

KEY TAKE-AWAYS

Executives and boards of directors are increasingly interested in the state of security and the overarching risk posture of the organization. Risk and security personnel are struggling to communicate effectively and link risk and security to corporate performance. A big factor in that reality is the inability to clearly define and communicate the business value of security and risk management initiatives.

This requires chief information security officers (CISOs) and chief risk officers (CROs) to formalize a security and risk management program that addresses risk, meets compliance requirements, directly ties activities to business performance, and communicates successes and challenges in language appropriate to a business audience—avoiding technical terms and operational metrics.

Other challenges that CISOs and CROs face include the need to:

- Map key risk indicators against business key performance indicators (KPIs).
- Fold in security costs from the start of any virtual data center initiative.
- Include a cyberthreat assessment step in all new business IT projects.
- Make business resilience an executive priority and part of enterprise culture.
- Reposition the perception of identity access management (IAM) for business and IT as enabling IT governance.

Conference highlights

Five Practical Tips to Link Risk and Security to Corporate Performance

Every board of directors must know that its organization is protected against reasonably anticipated risk. CIOs, CISOs and CROs often struggle to link risk management efforts to the value they provide to the business. Gartner offers five tips to solve this challenge:

1. Formalize a risk and security program.
2. Use KPIs to assess operational risk.
3. Link risk initiatives to corporate goals.
4. Don't use operational metrics in executive communication.
5. Communicate to executives, emphasizing what works and what doesn't.

Recommendations:

- Assess the maturity of the major elements of your risk and security program.
- Develop an executive reporting plan that addresses the needs of a business audience.

Securing the Next-Generation Virtual Data Center

Virtualization offers IT opportunities to reduce cost and increase agility; however, if this is done without implementing best practices for security, resultant security incidents will increase costs and reduce agility.

Security must be “baked in” from conception, not addressed later as an afterthought. The costs of implementing best practices are significant and must be included in any analysis of the projected cost savings of virtualization. If these costs are avoided, the risk of not investing must be accepted by the decision maker in the move to virtualize.

Recommendations:

- Evaluate virtualization solutions with security criteria in mind.
- Pressure security and virtualization vendors to plug all gaps in security.

The Gartner 2010 Cyberthreat Landscape

During the past two years, Gartner has seen major shifts in attacks against business systems:

- Targeted versus broad. Targeted attempts try to escape detection and achieve specific goals, such as stealing passwords or user information that can lead to identity theft.
- Changes in motivation. The rapid growth in identity theft points out big growth in financially motivated attacks. Cybercrime is the key growth industry through 2013.
- Changes in targets. Most new forms of attack are looking for vulnerable Web sites and vulnerable users.

The biggest change in the last 12 months has been the decline in the ability to prevent or shield vulnerabilities. In short, we are making it easier for attackers.

Recommendations:

- Become more efficient at dealing with old and new threats.
- Include a threat assessment step in all new business IT projects.

Creating a Resilient Organization Through Business Continuity Management and IT Disaster Recovery Management

Business resilience emerges when business and IT leaders work together across geographical, functional, business and decision-making boundaries to build an organization that rebounds, adjusts quickly and resumes operations wherever its people, processes and systems are located.

A truly resilient business intentionally designs resilience into its business—injecting knowledge, safety, protection and imagination into dispersed and far-flung organizations so they can bounce back from any kind of setback.

Recommendations:

- Make business resilience an executive priority and part of your enterprise culture.
- Form a multidisciplinary governance team, and monitor, measure and report status.

IAM: Enabling Governance and Risk Management in an Age of Business Challenges

Implementing effective identity access management (IAM) to support world-class governance, risk and compliance management (GRCM) demands a level of maturity and quality that mediocre IAM implementations can't achieve. GRCM places more demands on the quality of input from compliance monitoring and reporting, requires higher levels of integration for dashboards showing holistic views, and needs platforms and applications of broader scope.

A quality-focused IAM implementation can meet those needs.

Recommendations:

- Reposition the perception of IAM for business and IT as enabling IT governance.
- Integrate process planning in IAM and GRCM.

Workshop

A workshop for security and risk management professionals provided attendees the opportunity to determine how they stack up using Gartner risk program maturity benchmarks.

This tool provides clients with the opportunity to assess the maturity of the processes that make up their risk program, as well as the process components that compose the functional areas within it: risk management, information security, privacy, business continuity management and compliance.

As part of the workshop, attendees completed surveys assessing their enterprise's maturity on the following aspects of security and risk management:

- Risk governance
- Strategic planning that guides security and risk management activities
- Tactical planning and budgeting
- Organizational ownership of security and risk management programs
- Control and architecture frameworks
- Processes that support the goals of risk management
- Communication initiatives that address associates' responsibilities in handling sensitive business information
- Event detection and response

Key findings of the exercise:

- Some attendees were surprised that their enterprises are more mature in their risk and security assessment, while others were not surprised—and even expected to find—that their maturity level was low.
- The benchmark to date contains the data of 97 enterprises but Gartner expects to double that number in 2010. The industries of energy and utilities, and financial services score highest in the maturity assessment.
- Attendees included representatives from the public sector, business and consumer services, education, healthcare and insurance.
- Most attendees' organizations consisted of more than 10,000 employees.

Best practices:

- Learn from your operations and service management colleagues.
- Don't work in isolation; understand integration and relationship points with other IT services and operations processes.
- Improve one level at a time. Don't try to skip a level of maturity.
- Implement an iterative, ongoing maturity process.
- Use process performance metrics; reassess maturity progress every four to five months.
- Have realistic objectives; not all processes must reach Level 5.

Recommendations:

- Focus on process.
- Assign ownership and accountability for risk management.
- Educate your management team through the correlation of process maturity and program success.

Keynotes

Welcome address and Gartner analyst opening keynote

Hard times hit organizations of all sizes around the world. Despite early indications that some economies are poised to rebound and rebuild, many of us—or people we know—find ourselves knee-deep in economic uncertainty. Gartner recognizes that while scenarios for a return to growth vary, the time for action is now—enterprises must balance cost, risk and growth.

If the entire enterprise focuses exclusively on cost, everything looks like an unnecessary expense. Instead, model the economic impact of technology on the overall performance of an organization. Among other areas, performance should encompass revenue, market share, agility and innovation. And above all, make informed decisions on new tools and capabilities. [View the webcast here.](#)

Mastermind Keynotes show other organizations' strategies

- Vivek Kundra was appointed to serve as the first federal CIO of the United States by President Obama in March 2009. He discussed the challenge of changing the long-held belief that the public sector cannot be a leader in technology innovation. He said his goal is to sell the idea that the public sector can indeed solve the problems that customers face from a technology perspective, thereby improving customer satisfaction. [View the webcast here.](#)
- Mark Hurd, chairman and CEO at Hewlett-Packard Company, spoke on some of his visions and goals for HP, which include a plan to spend \$17 billion on R&D and \$20 billion on acquisitions to build out a model of converged infrastructure in which server, storage, networking and PC markets are integrated. With the world's data expected to double in the next four years, this converged infrastructure will be critical. He expects these coming innovations at HP to have the power to disrupt all of these infrastructure markets during this time. [View the webcast here.](#)
- Eric Schmidt, chairman and CEO of Google, Inc., stated that the boundary between enterprise and non-enterprise is becoming less and less pronounced when it comes to applications. CIOs are dealing with employees who want a seamless experience at home and at work, while enterprises are still trapped in inflexible 1980s architecture. He takes the position that enterprise is an important business, but the opportunity for a new platform that spans enterprise and consumer behavior is even more important. He sees this as the next billion-dollar business for Google. [View the webcast here.](#)
- Stephen Elop, president of the Microsoft Business Division of Microsoft Corporation, said Microsoft fully embraces “constructive disruption,” and that the corporation recognizes the shift that is happening in its marketplace as the pace of innovation accelerates in the cloud. Continuing to talk to users and apply the lessons learned from past experience is essential to keeping things in balance, he said. “Great companies recognize the disruption and power through them,” Elop said, while at the same time acknowledging the challenges Microsoft faces as it keeps pushing forward. [View the webcast here.](#)

What people asked about

How do we manage vendor risks from dozens of partners?

Addressing vendor and partner risks as they relate to security and compliance concerns is necessary and increasingly complex. An appropriate approach requires a combination of contractual expertise, governance, the application of technical controls and administration. Organizations must manage vendor compliance and security risks including regulatory, confidentiality, breach notification, availability and integrity. Key elements include vendor risk assessment, contract management, vendor assertion management, compliance management and reporting. Automation is available to assist in managing this information through IT governance risk and compliance management products and many mainstream vendor management products.

What should we do if we can't get management to pay attention to our ability to link risk and security to corporate performance?

The best approach in the absence of an incident is to get management's attention by periodically reporting (quarterly or twice-yearly) the status of your risk initiatives to executives, even if they haven't asked for such reports. That will help you to be ready to impress them when you do get the chance, which is sure to happen. You don't want to miss that opportunity to get in front of executives and show them how risk and security map to corporate goals.

How do we most effectively communicate the status of our security and risk management programs to executives?

You start by not using operational risk metrics in your communications to executives. They don't care about the number of incidents, for example. And they lack the context to understand those metrics. Instead, you tell them what's working and what's not working. Use language that they can grasp and appreciate—business language that focuses on results. Where possible, map key risk indicators to key performance indicators in the business.

Is the trend in identity and access management toward moving the responsibility for policy management to the data owner, rather than the IT department?

Yes. We see that there is a movement—as there should be—toward the custodian being the one to take care of IAM policy management. Most enterprises allow IT to control policy definition but there must be more business input in that process. However, expect the business to be reluctant participants. Yet it is essential that they participate so that they can begin to codify the behaviors in information access that they want and need.

What are the characteristics of a business-resilient enterprise?

In the broad view, business resilience enables an enterprise to put its organization back together and move on a dime after a business interruption. More narrowly, we find that these key factors engender business resilience—agility, a dispersed workforce, integration of electronic resources, the ability to rebound and resume decision making quickly, and the ability to operate at full speed (even in the face of adversity). One final characteristic is that any lack of resilience may be fatal to the enterprise.

Things to watch for

Increased scrutiny of data protection mandates: In this age of increased transparency and regulatory requirements, it seems like all stakeholders—vendors, business partners and members of your supply chain—are asking everybody for assertions of regulatory readiness and control data. It's become an unsustainable chore, as everybody has become mutually dependent on one another to ensure that their data is protected. Because of this increased desire for visibility, all parties are understandably nervous about the security of their data. This nervousness will only continue in the years to come during this age of hyperauditing.

The risk of software as a service, social media, cloud computing and the loss of control from employees using these services from their personal devices: In far too many organizations, the security department mission statement still reads that it's the onus of security to protect the organization from all threats, internal and external. That doesn't work in the new environment. Risk management is about accepting that we can't protect ourselves from everything, so we have to make conscious decisions about what we will do, and more importantly, about what we will not do. You should let the outside information in (think Facebook and other social networks) and share outbound information. Don't think you can shut out the two-way flow of information, because you can't stop it anyway. But start to accommodate it as part of your thinking in risk and security.

The growing maturity of enterprise resource management (ERM) when it comes to security: Client inquiries indicate that more CIOs and CROs are being asked to respond to the impact on the supply chain of security concerns. We're also seeing that security departments are getting better at responding to these issues. It will only increase in the years to come.

GARTNER SECURITY & RISK MANAGEMENT SPEAKERS

F. Christian Byrnes

Managing Vice President

French Caldwell

Vice President

Neil MacDonald

Vice President and
Gartner Fellow

Eric Ouellet

Research Vice President

Earl Perkins Jr.

Vice President

John Pescatore

Vice President and
Distinguished Analyst

Paul Proctor

Vice President and
Distinguished Analyst

Jeffrey Wheatman

Director

Roberta Witty

Vice President

ITXPO SPONSORS FOR THE SECURITY & RISK MANAGEMENT SYMPOSIUM COMMUNITY

2010 Security & Risk Management Marketplace

Archer Technologies

Arcsight

Cisco, IronPort Systems LLC

Fischer International

Fortinet

Guardium

Hitachi ID Systems

Lumeta

Nuspire Networks

Planview

Purewire

Secure Works

Solutionary

2009 Security & Risk Management Marketplace

Archer Technologies

Arcsight

Cisco, IronPort Systems LLC

Fischer International

Fortinet

Guardium

Hitachi ID Systems

IronKey

Purewire

Secure Works

Symark International

Symposium/ITxpo 2010

The World's Most Important Gathering of CIOs and Senior IT Executives

It's not too early to start planning for next year. We hope to see you again when we celebrate 20 years of Symposium/ITxpo, 18 – 21 October 2010, in Orlando, Florida. Keep up by visiting gartner.com/us/symposium as the latest news, alumni benefits and registration details are unveiled for this exciting event.