



Security & Risk Management
Symposium Community

Trip Report

Security & Risk Management
Symposium Community

Members: 444

This year's Gartner Symposium/ITxpo — held from 12 through 16 October in Orlando, Florida — was organized around the theme of IT and the economy. This report offers an overview of what was on attendees' minds and what they learned from Gartner analysts and each other.

Key Takeaways

Not surprisingly, the sagging economy and its consequences for security and risk professionals was a prominent topic. Other perennial issues of concern to security specialists were also much discussed, however — issues such as the security challenges brought on by the consumerization of IT, the global economy, identity and access management, and compliance and risk.

Conference Highlights

Report to the Board: Five Practical Tips to Link Risk and Security to Corporate Performance

A board wants to know that the organization is appropriately protected against reasonably anticipated risk. CIOs, chief information security officers (CISOs) and risk management officers (RMOs) struggle to link risk management efforts in security, privacy, business continuity and compliance to the value they provide at the line-of-business and executive levels. A handful of companies have figured it out, and five practical tips can get organizations started in solving this challenge:

- Formalize a risk and security program.
- Don't use operational metrics in executive communication.
- Use key performance indicators to measure operational risk. (Bonus tip: Link risk initiatives to corporate goals.)
- Report risk assessment quarterly, using simple, clear criteria.
- Communicate to executives, emphasizing what works and what doesn't.

Managing IT Risks During Cost-Cutting Periods

The financial crisis will drive proactive cost cutting in very short time frames, but cost-cutting risk is better controlled when staff and projects are aligned with service delivery, new capabilities and line-of-business budgets.

Risk management, compliance and security professionals can support IT organization and business cost-cutting initiatives by providing IT risk assessment support, ensuring that reductions in security budgets are appropriate and minimize risk-posture impacts.

The evaluation of sourcing alternatives for IT functions should include service, security and compliance requirements. Security staffing decisions should ensure that basic security capabilities and required project support are maintained.

- IT risk managers should work closely with IT financial managers and business analysts to initiate cost-cutting risk analysis before senior management imposes cost-cutting mandates.
- Compliance managers should confirm that proposed cost cuts do not impact regulatory, commercial or organizational mandates.
- Security managers should define and document current security operations and identity administration service levels to assess cost-saving opportunities and the budget and service risks that are inherent in sourcing decisions.

Beyond MarketScopes and Magic Quadrants: Architecting a GRC Solution

During the next several years, we will see the transition from compliance and risk management as a necessary, but unproductive, task to a focus on business performance as an element of governance, risk and compliance (GRC) investments. Of course not all GRC investments will focus on performance — an enterprise should have investments that bring value from tactical to strategic. To get the maximum value, GRC investments should be guided by common architectural and governance principles. Gartner recommends that compliance and risk officers:

- Ensure business alignment. The IT component of the GRC solution should be relevant to each enterprise's business goals and risks.
- When using Gartner methodologies to make decisions, don't just consider the most highly rated vendors and most mature technologies — a niche vendor may be best able to solve your problem.
- Link GRC initiatives to other critical business strategies and objectives, rather than having stand-alone GRC projects.

Workshop Explains the Gartner Risk Assessment Method

Gartner analysts led more than 40 people in a filled-to-capacity workshop on using the Gartner Risk Assessment Method (GRAM). (See G00158471 "Assessing Risks Using Gartner Risk Assessment Methodology"). This step-by-step methodology allows security teams to perform risk assessments quickly and effectively by giving them a simple template that helps quantify risks. The GRAM uses a simple two-axis chart to assess, first, the importance of a process to the overall health of the enterprise, and second, to assign a probability to that risk. The results can then be reviewed separately by subject matter experts in less than an hour, which prevents their feedback from getting bogged down in back-and-forth arguments. The GRAM also allows charting risks dynamically, showing how they can change over time and how those changes should affect risk mitigation efforts.

How Identity and Access Management Contributes to Your Key Business Imperatives

Identity and access management (IAM) processes integrate with other information security processes, such as threat and vulnerability management, risk and control assessment, and communications and relationship management. IAM processes must also integrate with business processes, such as employee "onboarding" and customer registration. By abstracting identity management and access controls from applications, IAM allows application developers to focus on business needs and allows them to make innovative use of new technologies that contribute to overall business agility. And through its security efficiency benefits, IAM can ensure that your workforce can quickly have the necessary access when needs change in response to new business challenges.

Security officers must make the business case for IAM by engaging all stakeholders across the business, showing how IAM can add value by helping:

- Attract and retain customers
- Build an innovative and agile organization
- Improve critical business processes and workflows
- Improve workforce effectiveness
- Maximize performance, profitability and competitiveness

Surviving the Threats Posed by the Consumerization of IT

Conditions are making it more difficult for organizations to maintain the security control that some of them would like. In particular, Web 2.0-style applications that don't need to be installed on users' PCs give users with Internet access a huge amount of freedom to run their choice of applications. While this does not create configuration issues, it still represents an investment in non-approved technologies and could represent data exposures. Beyond that, applications that don't need administrator rights to install and applications that users will be able to install in a virtual machine or in an isolated manner are here or will be soon. Digital natives are more proficient with technology, and they are entering the workforce and (in some cases) making technology demands.

With higher levels of user autonomy, the security focus needs to shift from security on the platform, to security that directly protects corporate data and the corporate network. Security officers must:

- Accept that consumerization is here to stay. You will not be able to say no to it.
- Accept that it is very unlikely the mainframe will come back. The risks of hoping for its return are severe.
- Match your security approach to the path your company is taking. If none is apparent, start with identity-aware networking.

Keynotes

Welcome Address and Analyst Keynote

Most IT budgets will take a hit from global economic problems, but the situation is not as dire as IT leaders who lived through the dot-com bust might expect. Gartner's recent surveys of CIOs show that at worst, IT spending worldwide likely will increase 2.3% in 2009, down from Gartner's earlier projection of a 5.8% increase. IT spending at worst will be flat in the U.S. and down in Europe.

IT budgets will be largely spared because IT runs almost all aspects of business, and IT is increasingly viewed as the means to improve and transform the business, but IT leaders still have to deliver. Economic downturns tend to amplify disruptive technologies, so IT leaders should research virtualization and modernization opportunities. IT leaders also should take stock of the whole IT portfolio to see what the business can run for less or live without. For every application and system, ask:

- Why is this needed?
- What does it cost?
- How can it be implemented with fewer resources?

Mastermind Keynotes Show Other Organizations' Strategies

Gartner analysts interviewed three IT leaders to gain insights about their strategies and outlook for 2009:

- John Chambers, CEO of Cisco Systems, said Cisco plans to work on dozens of projects in 2009 that aim to expand the company's scope beyond networking into networked-enabled processes to improve productivity. Cisco will use partnerships to help customers boost scale and speed. Cisco has a unique opportunity in the economic downturn to help its clients enable transformative business strategies, Mr. Chambers said.

- Joseph Eng, Executive Vice President, Systems and Technology at JetBlue Airways, urged IT leaders to show how IT can help transform and differentiate the business, as his group has done to make JetBlue a customer-centric airline. Mr. Eng described how JetBlue customers are empowered to make their own decisions and receive perks to make the trip better. This strategy has greatly helped JetBlue grow and has provided more opportunities for revenue.
- Steve Ballmer, CEO of Microsoft, insisted that what has been an apparently slow uptake of the Vista operating system among enterprises doesn't indicate a problem with Vista. In fact, he said, Vista's uptake is roughly comparable to the uptake of Windows XP at a similar stage. Ballmer also said Windows 7, Vista's follow-up, will be a true release, not a mere update. He acknowledged competition from Google but was critical of Google Apps, saying that it is "just not good enough today" for enterprise-level adoption. Cloud computing will also be a challenge for Microsoft, he said, since it involves a paradigm shift, but he predicted the company will adapt. Cloud computing will be delivered "piece by piece by piece," he said. "This is a technology that Microsoft is embracing, but it won't be ready the day after tomorrow."

What People Asked About

How can we do better with risk and security?

The simplicity of this question belies the complexity enterprises are facing. They need help with the fundamental issues as they move away from a technology-centric approach. They need to know how to measure, manage, report, and connect with the business. Enterprises should formalize their processes, write a risk and security charter, and implement risk assessment.

How do I change the culture of my company to care more about risk and security?

Start reporting on business unit risk posture without waiting for them to ask or care. The results will not be ignored for very long. This needs to be done carefully and accommodate corporate politics, but it can significantly raise awareness.

What should I do with a security team that has burned so many bridges that the CEO wants them fired?

Replace the CISO with a good communicator who understands how to balance business and protection. Move the purely technical people into operations doing the same jobs with less power to upset the business.

How can I deal with the security issues raised by virtualization?

Virtualization security must be "baked in" from conception, not addressed later as an afterthought.

Existing virtualization solutions address many security issues, but not all, and it will take several years for tools and vendors to evolve. In the meantime, IT organizations must make security a mandatory part of the evaluation of virtualization solutions and lab-test new approaches to security and management using virtual machine (VM) state inspection and security products that support the model. They should also exploit the new control points for security and management that virtualization provides — in hardware, in the hypervisor and in the virtual machine monitor (VMM). Finally, executives should rethink the organization: are separate groups really needed for desktop and server support? Are there routine security functions that security professionals are performing that could be handled by operations?

Things to Watch For

The key to making progress in security is staying ahead of changes, which means recognizing changes in business processes, threats and security technologies. The next step is applying a realistic mix of tactical and strategic steps toward increasing the effectiveness and efficiency of your security program. Key security challenges for 2009 will include reducing operational costs, supporting business changes, staying ahead of threats and demonstrating compliance. To deal with changing threats, changing business environments and continuing budget pressures, enterprises must become more effective and more efficient at protecting customer and business data. In the future, CIOs and CISOs will need to:

- Focus compliance spending on increasing the protection of business and customer data first, and then on reporting compliance to various regulatory regimes.
- Demand that all software (whether bought off-the-shelf, developed in-house or developed by an external service provider) is free of known vulnerabilities.
- Define security processes that integrate with business and operational processes and providing a path to move routine security processes to IT operations groups or outsourcers.
- Develop and monitor security metrics that can demonstrate progress in achieving security, risk and compliance goals.

ITxpo Sponsors for the Security & Risk Management Symposium Community



Official Sponsor of the Security & Risk Management Symposium Community

Returning or Joining Security & Compliance Marketplace in 2009

Archer-Technologies
Cisco Ironport
Configuresoft
ForeScout Technologies
Fortinet
Guidance Software
Hitachi ID Systems, Inc.
ISACA
PERI Software Solutions, Inc.
Verisign
Webroot

2008 Security & Compliance Marketplace

ArcSight
Dell MessageOne
Enterasys Networks, Inc.
IronPort Systems a business unit of Cisco
IT Governance Institute
Planview

Symposium/ITxpo Security & Risk Management Analyst Community

Larry E. Jr. Bradley Associate Director Consulting
F. Christian Byrnes Managing VP
French Caldwell Research VP
Joseph Feiman VP & Gartner Fellow
Arabella Hallawell Research VP
Neil MacDonald VP & Gartner Fellow

John P Morency Research Director
John Pescatore VP Distinguished Analyst
Paul E. Proctor VP Distinguished Analyst
Tom Scholtz Research VP
Ray Wagner Managing VP