



Security & Risk Management
Symposium Community

Trip Report

Security & Risk Management Gartner Symposium/ITxpo

Key Takeaways

This year's Gartner Symposium/ITxpo in Orlando, Florida, focused on the theme of "Driving IT. Powering Business." Most of the attendees seemed to be acutely interested in that issue — how to using technology to deliver business value — and the 308 members of the Security & Risk Management Community were definitely no exception.

There was plenty of interest in technology, of course, as you'd expect at the world's premiere IT event. We heard lots of questions and comments about emerging technologies and vendor and service provider selection. Among the solutions the attendees were most interested in were tools for network access control (NAC), security incident and event monitoring (SIEM), identity and access management and "malware" filtering.

But we saw more interest than ever before in broad, strategic issues, ranging from the impact of data breaches — clearly a problem that isn't going away — to the need to secure intellectual property and meet regulatory compliance requirements. Security and risk management are certainly maturing, both as professional disciplines and as enterprise concerns, but there's still a very long way to go. That's why so many Security & Risk Management Community attendees were seeking guidance in assessing and improving their security maturity. And it's also why Gartner has developed a brand-new interactive diagnostic tool — designed to help security and risk professionals overcome the initial obstacles to advancing security maturity.

Security and risk management continue to rise in the enterprise consciousness. The focus is plainly now much more on business-oriented risk and risk management — especially in relation to enterprisewide operational, financial and regulatory risk — than on traditional IT security. It's all about the business now, and the key takeaways that Gartner's security and risk management identified at this event all reflect that reality:

- Security and risk management professionals must view themselves — and work to be viewed as — business leaders, not simply as technology specialists.
- A strategic, business-aligned approach to risk — both assessment and management — is now far more important to businesses than the traditional and largely tactical focus on information security.
- The need to build greater security awareness — across the entire enterprise, and at all levels — is critical, and requires stronger business leadership and communications skills.

Conference Highlights

In his keynote address, Vice President and Gartner Fellow Neil MacDonald drove home the point that security and risk professionals must move beyond their traditional, "technocentric" — and highly risk-averse — role, to ask themselves what the business needs. "As IT professionals," he said, "our job is to understand the risk related to the use of information technology. We must communicate that risk so the business can make an educated and informed decision whether that risk is acceptable. It is not IT's job to say no."

Many of the best-attended and best-received presentations and workshops at Symposium/ITxpo focused explicitly on the crucial relationship between IT security and risk and business value. They included:

"Fifteen Ways to Spend Less and Get More Secure"

Most enterprises spend between 5% and 12% of their total IT budgets on security — but that spending doesn't guarantee that their critical data and operations are secure. Gartner actually recommends a much lower guideline for security spending: 3% to 6% of the IT budget. Neil MacDonald and Vice President and Distinguished Analyst John Pescatore recommended ways to make the most of your security "spend," including:

- Using free security features included in hardware from Intel and AMD and operating system (OS) and other software from Microsoft.
- Architecting to enable outsourcing — or replacement — of routine security processes.
- Limiting and standardizing remote-connectivity options.



“The Top 10 Audit Findings You Want to Avoid and Six Hot Technologies That Can Help”

A risk and security audit can waste time and valuable enterprise resources, especially if findings are inappropriate. Chief information security officers (CISOs) and other risk professionals should be prepared to negotiate with auditors, to ensure that audit findings address areas of genuine concern and value to the enterprise. While technology is not the answer — a broad range of innovative technologies can help. These technologies include:

- Identity and access management (IAM) tools to identify and control who has access to what systems and resources
- Change and configuration management and auditing technologies to address inadequate controls of system-level and privileged-user access
- Automated tools — including log centralization and analysis, security incident and event monitoring and forensics applications — to deal with the “hot button” issue of user activity tracking and analysis

“Security, Risk and Compliance Scenario: Fighting New Threats, Enabling New Business”

Enterprises are becoming dangerously complacent about security and its impact on critical business operations. The reality is that the damage from security vulnerabilities, and from threats such as identity theft and “phishing” is quietly increasing. In this deceptively low-key threat environment, John Pescatore says, enterprises must:

- Shift from a reactive approach to a mix of strategic planning and rapid tactical execution
- Ensure that compliance-driven security spending focuses first on protecting business and customer data
- Demand that all software — whether purchased “off-the-shelf,” developed in-house or offered by an external service provider — be free of all known vulnerabilities before implementation

“Assessing Your Information Security Maturity”

The security landscape has changed dramatically. For the first time in 20 years, Gartner research shows that the majority of enterprises have reached maturity level 3 (corrective). But that level is now the standard of due care, and enterprises cannot afford to be complacent. In this presentation, Managing Vice President Christian Byrnes recommended ways that chief information security officers (CISOs) can assess their security maturity, including:

- Developing a security process portfolio
- Measuring process maturity using a Capability Maturity Model Integrated- (CMMI-)type index
- Measuring and reporting program maturity

“Selecting the Right Governance, Risk and Compliance Solutions”

Moving from manual processes to automated systems controls can reduce the complexity and cost of governance, risk and compliance (GRC). French Caldwell, a Gartner Research Vice President, offered best practices for selecting the GRC technologies that deliver the greatest value, including:

- Conducting an enterprisewide risk assessment before choosing a GRC solution
- Ensuring that the IT components of the solution are aligned with the enterprise’s business needs
- Investing in a complete solution, not just technology

“How to Securely Implement Virtualization”

Virtualization — one of the hottest topics at Symposium/ITxpo — offers enterprises many potential benefits, including performance improvements and total cost of ownership (TCO) reductions. But Gartner estimates that through 2009, most virtual machines will be less secure than their physical counterparts. In this presentation, Neil MacDonald showed practical ways of addressing these risks, such as:

- Investing part of the TCO savings from virtualization in security
- Pressuring security and virtualization providers to fix the major identified vulnerabilities
- Not combining trusted and untrusted workloads with demilitarized zone (DMZ) virtualization

What People Asked About

“How can I communicate better — especially with senior management — about highly technical issues?”

One attendee asked, “How can I distill a complex, fast-changing threat environment down to one PowerPoint slide that my CEO will actually look at?” There’s no simple answer, but the first step is to speak the CEO’s language: use standard business language instead of IT jargon and talk about business needs instead of technical requirements.

“Which security certifications — for example, SANS Institute or Certified Information Systems Security Professional (CISSP) — are the most appropriate for my needs?”

It’s encouraging that security expertise is increasingly being formalized, so that enterprises can find the specific skill sets they need. But there’s no substitute for an established track record of dealing with a broad range of projects and initiatives. Managing Vice President Ray Wagner got a big laugh when he told a presentation that the most important certification of all is what he called “EXP”: experience.

“How do I meet my enterprise’s security needs in the face of limited resources and constantly shifting priorities?”

This was one of the most important issues at this event: how to do more — and more types of activities — with less. One important first step is to “routinize” many of low-level operational functions that security has traditionally performed, for example, getting application development teams to use vulnerability assessments tools as a standard part of their processes. This reduces overall costs, and offers the additional benefit of shifting some of the cost to other organizations’ budgets.

Things to Watch For

The overarching message of this Symposium/ITxpo’s Community events is certainly the need to approach security and risk management as a strategic business role, not simply as technical function. Security is still where the majority of the work is being done, but enterprises increasingly recognize that risk assessment and management is where the work needs to be done. That’s a message that’s finally moving beyond the large enterprises that have already established significant risk-related roles and organizations, and becoming entrenched even in small and midsize businesses (SMBs).

It all comes down to empowering the security and risk management professional — and the security- and risk-related organizations — within the enterprise. Simple, actionable recommendations that can help achieve that goal include:

- Power the business: Adjust project processes to optimize business trade-offs and flexibility, not just process consistency.
- Power the organization: Consider ways to expand your scope outside the IT organization, whether “virtually” or directly, personally or organizationally.
- Use “power tools”: Match the technologies you use to your current level of security maturity — because too much sophistication and complexity can be self-defeating.
- Power yourself: Design your own career path, by building your competencies in risk management and business execution and developing your organizational influence and credibility.

ITxpo Sponsors for the Security & Risk Management Symposium Community



AT&T
Autonomy
CA
Cisco
Dell
Fast
HP
IBM
Intel
LANDesk
Microsoft
NEC
Novell
Romania IT
Sterling Commerce
Symantec
Endeca
Vanco
Verizon Business

Security & Compliance Marketplace

APANI Networks
Configuresoft
Enterasys Secure Networks
ForeScout Technologies
Intelligent Wave USA
IronPort Systems, Inc.
IT Governance Institute
LogLogic
M-Tech Information Technology, Inc.
Oakley Networks
Trend Micro, Inc.
Verisign (Marketplace Sponsor)
Vormetric