



Security & Risk Management
Symposium Community

Trip Report

Security & Risk Management
Symposium Community

Members: 137

Key Takeaways

Perhaps the single biggest takeaway from the conference was that security and risk managers are expected to play many roles nowadays. Attendees showed great interest in strategic issues, such as business-oriented risk and risk management, especially as it relates to enterprise-wide operational, financial and regulatory risks, as opposed to traditional IT security. Other prominent issues included:

- Ongoing concerns within the security and risk community, including dealing with data breaches and securing intellectual property.
- The security challenges presented by new technologies. For example, Web 2.0 enables amazing productivity gains, but it also creates issues in terms of security and intellectual property rights.
- The impact of hardware-to-operating system virtualization. During the next decade, virtualization will create a new platform in the form of the virtual machine monitor (VMM) and hypervisor that will allow IT departments to radically change how they approach the security and management of server and desktop workloads.

Conference Highlights

The following were some of the key presentations in Las Vegas:

Measuring Risk Posture With Process Maturity

The leader of this workshop asked attendees how many of them had responsibilities for multiple areas within their organizations. The responses were:

- Security: 90%
- Risk management: 90%
- Compliance: 90%
- Privacy: 70%
- Business continuity: 50%

For security and risk professionals, their areas of responsibility are often mixed. Interest in this session showed that many in the field still seek guidance in assessing their organization's maturity when it comes to handling security threats. Using Gartner's interactive assessment tool (which is available to Gartner for IT Leaders subscribers in Security & Risk Management), workshop participants gained a better understanding of their organizations' security and risk maturity levels.

Security in the Age of Web 2.0

Web 2.0 offers a collection of lightweight technologies and techniques that simplify development of sophisticated code and content. Yet ease of use and user-friendliness will come at a price, namely the lack of security and neglect for protection of intellectual property. Web 2.0 empowers individuals, but it also increases their destructive power. The same characteristics that enable creativity, productivity and collaboration make Web 2.0 ecosystems prone to successful attacks and theft. CIOs, chief security officers (CSOs), senior architects and directors of application must accept that they are in a Web 2.0 world, and should:

- Extend enterprise practices on the assumption that their Web-enabled content and software will be used in unexpected ways, abused, stolen and attacked by outsiders and insiders.
- Apply application security along the entire software life cycle, considering the current status of technologies practically applicable to each software life cycle phase.
- Begin to build security into applications and buy software with security built-in.

Radically Transforming Security in a Virtualized World

Virtualization provides the foundation for a new approach to security and management that will transform how organizations secure and manage IT workloads during the next decade. This will dramatically reduce costs and increase infrastructure's ability to adapt to changing business requirements. Once virtualized infrastructure is in place, organizations can begin to do new and interesting things in terms of security and management. CIOs, CISOs, security architects and operations managers need to:

- Get involved in operations-led virtualization projects and ensure they are implemented securely.
- Make security a mandatory part of the evaluation of virtualization solutions.
- Lab-test new approaches to security and management using virtual machine (VM) state inspection and security products that support the model.
- Exploit the new control points for security and management that virtualization provides — in hardware, in the hypervisor and in the VMM.

Security, Risk and Compliance: Fighting New Threats, Enabling New Business

Every day, new vulnerabilities are reported, but vendors patch most security holes before an actual attack occurs. The biggest risk to enterprises comes from targeted attacks, many from insiders. In addition, phishing and identity theft attacks have caused the rise of “credentialed” attacks. As attackers increasingly move “up the stack” to applications and users, signature-based solutions are increasingly ineffective, and hard-coded security policy — whether in the form of antivirus agents or application authorization — is an inhibitor to IT agility. CIOs, enterprise architects and client computing managers should:

- Change the way IT systems and services are procured to require security be “baked in” from the beginning.
- Adopt a process approach to security.
- Change development processes to test applications for security vulnerabilities during the development process.

Identity-Aware Networks: Which Approach, if Any, Is Right for You?

Today's businesses must open their networks to business partners, contractors and guests. Their access needs to be regulated. Vendors offer multiple options for integrating identity and access management with network access control policies, including deep packet inspection, packet tagging, IPsec, virtual LAN “steering” and access control lists. Gartner recommends that security officers:

- Start with guest networking.
- Select an architecture that will evolve to a full-blown identity-aware network.
- Include all network access: wired and wireless, campus LAN and remote access.

Keynotes

Welcome Address

CEOs want cost reduction, more flexibility, support for growth from the IT organization, regardless of the economy. That's why 80% of CIOs expect major changes during the next three years — 40% of CIOs expect transformational change, according to Gartner's latest CIO Survey. Expect old metrics (such as IT spending as percentage of revenue) to give way to new metrics (such as IT spending needed to gain new clients). Seventy percent of CIOs say their organizations don't have the right skills to create the needed change. Therefore:

- Focus on pivotal roles and competencies
- Capitalize on talent globally
- Make IT attractive to digital natives

Analyst Keynote: Technology-Enabled Business Acceleration

Be counter-intuitive — while cutting costs, have other staff prepare for the return to growth. If you wait until the recession ends, you'll lose months of opportunity. Schedule meetings with business executives to go over the project portfolio and decide what to keep and what to cut. Web 2.0 enables amazing productivity. Plenty of Fish, a dating site, has 2.5 million users per month, generates \$10 million a year in revenue, and is run by one full-time and one half-time worker. You need to figure out how to employ IT resources for competitive advantage. For example, a context-aware network would know where you are, what you're doing and what you need. You also need to provide mass-produced, repeatable services, not technology, to the business by:

- Developing a usage measure like the kilowatt-hour.
- Changing the IT workforce from caretakers to service managers.

CIOs and other leaders need superlative communication and an ability to influence throughout the enterprise.

Keynote Panel: A Look Into the Labs

Gartner analysts interviewed four research leaders from major IT vendors:

- Rich Friedrich, HP Labs
- David Douglas, Sun Labs
- Guido Jouret, Cisco Emerging Technologies Group
- Steve Hoover, Xerox Labs

What are you working on now?

Friedrich said consumerization is the next big thing for HP — figuring out how enterprises can integrate consumer devices and technologies for business purposes. This includes location-based and context-sensitive services. Jouret said that Cisco is working on technology for distance collaboration that includes things like connected whiteboards that allow two engineers to work on the same drawing simultaneously. Also, Cisco is working on a “HealthPresence Pod,” a kiosk with connectors for medical equipment, such as a stethoscope or blood pressure cuff, that allow doctors to examine patients over distances. He said enterprises need to ask themselves, “Where do you collaborate?” to make the most of this kind of technology.

What technologies outside your own labs impress you?

Jouret: Advances in the automation of programming. Neural network models may help develop more sophisticated applications.

What is most important to drive innovation?

Strong enterprise leadership with vision, good communication and networking inside the enterprise. Hoover said: “Above all, know your customers.”

What People Asked About

What is an appropriate level of security?

A level of security that is aligned to business needs, agreed to and signed off by the business.

How can I address specific audit findings?

Negotiate with your auditors to arrive at resolutions that address the auditors’ requirements and provide value to the enterprise by addressing reasonably anticipated risk.

How can I build a risk and security program?

Develop and formalize a process catalog that is repeatable, measurable, and provides an appropriate level of protection. Subscribers to Gartner for IT Leaders can use an interactive tool to assess their enterprises’ levels of security and risk maturity.

Are virtualized environments inherently less secure than physical environments?

Security can be weakened by a rush to virtualize. Although virtualization offers opportunities to reduce cost and increase agility, these benefits won’t occur unless the enterprise first implements best practices for security. Security must be “baked in” from conception, not addressed later. The costs of implementing best practices can be significant, and such costs — or the possible costs of avoiding them — must be included in any analysis of the projected cost savings of virtualization.

What are some of the differences in securing virtualized environments I should be concerned about?

Many organizations mistakenly assume that their approach for securing VMs will be the same as securing any operating system and plan to apply their existing configuration guidelines and standards. However, simply applying the technologies and best practices for securing physical servers won’t provide sufficient protection for VMs.

What are best practices for beginning a network access control project?

Most organizations say that they are starting with guest networking. When guests access the network, they are only granted Internet access; they cannot get to sensitive data and applications on the corporate network. The next step would be to turn attention to your managed machines on the internal network. The best practice there is to monitor endpoints for compliance (for most organizations, compliance means up-to-date patches, current antivirus signatures and running a personal firewall on the machine). Quarantining endpoints is not common at this point; it’s more common for organizations to issue warnings to noncompliant systems. If you do need to quarantine noncompliant devices, ensure that you have an automated system for remediation.

Things to Watch For

More and more, security and risk management professionals are expected to be not just technology experts but business leaders as well. Those who embrace this new, more business-oriented role will be the people who thrive in the future. Business skills — in particular communications skills — will be one of the greatest future differentiators between those who succeed in the field and those who do not.

Taking an approach to risk that aligns with enterprise business goals is now more important than a tactical focus on information security. Most work continues to be done in security, but enterprises need to place more emphasis and spend more resources on risk assessment and management. Smaller and midsize businesses seem to have joined larger enterprises in beefing up their ability to deal with risk by establishing appropriate roles and responsibilities.

Security and risk professionals must move beyond their traditional technocentric and risk-averse mentality and come to grips with what the business’s priorities are. The IT professional’s job is to understand the risk related to the use of IT and to communicate that risk in a way that helps the business make informed decisions about whether that risk is acceptable. Gartner expects this trend to continue and accelerate, and security and risk professionals ignore it at their peril.

Interactive Polling Results

A number of sessions polled attendees about hot topics.

I am confident that we have successfully designed our roles, workforce competencies and skills to support the future state.

Strongly Disagree — 35%
Somewhat Disagree — 35%
Somewhat Agree — 29%
Strongly Agree — 1%

My company is well-positioned to anticipate and manage the changes that business transformation introduces:

Strongly Disagree — 23%
Somewhat Disagree — 42%
Somewhat Agree — 30%
Strongly Agree — 5%

Does your organization ban access to social sites like Facebook?

Yes — 25%
No — 68%
Don't Know — 7%

ITxpo Sponsors for the Security & Risk Management Symposium Community



Quest Software

Security & Compliance Marketplace

Fiberlink
IronPort, A Cisco Business Unit
TrendMicro, Inc.

