Gartner Information Security Summit 2009

21 – 22 September 2009 | London, UK

Celebrating its tenth anniversary in Europe, the Gartner Information Security Summit brought together over 370 attendees to learn from and network with a range of end users giving case studies, key solution providers on the showfloor and in sessions, and with the Gartner analyst community. Led by the Summit Chairs, Jay Heiser and Tom Scholtz the Summit took in over 60 presentations, roundtables and workshops furnishing attendees with the latest thinking on their strategy, tactical approaches, and key needs for 2009-2010.

THE AUDIENCE

The Summit attracted over 370 attendees, from 37 countries including 24 European nations represented. The core of the audience was naturally from the UK, with the next highest groupings coming from Scandinavia, Benelux, then Germany, Austria and Switzerland. In terms of industries represented the key sectors were government and public sector, financial services and manufacturing with a range of other sectors then present.

Audience seniority increased in 2009 as organizations continued to send representatives in order to gather key learning for the office, whilst not being able to send their teams — instead the team leaders and directors were the individuals present. The best represented job titles continued to be Director / Manager of Information Security / Security and variations there of with a presence from Risk, Compliance, and Business Continuity focused individuals.

Keynote Key Learning

Gartner Opening Strategy Keynote for 2009: Your Role in Information Security

Christian Byrnes

There is a story that says that to boil a frog you should place it in cool water and slowly apply heat. The frog will sit calmly in the water to the end, failing to detect the change. Many security practitioners may be sitting in tepid water already. Change happens.

The existence of security technology sufficient to protect normal IT installations is irrefutable. While rare, there are organizations that have succeeded consistently. New business uses of technology will continue to require some level of innovation in security, but for the most part we are entering a period of integration, consolidation and automation of security technology. And even those new uses may have less impact on our ability to secure IT — many of the vendor acquisitions of security companies are being done by infrastructure companies or service providers. It is reasonable to anticipate some lessening of new vulnerabilities in new product implementations over the next seven to ten years. Both IT and security have begun the climb toward their next maturity plateau and the time for security practitioners to do some career planning is now!

If this is so, then what job will the security practitioner be doing in ten years? Demand for deep technical skills will be reduced. More surface skill levels can be provided by least cost countries. We expect demand for specialized security architects to peak around 2016, then decline as mature security knowledge becomes part of normal architecture parlance. The one skill set that will continue to be in high (and ever higher) demand is that of the security interface to the business; the risk assessor, strategic planner and executive communicator. Governance, strategy, policy and assessment become the core of what was once a firewall and anti-virus technology domain.

Change happens.

Gartner Closing Thought Leader Keynote for 2009: The Future of Information Security

Jay Heiser

Contrary to some strains of modern philosophical thinking, the future looks a lot like the past and looking back is a good way of steering forward.

Ever since the founding of 'information' by what were the equivalent of accountants 8000 plus years ago, the focus has been on ensuring its integrity and accuracy — the modern day focus on confidentiality has a relatively short history…That perhaps distracts from the more fundamental requirement for the information security profession to help identify the best-fit security approach for the most appropriate information.

Restricting the reproduction and copying of information is no longer a simple task. But rather than trying to restrict its movement instead look to the positive advantages derived from community review, from the addition of addenda and development of that information, and on improved access to the relevant knowledge. Having finally, after 400 years, settled the debates around IP ownership sparked by Gutenberg, the Internet has blown the debate wide open again and its up to you to identify opportunities as opposed to focusing all energies on holding back the tide. Remember that History tells us we can't identify attacks we don't yet know exist — but neither should energy be devoted to plugging every vulnerability created by the scale and complexity of modern communications. Balancing security with commercial logic is at the heart of our role.

As information security professionals we are building on the legacy of the past. The last 8000 years demonstrate control of information flexing and changing and once again we are in a time where that balance is altering. The history of passports — ever since Nehemiah received a letter of safe conduct from the King of Israel — demonstrates technology and approaches being bypassed and superseded. You can expect your present ways of working to cave in and evolve to meet the results of innovation. Don't fight it; look to the past and learn to survive it.

Findings from The Gartner European Information Security Summit

Secure Remote Access for Non-Securable People

John Girard

Anyone who works remotely is in essence "unsecurable" and it's more constructive for IT planners to spend less time believing that they can "fix" remote access security. It is more productive to rationally examine why remote users and their work situations become unsecurable, then to take steps to minimize the risks of loss and exposure that fit each user's circumstances.

Articulating the Business Value of Information Security

Tom Scholtz

Credibility is a key pre-requisite for the ability to effectively communicate the business value of security investments to executives. You could have an excellent justification, but if the executives don't trust you, they will treat all your requests with suspicion. One important means of fostering credibility is to provide honest feedback on the results of security projects. No executive expects IT projects to be 100% successful, and pretending otherwise destroys your credibility.

The Elements of an Effective Identity and Access Management Program

Ant Allan

Key takeaway: Engagement and active involvement of non-infosec, non-IT stakeholders increasingly recognized as critical to the success of an IAM program

Key action point: *Develop* a compelling vision for IAM, aligned with business imperatives, that can be clearly articulated to a broad range of stakeholders

DLP MQ, The Content Aware Enterprise

Paul Proctor

Data loss prevention is the dynamic enforcement of policy based on the presence of sensitive content. Do not rely on the vendors to define your sensitive content. Do the work up front to define data types, use cases, and policy enforcement actions before you talk to vendors and you will substantially raise your prospects for selecting the most appropriate product and completing a successful implementation.

Linking Risk and Security to Corporate Performance

Paul Proctor

Organizations remain challenged to link risk and security to the business. Follow this five tips to improve budget justification and business appreciation for risk and security.

- **Tip No. 1:** Formalize a risk and security program.
- **Tip No. 2:** Map Key Risk Indicators (KRIs) to Key Performance Indicators (KPIs).
- **Tip No. 3:** Link risk initiatives to corporate goals.
- **Tip No. 4:** Don't use operational metrics in executive communication.
- **Tip No. 5:** Communicate to executives, emphasizing what works and what doesn't.

Gartner
Information Security Summit 2009

21–22 September | London

Exclusive offer for attendees of the Information Security Summit for Gartner Symposium/ITxpo this November

Or why not pass this along to a colleague to take advantage of?

Gartner Symposium/ITxpo, 2-5 November in Cannes is the industry's largest and most important gathering of CIOs and their senior IT leaders. Specifically designed to deliver the insights, tools and relationships you'll need to get through what may be the toughest year of your career. We'll have a laser focus on how all facets of business technology, across every IT leadership role in the organization, can help you balance cost optimization, risk mitigation and a return to growth.

We've organized the Symposium tracks according to 9 leadership roles plus highlighted what are going to be the hottest topics and core business objectives you can't avoid. Each role-based track includes dozens of targeted sessions, vendor insights and networking opportunities you need to transform your organization's IT strategies.

Symposium/ITxpo: The most effective use of your time to save your organisation money. A small investment for a large return.

Register today **with code MP-ESC19 to take advantage of a €500 discount off the standard delegate rate. Visit: gartner.com/eu/symposium to register, view the full agenda and for more information.**

gartner.com/eu/symposium