Gartner **Security & Risk Management** Summit 2012

19 - 20 September | London, UK
gartner.com/eu/security

TRIP REPORT

Strategic Roadmaps to Secure the Enterprise and Reduce Risk

SUMMIT CHAIRS' MESSAGE FOR ATTENDEES

Strategic Roadmaps to Secure the Enterprise and Manage Risk. This theme attracted hundreds of participants from all over Europe. Never have I seen an audience that was so involved and who were sitting on the edge of their seats. **Remember Nisha Pillai? "Be emphatic", "Focus on benefits (not features)", and "Big up your body language" - these were her key messages**. Being in the spotlight was hard for those who prefer to pull strings in the background, but change is inevitable – **as we learned in the Gartner keynote**. Making your information security strategy heard by the organization's executive board, and explaining your risk management roadmap to thousands of employees requires a new type of leader. **Lawrence Leyton, our motivational and inspirational illusionist, helped with such behavioral change**. Attendees of this event proved that they are ready.

They also showed that they are willing to work their way through the weeds, attending presentation after presentation, debating with peers in roundtables, challenging analysts in one-on-ones, and seeking out vendor updates on the show floor. Having a vision in place and following a plan to implement it – our security and risk leaders were eager to do both. Thank you everybody, presenters, exhibitors and attendees, for making this event a success.

Carsten Casper
Research VP,
Gartner

Karthik Cariappa
Senior Program
Manager,
Gartner Events

THE AUDIENCE

The Summit attracted over 450 attendees, from 30 countries including 19 European nations represented. The core of the audience was naturally from the UK, with the next highest groupings coming from Germany, Austria and Switzerland followed by Benelux, Nordic, France and the Middle East. 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. 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 Security Architects.

In 2012 the Summit brought together over 450 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 Chair, Carsten Casper the Summit took in over 40 presentations, roundtables and workshops furnishing attendees with the latest thinking on their strategy, tactical approaches, and key needs for 2012-13.

> ***Very interesting conferences showing us how to develop and increase security in the company and to have a good view of evolution of technologies.***
> Directeur Technique, Imsnetwords

PLAN AHEAD FOR 2013

Gartner Security & Risk Management Summit 2013
18 - 20 September
London, UK

KEYNOTE KEY MESSAGE

GUEST KEYNOTE:

THE WINNING MINDSET: SELF-MOTIVATION, INFLUENCE AND BEING FEARLESS!

The brave will die – The cautious never live!

'Fear of Failure', makes people scared to even try new things just in case they fail, so they don't even bother to try as failure for them = pain. So they move away from the possible pain of failure. It's time to be brave and you will achieve your goals…

Be Careful what you say to yourself!

So many times our own self-destructive internal dialogue can literally talk ourselves into negatives states of mind, so be careful what you say to yourself. Remember we are actually in control of all of this self-talk and therefore we have the ability to change it. Become aware of it so that you can change it to something that is useful.

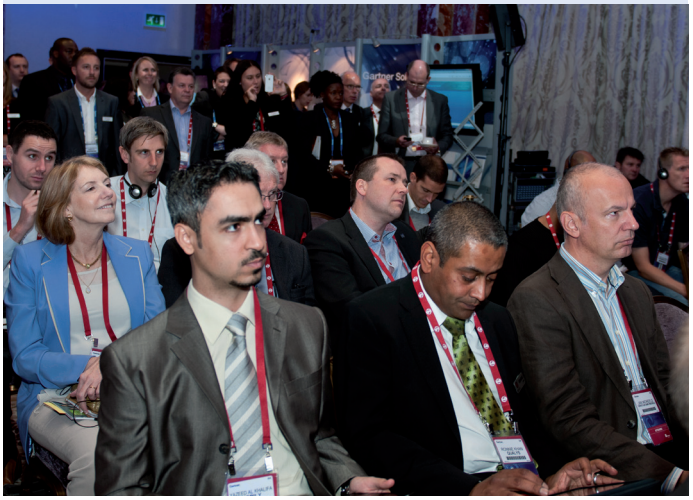
Focus on what you want rather than what you don't want!

If I say don't think of an elephant, what do you do? The mind can't process negatives, so if you focus on the wrong things then you end up with them! I don't want to fail - you end up focusing on failure!

So remember to focus on what you want rather than what you don't want.

Go to the mind movies!

Your mind movies that you play in your head control how you feel. Once you understand that you control that then you can learn to play different movies inside your head and ultimately change the way you feel. So go to the mind movies and make sure you chose a good movie!



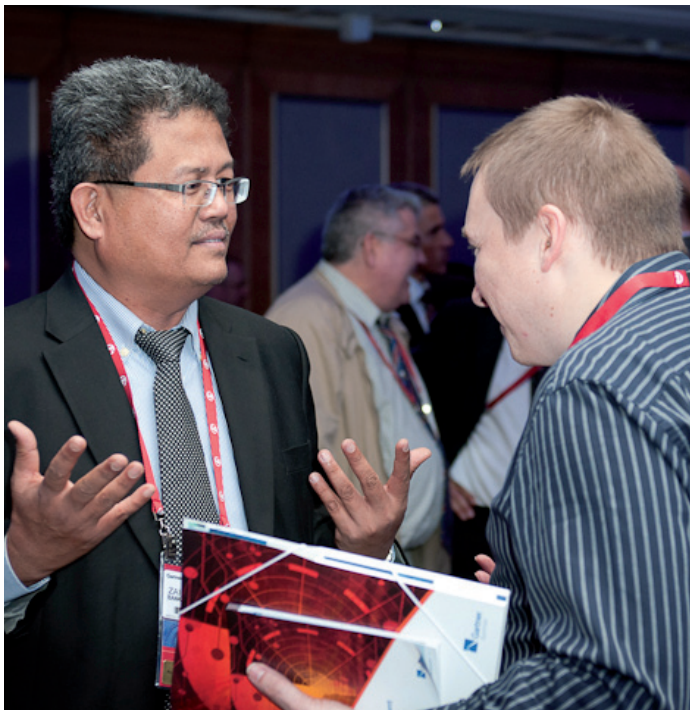
Getting Your Message Across
Nisha Pillai, BBC World News Anchor

In her keynote 'Getting Your Message Across', former BBC World new presenter, Nisha Pillai shared three simple but effective tips to aid effective communication, and above all boost personal authority.

With the aid of videos and on-the-spot exercises the audience was encouraged to:

- Be emphatic – in the style of Steve Jobs
- Focus on impact, not features – in the style of CISCO boss, John Chambers, and
- Boost their presence – in the style of Steve Ballmer.

It was a hugely interactive keynote which saw all the conference delegates up on their feet and COMMUNICATING in a matter of minutes. There were lots of laughs and lots of learning too.



Road Stories: Lessons Learned (and Fingers Burned) in IT Risk Management Practice.

Tom Scholtz, VP Distinguished Analyst

- Risk management is more an art than a science. An individual's experiences, values and goals have a significant impact on the way he or she interprets and accepts different risks. Risk appetite is a personality trait that differs widely between people.
- The best way to learn risk management is to practice it. And the risk management approach must suit the culture of the organization. Focus on continuous improvement in risk management practice, gained through experience.
- The term "risk manager" is arguably a misnomer. Risk managers usually fulfill more of an advisory function.

Road Maps to the Next Generation of Firewalls and IPS

Dionisio Zumerle, Principal Research Analyst

Recommendations:-

Advances in infrastructure protection technology continue to be primarily reactive to keep pace with new threats. New threats bring newer features into existing safeguards, rather than many new protection technologies.

An NGFW is a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks. A next-generation IPS indicates the necessary evolution of network IPS to deal with changes in both the way business processes use IT and the ways attacks try to compromise business systems.

Changing threat conditions and changing business and IT processes will drive network security managers to look for NGFW capabilities at their refresh cycle. The key for NGFW vendors will be to demonstrate first-generation firewall and IPS features while including NGFW capabilities.

What the new EU privacy legislation means for your organization

Carsten Casper, Research VP

Our analyst user roundtable on privacy in Europe was „sold out". Discussion topics in the group reflected the discussions that Gartner had with European clients in 2012. First, is the new EU data protection regulation a course correction or a tide change? Either way, attendees agreed that having a privacy management program in place is the best preparation for any new legislation, whether it hits us in 2015 like this new regulation or now in 2012 like the infamous EU cookie rules - which was the second major topic of the day. In addition to the UK, now also the Netherlands are getting more active with the enforcement of these rules that are unclear and burdensome for most, with little value for the consumer. Know what sort of cookie your sites use, and document well, but don't panic, was the agreed opinion of the group. Pay attention to tracking techniques in general, not cookies in particular, if you want to display a good approach to privacy.

How to Run, Grow and Transform Your Security Program

Paul Proctor, VP Distinguished Analyst

Recommendations:-

There is no such thing as perfect protection, but boards of directors and senior executives expect defensible assurances that their information and business operations are sufficiently protected. The answer lies in a set of risk control programs that are proactive, transparent, risk-based, measurable and process-oriented. Creating and formalizing these programs are relatively inexpensive, but developing mature programs requires high-level support, a strategic approach and adequate time to execute. Modern enterprises must also transform their programs to align with business need and address evolving cultural gaps between IT and the business.

Security and risk management is ready to mature and become a responsible and critical part of the business. Board members and executives are asking for more detailed reports on security and risk management. The business — not IT — is taking the lead on some roles, such as business continuity management (BCM), governance and policy. Business and IT leaders need to think about security and risk management investments in new ways.

- **Run:** Establish and run your risk program. This category represents the activities and investments directed toward the maintenance and operation of the current program, exclusive of IT operational elements. This would include program management, strategy, budgeting, process catalog, metrics and dashboards, policies, compliance, and oversight.
- **Grow:** Mature your program. This category represents the activities and investments directed toward assessing and maturing the program. This would include program maturity assessments, the identification of gaps and opportunities for improvement, and all subsequent activities and projects to address remediation and improvement.

- **Transform:** Integrate with the business and address evolving cultural gaps. This category represents the activities and investments directed toward optimizing the program and aligning with business need. This would include key risk indicator (KRI)/key performance indicator (KPI) mapping, Risk-Adjusted Value Management, behavior-driven security and other advanced activities.

Gartner for Technical Professionals —To the Point: Security Monitoring for the Cloud and in the Cloud

Trent Henry, Research VP

Recommendations:-

Moving sensitive resources to the public cloud brings new risks, and an important compensating control is improved monitoring. Cloud service providers will not provide this capability with ease; it's up to enterprises to choose and implement the proper architecture and solutions. Most organizations should plan for more monitoring than they do with traditional on-premises IT. How should they tackle it?

- If an organization's existing monitoring program and tools are mature, and they are engaged in small or gradual cloud deployment activities, then they should use existing on-premises monitoring systems to watch cloud systems, logs and events.
- If an organization does limited in-house monitoring or has outsourced it, and they anticipate a small cloud deployment, they should use a managed security service provider (MSSP) for cloud monitoring.
- If an organization has a large cloud deployment but little on-premises infrastructure, they should use specialized software-as-a-service (SaaS) cloud monitoring solutions.

Five Things You Always Wanted to Know About Authentication but Were Afraid to Ask

Ant Allan, Research VP

Investment in authorization, auditing and analytics has limited or no value without reliable authentication. Reliable authentication is undermined by firmly held but wrong assumptions or "myths" about the role of authentication and how it works. Authentication only corroborates users' claimed digital identities, so ensure that IAM processes address real-world identity proofing for new users. While passwords remain ubiquitous, enterprises must implement a password policy that balances risk, compliance and usability needs.

When choosing new authentication methods, first, carefully evaluate the authentication strength — don't just count authentication factors! – and, second, be sure to balance this against user experience, total cost of ownership and other needs and restrictions. Consider how contextual information can reinforce "traditional" authentication methods and evaluate vendors that can support this approach.

Securing the Access Layer: Identifying the Right Authentication Strategy for BYOD, Contractors, Guests and Employees

Timothy Zimmerman, Research VP

Recommendations:-

- Document the usage scenarios of who will access the network, what devices that will be allowed to use and how they will interact with the network and enterprise applications.
- Categorize the scenarios into trusted scenarios that will be embraced by the organization and therefore be able to access behind the firewall and untrusted scenarios that will be controlled but have limited access in a number of different ways depending on the organization and their risk posture. There may be a number that you will define as "blocked" due to compliance or internal policy.
- Define the device authentication policy based on the usage scenarios and the access methods defined in this step by step workshop.
- Implement device authentication, user authorization and policy enforcement and data security as separate systems/steps in the larger access control framework.

Security Considerations for Client Virtualization

Mario De boer

Recommendations:-

- Establish an overarching fraud management framework for your organization that includes multiple layers.
  - The layers of defense can be built over time, based on priorities and the complexity inherent to various implementations.
- Deploy Layer 1 endpoint-centric and Layer 2 navigation-centric solutions to start with.
  - These can be implemented relatively quickly and provide a good first layer of defense against malware-based attacks.
- Integrate mobile applications into your fraud management framework, to ensure a cohesive strategy, and shared user and account profiles.

- Recognize that the threat landscape can quickly change, pointing to the need for a layered approach and comprehensive framework.
- Make sure your business processes and organization are properly structured to effectively manage fraud prevention systems
  - Otherwise, important alarms and alerts will be ignored.

Crisis/Incident Management Overview

Roberta Witty

Key Findings

- Not every incident or business disruption turns into a crisis for the organization. However, every event must be managed by the organization to ensure that appropriate steps are taken throughout its life cycle to reduce the impact of the event, remove/eliminate the threat causing the event, or move to a higher level of management intervention and involvement.
- An incident will typically be managed by someone with day-to-day operational responsibility until it needs to be escalated to the crisis/incident management team.
- An incident that does turn into an organizational crisis is defined as any situation that threatens or is perceived to threaten the organization workforce's life, safety and livelihood, business operations, intellectual property, IT, or physical or virtual assets, resulting in serious interruption of business operations, damage to reputation and brand, direct financial loss, or negative impact to share value.
- A number of variables can cause a crisis to get out of control very quickly.
- Crises can be grouped into two categories: direct and indirect. A crisis/incident management program needs to address both types.
- A well-crafted crisis/incident management program has six key components.
- Addressing the expectations of all stakeholders of the organization is vital for effective management of and communications during the event.
- Crisis communications procedures, including well-crafted messages, are vital to ensuring the organization maintains control of the situation to keep fear, uncertainty and rumors at a minimum: Once you lose credibility, the game is over.

Protecting Data in the Public Cloud: Encryption, Obfuscation or Snake Oil?

Takeaways: Encryption fits only narrow data protection use cases, even more so in the public cloud. Whether or not you need protection from service provider access makes all the difference in encryption effectiveness. Emerging cloud encryption technology must be heavily scrutinized, especially because standards are absent.

SPONSORS

Throughout the Summit the show floor was buzzing with activity as attendees met with solution providers to discuss the latest innovations, services and product offerings. Many thanks to our sponsors for helping make Gartner Identity & Access Management Summit 2012 an outstanding experience for everyone involved.

PREMIER SPONSORS

f5 Networks

TREND MICRO

PLATINUM SPONSORS

ActivIdentity part of HID Global

AlertEnterprise

Cyber-Ark

Dell SecureWorks

EMC²

FireEye

Fortinet

Qualys

Veracode

vmware

websense SEE MORE • SECURE MORE • DO MORE

SILVER SPONSORS

airwatch mobile device management

Bromium

Dell SonicWALL

MaaS360 by Fiberlink

FIDELIS SECURITY SYSTEMS

hp

Kaspersky Lab

LogRhythm

MetricStream

MODULO Solutions for GRC Governance, Risk and Compliance

NIIT technologies

SOPHOS

tufin

VERDASYS