Delivering on Needs of Security & Risk Management Leaders in 2017

From learning how to re-evaluate and update your security and risk strategies and investments to meeting the evolving needs of the digital organization, Gartner Security & Risk Management Summit 2017 will cover the full spectrum of IT security and risk topics. Here is a snapshot of some of the topics.

1. How can I ensure that I have the right strategy in place including talent, skills, technologies as well as the right organizational structure?
   - Cyber attacks are not new but recent activities have highlighted the need to have a robust plan in place, especially with the proliferation of Internet of Things (IoT), connected devices and organizations moving to the cloud. Cyber security is a strategic priority for Australia’s national security with the threat of cyber-attacks dramatically increasing.
   - Gartner Essentials: Top Security and Risk Predictions for 2017
   - Managing Technology Risk and Cybersecurity Through the Lens of Business Value
   - Confront the Cybersecurity Talent Shortage
   - How to Build and Operate a Modern Security Operations Center (SOC)
   - Collaborative Techniques for Building and Developing Security Staff

2. How do I assess and control the security and compliance risks inherent in public cloud environments?
   - Cloud security remains a top concern for organizations. Increasingly, all organizations are confronted with conflicting and increasing demands for the secure use of a rich set of digital services encompassing private, hybrid and public clouds. The top three cloud security challenges facing organizations are: protecting information in multi-tenant environments (controlling the provider); virtualization and private cloud security (protecting the workload) and SaaS visibility and control (protecting the data).
   - The State of Cloud Security
   - Managing Cloud Service Provider Security
   - Are They Secure? Assessing Clouds, Partners and Suppliers (End-Users Only)
   - How to Operate a Cloud Access Security Broker (CASB)
   - Effective Governance of the Public Cloud
   - CASBs, CASBs, Everywhere ... Which One Do I Need to Protect My SaaS Solutions?
   - CASB Implementation Stories

3. How do I address the skills and talent shortage in security and risk, especially given the increased focus from the business?
   - Based on the Gartner 2017 CIO Agenda survey and drilling down further, the security and risk skills group was rated as the second biggest talent gap after the information/analytics/business intelligence skills group. The unemployment rate for cybersecurity professionals is zero. Organizations continue to face skills shortages in an era where the digital ecosystem continues to bring new threats. Security and risk leaders need to look at alternatives sources.
   - Confront the Cybersecurity Talent Shortage
   - Maverick Research: Disband Your Security Team Now!
   - Five Tests That You Must Apply to Your Security Policy
   - Collaborative Techniques for Building and Developing Security Staff

4. How can I build a trusted, secure environment that facilitates digital business and agile IT, as well as more predictable and stable business processes?
   - Digital business means that organizations are more dependent on digital systems than ever. Security cannot be seen to constrain innovation or agility, even as security requirements cannot be relaxed and CISOs have less direct control. Line-of-business colleagues are not waiting for security leaders to work out the implications of technological change — they are proceeding quickly with testing new tools of digital business to support their business processes.
   - Gartner Opening Keynote: Manage Risk, Build Trust, and Embrace Change by Becoming Adaptive Everywhere
   - Gartner Essentials: Aligning Security and Risk Management With the Bimodal Enterprise
   - Managing Technology Risk and Cybersecurity Through the Lens of Business Value
   - Guest Keynote: The New Rules of Trust in the Digital Age
   - How to Get Your CEO to Embrace Digital Risk Management

© 2017 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. For more information, email info@gartner.com or visit gartner.com.
5 How do I balance technology portfolio between traditional protection technologies and emerging detection and response capabilities?

New risks will continue to arise as organizations embrace other technology areas. The Internet of Things (IoT) specifically creates a pervasive digital presence that connects organizations and society as a whole. The industrial engagement of IoT will represent new risks to human safety, requiring security and risk management leaders to identify potential injury scenarios when considering vulnerabilities and consequences.

- State of IoT and IT/OT Security, 2017
- Know the Asset, Secure the Asset: ITAM’s Role in IoT Security
- Managing the Security Risks of IoT Innovation
- Gartner Essentials: Top Cybersecurity Trends for 2017
- State of Endpoint and Mobile Security 2017: From the Fire to the Frying Pan

6 How do I tackle the complexity and challenges of controlling cybersecurity or data I do not own or control?

“By 2021, 50% of data will be outside of the physical control of enterprise IT, up from 10% today”*. In the world of digital business, every enterprise is a link in a global chain. Data flows through and is stored in locations and third parties outside of the organization’s ownership and beyond their control, requiring enterprise risk and security teams to alter their cybersecurity strategy.

- State of Data Security 2017
- Data Security Survival Guide
- Gaining Control of Unstructured Data: Lowering Costs and Reducing Risk
- Effect of Regulatory Environment on Data Security
- Magic Quadrant for Enterprise Data Loss Prevention
- There Must Be Fifty Ways to Lose Your Data

7 What new technologies should I be thinking about implementing in my security and risk management programs?

User behavior analytics are important, as is understanding adaptive security architecture and how to institutionalize it. Artificial intelligence (AI) has matured to the point where it’s capable of delivering real business value. From a security perspective, AI can deliver context-based situational intelligence to improve security decision making. Blockchain has also the potential value for security as a means of supporting more distributed trust.

- Guest Keynote: The New Rules of Trust in the Digital Age
- The State of Security Behavior Management
- Building Trust Through Authentication, Identity Proofing, Fraud Detection and Behavior Analytics
- Security Monitoring and User and Entity Behavior Analytics
- How to Deploy and Operationalize User and Entity Behavior Analytics (UEBA) Tools
- What the CISO Needs to Know About the Blockchain

8 Digital business demands dramatic new approaches to security and risk management. What are the seismic shifts that I need to be aware of?

The big one is trust first. We are finished with “default to deny;” now it’s “default to allow.” That’s a fundamental change in how we do security. Digital business is about access and collaboration. You have to let people in to participate. The next big change is the idea that the weakest link in the security chain is the end user. In a digital world, people are part of the security function and part of a people-centric solution, not the problem. The third big change is about the convergence of IT disciplines and the distribution of security responsibilities.

- Gartner Opening Keynote: Manage Risk, Build Trust, and Embrace Change by Becoming Adaptive Everywhere
- Risk and Trust Culture Are Broken — Here’s How to Fix Them
- Guest Keynote: The New Rules of Trust in the Digital Age
- Building Trust Through Authentication, Identity Proofing, Fraud Detection and Behavior Analytics
- Jump-Start Your Security Awareness Program
- Collaborative Techniques for Building and Developing Security Staff

9 What is the impact of the new EU General Data Protection Regulation (GDPR) and how to I ensure compliance?

When the EU General Data Protection Regulation (GDPR) comes into effect on 25 May 2018, a single complaint could result in an audit and a fine for improperly handling personal data unless IT leaders have adjusted their data management and backup strategies to be ready. Start modifying plans, policies, processes and technologies today.

- Data Security Survival Guide
- Effect of Regulatory Environment on Data Security
- Magic Quadrant for Enterprise Data Loss Prevention
- State of Data Security 2017

10 As an information security professional, how do I convey my vision and establish true partnerships and trust in the organization?

Information security programs are under more scrutiny and pressure than ever before. Boards are seeking confidence that security risks are being adequately managed and that programs are legally defensible. Digital business means that organizations are more dependent on digital systems than ever. Security cannot be seen to constrain innovation or agility, even as security requirements cannot be relaxed and CISOs have less direct control.

- Gartner Opening Keynote: Manage Risk, Build Trust, and Embrace Change by Becoming Adaptive Everywhere
- Managing Technology Risk and Cybersecurity Through the Lens of Business Value
- Hacked! What Do You Tell the Top Dogs?
- Selling Your Vision and Values: The Art of Persuasion
- How to Get Your CEO to Embrace Digital Risk Management
- Develop a Pragmatic Vision and Strategy for Digital Business Security

View further information on topics and the full agenda at [gartner.com/ap/security](http://gartner.com/ap/security)

By 2018, 90% of organizations will implement at least one form of integrated data loss presentation (DLP), up from 50% in 2016

By 2019, 25% of mobile-ready enterprises will deploy mobile threat defense capabilities on enterprise-issued mobile devices

3 ways to register

Web: gartner.com/ap/security
Email: apac.registration@gartner.com
Phone: +61 2 8569 7622