

IT Security Directors

The Urgent Need to Manage Risk While Growing the Business

As an IT Security Director, you are responsible for the security of the entire IT enterprise.

Business Issues

There is constant pressure on the enterprise to minimize the business risks associated with information technology. The race to expand client and partner relationships through technology, coupled with the rapidly changing world we live in, highlight the urgency to closely examine and manage security-related issues. Specific business objectives covered in the IT Security Directors Membership Program include:

- Managing IT risk with limited budgets and external support
- Preserving business agility while providing a secure environment
- Balancing the need for protection against the need for commerce
- Managing the risk exposures of technology use
- Complying with legal, financial and regulatory requirements
- Developing effective business continuity and disaster recovery plans
- Planning for external threats to critical infrastructure

Who Benefits

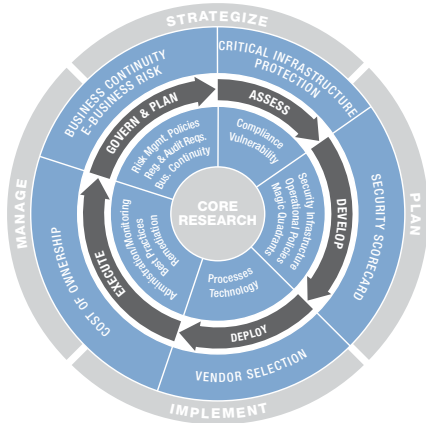
CIO, Chief Technologist
Chief Security Officer
Chief Risk Officer
IT Security Director, Officer or Manager
SOC Manager
Network Security Manager
Business Continuity Planner

Technology Issues

The issues surrounding security implementations are significant. The technologies and applications involved are often complex. In addition, security management must encompass virtually every device within the IT infrastructure. Some specific technology issues include:

- Responding to security incidents and developing resilience to disasters
- Supporting new technologies, software releases and software patches across a large number of devices
- Analyzing the security information generated by firewalls, intrusion detection systems (IDS) and server logs
- Securing information from piracy; keeping customer data private
- Creating efficient and auditable user administration
- Exploiting public key infrastructure for external applications
- Ensuring appropriate use of air gaps and security layers to protect critical infrastructure

IT Security Directors



No matter where you are in the security life cycle, Gartner provides you with integrated, concrete value at each stage—from planning and evaluation to management and, ultimately, measurement of return on investment.

Member Benefits

Key Insights

Member Portal provides relevant research to address the business and technology issues facing IT Security Directors, covering five crucial categories: Security Policies and Architecture, Business Continuity Planning, Security Infrastructure, Security Administration, and Critical Infrastructure Protection.

Security Executive Report “Securing the Enterprise” provides the focused, in-depth guidance you need to make critical decisions.

Monthly Spotlight highlights what is new and relevant.

Analyst Teleconferences exclusive to members address relevant topics and trends.

Alert Profiles auto-enlist and ensure you are notified when Gartner research covers topics of interest to you.

Monthly Newsletter highlights what’s top of mind for Gartner thought leadership, addressing time-sensitive key issues.

Gartner Core Research provides access to all research on gartner.com, analyst inquiry and the highly acclaimed Talking Technology audio series.

Gartner Presentation Library provides access to the latest analyst presentations on IT Security to strengthen your business cases.

Gartner Events include complimentary access to a Gartner theme conference of your choice.

Key Services and Tools

Decision Tools for Vendor Selection—Provisioning Model

The goal of this Decision Driver® vendor-evaluation model is to assist organizations in the evaluation and selection of the best provisioning solution to their business requirements. This model evaluates product-specific criteria as well as the required investments for significant vendor solutions.

TCO® Manager Model for Security

This charter group subscription provides high-level security benchmarking against an early adopter peer group and individual discussion of important findings. It leverages proven Gartner total-cost-of-ownership (TCO) methodology and includes a two-hour kick-off teleconference as well as a two-hour review of key findings.

Workshops (choose one of four one-day sessions): Security Scorecard

Evaluates the health of member organizations’ security infrastructure and processes. The workshop addresses four key areas, including Security Policy and Architecture, Business Continuity Planning, Security Infrastructure, and Security Administration.

Security E-Business Risk Assessment and Roadmap

Assesses the risk assumed by the member’s current e-business initiatives. The workshop establishes a starting point and objectives for the development or evolution of a security risk management program, using a unique methodology to facilitate discussion with members’ key executives.

Digital War Games 101—Critical Infrastructure (CI) Protection

An assessment of the current state of protection present in the critical infrastructure used or provisioned by an enterprise. Consists of targeted exercises to determine what critical infrastructure the enterprise is dependent upon and illustrates how vulnerable it is to attack.

Critical Infrastructure Protection (CIP) Scorecard

Helps executives in utilities, telecommunications, financial services, government and other key industries understand how to reduce the security risks to the critical infrastructure that they provision. Assesses the enterprise’s current security program using ISO 17799 and industry-specific criteria.