

Managing IT Security Risk in a Dangerous World

Mark Nicolett

In today's risk-intensive security environment, effective IT security stands on four pillars: security policies and architecture, security infrastructure, security administration and business continuity planning.

ANALYSIS

The consequences of less-than-perfect IT security are more serious than ever before. The havoc wreaked worldwide by the Nimda and SQL Slammer computer virus attacks highlights the existence of an increasingly effective underground society of hackers and confirms the need to build better defenses against cyberattacks. The impact of these highly publicized attacks is, however, dwarfed by the business losses caused by internal security lapses. A series of financial reporting scandals involving high-profile enterprises demonstrates an urgent need for information security techniques that improve the trustworthiness of enterprise transactions and audit trails. A series of legislative and regulatory initiatives — including the Graham-Leach-Bliley Financial Services Modernization Act, the Healthcare Information Portability and Accountability Act (HIPAA) and the European Data Privacy Directive — demands better execution in the areas of security and privacy, and raises the legal and financial stakes for enterprises that fail to meet their standards. These changes in the business, regulatory and IT environments also are increasing the need for comprehensive, enterprisewide business continuity planning that includes IT practices and processes.

Gartner has identified four pillars of enterprise IT security:

Security Risk, Organization, Policies and Architecture

A key element of effective IT security risk management is to identify exposures and their potential costs so that security policies — and an overall security architecture — can be developed to minimize these exposures and costs. Security policies should also enable an enterprise to take the greatest amount of risk necessary to support business requirements. Although this planning and design work is essential, risk is not managed until security policies and architectures are implemented. Implementing a security architecture requires an effective security governance model. Enterprises must determine the aspects of security to be centralized, the implementation of regional or departmental aspects of security, the methods to obtain funding, and the ways IS organizations and business units will be accountable for security. The scope of planning and development in this area should include:

- Risk management
- Regulatory issues
- Confidentiality and intellectual property protection
- Business application security
- Security services and sourcing

Security Infrastructure

An enterprise's security infrastructure is made up of the tools, technologies and tactics that are deployed to protect the network perimeter and internal resources. Unfortunately, for the world's security administrators, each wave of new technology renders existing security architecture obsolete. PCs made the host-centric security model irrelevant, distributed applications running across local-area networks reset enterprise security and the inclusion of external networks in the enterprise topology did the same for client/server security. Java and network computing have placed even the applications running on enterprise networks beyond the control of security administrators. Mobile devices and wireless connections bypass firewalls and enable sensitive information to be accessed by devices clipped to employees' belts. Traditional security infrastructure focuses on hardening the perimeter, but internal resources are now increasingly

exposed to external access by outward-facing applications. In this fast-changing environment, enterprises must have a hardened interior and a layered approach to security, with an infrastructure that includes:

- Firewalls
- Intrusion detection and prevention
- Antivirus protection and content filtering
- Mobile and wireless security
- Encryption
- IT security management

Security Administration

Enterprises cannot realize satisfactory returns on their investment in security planning and policy development without effective execution and implementation. Sound security administration focuses on operational technologies and best practices that maintain secure access to applications and resources, and on ensuring the integrity of system definitions and configurations. The scope of security administration includes:

- Web services and public-key infrastructure
- Vulnerability assessment
- Security configuration and patch management
- Identity and access management

Business Continuity Planning

Business continuity planning has evolved beyond its traditional focus on disaster recovery to include planning and design for IT and business process resilience. This evolution is driven, in part, by the growing linkage between IT and business processes as enterprises deploy more real-time, outward-facing applications that support critical business processes. Enterprises must implement comprehensive business continuity planning programs that address business recovery (that is, recovery of the workspace), business resumption planning (for key business processes), contingency planning and crisis/emergency management. Business continuity planning should be integrated into business processes and the IT life cycle, and address the following concerns:

- Business continuity planning strategies and best practices
- Business continuity planning technology and tools
- Business continuity planning services

Featured Research

"Risk Management 2002 and Beyond: Formal and Integrated" — Successful enterprise risk management encompasses strategic planning, operational management and financial controls.

By Simon Mingay

"Elements of a Successful IT Risk Management Program" — Effective IT risk management protects the interests of management, shareholders and other stakeholders. **By Roberta Witty**

"The Myth of Quantitative Risk Analysis" — Justifying IT security spending requires realistic scenario planning, not unworkable attempts to quantify risk. **By Conal Mannion and Alain Dang Van Mien**

"Force Vendors to Make Software More Secure" — Having more-secure software starts with vendors taking more responsibility for the security of their products. **By Arabella Hallawell and Rich Mogull**

"The Role of the Chief Information Security Officer" — The demand for information security skills, including those at the most-senior levels, increases as enterprises examine their IT skills portfolios. **By Roberta Witty**

"Secure Your Enterprise First" — Addressing basic security concerns takes priority over high-profile security concerns, such as terrorism. **By Rich Mogull**

"Update Your Internet Server Security" — Recent malicious-code attacks show that Web servers must be a key focus of enterprise security. **By John Pescatore**

"ROI Drives Identity and Access Management Implementation" — Identity and access management offer cost-effective ways to manage user account and access rights. **By Roberta Witty**

Mark Nicolett

Vice President, Research Director

secmember@gartner.com

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509