

## **2.0 A Time of Reckoning for Information Security**

Following the Sept. 11 terrorist attacks, the dot-com collapse, distrust due to corporate and government scandals, and the economic downturn, few enterprises had the will or spirit to invest aggressively in their IT infrastructures unless absolutely necessary. This situation is now changing. The next several months promise opportunities for security professionals to leverage executive attention and to demonstrate value.

However, failure to minimize visible threats (such as spam and increasingly creative viruses, worms and spyware) or overspending to meet legislative initiatives could lead to questions about the skills and relevance of in-house security professionals, and more reliance on external consultants and outsourcing solutions.

Being proactive in information security requires removing vulnerabilities before threats arise. The best way to do that is to buy the most secure hardware and software, and to force all vendors and business partners to continually improve their security. Perfect security is impossible, but continual scanning for new vulnerabilities and monitoring for new threats are critical factors. In security, the best defense is a good offense, and the more proactive you can be, the more secure you will be.

The research in this chapter addresses the following Key Issues:

- What does an IT security director need to know about organizational risk management?
- What technologies may expose enterprise IT systems and data to damaging security breaches?
- How can organizations show return on investment for security, what are the metrics that business management should see and how much should be spent?
- What are the most effective technologies and best practices to protect networks, systems, applications and data?

## 2.1 Key Organizational Risk Management Issues

### Key Issue: What does an IT security director need to know about organizational risk management?

The Gartner executive program survey is an annual snapshot of the plans, priorities and concerns of CIOs around the world. Based on responses as of January 2005 from 1,300 CIOs in more than 30 countries, security remains highly important to organizations (see Figure 2-1). The survey sample represents more than \$57 billion in IT spending.

The survey shows that CIOs expect IT budgets to increase by an average of 2.5 percent in 2005. Although there are regional variances, this is the most positive picture since 2002. Survey results also shows that the IT organizations will be expected to start contributing to business growth in 2005, and that CIOs are turning to business processes and business intelligence to meet this challenge.

Interestingly, public-sector organizations share many priorities with their private-sector counterparts. In 2005, security and data protection concerns rate higher in the

public sector because many services incorporating the public’s trust are online but this does not mean that public-sector IT is less secure. Instead, it means that in the absence of revenue growth imperatives, IT contribution comes primarily from the quality and costs of current IT services.

Public-sector management priorities reflect the need for secure, high-quality IT services that concentrate on security and business continuity, and demonstrate the business value of IT. Delivering these services, while ensuring that the agency is aware of them, provides the CIO and IT organizations with a way to manage expectations in an environment of executive change.

### 2.1.1 Most Important Problems Facing IT Organizations

In a survey of prospective attendees to Gartner’s IT Security Summit 2005, participants were asked to identify their top three priorities (see Figure 2-2). Although skewed toward those with security interests, the No. 1 priority of budget and cost containment shows the understandable continuing sensitivity to this issue.

**Figure 2-1: Gartner Executive Survey: Top Technology Trends in 2005**

To what extent is each of the following technologies a priority for you in 2005?	Ranking		
	2005	Top 5 responses	Average 2005
Security enhancement tools	1	600	7.68
Business intelligence applications	2	599	7.36
Mobile workforce enablement	3	435	6.68
Workflow management deployment and integration	4	430	7.32
Enterprise resource planing (ERP) upgrades	5	406	6.54
Storage management	6	393	7.08
Voice and data integration over IP	7	365	6.74
Customer relationship management (CRM)	8	355	6.26
Business process integration tools	9	313	6.72
Server virtualization	10	309	6.58

Source: Gartner

Because of risk factors, security remains a high concern. Combining items two and five on the chart easily surpasses cost issues so neither issue can be ignored. Regulatory and compliance issues have pressured IT and information security budgets, and diverted some attention from making the organization more secure.

## 2.2 The Security-Related Impact of New Technologies

**Key Issue: What technologies may expose enterprise IT systems and data to damaging security breaches?**

*Strategic Planning Assumption: Through 2009, each new wave of technology will render existing information security measures obsolete, increasing security exposures in new and legacy environments (0.8 probability).*

The continuing cycles of technology show why security will not disappear from the top five list of executive concerns. After 20 years of experience, most companies consider mainframe security to be robust and manageable. Now, companies expect robust, manageable security in 20 weeks or sooner whenever new technology rolls in or business fundamentals change (for example, outsourcing, business partnering or organizational centralization).

During the change, management's focus in terms of funding and resource allocation shifts from the old to the

new, creating a security gap between the desired and achieved levels of control. Enterprises will often rely on outside support, such as consultants and outsourcers, at the onset of any change.

Security funding will shift from traditional solution purchasing to a broader, better-defined risk management process involving investment in security segments:

- *Keeping the Bad Guys Out:* Firewalls (personal), firewalls (deep packet inspection), intrusion detection/prevention, virtual private networks, antivirus, anti-spam, Web filtering, mobile data protection, managed security services, security monitoring and correlation
- *Letting the Good Guys In:* Identity management, user provisioning, extranet access management
- *Keeping the Wheels On:* Business continuity planning, vulnerability management, security operations

Each wave of technology obliterates the security architecture appropriate for its predecessor (see Figure 2-3). For example, PCs broke the host-centric security model. Networked PCs eroded the gains that had been won in securing individual desktops. Distributed applications running across LANs reset security maturity to zero, and the inclusion of external networks as a part of the topology reset client/server security. Wireless networking devices usually ship with security defaults off and are often installed outside the view of the IT organization. Evolving Web services allow data to bypass firewalls and introduce yet another set of security issues.

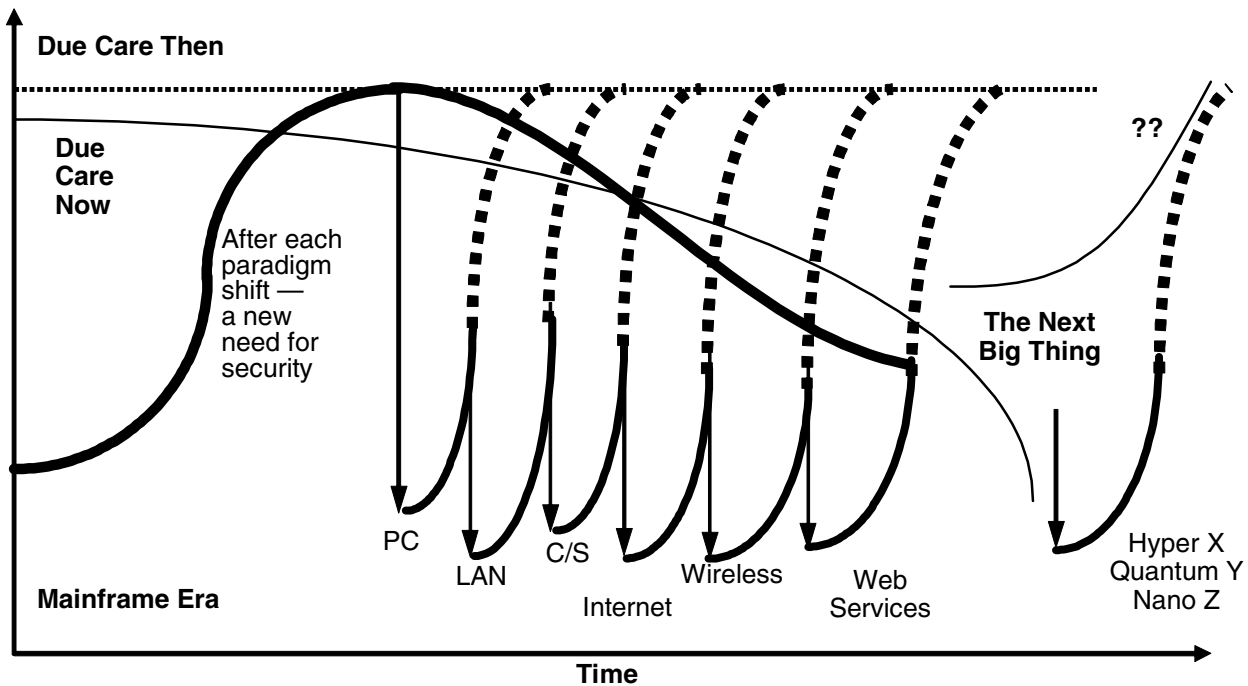
**Figure 2-2: Gartner Survey Results: Problems Facing IT Organizations**

**What is the largest problem facing your IT organization in the next 12 to 18 months (three most important)?**

Budgets/cost containment	438
Developing formal strategy for enterprisewide IT security	364
Staffing and skills	328
Aligning IT with the needs/requirements of the business	292
Have a mature enterprise security implementation	278
Ongoing management and measurement of security effectiveness	251
Regulatory/compliance	276

Source: Gartner

**Figure 2-3: The Impact of Disruptive Innovation on Information Security**



Source: Gartner

C/S client/server

**2.2.1 Security Vulnerabilities in the Supply Chain**

*Tactical Guideline:* Each stage of a business relationship carries security requirements. Virtually all organizations will experience increasing trading-partner distrust due to information security vulnerabilities.

Until the Internet became ubiquitous, e-commerce had been focused on the buy-and-sell process, with organizations struggling with electronic data interchange (EDI) to reduce paperwork and the implied costs. This view is limiting. Each stage of a customer-supplier relationship (and in government operations for regulatory activities and citizen services) benefits from the implementation of one or more electronic business tools.

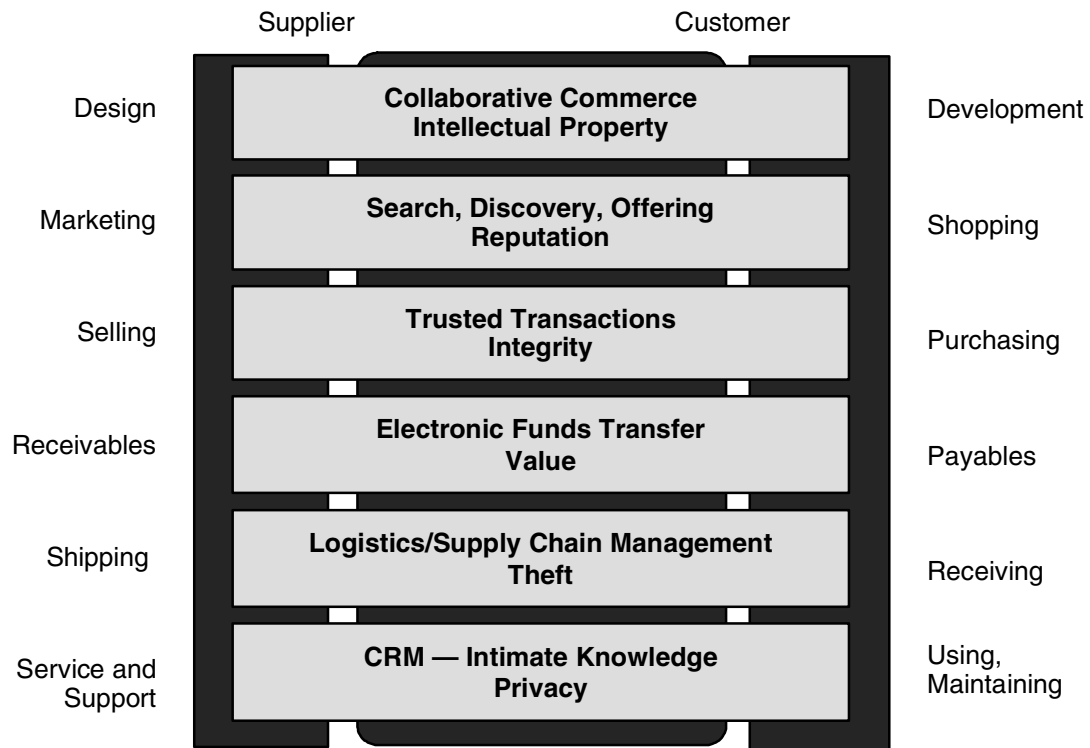
The shift to the Internet as a primary medium for e-business has introduced a new set of security concerns. Each set of relationships — between buyer and seller, and between specific departments and applications within the company — has its own set of security requirements (see Figure 2-4). For example:

- Collaboration through unmanaged instant messaging may reveal sensitive intellectual property to competitors.
- Vulnerable Web pages can be corrupted by threat agents leading to a loss of confidence in the merchant.
- Electronic funds transfers may be sent to rogue accounts.
- Logistics information may be used to hijack trucks carrying valuable cargo.
- Sensitive customer information, including preferences and credit card details, may be stolen and used inappropriately.

The nature of e-commerce extends new and untested platforms externally. Companies are often not prepared to support outside users on core systems. Identification, authentication and authorization of the players have become increasingly important in open e-business.

**Action Item:** Apply risk assessment to each new business process to determine the appropriate defensive action.

**Figure 2-4: Business Relationships and Their Security Requirements**



Source: Gartner

CRM customer relationship management

### 2.2.2 The Evolution of Cyber Threats

#### Strategic Planning Assumptions:

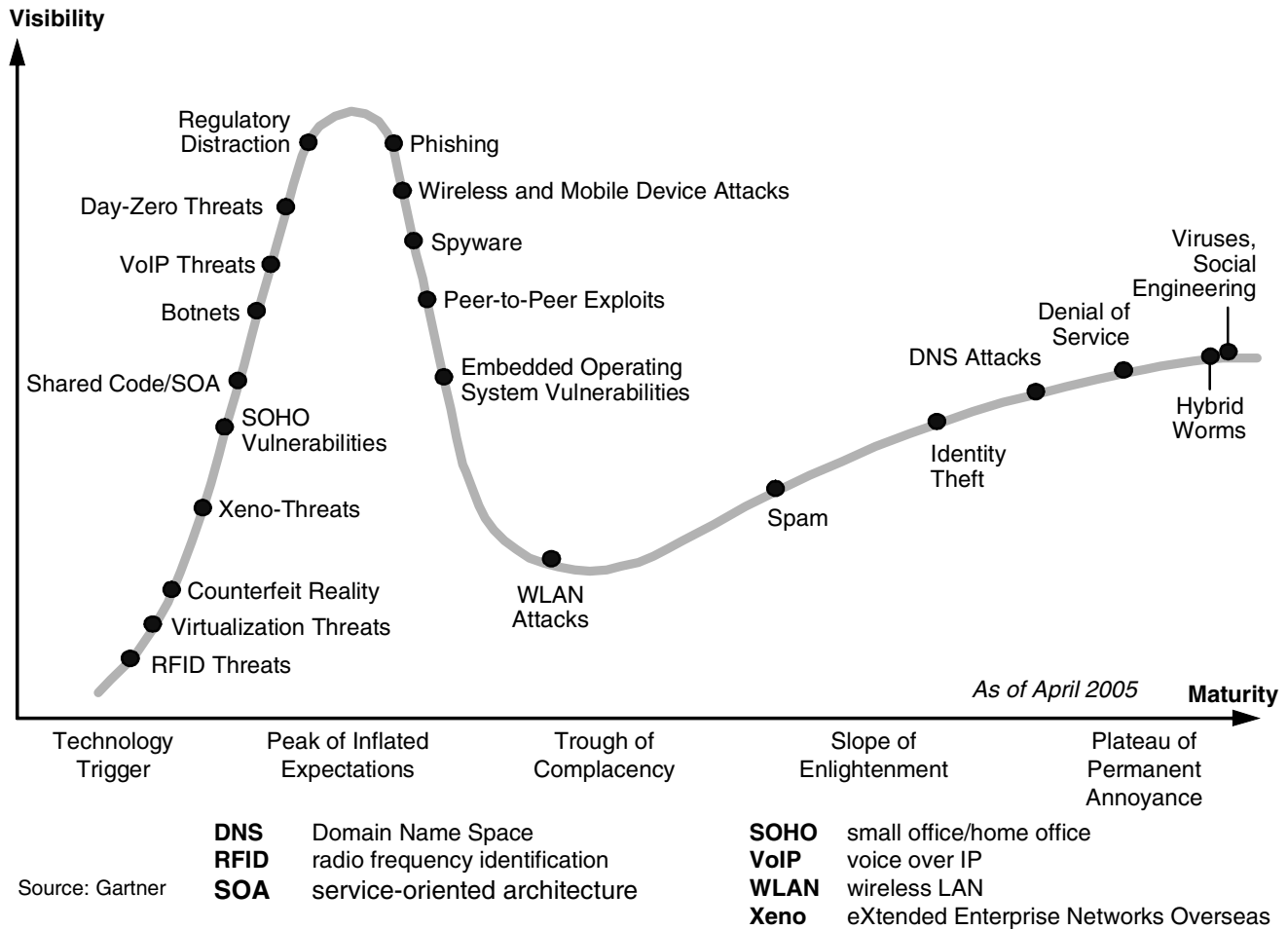
- Security best practices on virtual machine clients will be adequate through 2005 (0.6 probability).
- If phishing antidotes are not implemented, consumer trust will erode and annual U.S. e-commerce growth will slow to 10 percent or less by 2007 (0.6 probability).
- Cyberattacks that exploit vulnerabilities where a patch has been available for less than 30 days will increase from 15 percent of total cyberattacks in 2003 to 30 percent in 2006 (0.6 probability).

Information security threats will continue through the planning period; take a comprehensive, defensive view to achieve due care. Figure 2-5 is Gartner's Hype Cycle for Cyber Threats, which illustrates the evolving impact of cyber threats on an enterprise. Following are definitions for those threats found on the Hype Cycle.

- Radio frequency identification (RFID) security issues relate to privacy concerns and mislabeling.

- Virtualization threats will appear as attackers shift from targeting operating system vulnerabilities to hypervisor weaknesses.
- Possible Xeno (eXtended Enterprise Networks Overseas) threats arise because of outsourcing.
- As minimally supported small office/home office installations grow, new threats to corporate networks emerge.
- Service-oriented architectures mean that a vulnerability in a piece of shared code may affect other areas.
- Botnets are already creating swarms of denial-of-service attacks.
- As voice moves to IP (Internet Protocol), security is lagging behind, particularly in signaling systems.
- Day-zero attacks occur before patches and signatures are available.
- Companies working toward regulatory compliance may be distracted from security vulnerabilities.
- Phishing leads to identity theft.

**Figure 2-5: Gartner's Hype Cycle for Cyber Threats, 2005**



- Spyware can report user behavior to an external party without the user's knowledge.
- Spam consumes resources.
- Seeking any open port, instant messaging programs can put networks and information at risk.
- As control devices move from proprietary operating systems to commercial operating systems, they become more vulnerable.
- Unprotected wireless LANs (WLANs) can lead to confidential information leaks.
- Identity theft is a rampant and growing cybercrime.
- Hybrid worms have moved rapidly through the hyperbole.
- Viruses remain a recurring source of problems.
- Directory network service, social engineering and denial-of-service attacks are almost unfashionable in

terms of hype, but remain dangerous threats that organizations must address.

**Action Item:** Evaluate the changing threat landscape in the context of your defensive requirements. As threats mature, so do defenses.

### 2.2.3 Regulatory Distraction: Regulations vs. Auditors

Most organizations are using regulatory pressure to fund security projects and to integrate security more tightly with business units. It's the excuse that security professionals have been waiting for to force business integration. But some organizations are completely distracted by reporting, ongoing audits and putting out the fires of remediation. Organizations must focus on getting secure before worrying about showing that they are secure. Such an effort entails protecting customer data first, then documenting it — not the reverse.

Most of the current regulatory burden is the result of increased reporting requirements and audit activities, particularly due to the U.S. Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley) Section 404 and its extensive documentation and audits. A chief executive officer won't go to jail under Sarbanes-Oxley if there's a control deficiency but will be sentenced only if he or she perpetuates the fraud by trying to cover up the problem. (Though there might be other implications if too many deficiencies become public.)

Compliance changes priorities but shouldn't reduce security. Security departments need to manage compliance reporting and remediation without losing focus on top security concerns. For example, not all auditors are experienced in IT and may make unreasonable requests. These should be disputed with management. Overall, IT must let management know when generating compliance reports starts to interfere with core security operations that could hurt the business.

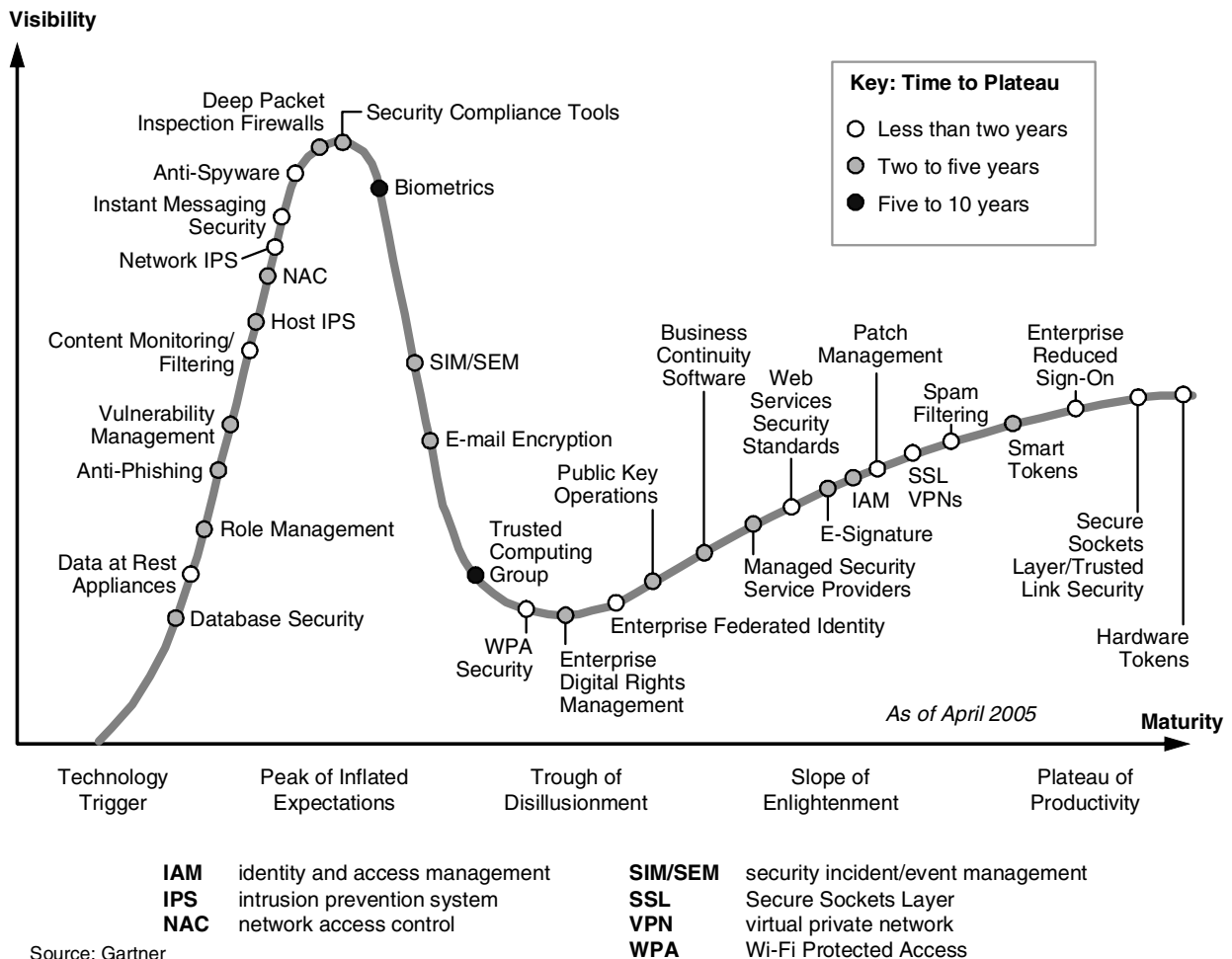
Organizations need to do "good enough" security regardless of the presence — or absence — of laws that suggest doing something more. In the absence of specific regulatory guidance, auditors wind up defining "good enough" security.

### 2.2.4 New Security, Privacy and Risk Technologies

**Tactical Guideline:** Avoid letting Hype Cycle variations and the relative popularity of a particular security solution dictate plans.

Each new wave of technology disrupts existing security measures and introduces new vulnerabilities. Each new technology in security, privacy and risk follows the Hype Cycle (see Figure 2-6). Determining when to adopt an emerging technology is a critical decision. If the technology is adopted too soon, the company will suffer the pain

**Figure 2-6: Hype Cycle for Security Technology, 2005**



and expense of an immature technology. If the technology is adopted too late, the company runs the risk of being left behind by competitors that have made the technology work to their advantage.

In the case of information security, failing to deploy defensive solutions at the right time can leave the organization vulnerable. Delays in identity, authentication and access control products or services can leave the enterprise in a catch-up mode regarding business opportunity.

**Action Item:** Investing in an overhyped technology too early can result in a complete waste of enterprise security funds. Enterprises should focus on business needs and threat assessment to prioritize security needs. This analysis should be combined with the Gartner Information Security Hype Cycle to deflate the hype spread by security product and service vendors.

## 2.3 The Business Value of Information Security

**Key Issue:** How can organizations show return on investment for security, what are the metrics that business management should see and how much should be spent?

*Tactical Guideline:* Measuring the business value of information security will continue to be based on a balance of security as a cost of doing business, risk reduction and return on investment (ROI). ROI is shown through improved business opportunity, enhanced trust relationships and displaced costs.

Despite attempts to quantify information security ROI, for the most part, investment in information security is a cost center and a cost of doing business, particularly when trust and other elements of information security are expected by business tradition or required under regulatory and audit concerns. The expense can be justified as cost avoidance, measurable in preventing direct loss. For example, appropriately applied security features can prevent the theft of intellectual property.

Less measurable, but calculable under risk assessment processes, is the potential lost value that can result from a loss of customer or stockholder confidence. Cost avoidance can be found in regulated industries where companies and even individuals may be fined or

incarcerated for failing to provide due-diligence security for the organization or data it must protect.

### 2.3.1 Key Security Industry Trends

One of the most significant trends in the security industry is the consolidation of one-off point products into security platforms and dramatically improved management tools. This combination of consolidation, advanced feature sets and enterprise-class management tools will enable enterprises to spend less on security, while improving their overall security posture. In forming this estimate, Gartner took into account emerging technologies, but it's possible that a totally disruptive technology could appear that changes the landscape.

Four key trends are changing the security market and security architectures:

- The transition from stateless packet inspection and intrusion detection to deep-packet inspection and intrusion prevention
- The rise of identity and access management solutions that consolidate provisioning, authentication and management of access controls
- The combination of asset identification, vulnerability scanning and patch management into vulnerability management solutions
- Consolidation of auditing, monitoring and active management of security products with security management tools

### 2.3.2 Information Security Spending

*Tactical Guideline:* Security managers should include estimates of measurable security improvement with every request for spending. Business units should include security spending in all IT project requests, rather than depending on security spending.

Gartner estimates that average security spending as a percentage of the IT budget when including staff salaries and external services will flatten to the 5 percent to 6 percent range as companies become more efficient. This is an estimate of what enterprises actually spend (the most secure organizations probably spend less than average).

The lowest-spending 20 percent of organizations, the most efficient ones, can safely reduce the share of security in the IT budget while improving their security profile.

### 2.3.3 Delivering a Security Service Level

Though knowing proper measurements is not easy, enterprises must measure their information security programs, processes and procedures. System outputs — viruses quarantined, spam messages blocked, intrusions detected and prevented — are only part of the equation. Using anecdotal security cleanup costs are usually “guesstimates” hyped by vendors. Outside the office door of most CIOs are service-level performance charts but security is often absent.

Everyone agrees you can't improve what's not measured, yet security groups avoid metrics. Gartner has defined eight key metrics that provide a baseline for measuring the status and trend of an information security program:

- *Process Improvement*: How many machines are involved in each virus incident? How many weeks between critical patch issued and implemented?
- *Attack Resistance*: What percent of known attacks are we vulnerable to? When did we last check?
- *Efficiency and Effectiveness*: What is our security spending as a percent of revenue? What percent of downtime is due to security incidents?
- *Internal “Crunchiness”*: What percent of our software, people and suppliers have been reviewed for security? What percent of my critical data is strongly protected?

Other security metrics can be applied according to particular business drivers. The metrics represent values that are relatively easy to obtain, even though some are difficult to improve. Each company needs to define an acceptable service level for each value, and track performance against that service level.

Management has been surprisingly willing to accept the risks of “something happening” because many risks seem remote compared to the expense of implementing a comprehensive security architecture or continually buying the latest “widget.” Despite heightened awareness that a significant cybersecurity event can be costly in terms of cleanup, lost intellectual property, regulatory fines and loss

of reputation, company boards will demand more security budget justification as the pressures continue to build for demonstrating results as economic conditions improve. Company-specific costs of security problems, developed by financially oriented professional staff, will be more valuable than hand-waved warnings. Information security managers need to be realistic in estimating the value of their efforts and conservative in budget requests.

### 2.3.4 The Role of Chief Information Security Officer

Ten years ago, typical information security tasks were predominately operational in nature. User provisioning, security configuration and perimeter management have changed in detail over the last decade, but they have not changed in significance.

Quite the opposite is true. Not only have organizations transferred knowledge of these tasks to persons with relatively less experience, but products have become increasingly sophisticated and automated, allowing the same functions to be performed at a lower personnel cost. During the same 10 years, and arguably at an increasing rate during the next two to five years, the emphasis within the information security space has become increasingly strategic, especially in the largest corporate and government organizations.

The ability to determine what constitutes risk, and especially the privilege of reporting that risk to executive decision makers, is a highly political activity. Generally, it is a privilege that has been denied to technically oriented information security specialists who have been forced to report their concerns up through the filter of the CIO's organization.

Increasingly, information security is being given greater independence. Through a dotted-line report to a chief financial officer, chief risk officer or chief compliance officer, or even as a direct report, the chief information security officer (CISO) is being given a reporting mechanism that lies outside of the IT department. Especially at highly regulated organizations, this is viewed as an important governance mechanism. Theoretically, the CISO is able to provide a more realistic picture of IT risk when not subjected to the pressures of accommodating the IT organization's agenda.

## 2.4 Most Effective Security Technologies

**Key Issue: What are the most effective technologies and best practices to protect networks, systems, applications and data?**

### 2.4.1 “Do Need” Security Technologies

According to Gartner, the security technologies that enterprises will likely need include:

- Host-based intrusion prevention system
- 802.1x
- Quarantine and containment
- Personal intrusion prevention and URL blocking
- Gateway spam and antivirus scanning
- Security audit capabilities
- Vulnerability management
- Web services security
- Identity management
- Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
- Business continuity plan
- PC lockdown cables and anti-tamper alarms

Understand the current and emerging technologies on the “do need” list. Many of these represent next-generation approaches to information security. For example, vulnerability management not only implies advancement from passive vulnerability monitoring to near-continuous monitoring, but also integration with workflow and rules engines to correct vulnerable states without creating system conflicts.

In the case of gateway spam and virus scanning, defenses are moving out from the desktop and e-mail servers to the edges of the enterprise boundary, and beyond to the Internet service providers (ISPs). Stand-alone products

are converging, represented here by personal intrusion prevention, which includes antivirus, anti-spyware, intrusion prevention and a desktop firewall. URL filtering was viewed as a porn-blocking solution, but now the function blocks access to malicious sites needed as a first line of defense.

Business continuity planning is essential for several reasons: keeping the wheels on part of information security, anticipating natural or other disasters, and ensuring that the enterprise can stay functioning. Finally, the enterprise must have well-trained professional staff managing its information security program.

### 2.4.2 “Don’t Need” Security Technologies

According to Gartner, the security technologies enterprises will likely not need include:

- Personal digital certificates
- Quantum anything
- Passive intrusion detection
- Biometrics (outside of user-held templates)
- Tempest shielding/paint
- 500-page security policies
- Security awareness posters
- Default passwords

Gartner’s advice reflects the positions of these technologies on the Hype Cycle. For the most part, technologies on the list of “don’t needs” can be avoided. For example, although some enterprises will benefit from digital signatures, they are exceptions. Quantum key distribution may be necessary when quantum cryptoanalysis is available to threat agents — not for another 10 to 20 years at minimum, despite discussion of high-speed crossbar latches replacing transistors. Gartner continues to be unconvinced that biometrics, which authenticate beyond a locally stored template, will have broad-scale near-term usage. No one really reads or benefits from 500-page policy manuals.

Although security awareness posters may represent an effort, they are ineffective and give a false impression that an organization is doing something about security. Security posters, along with login and e-mail message disclaimers, fit into a unique category. These measures allow an entity to claim that it is on top of security, but these elements ultimately do little to improve security. Instead, they are used as attempts to avoid liability, and to demonstrate to regulators and auditors that a company is applying due diligence. They do nothing of the sort.

## 2.5 Recommendations

- Demonstrate security service level.
- Benchmark and justify IT security spending.
- Avoid the hype and, in fact, anticipate it.
- Anticipate that disruptive technologies and business process evolution will continue to drive security.
- Adopt the philosophy that security needs to be built into IT systems and business processes.

