

2.0 Information Security — Establish a Strong Defense in Cyberspace

With more than 600 million individuals worldwide now on the Internet, cybercriminals are taking advantage of unsophisticated users and enterprises and unsecured machines to usher in a new era of high-profit, low-overhead crimes targeting information and intellectual property. Despite many misconceptions that downplay the ability of cyberterrorists to destroy critical infrastructures easily and massively, the threats are very real and should be taken seriously.

Many enterprises, possibly overwhelmed by the effort, costs and conflicts that arise in attempting to implement effective security measures, have adopted the erroneous “security by obscurity” philosophy, thereby assuming they are protected by their relatively small presence in cyberspace. However, it takes only one unsecured machine on a network to create potential risk for everyone else. The risks *and* the costs of defenses are high, and the trend is moving both upward.

Gartner’s assessment is that, at its highest level within the enterprise, information security’s top vulnerabilities are:

- Fundamentally insecure commercial software
- An inadequate patch update model
- Misguided users who believe crime happens to “someone else”

Drilling down, a number of new technologies will add to the challenges:

- *Web services* will produce discontinuities in new application security.
- Insecure *wireless* LANs represent a serious point of potential failure for enterprise networks.
- *Intrusion detection systems* are not the panacea that enterprises are seeking.
- *Instant messaging* is creating worrisome “holes.”

As enterprises turn their collective attention away from tactical security issues stemming from homeland security initiatives and back to infrastructure security, they will witness an evolution from after-the-fact improvements to more secure and thus more expensive products resulting from “secure out of the box” software initiatives.

Protecting intellectual property is difficult. New laws in the wake of corporate financial-reporting scandals will force applications of information security techniques to improve the trustworthiness of enterprise transactions and the audit trail.

Strategic Planning Assumption: *By 2008, standard liability disclaimers in software licensing agreements will no longer protect software vendors against lawsuits stemming from breaches of fundamentally insecure software (0.7 probability).*

Tactical Guideline: *Cybercrime is an international growth industry. Security by obscurity will not work at the individual, enterprise, national or international levels.*

This chapter addresses the following Key Issues:

- How do new technologies and business processes disrupt security structures and introduce new vulnerabilities?
- What information security solutions are offered to the market, and how are they evolving?

2.1 Assessing “Cyber-Threats” From the Enterprise Perspective

Key Issue: How do new technologies and business processes disrupt security structures and introduce new vulnerabilities?

Strategic Planning Assumptions:

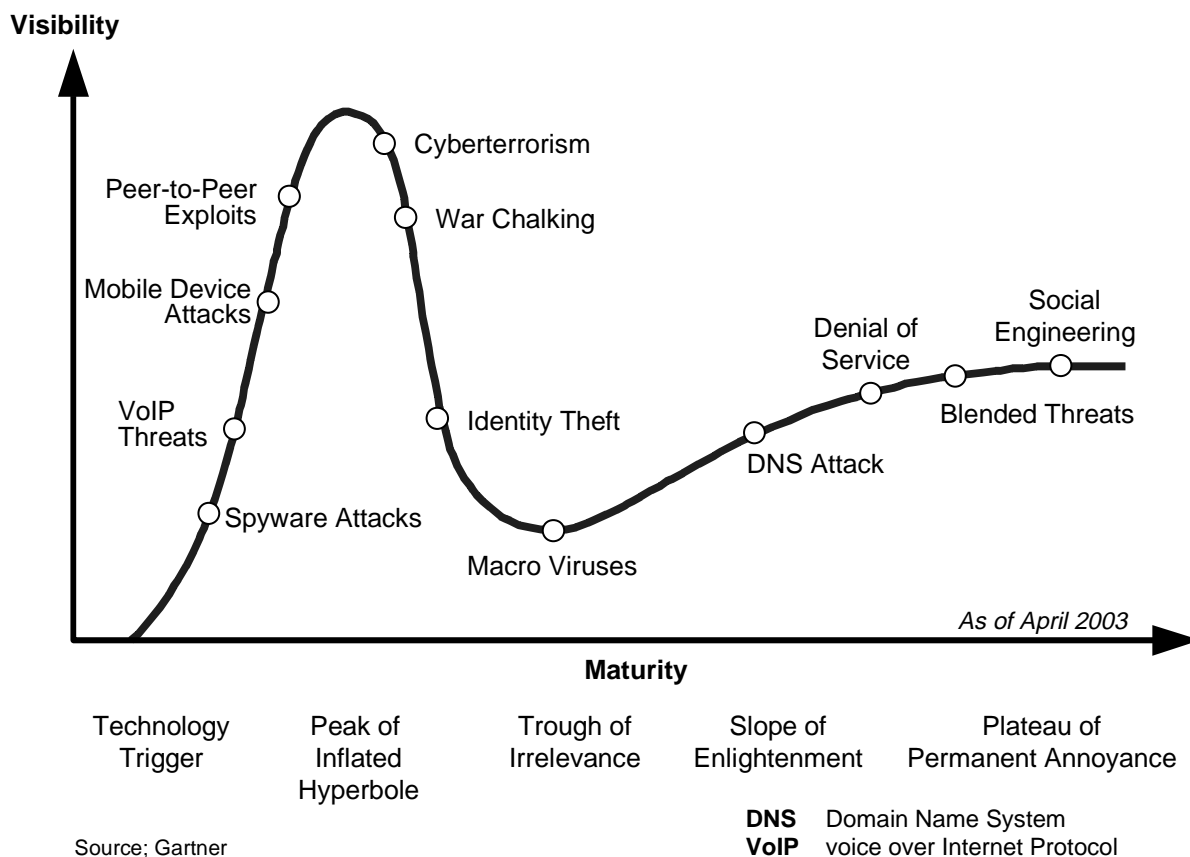
- *By year-end 2003, 90 percent of intrusion detection system deployments will fail if false positives are not reduced by 90 percent (0.7 probability).*
- *By 2006, enterprises that rely on only proxy and stateful packet inspection will experience successful application-layer attacks at twice the rate of enterprises that use leading deep packet inspection approaches (0.6 probability).*
- *By 2005, enterprises will longer use software-based application proxy firewalls (0.6 probability).*

Gartner’s Cyber-Threat Hype Cycle (see Figure 2-1) characterizes the progression of a number of “cyber-threats” from Technology Trigger through the Trough of Irrelevance and finally to the Plateau of Permanent Annoyance:

- Delivered using viral methods, *spyware* programs, which probe a target machine and report findings to an advertiser or other party without the user’s knowledge, can be used for harm.
- As *voice over IP* expands, it carries with it Internet-style risks.
- Though few viruses are found on *personal devices*, it is only a matter of time before these become uniform platforms of exploitation.
- Instant messaging and other *peer-to-peer programs* seek open ports as a means to put networks and information at risk.
- *Cyberterrorism* has gone past the peak and will remain there, barring new physical attacks or more evidence of cyberterrorist intent. Those that hype cyberterrorism cause more loss of confidence than actual attacks.
- *Identity theft* is a rampant cybercrime mostly accomplished via pedestrian means such as “dumpster diving.”
- *Macro viruses* are at the low point, as virus writers and antiviral software companies “up the ante.”
- A minivovement to find and mark free wireless Internet access locations primarily causes theft of service. If enterprises don’t protect *wireless LANs*, other harm can follow.
- *Blended virus and worm threats* have moved rapidly through the hyperbole.
- *Directory network service, social engineering and denial-of-service* attacks are almost passé in terms of hype but remain dangerous threats that enterprises must address.

Action Item: Enterprises should evaluate the changing threat landscape in the context of their specific defensive requirements. As threats mature, so do defenses.

Figure 2-1: Gartner's Cyber-Threat Hype Cycle



2.1.1 Securing the Enterprise From the Inside and Out

Strategic Planning Assumptions:

- By 2005, financially or politically motivated attacks will represent 30 percent of total incidents, and 60 percent of the incident costs incurred by enterprises (0.6 probability).
- Through 2008, enterprise insiders, working alone or in conspiracy with outsiders, will account for a majority of financial losses resulting from unauthorized use of computers and networks (0.8 probability).

Tactical Guideline: Create and enforce legal agreements defining legitimate use of proprietary intellectual property by trading partners and employees.

Today's business processes are often designed for speed and convenience, not security. With that in mind, enterprises face a conflict between security and commerce as limiting insider access to information certainly cripples the ability to make mischief, but it also cripples the ability to make revenue. Generally, this conflict is resolved in favor of open access.

Historically, insiders have been responsible for the vast majority of loss-bearing computer security breaches.

Though insiders may only be responsible for 30 percent of all breaches, those breaches account for up to 70 percent of the incident costs incurred by those enterprises. Insiders have both the means and the opportunity to conduct security breaches as a result of key modern business practices that demand intensive information sharing.

Externally, almost all enterprises connect digitally to share information with other organizations such as customers, suppliers, outsourcers, or regulators (see Figure 2-2). In that context, the risk that confidential information will be stolen or misused is amplified. Many enterprises don't have processes for establishing and enforcing agreements on shared use of intellectual property. Without such legal agreements, misuse is more likely and less subject to recovery.

Action Item: Enterprises must take steps to secure themselves against rogue insiders or resign themselves to suffering losses from insider crimes.

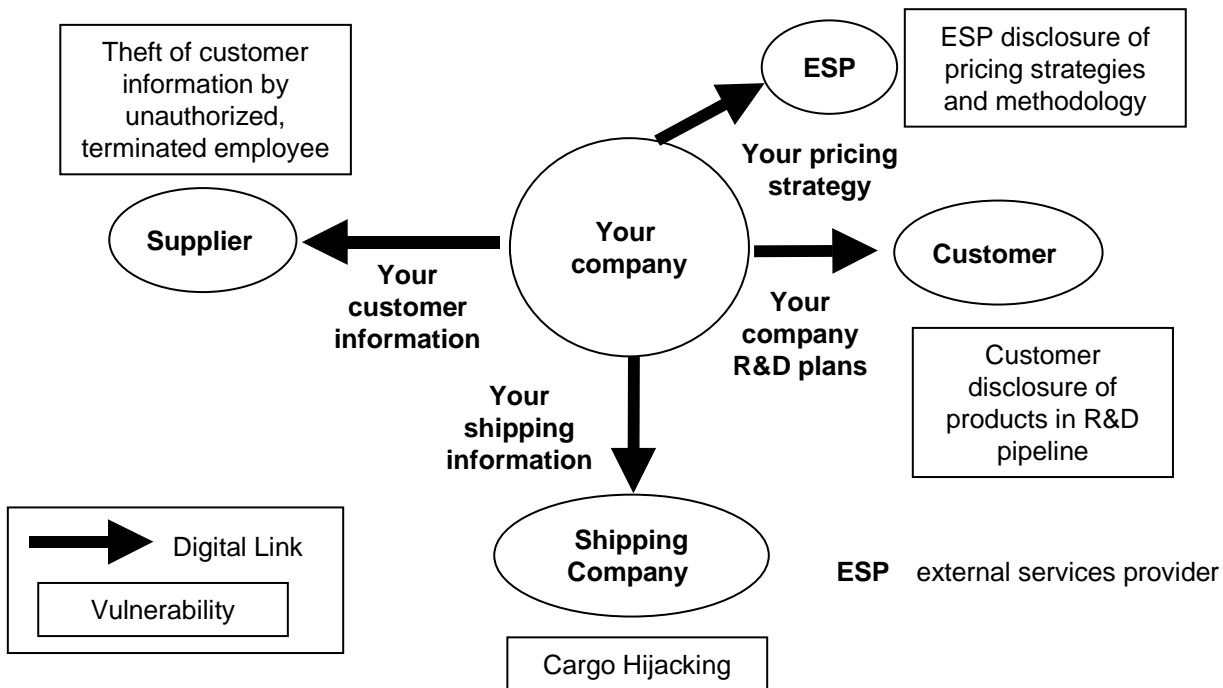
2.1.2 Establishing Security Management Governance

Tactical Guideline: Centralize security management under a governance arrangement.

Within the enterprise, governance defines who has input and decision rights in particular domains. Established IT governance arrangements can often be extended to include security (see Figure 2-3). The four decision domains are:

- A board-level domain, “risk strategy” establishes the enterprise’s attitude toward risk. For example, will the enterprise be the first to deploy new technologies in its markets, regardless of security issues?
- Based on risk strategy decisions, the “security policy” domain must not only determine which behaviors are acceptable but also the security responsibilities of various parties inside and outside the enterprise.

Figure 2-2: Multienterprise Security Is as Strong as Its Weakest Link



Source; Gartner

Figure 2-3: Security Governance Arrangement Matrix

Domain Style	Security Policy		Security Architecture		Business Application Security	
	Input	Decision	Input	Decision	Input	Decision
Business Monarchy						
IT Monarchy						
Feudal						
Federal						
Duopoly						

Source: Gartner

- The “security architecture” domain must choose which technologies and processes will be used to ensure enterprise security, based on policy.
- The “business application security” domain must decide how security that is consistent with the architecture will be implemented within each application. Enterprises with polyglot security architectures have difficulty getting an overview of their security status and effectiveness.

Regardless of how governance is established, failure to centralize reporting and define a security strategy for the enterprise will result in a security program that is fragmented, slow to understand and react, and prone to failure.

2.1.3 Creating a Security-Aware Enterprise Culture

Tactical Guideline: *Once desktops are locked down, awareness is critically important. Until then, focus on locking down the desktops.*

In essence, a security-aware culture is alert to threats and knows what to do when they occur. Management establishes the foundation for such a culture by implementing sensible policy, training employees, and taking action quickly and visibly when threats arise.

Employees must know the following:

- The enterprise’s policies. Employees can’t take care to limit their own and others’ violations if they don’t know what is permitted.
- The common threats. Employees should know how to recognize common threats, such as viruses, and avoid or limit them.
- The impact. Employees should understand the potential seriousness of specific threats to the enterprise.
- How to report and respond. Employees must know how to summon help quickly when they see a threat. Moreover, security managers should ensure that desktops are locked down.

2.1.4 Evolving an Enterprise's Security Architecture

Tactical Guideline: Each stage of an e-commerce relationship, from collaborative commerce to customer relationship management, carries unique security requirements.

Strategic Planning Assumption: Enterprises failing to acknowledge and address the variable risk factors within the first two years of launch will reach only 50 percent of their Web commerce objectives due to trading-partner distrust and the compromise of sensitive information (0.7 probability).

Over time, the enterprise security model will transform itself based on the prevailing technologies, cultures and perceived threats. In the mainframe era, enterprise security was based on the "fortress" model, meaning it was static and undifferentiated, difficult to change, location-specific, and reliant on strong walls and a locked gate.

The emerging "airport" security model is more flexible and situational, with multiple zones of security based on role. "Gates" to zones can employ multiple overlapping technologies for identification, authentication and access control. Simply put, the result is a series of fortresses within the fortress.

Point-to-point "dynamic trust" uses multiple overlapping or alternative technologies to ensure that a party to a transaction can directly identify and authenticate himself or herself to any other person, and prove his or her right to participate. This is the model for a world heavily populated with intelligent wireless devices. The point-to-point model is required for a world in which high levels of commerce are conducted wirelessly, anywhere, anytime.

Action Item: Evolve the enterprise security model over time to a point-to-point architecture.

2.1.5 The Information Security Hype Cycle

Tactical Guideline: Enterprises should evaluate the changing information security landscape in the context of their specific defensive requirements and avoid letting the vicissitudes of the Hype Cycle and the relative popularity of any particular security solution dictate plans.

Each new wave of technology disrupts security measures and introduces new vulnerabilities. Overlaying that local source of chaos, each new technology in the security, privacy and risk management domain follows the Hype Cycle (see Figure 2-4).

Determining when to adopt an emerging technology is a critical decision. If an enterprise launches its efforts too soon, it will suffer the painful and expensive lessons of deploying an immature technology. If it delays investment for too long, it 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 at the right time can leave the enterprise vulnerable.

Action Item: Investing in an overhyped technology too early can result in a complete waste of enterprise security funds. Enterprises should focus on their assessment of business needs and threats 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.

2.2 Security Functionality via Network Security Platforms

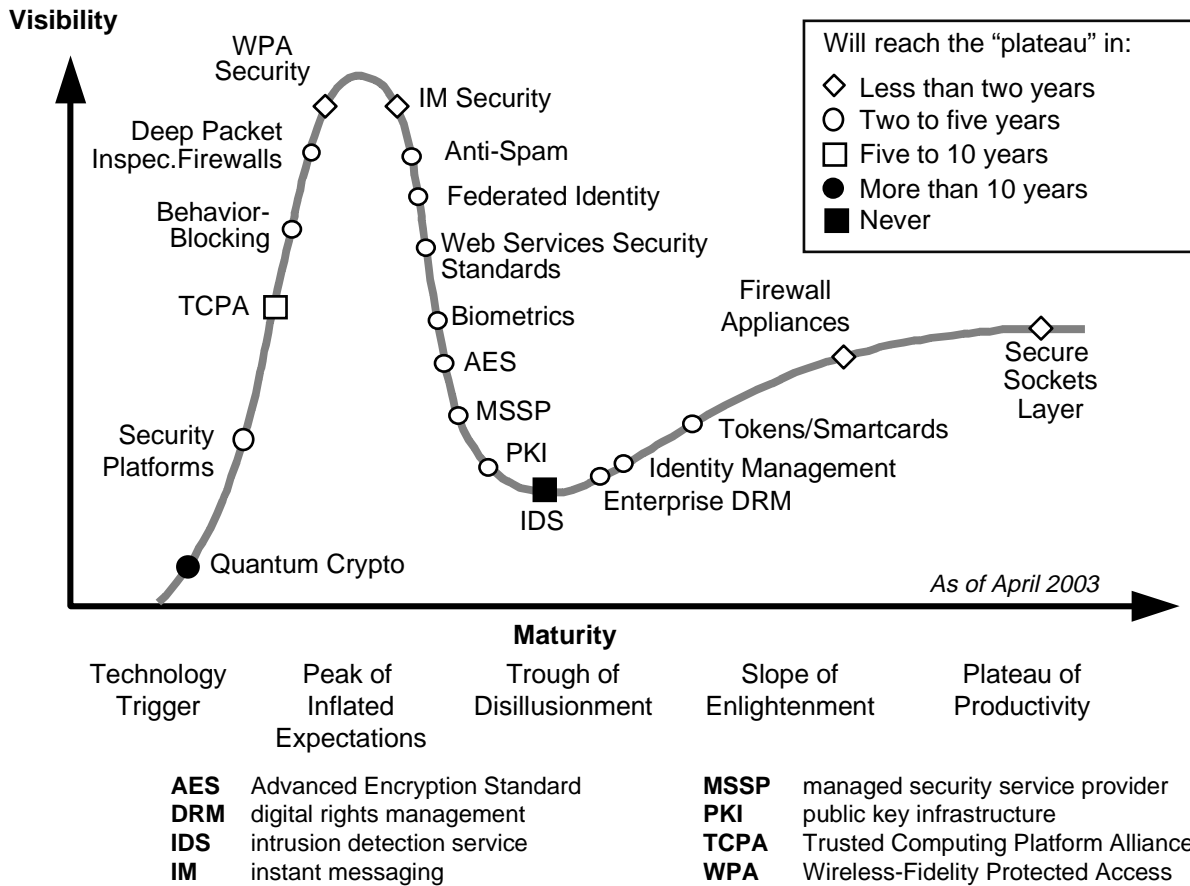
Key Issue: What information security solutions are offered to the market, and how are they evolving?

Strategic Planning Assumptions:

- By year-end 2004, advances in nonsignature-based intrusion detection technologies will enable network-based intrusion prevention to replace 50 percent of existing intrusion detection system deployments and capture 75 percent of all new deployments (0.6 probability).
- By 2006, 60 percent of firewall and intrusion detection functionality will be delivered via network security platforms (0.6 probability).

Enterprises face a degree of risk in attempting to bundle too many capabilities into security platforms or appliances (see Figure 2-5). Some of this can be attributed to the propensity of enterprises to acquire best-of-breed applications, or at least "best" for their security profile, regardless of source or product integration.

Figure 2-4: Gartner’s Information Security Hype Cycle



Source; Gartner

For example, an intrusion detection system (IDS) taxes resources because it requires full-time monitoring and an incident response process. IDSs, firewalls, vulnerability assessment tools and gateway antivirals are showing signs of combining into security platforms, generally on Linux platforms, with blade technology to add functions.

Suppliers, in turn, risk complexity in adding components that span buying centers, unless an enterprise/infrastructure value statement can be credibly made.

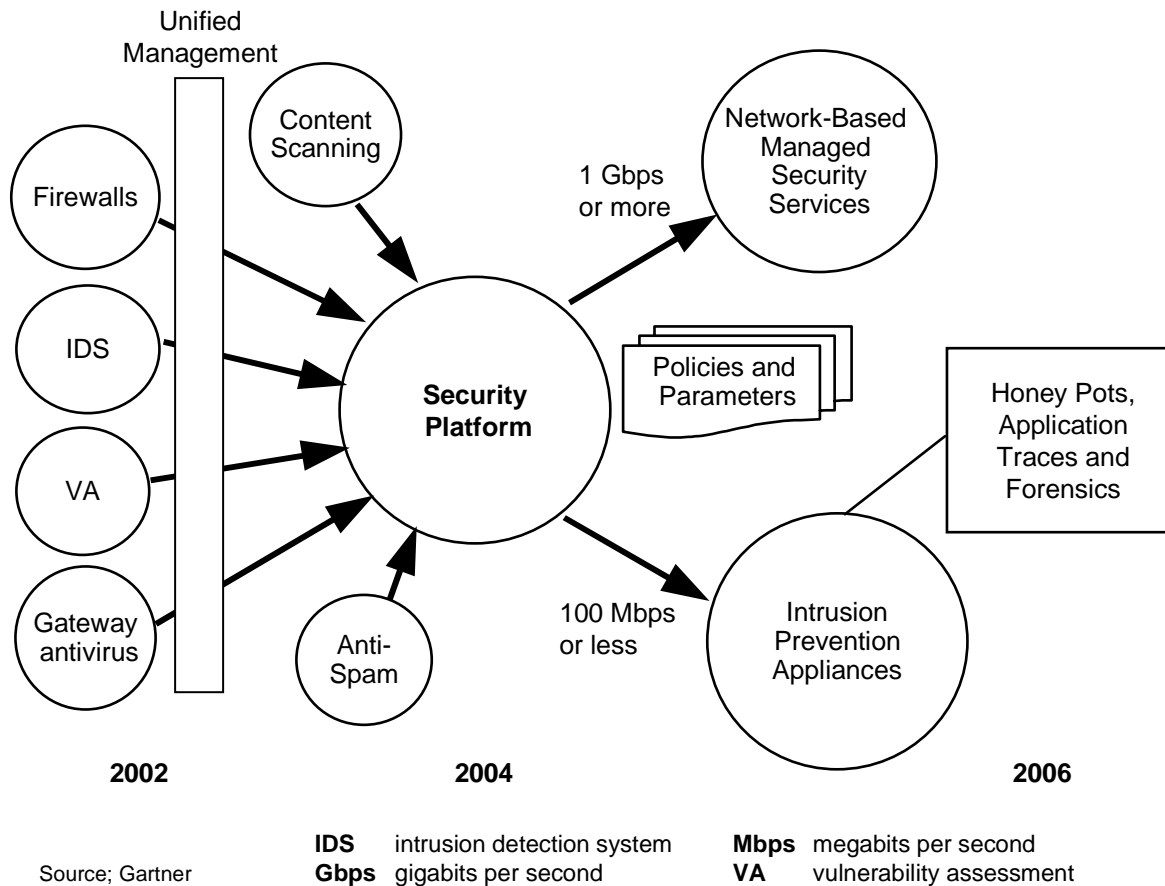
Some enterprises will see efficiencies using managed security service providers (MSSPs), while other enterprises will view the evolution toward intrusion prevention appliances appealing. Besides detecting patterns of problem traffic, MSSP services and appliances will use correlated algorithms to drop malicious traffic and will

eventually offer computer forensic capabilities to help prosecute threat agents.

A risk exists in attempting to bundle too many capabilities into security platforms or appliances. For example, most of the elements in Figure 2-5 represent network security responsibilities, but anti-spam and content scanning may fall to e-mail management. Enterprises show a preference for acquiring best-of-breed applications, or at least best for their security profile, regardless of source or product integration. Suppliers risk complexity in adding components that span buying centers, unless a strong enterprise or infrastructure value statement can be made.

Action Item: Work to build cross-disciplinary, cross-application owner awareness of security issues seeking synergy in future security solutions.

Figure 2-5: ‘Best of Breed’ Solutions Are Needed on Security Platforms



2.2.1 Consolidating Business Tools

Strategic Planning Assumptions:

- Through 2006, the IT security management market will comprise several submarkets that will be driven by loosely coupled buying centers within enterprises (0.7 probability).
- No single suite solution will capture more than 10 percent of the overall IT security management market (0.7 probability).

Integration is emerging as the name of the game. Though tools abound for consolidating the security management of networks and servers, the maturity of the market often requires significant integration for effective business tool use. As a result, growing from network and enterprise system management tools, the quest for integrated security “dashboards” and monitoring stations is on.

Similar to bundling products, there is supplier risk in cramming too many capabilities into these solutions.

In the initial stages, enterprises will need to build on existing systems, and pressure suppliers for standard interfaces and reporting standards — such as Simple Network Management Protocol (SNMP) and evolving XML (Extensible Markup Language) equivalents — plus correlation algorithms to allow for real-time monitoring of enterprise security, network and server performance across regions, and across communities of interest for mutual defense against common threats.

Helpful additions include:

- Volume measurements on e-mail systems to detect denial-of-service and spam attacks
- Web-server monitoring tools to check for unauthorized changes

- Content-scanning reporting tools
- URL blocking
- Vulnerability assessment
- Antiviral performance reporting

The problem of scope is apparent. With an excessive number of data points, and the need to tune sensitive sensors and to set triggering thresholds appropriately, centralized security reporting could easily overwhelm those responsible for monitoring the system with false alarms and uncorrelated data. Information must be extracted from the data, and knowledge must be derived from that information. Today, human operators provide those higher values.

Action Item: Avoid the “yet another monitor” syndrome by focusing on the action-oriented knowledge that network security monitors can bring to the enterprise.

2.2.2 The “Good Enough” Information Security Solution

Tactical Guideline: *Avoid vendors with overhyped but weak security products, or those with strong products but poor business practices. The best information security solution is often “good enough.”*

This is a time of great stress for information security practitioners. Factors such as the inhibiting effects of the economic downturn, buyers’ remorse over previous grand plan security initiatives, a defensive stance driven by modern political realities, continuing vulnerabilities, demands for privacy, and regulatory issues are creating great stress for information security practitioners. The result is that enterprises tend to implement “good enough” products and services while navigating through minefields of overpromoted products, or products so advanced that the need is not readily apparent.

The two vendor categories at the extreme ends of the market spectrum are most likely to fail (see Figure 2-6).

- “Smoke and mirrors” vendors hype their security solutions to drive business, but the failure to live up to that hype causes customer erosion.
- “Field of dreams” and “white coat” vendors have strong security solutions, but their business practices and

customer relationship management strategies make their products undesirable to most enterprises.

Enterprises are advised to identify products that fit between market share leaders in the “good enough” category and those with just enough proven, advanced technology to provide an edge against security threats.

Action Item: Enterprises should limit their procurement analyses to vendors with a good balance between business sense and knowledge of information security technologies.

2.2.3 The Outsourcing Option and Evaluating Security Providers

Strategic Planning Assumption: *By 2005, 60 percent of enterprises will outsource monitoring of at least one perimeter security technology (0.6 probability).*

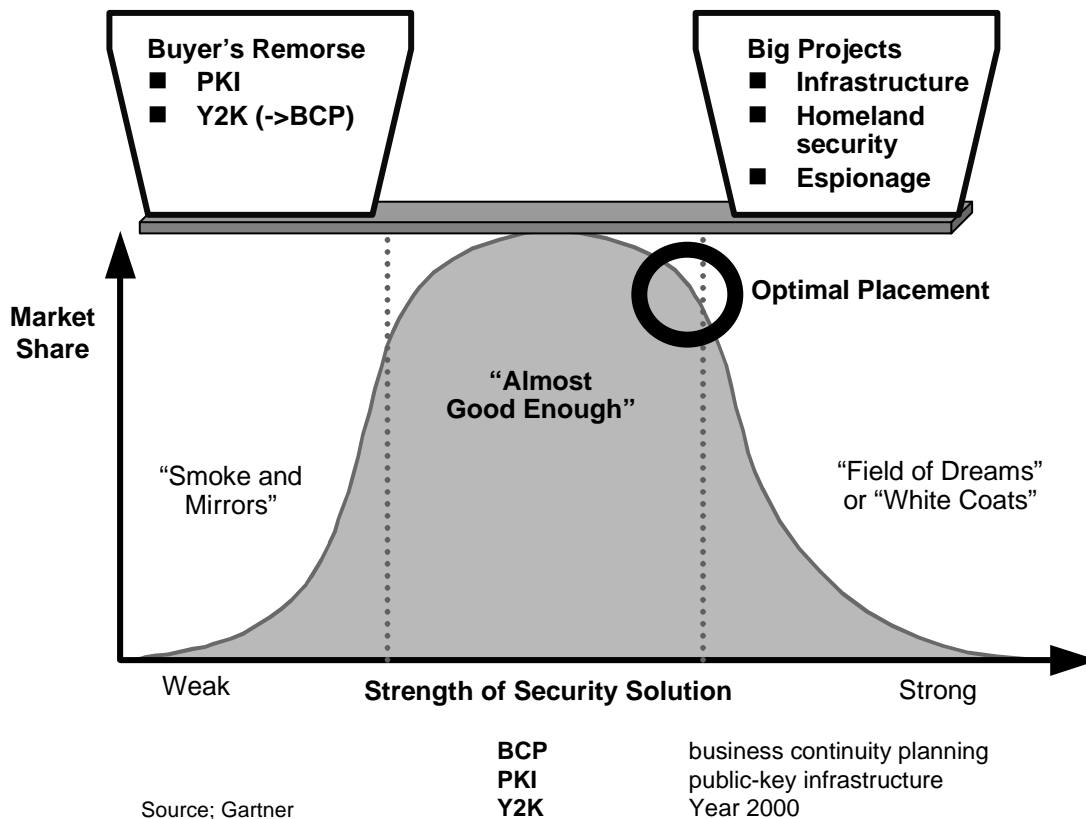
Most enterprises have focused attention on security functions that are designed to keep the “bad guys” out. But most enterprises do not have the resources to do an effective job keeping the “bad guys” out and letting the “good guys” in as demanded by e-commerce and business-to-business activities.

Outsourcing the “bad guy barrier” is a driver for the managed-security market but the market is still developing. Although a few vendors have been offering services for years, the past two years has brought growth in the number of vendors and the range of managed-service offerings. Processes for correlating security incidents across multiple MSSP customers remain based on human operators and network operations centers, but are maturing in the technology.

Target customers include those without core competencies in information security, enterprises that have addressed perimeter security and gained experience in putting their security architectures in place and who are looking for efficient operations — but not at the expense of their security postures.

Action Item: Evaluate MSSPs that have approximately 50 professional service professionals, because those companies are likely to become your enterprise security provider.

Figure 2-6: The Information Security Market Balancing Act



2.3 The Role of Government in Fighting Cybercrime

Strategic Planning Assumptions:

- *By 2006, increasing incidence of large-scale for-profit cybercrime conducted by terrorists and organized criminals will force governments to take an active role in promoting common defenses in cyberspace (0.6 probability).*
- *By 2007, widely accepted legal norms for assessing civil damages resulting from negligent information systems security will have been established in the United States, by statute or by case precedent (0.8 probability).*
- *By 2008, at least one such lawsuit will result in a judgment or settlement for more than \$10 million in favor of the plaintiffs (0.6 probability).*

The U.S. National Strategy to Secure Cyberspace proposed that the United States was in imminent danger of devastating cyberattacks by hostile nation-states and terrorists, and then said, in effect, that the government should take no active role in creating a common defense against such attacks. Simply put, either the rhetoric is overblown or the program is underpowered.

Though the “computers kill everybody” scenario is unlikely in the near future, there’s plenty of room for cyberattackers to operate at higher levels than seen to date. Any scenario that assumes that cyberattacks will just go away is unlikely.

Many ways exist to reduce the frequency and impact of successful attacks.

- Enterprises and users at every level can start paying attention to security basics — such as staying up to date with patches and antivirus definitions, using firewalls, using stronger passwords and other forms

of strong authentication — which is the equivalent of fastening seat belts before driving.

- Software vendors can produce software without gaping vulnerabilities.
- Governments, in turn, can take steps, regulatory or otherwise, to encourage such behaviors from vendors, enterprises and users.

As computer-enabled crimes and electronic surveillance by government, commercial enterprises, and even individuals, increase in frequency and severity, people everywhere are concerned about cyber-threats to their interests. U.S. businesses other than healthcare and financial services organizations are still essentially free to do what they like with information they gather on customers and other enterprises, but the tide is turning.

In early 2003 the European Union (EU) informed Microsoft that it had to revise business practices on Passport to conform to the Data Protection Directives. The EU's definition of privacy is likely to dominate in industrialized nations within five years. By year-end 2004, Gartner expects that 75 percent of enterprises will be required to provide security status information to multiple government agencies. Enterprises with immature security programs

will spend up to 15 percent of their security budget to comply, and will push back on software vendors to reduce the administrative costs that go with endless rounds of patches.

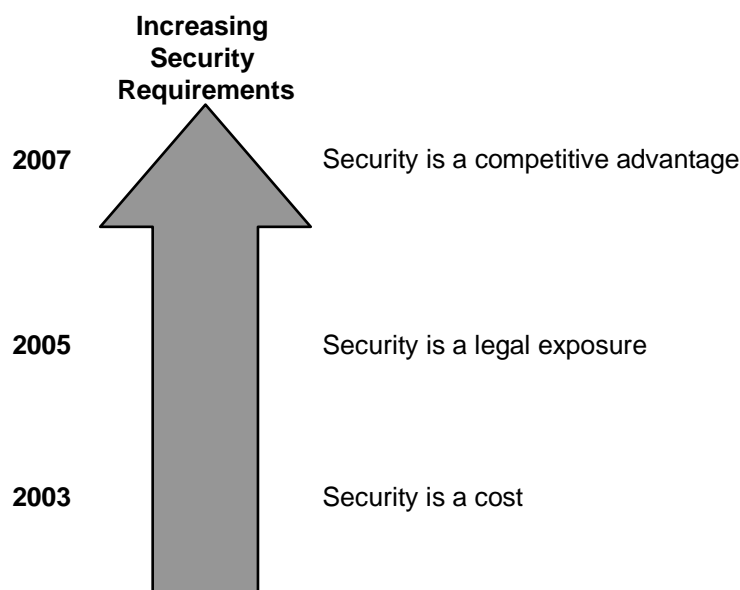
Even without regulatory requirements, Gartner estimates that the cost to mitigate the damage from a successful attack is at least 50 percent higher than the cost to prevent it. Enterprises that focus on real risks and pay attention to their program's risk-reduction effectiveness will receive the best return on their security investments.

Action Item: It's best and least expensive in the long term to develop a capable program before being forced to act by legislation.

2.4 The Business Value of Information Security

Tactical Guideline: *The business value of information security can be calculated on the basis of risk reduction, security as a (decreasing) cost of doing business, and return on investment via enhanced trust relationships and improved business opportunity.*

Figure 2-7: The Business Value of Information Security



Source: Gartner

In today's environment, many boards of directors and CEOs need little convincing that risk reduction — for example, via improved security — is worth the money (see Figure 2-7). The tribulations of New York-based businesses and their employees during the Sept. 11 disaster drove home the importance of business continuity planning.

The Sarbanes-Oxley Act of 2002 has convinced corporate officers of the wisdom of investment to secure critical business information against unauthorized access, internal or external. Soon, civil liability for insecure software and lax security will convince remaining laggards that security really does matter.

Few enterprises that have strong security will brag about it publicly. Instead, code words such as “risk” and “trust” will be used to signal superior security to markets, trading partners and customers. In any case, unsecured enterprises will face higher costs from poorly administered, expensive security programs, intellectual property losses, theft and lawsuits. Superior security is a competitive advantage, and poor security will be increasingly disadvantageous.

2.5 Security Is a Process, Not a State

Certain laws will operate continuously throughout the next five years:

- Moore's Law, which specifies rapid growth in the lowering price and increasing power of transistors
- Metcalfe's Law, which describes the utility of a network as the square of the number of nodes on the network
- Guilder's Law, which specifies a rapid rate of growth in bandwidth availability

The result will be a man-made environment that is dense in intelligent, communicative machines, which is what Gartner calls a “World Without Secrets.” New computing and network technologies will continue to render security technologies and architectures obsolete or irrelevant. New vulnerabilities will spawn new attacks, and defenders will be forced to adapt, over and over.

The world, including its computer networks, will remain a very dangerous place, especially for the unprotected. Security administrators and vendors, citizens and

governments will continue to struggle for a lead against increasingly capable cybercriminals. If not, they will lose.

Security is a process, not a state, so enterprises must take steps to guard against security threats:

- Monitor — Stay abreast of the latest threats, internal and external
- Assess — Stay abreast of the latest defenses and their effectiveness for the enterprise
- Act — Continuously rebalance risks and defenses

2.6 Information Security Marketplace Summary

After the dot-com failure, the tragedy of Sept. 11, the recurring events causing distrust in institutions, the economic downturn and the uncertainties of the world climate, few enterprises have had the will or spirit to invest aggressively in their IT infrastructures unless absolutely necessary. Instead, the trend has been toward tactical steps. However, each of those events signals the need to respond.

Furthermore, and perhaps more importantly, new laws and regulations in healthcare, financial services and education — as well as the laws covering corporate responsibility and privacy — suggest that enterprises will face higher levels of accountability than ever before, requiring adequate security protections throughout an enterprise.

New platforms and new styles of doing business have been developed, but they have come at the cost of inadequate security, which now must be added. Technology providers should assume that they are at risk for legal liability if their products and services are inadequate with regard to security metrics. Cyclical economic downturns are opportunities to be reflective and creative, a time to clear out old thinking and old systems, and to be economical in doing what needs to be done.

Enterprises should rise above the tactical, patch-oriented approaches of the past. They should plan for and implement holistic security programs to meet legal and moral requirements for due care, due diligence and adequacy in their information protection programs.

2.7 Recommendations

- Enterprises should assume that legal liability for poor security practices is on the horizon, and act accordingly.
- Security market providers and software vendors should assume that insecure products and services will be the basis of future legal liability claims.
- Enterprises should develop an enterprisewide, cross-application view of their information security requirements, beginning with policies and cultural change.