GartnerG2

REPORT

January 2002

Prioritizing Security Efforts: Create Structure from Disorder

Viewpoint

Executives face many complex decisions about where to prioritize finite security efforts and spending.

GartnerG2's "Security Rationalization Model" can help you make these difficult decisions.

Dynamics

- A security program is meant to protect your organization's information, physical and human assets.
- Structuring an appropriate security program begins by assessing your company's six "Security Response Categories."
- Your company's security profile will help you determine how and where to make the most effective security investments.

Predictions

- Too many organizations will under-assess the dimensions of risk, assets, and environment because they lack a decision framework.
- Companies will be tempted to view all *security response categories* equally, resulting in overly expensive security programs.
- Most businesses will include security requirements in contracts with any new partner using electronic channels.

Recommendations

- Complete the GartnerG2 "Security Rationalization Model" to determine security priorities as percentages of security spending.
- Begin reporting security and privacy to a board of directors subcommittee. Raise accountability to the executive level.
- Enact security awareness programs among employees. Assure that IT conforms to baseline technical security standards.

Dig Deeper

- Related Research from GartnerG2
- Gartner Core Research
- Methodology

Rich Mogull

"Two essential factors to consider are the degree of technology solutions and the management structure needed to support security."

Viewpoint

It's not just how much you spend

Data and network security is a chess game of compromises, of finding the balance between getting work done and keeping the enterprise safe. For an executive making security decisions, the road ahead is a tough one. Consultants and vendors can recommend dozens of security measures and technologies, but it is difficult to determine the appropriate balance of security measures at an appropriate cost for the enterprise.

This report guides the executive through the security management prioritization and structuring process. It is designed to help you determine *where* to prioritize and *how* to structure, not *how much* to spend.

Know yourself as you know your enemy

To properly prioritize and structure your security efforts you need an understanding of your company, and the environment it operates within. This can be done using external audits by security experts and consultants, but limited tools are available to assist the general manager in evaluating the results or determining the scale of any external engagements before they begin.

The first step is to know yourself. Look at the following six "Security Profile Model" categories:

- **Enterprise profile:** Consider core information: your organization's size, distribution, degree of regulation and holding status (public or private)
- **Asset profile:** Security is about protecting your assets and your ability to do business. The nature of your assets will change your risk, the threats, and the optimum ways to protect them.
- **Cultural profile:** Company culture is the single most important factor in defending the enterprise. Understanding how security is perceived and how the organization responds to security at all levels is essential.
- **Technology environment profile:** You don't need to know the technical specifics of your company's enabling technologies, but it is important to understand in general terms how the company depends on key technologies.
- **Relationships profile:** No business operates in a vacuum. Relationships to other companies, the government, and customers directly affect security.
- **Existing security profile:** This is more about policies, plans, programs, education, and structure than any use of particular technologies.

Dynamics

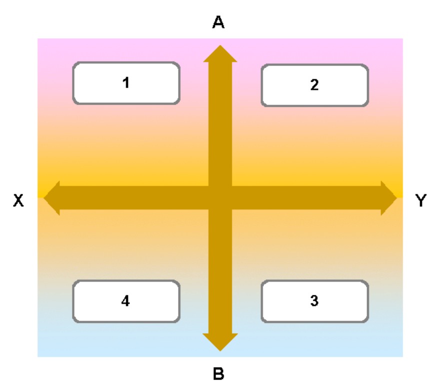
Where to spend time and money

From a structure perspective, we break security down into six broad "Security Response Categories":

- **Policies and plans:** The "prep work" and "corporate laws" that define enterprise security on paper and serve as a roadmap. This includes high-level policies, detailed plans, guidelines and procedures.

- **People and management:** the human side of security, including who to hire, how to educate personnel, and how to manage the process.
- **Technology:** the hardware and software—sometimes involving the exploration or development of new technologies.
- **Risk management:** the process, plans, and tools needed to mitigate known and unknown risks. In some cases it will be a business continuity plan; in others, fraud prevention mechanisms.
- **Physical security:** The security for physical assets and facilities, including security forces and the technologies (like access cards) of physical security.
- **Auditing, testing, and monitoring:** The feedback to measure the health of the enterprise and effectiveness of security efforts. In some cases, it involves penetration testing to test security; in others, audit systems to limit fraud.

Figure 1: Prioritization map with numbered quadrants



Source: GartnerG2, January 2002

The enterprise profile

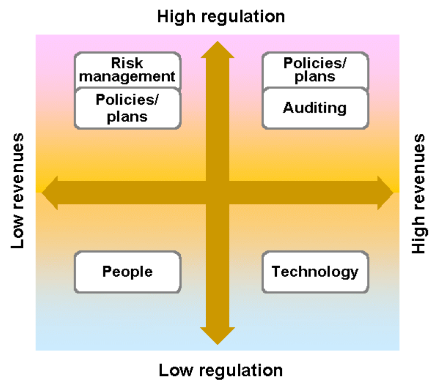
The e*nterprise profile* helps you examine some essential parameters of your company, agency or department, and how you do business. It helps in determining how to approach the security structure from a “common sense” standpoint. For example, some larger companies operate globally, and face more legal and cultural issues. On the other hand, smaller companies with a single location may not be able to survive a catastrophic event. Key information to consider includes:

- Corporate revenues
- Degree of industry regulation
- Number of employees
- Number of office/work sites
- Number of countries in which you do business
- Are you public or private?

- Stakeholder tolerance for risk

Let's break down two of the more important factors, *corporate revenues* and *degree of industry regulation*, and show how their relationship affects the prioritization process:

Figure 2: Revenues and regulation



Source: GartnerG2, January 2002

1. Small companies in a highly regulated industry need policies and audits. They are probably less problem-tolerant, so risk management and business continuity takes a slightly higher priority than policies.
2. Large companies in highly regulated industries need to place a high priority first on policies and plans, and then on auditing, to ensure legal compliance and to limit internal fraud.
3. Large companies in less regulated industries might find they invest more in technology, especially if they have higher turnover rates and concerns about the loyalties of a liquid workforce.
4. Small companies in less regulated industries should place more of an emphasis on people and corporate culture, since there are fewer resources to manage and less to spend on security.

Caveat: This is not to say that any company can ignore all other aspects of security. This is a framework for *prioritization*, not inclusion or exclusion.

The asset profile

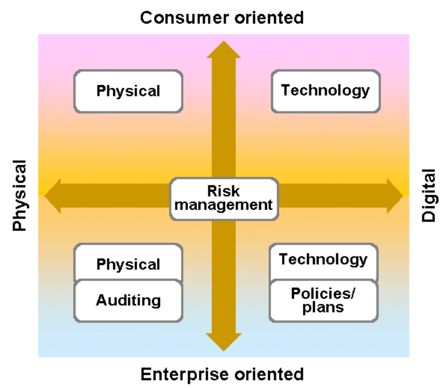
The a*sset profile* involves classifying assets, including the often-critical *intangible assets*. The *asset profile* is less about inventory and more about classification of the full array of corporate assets. A large retail operation that depends on consumer physical assets, for example, needs more physical security. A media company that depends on consumer digital content and distribution should invest more in technology solutions. The volume of assets plays a role, but the nature of the assets often offset the importance of volume. Key questions to consider:

- Are principal assets physical, information, or human? (Information assets are recorded and reusable. Human assets—knowledge workers—are hard to replace.)

- Are assets consumer-oriented or company-oriented?
- How closely tied are physical, human and information assets (e.g. online only retailer vs. traditional retailer without an online ordering system)?
- Do assets include regulated information (e.g. financial, medical)?
- Can assets easily be re-distributed? (e.g. digital music)?
- Do material assets include client databases with sensitive information (non-public personal information)?

Let's examine the interaction between two of the more important element, the *nature* of an asset (physical vs. digital), and its *target market* (consumer vs. *corporate*):

Figure 3: Nature and market



Source: GartnerG2, January 2002

In dealing with assets, either physical or digital, risk management (particularly insurance) is of paramount importance. The degree and nature of risk management (insurance vs. disaster recovery) will vary based on company resources and the nature of the asset.

- Companies with extensive consumer-oriented physical assets, such as retail stores, should emphasize physical security—including electronic solutions like cameras and anti-theft tags—since their greatest risk is from shoplifting or employee theft.
- Although electronic copyright protection has limited effectiveness in protecting highly portable digital assets such as music, video or software, it *can* help reduce losses. Companies with such assets need to take a hard look at technology security solutions. Since no copyright protection software is invulnerable, another important aspect of risk management will be to design a business model that accounts for loss.
- Businesses that depend on corporate-oriented digital assets need to invest in security products that protect their information repositories. Generally, loss of individual information items will have little impact on the overall health of the enterprise. Protecting against the loss of major repositories with large amounts of data is of greater concern.

- Physical security is still important. While corporate-oriented physical assets, such as servers and manufacturing equipment, are typically of higher value than consumer assets, they are difficult for an external attacker to steal. The greatest risk to such assets is from accidental loss or internal theft. Therefore, auditing, monitoring and tracking tools and processes should take top priority.

Cultural profile

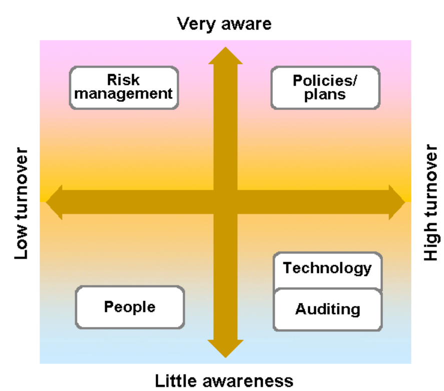
Corporate culture is the most important element to effective security within a company. A strong understanding and appreciation of the need for security among employees can help offset deficiencies in other areas. It can reduce losses as well as save on other security expenditures. As powerful as such a culture is, however, it can be difficult to measure. And if it doesn't already exist, it can be difficult to develop. When examining culture, ask these questions:

- How "security aware" are employees, management, executives, and the board of directors?
- What is the rate of turnover?
- Do employees know how to recognize security issues?
- Would they be willing to report or respond to these issues?
- Do they know how/where to report problems?
- How does management respond to reported problems?

If employees are willing to challenge visitors, ancillary workers (housekeeping, delivery), *and* known coworkers who neglect to wear a security badge, it indicates a positive physical security culture. Likewise, if employees report suspicious e-mail (not just viruses) to security management, it is also indicative of a positive information security culture.

Two critical cultural factors that affect the environment the most are security awareness and turnover rates:

Figure 4: Awareness and turnover



Source: GartnerG2, January 2002

1. The most secure companies are extremely security-aware and have low turnover rates, thus maintaining a stable culture. Such companies need to examine their risk-management efforts to ensure business continuity should they be struck by an event, such as a natural

disaster, that overwhelms the culture.

2. Highly aware companies with high turnover risk losing security awareness if new employees don’t feel personally vested in the well-being of the organization. Such organizations should develop policies to maintain security awareness despite personnel turnover.

3. In situations with high turnover and limited awareness, security is at serious risk. Employees don’t recognize security issues, nor do they have much personal investment in the enterprise. Technology can compensate somewhat for a liquid workforce, and extensive auditing—integrated into business process—can limit loss through checks and balances.

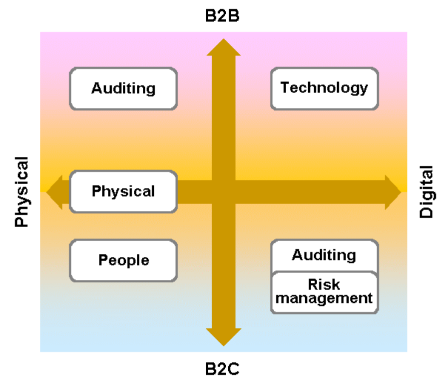
4. Companies with little turnover and little awareness can benefit most from educating existing employees. Stability enhances the ability to develop a more conscious security culture.

Relationships profile

Business is about relationships-—with clients, partners, suppliers, and even the government and the press. Relationships may open new business opportunities, but every new door opened complicates the security environment. In examining relationships, consider the *source*, and the *nature* of the relationship. A real-time Internet interaction with a consumer in the e-commerce world is quite different from a paper-based business-to-business exchange.

- How dependent is the company on business-to-business and business-to-consumer relationships?
- Is the relationship more dependent on physical or digital channels?
- Do business relationships depend heavily on electronic data exchange over networks?
- Does the company depend on real-time interactions with customers, suppliers, or partners using electronic systems?
- Are relationships more dependent on physical interactions such as retail transactions, mail, paper exchanges, or shipping of materials?
- What is the sensitivity of information exchanged in the relationship? Is it openly available, or non-public, personal information?

Figure 5: Channel and target



Source: GartnerG2, January 2002

1. In B2B relationships over physical channels, such as for services or supplies, it is important to audit for channel continuity. A breakdown in the delivery of goods or services can seriously damage the relationship. Careful auditing can also reduce the likelihood of fraud—on either side. Physical security is a secondary priority to auditing, but necessary, especially with the exchange of goods.

2. A B2B relationship over electronic channels needs greater investment in technologies to secure the channel from attack and error. Many of these relationships involve automated data exchange where a single small error can have dramatically negative (and material) results. An unsecured electronic channel can be a gold mine to a competitor or malicious attacker.

3. Auditing for incidents and fraud is critical for risk management to work effectively in consumer-oriented digital relationships. A consumer relationship using digital channels faces some of the greatest risks, it is impossible to prevent fraud and consumer relationships tend to be volatile. Security breaches will happen, and risk management (including fraud prevention) is essential. Although technical security is important, it does not rate highly in this model because the need can be met with baseline controls.

4. Employees are the best defense in consumer relationships over physical channels. Because of the greater reliance on face-to-face contact, well-trained and aware employees can have a dramatic impact on limiting loss and maintaining positive relationships.

Technology environment and existing security

Your technology environment includes the myriad of systems and devices you use to enhance your business. Assessing your technology environment isn't about inventories of hardware and software; it's about the degree to which you use and depend on major technologies. Two key factors to consider are the reliance on desktop PCs, and the access of systems to the Internet.

Existing security includes more than just firewalls and access badges. It includes policies, organizational structure, training, incident response, and procedures as well as key technologies for information and physical security. Security can rarely be determined by looking at a balance sheet. Often, security programs are incorporated into a variety of business units without any centralized reporting. Two essential factors to consider are the degree of technology solutions (firewalls, strong authentication) and the management structure needed to support security (dedicated office vs. no central management).

Predictions

- **Too many organizations will under-assess the dimensions of risk, assets, and environment because they lack a decision framework.** Important factors will be missed, resulting in wasted spending or preventable security incidents with material loss. Internal security assessments focus on known gaps, and fail to balance enterprise needs due to "tunnel vision".
- **Companies will be tempted to view all *security response categories* equally, resulting in overly expensive security programs.** Executive mandates to "improve security" will result in wasteful bottom-up spending to fill perceived gaps without understanding the overall security needs of the enterprise.
- **Most enterprises will include security requirements in contracts with any new partner using electronic channels.** Security on both sides of a relationship will be established formally as blind trust in partners fails.

Recommendations

- **Complete the GartnerG2 "Security Rationalization Model" to determine security priorities as percentages of security spending** While this framework describes a thought process for examining enterprise security, it is not a substitute for the underlying model, and the model is not a substitute for engaging security professionals. Use the model to self-analyze and look for major gaps. Use professionals to fill those gaps. The model will provide you with specific percentages of security spending to devote to the *security response* categories. The framework and model will also help you ask internal and external security experts the right questions.
- **Begin reporting security and privacy to a board of directors subcommittee. Raise accountability to the executive level.** Security and privacy cannot be managed solely at the information technology level. It requires board oversight. Assign formal responsibility within the board of directors, and place accountability with an executive-level office—the chief security officer, chief information security officer, chief operating officer, chief executive officer or risk management officer.
- **Enact security awareness programs among employees. Assure that IT conforms to baseline technical security standards.** Create a "Security Aware Enterprise" (see Dig Deeper) through education and awareness programs to assure that employees are security assets, not security liabilities. Implement baseline technical security, such as installing the latest software patches, properly configuring firewalls, and removing outdated system accounts. See GartnerG2 and Core research for specific guidelines.
- **Brainstorm all material corporate intangible assets and get a balance sheet list of tangibles. List current protection next to each.** The goal of security is to protect assets, tangible or intangible, and business continuity. Immediate gaps can be discovered through intensive analysis of assets and the protections allocated to them.

Dig Deeper

Related Research from GartnerG2

Report: Building the Security-Aware Enterprise
By Rich Mogull *(15 January 2002)*

Gartner Core Research

Cyberattacks, Prepare Your Enterprise Now
By Rich Mogull *(20 September 2001)*

Summary: A significant increase in cyberattacks is likely to follow the events of 11 September 2001. Enterprises must understand this threat and take action to limit their vulnerabilities.

The Price of Information Security
By Roberta Witty, John Girard, Joyce Graff, Arabella Hallawell, Bradley Hildreth. Neil MacDonald, William Malik, John Pescatore, Martin Reynolds, Kathryn Russell, Vic Wheatman, John Dubiel, Alan Weintraub *(8 June 2001)*

Summary: This report is Gartner's first release of the total cost of ownership for Information Security model—best practices for information security expenditures, including the costs for people, hardware, software, external services and physical security for all information security activities in which an enterprise might be engaged.

Methodology

Findings are based on industry experience of Gartner G2 analysts, conversations with vendors and clients, and supporting Gartner Core research.