Creating a Security Architecture: Introduction

Steve Hunt

Contributing Analysts: Gene Leganza, Phil Rosch and Michael Rasmussen

Giga Position

The security architecture is a framework of processes, documents and technical descriptions in support of the business security requirements. Creating the architecture grows out of the company’s vision and draws on the efforts of many individuals within an organization. The technical guidance included in the architecture documents relates well to the needs of the business.

However, most organizations suffer inefficiencies, lack of direction and overall ineffectiveness in their security organizations due to incoherent or non-existent security architectures. IT strategy and architecture teams generally do a bad job including comprehensive security requirements in their own documents. Only by sheer good fortune do organizations avoid catastrophe. Not surprisingly, many security managers and CIOs are reconsidering how much luck they can tolerate and, conversely, how much they would rather be prepared. A well-considered security architecture is the first and best security measure to deploy.

Proof/Notes

Imagine how ineffective a security operation might be if staff spent most of their time chasing technical vulnerabilities with technical fixes, or if no one knows how or when to upgrade patches on operating systems and firewalls? Left to their own devices, IT security staff will overengineer security, attempting to plug every hole to the extent of their budget and abilities, regardless of whether that hole represents a measurable threat to the business. But this is exactly how most organizations operate their internal security practice.

The purpose of creating a security architecture is to avoid the “firefighter” culture of IT security, maximize the time and efforts of security staff and ensure that all technical measures actually map to and derive from genuine business requirements. Done properly, the architecture will formalize and clarify the business and technical requirements for security and risk management for the benefit of security and technical staff of various agencies and business units throughout the organization (for more information about understanding business needs, see Planning Assumption, Business Risk Management: The Business Language of Security, Steve Hunt).

Many people will use the security architecture for a variety of specific uses. As such, the process of creating the architecture requires writing a usable architecture document. The document will describe the current state of security, both technically and organizationally, and discuss the steps required to reach a desired state. Those steps will conform to identified standards, regulations and limitations, always reflecting the categories and principles of good security.

Architecture is a process, not a project. It uses security and technology as its vernacular, but focuses on the business requirements and, most importantly, critical application platforms. It is influenced by and synthesizes many forces, such as corporate culture, industry practices, regulations and published best practices, to name a few (see Figure 1).
Creating the Document

Begin the architecture process by laying out a document with at least five sections: principles, direction, standards, blueprints and metrics:

**Principles**
The security architecture document should begin with introductory principles, or a mission statement. We have seen these opening words written very succinctly, or in a verbose way. Either way, write the mission statement in a style most familiar and most easily received in your corporate culture. Here are examples:

“Nirvana Corporation aims to grow shareholder value by minimizing risk whenever appropriate, and by improving operational efficiency, thereby reducing costs and simultaneously closing windows of opportunities for bad things to happen.”

Or the more pithy, “Reuse before you buy, buy before you build and build for reuse.”

Statements like these set the tone for the whole document. All readers clearly understand that their respective responsibility lies in maximizing shareholder value by coherent and cost-effective efforts.

**Direction**
The second section of the document should detail the business requirements and the drivers or the thinking behind those requirements. Organize the requirements by business unit, customer type or any other category that makes sense. This is where the input of business unit managers, executives and product managers is most crucial.

**Blueprints**
Just like it sounds, this section consists of network diagrams, technical descriptions, techniques, etc. that are relevant to the technical deployment of security measures. It will list the locations and descriptions of major network segments (demilitarized zone (DMZ), various local area networks (LANs), remote offices, etc.),
each security device (router, switch, firewall, sensor) and significant servers and resources (mainframe, application servers, data repositories). The technical descriptions will detail configurations, data flow and the nature or purpose of each device.

This section must also include a subsection on security maintenance, that is, who is responsible for updating, upgrading, configuring and/or physically managing each device, and service-level agreements (SLAs) for doing so in a timely manner.

Standards
All security decisions are influenced to some extent by standards, ranging from relevant government regulations (e.g., the US Health Insurance Portability and Accountability Act (HIPAA)), specific industry requirements (e.g., the US Gramm-Leach-Bliley Act (GLBA)), international standards (e.g., International Standards Organization (ISO)) and certainly internal organizational standard practices (see Types of Internal Standards, below). Standards guide the functional behavior of working parts and link services and technology to their users. They provide the scope and criteria through which the technology decisions are identified, created and selected.

Metrics
At some point, both the business side of the house and IT will be interested in measuring the success and performance of the security measures and processes. Giga’s recommended areas to be measured fall into seven categories and may be thought of as viewing the organization from the customer’s point of view, an operational view, an innovation and learning view, and a financial view:

1. Awareness and communications (customer view): Every security organization will improve its effectiveness if it can garner the support of the employees. Awareness programs, including posters, lunchtime workshops, e-learning, etc., can create an environment where employees are “security deputies.” Also, some companies offer an intranet security information Web site to great effect. Approaches include:
   a. Awareness program
   b. Compliance manual
   c. Security manual
   d. Security Web site
   e. Customer satisfaction

2. Administration and technical support (operational view): Organizations should measure how long it takes and how much it costs to add, modify or delete user profiles or to update systems with changes or patches. Service levels should be created for customer-facing products and services. Areas to consider are:
   a. Rights and privileges
   b. Change management
   c. Problem management
   d. Configuration management

3. Architecture and standards (operational view): The primary metric of success in the creation of an architecture and standards program is the overall reduction in products/vendors. IT complexity exacerbates the cost and recovery times of an effective security program. Life-cycle management tracks products as emerging, mature, declining or obsolete. Areas to evaluate include:
   a. Security architecture
4. Policies, practices and procedures (operational view): Each policy and the resulting practices and procedures must have a business case supporting its creation and a carrying cost to maintain the policy. Metrics around the carrying cost of policies and the extent to which they influence behavior are essential to maintain support of the business units that capitalize on the security program. Evaluations include:
   a. Policy development process
   b. Risk assessment

5. Organization and planning (innovation and learning view): The importance of the depth and quality of staff metrics was driven home to many organizations after the Sept. 11 tragedy. Metrics around depth and learning will indicate gaps in emergency coverage of key personnel. Areas to review include:
   a. Quality of staff
   b. Skills and bench strength
   c. Reporting relationships
   d. Education program
   e. Business requirements process
   f. Education

6. Financials and metrics (financial view): Ultimately, all organizations’ products and services will be measured in terms of expense and effectiveness in meeting the organization’s goals. Unit costs and product costs for all security products services must be tracked to determine the impact of optimization efforts. While Giga recommends a “corporate tax” expense recovery methodology, we also recommend that unit costs and service levels be measured as if they had to stand the scrutiny of a chargeback cost-recovery environment with unhappy customers. Look at:
   a. Funding
   b. Staffing
   c. Cost recovery
   d. Operational
   e. Financial

7. Audit (financial view): Audit controls and metrics are an integral part of all business functions and an even greater part of an effective security program. Auditors and security staff are in the same business: protecting the assets of the company. The extent of their ability to collaborate effectively has an ongoing effect on crafting the goals of the security program. Be sure to have controls in place.

**Scoring**

By comparing scores in progressive assessments, the security manager can draw a fairly accurate picture of the areas for improvement and the progress already made. We suggest tracking relative scores in each area along with background information, implications and recommendations as shown in the table below. From one assessment to the next, the security manager or chief security officer should be able to see clear improvements or degradations in service.
Collaborative Roles

The process of creating the security architecture actually includes many phases and deliverables, not just the writing of a single document. First, there will be many people representing a variety of organization roles who will contribute to the process. For example, liaisons from each business unit will work with the CIO’s strategy team, or equivalent, to articulate the business requirements. Technical and marketing-oriented product managers will add the functional requirements of the major applications. And various IT staff will contribute setup and support mechanisms as well as a rollout plan (see Figure 2). For more detail on the collaborative nature of architecture, see Planning Assumption, A Collaborative Architecture Development Model, Jost Hoppermann and Randy Heffner.

Types of Internal Standards

Giga has identified four common types of product standards, descriptively named (1) Custom, (2) Buffet Table, (3) Must Use and (4) Sunset Rules. They describe which products may be used, by whom and under what conditions:
1. Custom: These standards are applicable only to specific business units, in a one-off manner. For example, the help desk, in particular, will use such-and-such Remedy products. Or the IT security administration team will use BMC’s Control-SA. These are Custom standards.

2. Buffet Table: This is a variation on the Custom standard. Just like a smorgasbord that gives you many options to choose from, the Buffet Table standard will provide a comprehensive list of approved products for a particular task or function. For example, business units may deploy a Web single sign-on function using any one of the follow products: Netegrity Siteminder, IBM/Tivoli Identity Manager or Entrust GetAccess.

3. Must Use: This is the converse of the Buffet Table. In this case, one discrete product is mandated. For example, Unix servers must run Sun Solaris version 9., or desktop systems must use Microsoft Windows XP operating system.

4. Sunset Rules: Every organization will have some legacy products that may be in the process of being discontinued. In this case, Sunset Rules are listed. These are the products on “life support” only. No new development, upgrades or acquisitions are allowed. Network Associates’ Gauntlet Firewall or PGP software may be on such a list, since both products have been canceled from the vendor’s product line.

Alternative View

The main assumption we have made in our position is that a company or organization will achieve greater efficiency and effectiveness with a coherent security architecture process and document than it would without. Yet, there certainly are organizations for which this would not apply. When the CIO or some other manager is well versed in the requirements of the business units, and he or she is also the manager of a tightly organized security team, the security architecture may simply be an element of the existing IT strategy and architecture initiatives. In fact, this may be the perfect world. A security program certainly should be a reflection of the enterprise architecture.

Findings

Most organizations do not have a security architecture, or do not have an effective one. Organizations will avoid dangerous gaps in the security topology and the risk of overengineering the environment far beyond the requirements of the business if there is a well-constructed and coherent security architecture document and process in place. Improving efficiency not only reduces effort and cost, but also closes windows of opportunity for bad things to happen.

Recommendations

Build the day-to-day security defenses around a thoughtful security architecture that is efficient and effective in light of business requirements. Draw the requirements from business requirements, industry practices, standards and regulations, pertinent legal issues, the needs of your business partners and externally published best practices.

Write out the architecture in clear and usable documents describing the current state and the steps toward the desired state in several categories or chapters: principles, direction, standards, blueprints and metrics.

Involve a variety of individuals, from business units, corporate management and throughout IT, including business unit liaisons, the CIO’s strategy team, standards teams, product managers (both technical and marketing) and IT education and support staff.

Articulate standards from a functional point of view, as well as a technical or compliance point of view. Group standards by government, industry, international quality and internal. Label standards as some variation of Custom, Must Use, Buffet Table and Sunset Rules.
References

Related Giga Research
Planning Assumptions
Business Risk Management: The Business Language of Security, Steve Hunt
A Collaborative Architecture Development Model, Jost Hoppermann and Randy Heffner
Best Practices in Managing IT Security, Steve Hunt and Phil Rosch
Optimal Extranet Security: A Methodology, Steve Hunt
 Structures and Processes for Effective Enterprise Architectures, Gene Leganza
The Evolution of the Firewall, Steve Hunt
Security Maintenance — Essential Components in Security Architectures, Michael Rusmussen

IdeaBytes
Common Mistakes in Application Architecture and Design, Randy Heffner
Best Practices in Security: Buy vs. Build Staffing, Phil Rosch
Defining the Chief Security Officer — a Position Description, Phil Rosch