

Designing a Security Architecture

By Richard Williams

Information Security has become a top priority for many enterprises. Whether mandated by external regulations or by executive orders, many MIS/IT/Information Security teams are now working to create an effective information security architecture. In this article, we will examine issues that face every enterprise, including analysis and planning, prioritizing, and creating an auditable plan to protect the enterprise from the "inside out." The article will include topical information, including the following:

- ▲ Understanding security
- ▲ Evaluating threat/vs asset value
- ▲ Creating an architecture which fits the business framework
- ▲ A layered examination of security, including network access, application access, external access, and physical access

This article contains a sample of issues an IT administrator will contend with, along with resources to links to go further. Because of the difficulty to create detail in the scope of the article, a "where to go for more information" hyperlink table of additional useful information will also be included at the end of the article.

Understanding Security

Security architecture differs from other kinds of security in that it assesses then addresses enterprise requirements from a strategic (as opposed to tactical) perspective. When possible, the ability to understand your security requirements should be attained and planned-in before specific security issues are implemented. To know the enemy is beneficial, but it is equally important to know your own assets, where they are deployed, and their worth in your enterprise. Here is a look at how this might break down:

You are creating a protection plan for your company's "crown jewels." Often these include critical and proprietary information located on computers and other information systems within

your enterprise. You need to protect the information, as well as the computer/information systems, from various kinds of attacks, damage, and loss.

To know the enemy is beneficial, but it is equally important to know your own assets, where they are deployed, and their worth in your enterprise.

We are now looking through multiple perspectives, including external access and physical security, network security, application and computer-specific security, looking from the "outside in," as well as from the "inside out." Add user and group access and file permissions, and hardening operating systems, and as you can see, security architecture becomes very complex. These perspectives must also be balanced against other business perspectives, financial and otherwise. In a gross generalization, we can safely say that whatever model or security architecture you use, you are trying to deliver data that's available, reliable, and safe. Consider figure 1.

Confidentiality keeps unwanted eyes, ears, or fingers off your information. Integrity keeps people from modifying your information. Availability keeps access to information within your business ready at all times. Your security architecture should deliver this "ground truth." Delivering these among the many challenges in

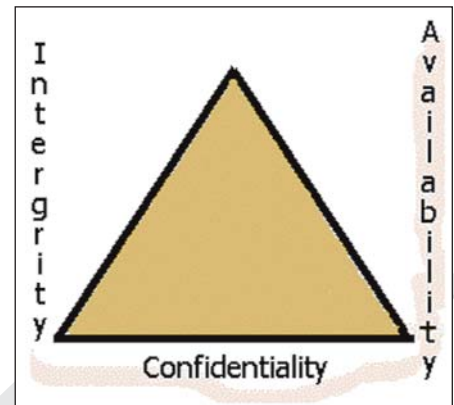


Figure 1: CIA Triad

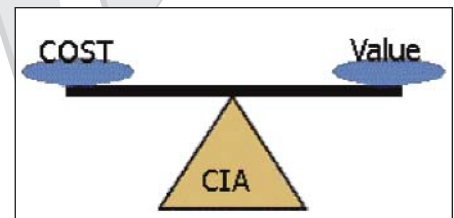


Figure 2: Balancing C.I.A.

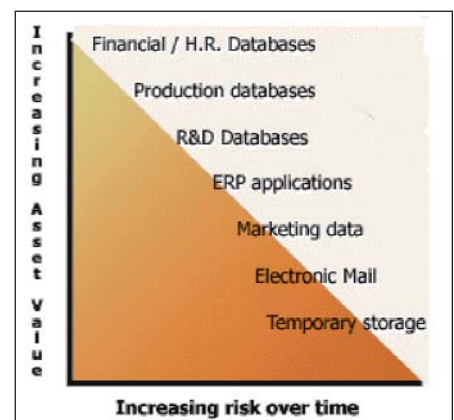


Figure 3: Assets increasing value over time

your security architecture is not as easy as it may seem.

Dollars and Sense

When planning your security architecture, you are governed by overriding factors, including

time and money. In some cases, spending one makes more sense than the other. For example, a small business putting together their first security architecture may have cost overriding all, while at the other end, non-compliance with a regulatory (or other) standard could cost a large enterprise millions in comparison to "relative" pennies required for the appropriate security architecture. To build or buy is an important decision. But in any case, balance your needs for data confidentiality, integrity, and availability against the cost of the protection and the value of the asset being protected.

It is also important to understand that although few enterprises can afford to start from scratch with regard to implementing security, the strategic view of your enterprise security architecture is a view of where you want to be. You may currently address physical access with Intrusion Detection Systems, gateways, and firewalls. These are integral elements of a good architecture, but alone they may not adequately address the risk to your enterprise. Keep moving forward with planned steps to reach a secure destination.

Evaluating Threat/vs Asset Value/vs/Vulnerability/vs Impact...

To create the appropriate architecture for your enterprise, you need to strike a balance between the value of assets being protected compared against the cost of the protection. Whether you call this a risk analysis profile or some other term, use it to determine the assets being protected in your enterprise, their value, and the corresponding risk to the assets. As a general guideline, protect the highest valued assets most stringently.

Create a Security Architecture that Fits the Business Framework

As we have seen, there are multiple perspectives in your security architecture or framework. Not coincidentally, many models exist which may match one, some, or all of your important perspectives. There are many framework examples, including the "Zachman Framework," the "Federal Enterprise Architecture Framework," "red book" or "orange book," and many other reference models (see the hyperlink section for reference links to these and other Frameworks). In each case, the common goal is to create a balance between the enterprise business needs, and the information systems which are supposed to support them.

For example, figure 3 shows assets increasing in value (up the vertical axis), facing increasing risk over time (on the horizontal axis extending to the right).

This simplistic representation shows the most highly valued assets facing the least exposure to risk over time, descending in value to assets that can withstand increased exposure to risk over time. Whatever method you use, determine the assets in your enterprise, and their associated value. Revisit these models when you acquire new or significant additional assets so that their value is properly established and defended. In this way there is an evaluation of what assets are present and their corresponding value within the business framework. Protecting these assets accordingly provides an initial security architecture which is in alignment with your business framework.

Network Security Architecture—It's Not Just Firewalls Anymore

As your user community has grown more sophisticated, so has the potential for accidental or intentional misuse or attack. Your information architecture

is no longer safe inside the digital "barbed wire" of Intrusion Detection Systems—a majority percentage of data loss in enterprises today occurs via credentialed accounts. Similarly, reliable and correct delivery of information on your LAN or WAN is no longer guaranteed via TCP/IP, with address spoofing and snooping available to anyone on your network, unless network security is active from the "inside out" as well. Evaluate this short list of network security mechanisms, in addition to your existing network security:

▲ Data integrity checks and data

encryption—Stored before and compared after critical data transmission, integrity checks can include encrypted totals, which can identify data transmission errors. Network transmissions using encrypted totals need to use the same encryption at each end of the transmission, either via the network or via the application after delivery. Using different encryption methods for different types of transmissions or different data streams make data transmission even more secure. SSH, SSL, and Secure Telnet are examples of network applications which encrypt their data in transmission.

▲ Transmission logging

—Storing an audit trail for the transmissions/applications that transmit data can include the transmission date, time, source and destination, and transmission type.

▲ Transmission loss

—In some cases data loss on an otherwise reliable network can indicate port scanning activity (someone viewing transmission samples looking for vulnerabilities, or perhaps just looking). With 65,535 TCP ports on a system, active data transmission to well known ports such as http (port 80) or telnet (port 23) are the tip of the iceberg, but are often at the attacker's spearhead. Defenses against this activity include keeping port scanning tools off of the network (a published mandate in security policies known to all employees, backed up by periodic review of hardware and software inventory on computers). Keeping unused ports closed, and current network patches on systems also enhances network security.

▲ Change control review

—While many system and network administrators view change control as cumbersome and in the way, reviewing network devices or software before they are introduced allows a larger perspective, including the security and business framework. The extra time spent here is inexpensive insurance over the system's lifecycle.

Application Security

Within an enterprise there are many applications used for data input or reporting, communications, database access and management, and web services. The matrix is very complex, but each application should comply with your basic security architecture and business framework. It's important to provide the highest level of application security without impairing the business capability.

The Five Ws

Who, what, when, where, and why? These questions should have clear, documented, auditable answers before the installation of any applications software. In addition, the answers should be periodically reviewed within the security architecture to make sure they remain relevant and adequately addressed throughout the lifecycle of the application. Who is the application's primary user community? What is their business function? When do they require access

to the application? Where is the application installed, and from where is it accessed? Why is the application important? How does it meet business needs? As each question is answered, security architecture issues will fall out. For example, a communications application is used by sales staff via remote access from anywhere in the world at any time. The access allows sales to enter orders, query inventory and/order status, query ERM application modules, and modify personal account information within specific sales parameters. Again, a visualization tool aides in this evaluation—see figure 4:

You can see many communications and application security issues emerge from this simple case description. These issues may include remote access via VPN or IPSEC tunneling, http or https access, middleware application security, including boundary testing, address checking, and security testing to insure that credentialing to the queried applications is appropriate and at the level required to do business, but no higher.

Match each of the assets valued in your enterprise security plan against this simple set of questions and be prepared to address security concerns that emerge. Keep in mind that the goal is to enable business processing while safeguarding assets at the highest level possible. Often this is accomplished by providing the lowest level of access required for a specific business task as well as testing the application for security (specific test plans will depend on the application being tested).

External Access

Your security architecture should also allow external access at the least privilege required level. In the previous example, sales staff access may happen from anywhere in the world. Your security architecture should allow this access with a secure application, providing the highest level of security for accessing only the application(s) they require for their business function.

An example of this might be a health care provider providing web-based access to their client base for a variety of services, including accounts receivable, patient records, or general health information service. In this scenario, the who, what, when, where, and why may resolve to hundreds of thousands of annual visitors, accessing applications to get claim forms, to pay for medical services, or to ask a general medical question. Access could occur from anywhere in the world for specific application access.

The corresponding network security requirements to fit the business framework might

Users	System	Who	What	When	Where	Why
Bill	SellIt01	smusa01	Create, query inventory, query ERM, modify personal account information	7x24	VPN01,office	USA sales manager
Cindy	prweb	mkt01	Web design for SellIt01	7x24	office	Marketing, P.R
John	SellIt01	sales01	Create orders, query inventory /order status	7x24	VPN02,office	Sales rep region 1
Sandy	SellIt01	sales02	Create orders, query inventory /order status	7x24	VPN02,office	Sales rep region 2
Steve	SellIt01	sales03	Create orders, query inventory /order status	7x24	VPN03,office	Sales rep region 3

Figure 4: The Five Ws

Use these links to help create your security architecture:

- <http://www.cisecurity.org/>
- <http://www.sans.org/score/>
- <http://www.itsecurity.com/dictionary/biba.htm>
- <http://e-government.cabinetoffice.gov.uk/Resources/FrameworksAndPolicy/fs/en>
- <http://www.attackprevention.com/ap/library/securitymodels.htm>
- <http://www.crime-research.org/news/07.06.2004/320/>
- <http://www.itsecurity.com/dictionary/cw.htm>

include http and https access passed from public networks to the private corporate LAN or WAN, thus allowing middleware applications to query patient record databases and payment processing applications. These systems could be in separate data centers, thus requiring data transmission on the corporate network to pass from the internal web/middleware systems to the database systems, to the financial systems, and return the requested information to the viewer while completing internal processing, all within HIPAA requirements for data security.

In a complex transaction model, having a security architecture and business framework to work within provides guidelines and limits, helping to insure that business is done efficiently while maintaining the highest level of security possible. It is no longer enough to determine that the data is secure in transmission. Servers may face denial of service attacks, which can deny remote access entirely or have their very identity on the network assumed by an attacking

system (I.P. address spoofing). These kinds of attacks are catastrophic when each second of real time represents hundreds or thousands of transactions.


Physical Access

With today's "e-anywhere" computing occurring via handheld wireless devices including phones, PDAs, hand-held computers, and wireless laptops, the limits of physical access security have never faced stronger challenges, while the requirements within the enterprise continue to skyrocket. Evaluate the kind of physical access required with the potential threat. For example, are your enterprise assets located in an area subject to natural or environmental threats, such as earthquakes, hurricanes, tornadoes or floods? Are your global resources in areas subject to terrorism, civil unrest?

What about the likelihood of corporate data theft or destruction by disgruntled employees or ex-employees?

It's likely that your organization faces some of these risks. In addition, organizations may face people walking away from systems with active logins, leaving the server room door open, or leaving keys in the server racks in machine rooms. The scope, detail, and expense of your physical access security plan should also be compared to the value of assets and secured to the highest degree possible without adversely affecting normal business functions. Installing screen locks that become active after fifteen seconds of idle time may cause considerable productivity loss, as well as increase employee irritation. Requiring all documents to be shredded before disposal may only be required where vital data can be compromised.

The Sum of the Parts

Security architecture in your enterprise is not a static, set it and forget it endeavor. Ongoing scrutiny, review, and modification of each of the areas presented provide a basic groundwork for security architecture. Providing and maintaining the maximum level of security required at each level is a task measured in man years, not man hours. But when compared to the value of the jewels in your enterprise, isn't it worth it? 

Richard Williams is a Senior Technical Support Specialist for Symark Software in Agoura Hills, California with over 20 years in systems administration, architecture, and design.

