Global Information Assurance Certification Paper

Security Architecture Model Component Overview

November 27, 2001

Scott M. Angelo

SANS Security Essentials
GIAC Practical Assignment
Version 1.2f (amended August 13, 2001)

In the dynamic world in which companies operate, securing transactions, data, and infrastructure components is much more complicated. A successful security architecture combines a heterogeneous combination of policies and leading practices, technology, and a sound education and awareness program. The recipe for pulling these components together to meet the standards set forth in the policies is the security architecture.

For most companies, the security architecture must provide a framework for integrating existing products and tools to meet current needs, as well as accommodate migration paths and anticipate future business directions.

Developing the Security Architecture Model

How does an organization go about developing security architecture model specifically for eCommerce? When referring to eCommerce, one often thinks of online storefronts such as amazon.com, or industry exchanges such as covisint.com. These large-scale business models are not representative of most corporate needs. The entry points for most companies into eCommerce are less aggressive in nature. Often consisting of web enabling an existing application to the Internet. (i.e., HR Employee Self Service). However, this doesn't necessarily equate to less risk!

> "For the third year, we asked some questions about electronic commerce over the Internet. Here are some of the results:
>
> - Ninety-seven percent of respondents have WWW sites.
> - Forty-seven percent conduct electronic commerce on their sites.
> - Twenty-three percent suffered unauthorized access or misuse within the last twelve months. Twenty-seven percent said that they didn't know if there had been unauthorized access or misuse.
> - Twenty-one percent of those acknowledging attacks reported from two to five incidents. Fifty-eight percent reported ten or more incidents.
> - Ninety percent of those attacked reported vandalism (only 64% in 2000).
> - Seventy-eight percent reported denial of service (only 60% in 2000).
> - Thirteen percent reported theft of transaction information (only 8% in 2000).
> - Eight percent reported financial fraud (only 3% in 2000)."[1]

Information Security and eCommerce go hand in hand. "Unauthorized users are targeting companies' Internet connection as a point of attack, with the percentage of attacks rising steadily over the past five years, while breaches occurring via internal systems and remote dial-in are still heavily exploited by various means. Most of which could have been prevented with a security architecture in place."

While it is apparent why companies regard security highly when embarking on an

eCommerce initiative, the reasons for building a security architecture are: 1) enable a business gain (productivity enhancements and/or revenue growth), 2) sustain existing growth, and 3) prevent a business loss.

The following is a more comprehensive list of Security Architecture drivers:

- Brand image customer and consumer confidence and trust
- Avoids costs associated with loss
- Increases business focus
- Privacy Regulations (i.e.,Health Care and Financial Services Industries)
- Secure Information Exchange
- Business process improvement
- Remote access to internal operations

Aligning the Strategic Vision with the Business Vision

The successful alignment of security controls with business objectives requires a "sound" understanding of the organizations:

- Business,
- Technology that supports key business processes, and
- Security controls in place

This is where it is most apparent that developing a comprehensive security architecture is a critical success factor in eCommerce ventures. Security architectures provide a scaleable framework for integrating people, process, and technology related controls that address both current and planned business objectives.

At its highest level, the security architecture model should provide the core infrastructure that supports the companies' strategic business vision. This vision then serves as the catalyst for the security architecture model that includes detailed technical designs, product selection, development, implementation, support, as well as the ongoing management of an information system and technology infrastructure.

Accordingly, the relationship of Information Technology (IT) to the business must be well understood in order to properly align the security architecture model with critical business processes. Gaining this understanding will enable the architecture model to be more clearly focused on matters of importance to the business and concentrate security activities on those areas. It will also greatly enhance the architecture model's credibility as a well-rounded model that incorporates the technology and the security and integrity of that technology to the achievement of business objectives that are important to the organization. With regard to security architecture models, this is critical to the model's ability to link IT security and recommendations for improvement to specific business needs and values.

The value of technology to an organization is based upon the role it plays in the following

highly interrelated areas:

- Achievement of business strategy,
- Leveraging policy, rules and human knowledge,
- Promotion of operational efficiency and effectiveness, and
- Facilitation of operational control and nimbleness in periods of rapid change.

Understanding the business will help develop a business frame of reference for the assessment of IT security effectiveness and the development of strategies for improvement that are highly relevant and valuable to the organization. Components of the security architecture model must address real business risks and be able to relate any security deficiencies to these business risks in order for the controls to have meaning and value to the data owners.

The key objectives of understanding the business are:

- Identify the most important business processes in the organization to ensure that the security architecture model and improvement strategy activities are properly focused on areas of value.
- Understand the nature and the extent of IT dependency of key business processes to understand the importance of IT's role in the organization.
- Gain an understanding of the business and IT strategies to determine the impact of anticipated future changes on the nature and the importance of IT's role in the organization and appropriate security architecture model.
-

- Identify other known significant factors that may impact the nature and importance of IT's role in the organization and the importance of data and systems integrity within the organization.

Security Risk Management Process

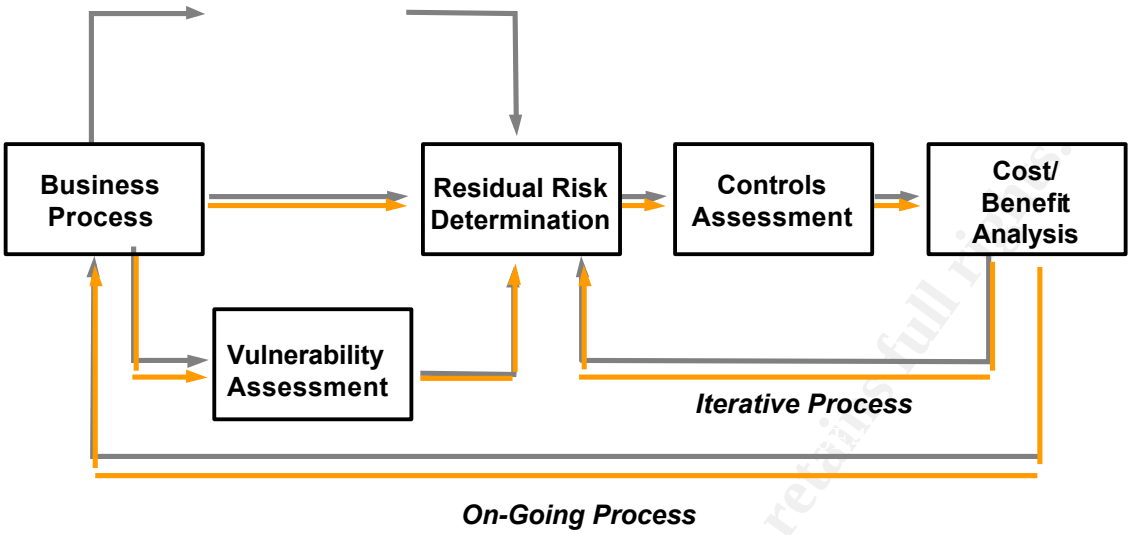
The first step in the process of a new eCommerce application (the risk management process should be invoked for any modification that could potentially impact risk) should be to list the business gains versus the known risks and constraints. This involves assessing the risks (business, technical, legal, etc.), which is where many projects fail. Business owners may not understand the risks from a technical perspective, and technical resources may not be focused on the business issues. Education and cooperation are important throughout the process. There has to be a balance between business risks and the controls in place.

In order to adequately understand and apply the risks to the business process at hand, you have to clearly understand the information "architecture" of the business process and how it will be supported from an information technology perspective. During this phase, the initial questions should address the scope of the project from an Information Architecture Perspective and should answer the following questions (Refer to the Application Review Process on page 11 for a more detailed overview):

- Does it involve a single application (or a single business need), or are there multiple applications?
- If there are multiple applications, are they interrelated or standalone; that is, will they rely on the same data, or the same participants, or are they functionally independent?
- Where does the data reside?
- Where does the data need to go?
- Do I need to build a new data repository?
- Is the application an existing one that is being moved to the Internet, or is it being developed specifically for the Internet?
- Is it a point application or does it involve redesigning a specific business process, or even overhauling an entire business model?

Now that the functional requirements of business process are better understood and the supporting technical specifications (unique information architecture and the technology infrastructure that is required to support it) have been identified, an assessment of the relative risk can be conducted. The risk can be evaluated at a specific technology component level (OS, network component, application, DB, code, etc.) and/or ultimately at the residual risk level.

Once the project team has identified and understands the associated risks, a comparison of the risks against the existing security architecture is required to identify potential control gaps. The gap analysis/controls assessment also serves as an opportunity to revalidate the effectiveness and ROI of the existing security architecture in supporting the continued eCommerce needs of the organization. In the event that a gap is identified, as a result of a new requirement, technology vulnerability, etc., the project team should develop a risk mitigation plan including a cost/benefit analysis. The overall plan should be presented to the business owners and culminate with senior management recognition of the residual risk, and a formal acceptance (such as a sign-off) of it.



Risk Management Process

The development, integration, and implementation phases follow, and should include an emphasis on building secure applications. Training classes for application developers are often a good idea, especially if the in-house staff is unfamiliar with Web-based authentication methods, cryptography tools, and general secure coding practices. Pre-production testing should focus on security as well as functionality, perhaps through the use of in-house or external vulnerability assessment teams. In some companies, internal audit may also be involved in this phase.

Before the new project goes into production, the project team should implement a post-production change control plan, to cover roles, responsibilities, and priorities for any additions, modifications and/or deletions (i.e., installing vendor patches, creating and installing internal patches, network service/port modifications, end user issues, etc.). Finally, the new project should be added to the enterprise business recovery plan.

Unfortunately for the teams designing and building eCommerce security architectures, there are no clean slates. Very seldom will anyone have the opportunity to build a new solution from the ground up. Most of the time, there is an existing infrastructure in place, and legacy systems and applications with which to interoperate making the introduction of new protection mechanisms potentially challenging. Part of the role of the security practitioner is to consolidate internal and external requirements, assess existing capabilities, and build migration paths.

Security Steering Group (Leverage Model)

"Risk management is not the only business principle associated with IT security.

Marketing is another that security professionals would do well to take advantage of. Indeed, the effectiveness of a comprehensive security program/strategy (or even an individual project) is dependent on the degree to which key enterprise constituencies understand it, embrace it, and invest in it. We believe traditional marketing practices are essential to achieving such "buy in" and to relating security to the enterprise's business success. Specifically, target audiences should be identified (Executives, IT managers, end users, etc.) and individually analyzed, to support the creation and delivery of customized messages."[2]

Maintaining the knowledge of the business, supporting technology, and security model is not a part-time initiative. Developing an effective security architecture that is built on the comprehensive knowledge of the organization is a non-trivial activity that requires active marketing to multiple resources that can adequately represent the business objectives and/or needs of the organization. The establishment of an Internal Security Steering Group will help facilitate the actions necessary to design, build, implement and maintain a pragmatic security architecture model. Membership in the steering group could include but is not limited to the following parties:

- Data/Business Owners,
- Security,
- Audit,
- Information Technology, and
- QA

This leverage model can effectively reduce the overall level of effort in designing, implementing, and managing all of the critical components that an enterprise security architecture is comprised of thus increasing the Return On Investment (ROI), reducing the Total Cost of Ownership (TCO), and effectively managing risks.

Basic Security Requirement Model

One of the most important aspects of any security architecture model is the ability to manage/maintain an accurate and consistent level of security controls. An integrated risk management program is critical in securing business objectives requiring the enforcement of confidentiality, integrity, availability, and accountability.

Confidentiality
Confidentiality ensures the protection of data from unauthorized access throughout an organization's information architecture, which extends to all data directly associated with the architecture's applications, data stores, communication links and/or processes.

Integrity
Integrity ensures that data, services, and other controlled resources are not altered

and/or destroyed in an unauthorized manner. Integrity based controls provide safeguards against accidental, unauthorized, or malicious actions that could result in the alteration of security protection mechanisms, security classification levels, addressing or routing information, and/or audit information.

Availability
Availability ensures the reliable and correct operation of information and system resources for which the loss of information and/or resource access would cause adverse results. Availability based security requirements include controls to prevent, detect, and/or monitor accidental, unauthorized, and/or malicious activities that could negatively impact the availability of critical information.

Accountability
Accountability requirements ensure that events can be associated to specific users and/or processes responsible for those actions. The overall goal is to be able to verify, with 100% certainty, that a particular electronic message can be associated with a particular individual, just as a handwritten signature on a bank check is tied back to the account owner. Accountability based controls include identification and authentication mechanisms, and access control.

Security Architecture Model Components

The intentional planning process (strategic vision) involved in developing the security architecture model will help reduce the accumulation of point solutions thus reducing the total cost of ownership. The presence of multiple point solutions is symptomatic of organizations lacking basic risk management processes and breed unnecessary complexity. Hence, the security controls are tactical in nature and are implemented in response to a "perceived" need versus a validated need. Additionally, the associated time, money and/or resource requirements of managing "Tactical" point solutions can be significantly higher than those of a strategically designed security architecture.

One of the primary goals of a security architecture is to provide clearly defined control solutions. Corporate data classification and its corresponding data security model provide such a solution that consolidates requirements into meaningful categories, and provides predetermined minimum controls for each. This can potentially save time and money by applying consistent and repeatable solutions.

Data Classification Model
A Data Classification Model is a key component in establishing a risk based Security Architecture designed to promote wider sharing of information, as well as ensuring that sensitive items of information are identified as requiring additional controls. A typical model can consist of four categories (unclassified, low, medium and high) and the criteria by which the information is classified.

Because of increasing information sharing and the cost of securing information, it is important to classify information correctly. Under-classification of sensitive information can have serious consequences. For example, sensitive data might be intercepted if not adequately protected in transmission. Over-classification can also be damaging in terms of efficiency and missed opportunities for knowledge sharing, as well as undermining the credibility of the classification system.

Data Security Model (Information Handling Procedures)
The Data Security Model builds on the Classification Model in that it uses the classification component to direct and assist the end user in ensuring that the information is secured in the appropriate manner. The security requirements for each classification level are defined, based on the organization's particular application of the technology. The model includes categories for security, and the criteria by which the information is to be secured.

Categories relate to both business processes (applications and data) and information technologies (hardware, software and services) that support that environment. The categories define a comprehensive structure for IT risk management issues and represent the components of the information systems environment (i.e., processes, users, physical devices, and the facilities where they are located).

To be effective, the development of the technical architecture must be accompanied by an explicit business process that ensures the integration of security into eCommerce projects from their inception. This avoids the last-minute rush to add security controls after the project has been developed which can be a costly proposition.

A large percentage of organizations already have internal processes such as software development, project development, or life-cycle management. The utilization of these processes can be adapted and expanded to ensure that appropriate security components are included in every phase. A high percentage of security efforts within organizations rely on perimeter network access controls exclusively. Although perimeter security is very important, it is by no means a comprehensive solution to risk management and/or mitigation. Organizations need to put just as much effort into securing the technology infrastructure (i.e.,OS, applications, and network components) that the eCommerce infrastructure/critical corporate applications relies on.

> "Is it that we should ignore the insider threat in favor of the outsider threat? On the contrary. The insider threat remains the greatest single source of risk to organizations…But what I am saying is that it is important to avoid underestimating the external threat. It is not only growing disproportionately, but it is being fuelled increasingly by organized crime and motives related to espionage."[3]

It's also extremely important to put nontechnical controls such as developing and

incorporating secure practices into the organization's business cycles, on an equal footing with technical controls both inside and out.

Regulatory Requirements

The balancing act of implementing the appropriate security architecture model can be offset by mandatory requirements that are governed by some regulatory bodies depending on the particular industry. A perfect example is the Health Insurance Portability and Accountability Act of 1996 (HIPAA) that mandated regulations that govern privacy, security, and electronic transactions standards for health care information. HHS has published final regulations related to electronic transactions and privacy. Other final and proposed regulations are expected this year. Together, these regulations will require major changes in how health care organizations handle all facets of information management, including reimbursement, coding, security, and patient records. [4] HIPAA breaks the requirements to guard data integrity, confidentiality, and availability into four categories for further clarification:

1. Administrative Procedures
2. Physical Safeguards
3. Technical Security Services
4. Technical Security Mechanisms to Guard Against Unauthorized Access to Data That Is Transmitted Over A Communications

Consequently, a health care organization still needs to determine the applicability of the requirements based on their own unique business operation model.

Leading Practices

Various groups and/or professional organizations have developed their own set of security related standards that can be used as a baseline for determining what's appropriate for their own organization. Some well known standards include:

- ISO 17799[5], which provides detailed security standards for organizations to use as a baseline when designing their own security architecture model.

Additional Security Architecture Model Components

Components of a Security Architecture Model can be broken down into logical categories. These categories include:

- **Detection**: Organizations must have methods to detect information technology intrusions and potential vulnerabilities. The detection processes must be in place and operating properly at all times. Any downtime in the operation of detection systems can expose the company. So, management must support and implement these processes. Detection systems are reactive in nature, and management must be proactive in establishing detection methods.

- **Prevention**: Management must be proactive in having methods that prevent unauthorized access to their systems. Prevention based controls should deter potential intruders from attempting to access an organization's information. Since information is a critical asset, preventing unauthorized access and/or manipulation of it is extremely important.
- **Monitoring**: Management must monitor the security architecture model to ensure it's in alignment with the organizations business strategy, security policies, and their technology requirements. Regular assessments should verify that the goals of the organization's security framework are met and that the policies are properly enforced.

-
- **Management:** Detection, prevention, and monitoring plans should be communicated to the users. After they are communicated, the plans must be properly executed, supported by the end users, and regularly assessed and evaluated for continued relevance. The processes must be flexible so the organization can effectively adjust to changes as they occur. The organization must choose the correct automated security management systems for their unique requirements.

Each one of these categories can consist of multiple individual processes that provide some form of additional control mechanism. Depending on the complexity of an organization and their business objects, the components of a Security Architecture Model can become numerous and challenging. However, the consequences of not employing the appropriate components can be detrimental to an organization's reputation.

> " FBI has continued to observe hacker activity targeting victims associated with e-commerce or e-finance/banking businesses. In many cases, the hacker activity had been ongoing for several months before the victim became aware of the intrusion. The NIPC emphasizes the recommendation that all computer network systems administrators check relevant systems and consider applying the updated patches as necessary, especially for systems related to e-commerce or e-banking/financial businesses." [6]

The following two processes are key components within the management category:

Change Control Process

Change management is the process of effectively managing the necessary changes to the Security Architecture Model. Use of this process is imperative to maintaining the effectiveness and accuracy of the Information Classification and Security Models as effective change management allow the models to stay consistent with the organizations tolerance to risks.

Furthermore, an effective well-integrated change management process includes workflow mechanisms to ensure that change requests are monitored, reviewed, approved and tested prior to implementation.

Compliance Monitoring Process
Periodic compliance reviews of security components associated with the Security Architecture Model are critical in maintaining the acceptable risk level and managing the effectiveness and appropriateness of the controls in place.

Compliance reviews may include use of the classification and security models, compliance to the classification and security models and procedures, compliance to the exception processes and documentation reviews. In addition, as part of an internal audit program (role for internal audit within the leverage model), process audits may include reviews of the classification of information to determine if the appropriate levels of classification and security assigned were assigned. An active compliance monitoring process is also a positive indicator of an organizations continuous commitment to security. The lack of any type of monitoring process only breed's contempt within an organization, which only serves to increase the potential risk of unauthorized activity.

Conclusion

An information systems security approach is built on comprehensive Enterprise Security Architecture Model and delivery methodology. An Enterprise Security Architecture Model provides the technical acumen, delivery roadmap, proven processes and other resources needed to ensure the appropriate level of risk management within an organization based on their unique business objectives.

An Architecture Model should be designed to view the enterprise-wide perspective, helping to ensure that all facets of information security issues are considered—from mainframe and ancillary systems, software packages, and hardware to all communication systems and points of connectivity.

Finally, the Enterprise Security Architecture Model provides a framework for a consistent and unified approach to assisting organizations in the assessment and testing of their existing information security infrastructure, developing an approach for implementing improvements, and finally, deploying the recommended improvements. The Security Architecture Model is not designed to leave a company with just an implementation plan or a watered down security solution. Rather, it is intended to take an organization through the complete implementation and deployment process, including the preparation and planning, detailed design, configuration, integration, testing, and finally production.

Application Security Review (ASR) Process

Overview
eCommerce Architectures utilize Internet and World Wide Web technology to enable communication between itself and it's end users/subscriber's organizations. As such any application system deployed must support the Confidentiality, Integrity and Availability of the information managed by the corresponding application(s). All new applications entering the organization's Domain should be required to go through a documented Application Security Review process. This is an interactive process that an internal Information Security Group (ITG) will help collect/manage for completion. At every step during the ASR process, the ITG will guide the application owner to meet the ASR requirements. This will ensure consistency with and the effective of the ASR process.

To support the organizations application security requirements, the following information should be used to benchmark application security requirements. This information is subject to change, based on the evolving security needs of the organization and its end users.

Purpose
The purpose of the ASR Process is to ensure that security architecture controls for a sensitive application (Financial, Confidential and/or Sensitive) adequately satisfy: an organizations Risk Management tolerance and the minimum control requirements necessary to protect its interests.

Completing the Application Security Review Process
The application security review process should be completed prior to the application going into production and should be updated whenever a change is made to the actual application.

The following documentation should be completed as part of the Application Security Review process.

> Application Narrative: This is used to provide a complete description of the elements of the application's environment. The elements of the narrative must include descriptions of the infrastructure used by the application, software used (operating system, firewall, web server, etc.), people (including users, administrators and support), procedures and data. Each element should be clearly and fully explained in narrative form and should support the related logical architecture and network diagrams. Description should be a non-technical explanation of the application.
>
> Data Narrative: This should be used to define the elements of data used by the

application. This includes data used to identify and authorize a user as well as data used for transaction processing. When describing the transaction data used by the application, the narrative should reference transactions, necessary data inputs for each transaction, subsequent authorizations and data work-flow, initial input checking and validation, processing (including description of temporary files), storage and output of related data. Each element should be clearly and fully explained in narrative form and should support the related logical architecture, data and network diagrams. Description should be a non-technical explanation of the application.

Flow Charts:
Logical Architecture Diagram: This diagram gives a brief overview of the application's architecture. It is a high-level diagram, which provides all major components of the application. This diagram should flow together with the Application Narrative.

Data Workflow Diagram: This diagram should include a high-level Process Flowchart. The Process Flowchart is a non-technical, high-level work process flowchart. The application's sources of input, master files, outputs, reports/screens and major processing programs or modules should be clearly identified. It is within this diagram classification of data must be specified. What kind of data is it? How is it separated? What is the user experience? It provides the flow of data from a technical view, Intranet and Extranet boundaries and where data is stored.

Physical Network Architecture Diagram: This is a technical diagram depicting the network features and architecture of the application. From this diagram, we should understand what type of hardware is used across the application. Where does each component of the application within the Network Environment? What services and daemons live on each machine? What ports are opened between network tiers?

The combination of this information (Application and Data Narratives, Logical Architecture Diagram, Data Flow Diagram, and Physical Network Architecture Diagram), will provide the organization with the appropriate level on information to make pragmatic Risk Management based decisions regarding the design, implementation and continuous management of a security architecture.

The security architecture and design comprises two separate but equally important areas. The first is the technical controls, the various hardware and software elements required to secure the overall infrastructure. The second is the nontechnical controls, or processes and procedures. These two areas of the security architecture and design—in combination—are implemented to protect the confidentiality, integrity, and availability of the data contained

in the system per the Application Security Review.

---

[1] 2001 CSI/FBI Computer Crime and Security Survey

[2] Bouchard, Mark, "IT security: Marketing makes it work" META Group, November 26, 2001

[3] Schultz, Dr. Eugene in an editorial for Information Security Bulletin (Vol. 6, #2, March '01

[4] HIPAA Electronic Privacy, Secuirity, and Electronic Transaction Standards http://www.aha.org/hipaa/hipaa_home.asp

[5] ISO/IEC 17799, International Standard, Information Technology – Code of Practice for Information Security Management, First Edition 2000-12-01 http://www.iso17799software.com/what.htm

6 NIPC Advisory 01-003: March 08, 2001, Update to NIPC Advisory 00-006 "E-Commerce Vulnerabilities" http://www.nipc.gov/warnings/advisories/2001/01-003.htm