Using Enterprise Security Architectures to Align Business Goals and IT Security within an Organization

By Edwin Covert, CISSP, CISM, PMP
Director, Information Assurance Programs
Applied Network Solutions
**Introduction**

Over the course of many years and many clients, information security practitioners have discovered a lot about how information security truly functions in the real world—where it succeeds and where it fails. As an industry focus, it has become abundantly clear that a tremendous amount of attention is given to those things that are shiny and are easy to implement. It is fundamentally a result of the fact that practitioners are overworked as both our environments as well as our client’s environments are changing rapidly. Information security focuses too much on the implementation of controls and not enough on how those controls are driven by business goals. Business should drive security controls; too often it does not. It is posited here that this is because there is no ability to effectively translate business goals into security controls. What is not being done today in an effective manner is setting up the framework for making valuable business-driven, risk-based solutions. This framework is known as an enterprise security architecture (ESA). The concept of an ESA was initially put forth by The Gartner Group in a white paper entitled “Incorporating Security into the Enterprise Architecture Process” (24 January 2006). Since its initial publication, companies and practitioners have watched information security mature as a discipline from being an afterthought, or perhaps as bolt-on process, to a already-completed project to becoming more integrated into the overall enterprise architecture of our clients. However, a significant amount of work is left undone. Organizations are not utilizing the idea of the ESA to its full potential. As technological solutions advance and platforms and processes converge, organizations forgot to ensure that what they are deploying must align with their ESA. This white paper aims to serve as a red flag reminder about why the ESA is important.

**Enterprise Security Architecture**

Implementing an ESA means applying a comprehensive model for an organization's security processes, information security systems, as well as personnel and organizational sub-units, so that they align with the organization's core goals and strategic direction. The goal of an ESA is to make sure that business goals and IT security are aligned. An ESA will allow traceability from the business strategy down to the underlying technology.

According to Enterprise Security Architecture, A Business Driven Approach by John Sherwood, Andrew Clark, and David Lynas, information security is the “enabling technology of electronic business (p 5).” Security is used to protect business assets. In most organizations, a requirement is identified by a particular business user. From there, some sort of specification is designed or developed. Security or the IT department then moves smartly off to find a technical solution to that problem. Enterprise Security Architecture, A Business Driven Approach advocates the Sherwood Applied Business Security Architecture (SABSA). It is a hierarchal structure as shown below:
At an elemental level, the model is composed of five strata that interlock with each other. Starting with the contextual layer, business processes and models are understood. From there, the conceptual layer is added with specific control objectives as well as business attributes. Logical elements are then added with specific designs to meet those control objectives. The physical level in this model deals with procedures, users, and infrastructure. The component level, the last layer in this model, is concerned with the actual tools and products to be implemented. In each case, a review of operation security is on-going.

The SABSA model is an excellent starting point for any ESA discussion. However, there are other models available to the practitioner. Another model is the Open Security Architecture (OSA). OSA, according to its vision, “distills the know-how of the security architecture community and provides readily usable patterns for your application. OSA shall be a free framework that is developed and owned by the community.” Because OSA is community-based, it has prompted its users to create patterns of controls for common scenarios. These patterns are based on architectural diagrams depicting those scenarios and are derived from the National Institutes of Standards and Technologies (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations.

Both the SABSA and OSA have benefits and drawbacks. SABSA mandates that every security function must be derived from a specific business requirement. While this is an excellent piece of security advice, it can be cumbersome for the novice. OSA is very accessible to the more novice user, but utilizes the templated approach mentioned above that can seem like a one-size-fits-all method.

Benefits of an ESA
Regardless of the architecture model used, it is important to select one and to follow it. An ESA can eliminate tactical approaches to security. Often aggregation of tactical solutions across multiple business requirements is how organizations end up with a plethora of tools and processes that don't work together and don't provide a meaningful picture of how secure they are, i.e. long term strategic situational awareness. An ESA also forces participants into two additional beneficial end states. The first is discussion. Security practitioners and business managers must come to a common language for discussing their requirements. Security needs to protect business and business managers need to protect and enhance revenue. Without a common framework, neither can understand what the other is talking about. By using an ESA, each side can begin to understand the unique language of the other.

The second function of this approach is that by enforcing this ESA, costs are reduced. This is accomplished by homogenizing IT security products from their current state of different point solutions originally designed for individual needs. As products are streamlined to ensure they are in compliance with the ESA, economies of scale should become apparent. No longer should an organization need two distinct IDS systems with two sets of skills that have to be maintained and two separate costs of ownership metrics.

Implementing an ESA is not an easy task. As evidence, if it were non-trivial, it would have been done already. However, the difficulty of doing this should not be an impediment to
its completion. In fact, it should be looked on as a challenge to be undertaken for the benefit of the organization. After all, if security practitioners are not providing benefit to the team or group or company, why are we there?

The actual method of implementation will be highly dependent on two factors. The first factor is the methodology your organization chooses to implement. It is recommended that you take advantage of one of the open methodologies as opposed to the versions individual vendors offer. This restricts the organization less in the long term. The second factor of significance is the who the organization chooses to assist in the implementation. If there is the intellectual infrastructure available within the organization, it is recommended to use internal resources. Unfortunately, many organizations and corporations lack these capabilities as they have tended to focus on their core functions and information security is not often considered one of those. However, many consulting and other outside organizations exist and are very capable of providing assistance in developing an ESA. Prudence dictates that the same caution be exercised when selecting a methodology. Examine potential vendors and consultants based on the model they use. Common questions to ask include: “Will I still be able to fully utilize the model if I switch vendors later?” and “What is updates to my architecture cost over time?” These questions are obviously not all-inclusive.

Summary
This paper started with the premise that information security focuses too much on the implementation of controls and not enough on how those controls are driven by business goals. Without a common framework, such as provided by an ESA, this will never change. An ESA allows security practitioners to provide measurable benefit and value to an organization at the same time as reducing costs. While difficult, it is a necessary starting point for securing the assets of the organization.

About the Author
Edwin Covert is the Director, Information Assurance Programs for Applied Network Solutions (www.ansfederal.com). He holds the Certified Information Systems Security Professional (CISSP) and the Certified Information Security Manager (CISM) designations and has fifteen years in the information security and information assurance arenas. He also holds the Project Management Professional (PMP) certification. He has worked in the federal, military, and commercial sectors and is the author of numerous papers and presentations.

References

