The Perusal and Review of Different Aspects of the Architecture of Information Security

Vipin Kumar
Research Scholar, CMJ University, Shillong, Meghalaya (India)

Abstract

The purpose of the security architecture blueprint is to bring focus to the key areas of concern for the enterprise, highlighting decision criteria and context for each domain. Since security is a system property it can be difficult for Enterprise Security groups to separate the disparate concerns that exist at different system layers and to understand their role in the system as a whole. Computers and Information technology has impacted every aspect of modern life and business. It’s use for decision making and controlling important operations without human supervision have made its entry in both public and private sectors.

Keywords: *Architecture of Security, Incorporating Security, Methodology for security, Goals of Security.*

Introduction

Enterprise information security architecture (EISA) or simply information security architecture is the practice of applying a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel and organizational sub-units, so that they align with the organization's core goals and strategic direction. Although often associated strictly with information security technology, it relates more broadly to the security practice of business optimization in that it addresses business security architecture, performance management and security process architecture as well.

Enterprise information security architecture is becoming a common practice within the financial institutions around the globe. The primary purpose of creating enterprise information security architecture is to ensure that business strategy and IT security are aligned. As such, enterprise information security architecture allows traceability from the business strategy down to the underlying technology.

Incorporating Security

Enterprise information security architecture was first formally positioned by Gartner in their whitepaper called “Incorporating Security into the Enterprise Architecture Process”. This was published on 24 January 2006. Since this publication, security architecture has moved from being silo based architecture to an enterprise focused solution that incorporates business, information and technology. The picture below represents a one-dimensional view of enterprise architecture as a service-oriented architecture. It also reflects the new addition to the enterprise architecture family called “Security”. Business architecture, information architecture and technology architecture used to be called BIT for short. Now with security as part of the architecture family it has become BITS.

Security architectural change imperatives now include things like

- Business roadmaps
- Legislative and legal requirements
- Technology roadmaps
- Industry trends

- Risk trends
- Visionaries

Goals

1. Provide structure, coherence and cohesiveness.
2. Must enable business-to-security alignment
3. Defined top-down beginning with business strategy
4. Ensure that all models and implementations can be traced back to the business strategy, specific business requirements and key principles.
5. Provide abstraction so that complicating factors, such as geography and technology religion, can be removed and reinstated at different levels of detail only when required.
6. Establish a common "language" for information security within the organization

Methodology

The practice of enterprise information security architecture involves developing an architecture security framework to describe a series of "current", "intermediate" and "target" reference architectures and applying them to align programs of change. These frameworks detail the organizations, roles, entities and relationships that exist or should exist to perform a set of business processes. This framework will provide a rigorous taxonomy and ontology that clearly identifies what processes a business performs and detailed information about how those processes are executed and secured. The end product is a set of artifacts that describe in varying degrees of detail exactly what and how a business operates and what security controls are required. These artifacts are often graphical.

Given these descriptions, whose levels of detail will vary according to affordability and other practical considerations, decision makers are provided the means to make informed decisions about where to invest resources, where to realign organizational goals and processes, and what policies and procedures will support core missions or business functions.

A strong enterprise information security architecture process helps to answer basic questions like:

- What is the information security risk posture of the organization?
- Is the current architecture supporting and adding value to the security of the organization?
- How might security architecture be modified so that it adds more value to the organization?
- Based on what we know about what the organization wants to accomplish in the future, will the current security architecture support or hinder that?

Implementing enterprise information security architecture generally starts with documenting the organization's strategy and other necessary details such as where and how it operates. The process then cascades down to documenting discrete core competencies, business processes, and how the organization interacts with itself and with external parties such as customers, suppliers, and government entities.

Having documented the organization's strategy and structure, the architecture process then flows down into the discrete information technology components such as:

- Organization charts, activities, and process flows of how the IT Organization operates
- Organization cycles, periods and timing
- Suppliers of technology hardware, software, and services
- Applications and software inventories and diagrams
- Interfaces between applications - that is: events, messages and data flows
- Intranet, Extranet, Internet, e-Commerce, EDI links with parties within and outside of the organization
- Data classifications, Databases and supporting data models
- Hardware, platforms, hosting: servers, network components and security devices and where they are kept
- Local and wide area networks, Internet connectivity diagrams

Wherever possible, all of the above should be related explicitly to the organization's strategy, goals, and operations. The enterprise information security architecture will document the current state of the technical security components listed above, as well as an idealworld desired future state (Reference Architecture) and finally a "Target" future state which is the result of engineering tradeoffs and compromises vs. the ideal. Essentially the result is a nested and interrelated set of models, usually managed and maintained with specialized software available on the market.

Such exhaustive mapping of IT dependencies has notable overlaps with both metadata in the general IT sense, and with the ITIL concept of the Configuration Management Database. Maintaining the accuracy of such data can be a significant challenge.

Along with the models and diagrams goes a set of best practices aimed at securing adaptability, scalability, manageability etc. These systems engineering best practices are not unique to enterprise information security architecture but are essential to its success nonetheless. They involve such things as componentization, asynchronous communication between major components standardization of key identifiers and so on.

Successful application of enterprise information security architecture requires appropriate positioning in the organization. The analogy of city-planning is often invoked in this connection, and is instructive.

An intermediate outcome of an architecture process is a comprehensive inventory of business security strategy, business security processes, organizational charts, technical security inventories, system and interface diagrams, and network topologies, and the explicit relationships between them. The inventories and diagrams are merely tools that support decision making. But this is not sufficient. It must be a living process.

The organization must design and implement a process that ensures continual movement from the current state to the future state. The future state will generally be a combination of one or more

- Closing gaps that are present between the current organization strategy and the ability of the IT security dimensions to support it
- Closing gaps that are present between the desired future organization strategy and the ability of the security dimensions to support it
- Necessary upgrades and replacements that must be made to the IT security architecture based on supplier viability, age and performance of hardware and software, capacity issues, known or anticipated regulatory requirements, and other issues not driven explicitly by the organization's functional management.
- On a regular basis, the current state and future state are redefined to account for evolution of the architecture, changes in organizational strategy, and purely external factors such as changes in technology and customer/vendor/government requirements, and changes to both internal and external threat landscapes over time.

Architecture of Security

An Enterprise information security architecture framework is only a subset of enterprise architecture frameworks. If we had to simplify the conceptual abstraction of enterprise information security architecture within a generic framework, the picture on the right would be acceptable as a high-level conceptual security architecture framework.

Other open enterprise architecture frameworks are:

The U.S. Department of Defense (DoD) Architecture Framework (DoDAF)

Extended Enterprise Architecture Framework (E2AF) from the Institute For Enterprise Architecture Developments

Federal Enterprise Architecture of the United States Government (FEA)

Capgemini's Integrated Architecture Framework

The UK Ministry of Defence (MOD) Architecture Framework (MODAF)

NIH Enterprise Architecture Framework

Open Security Architecture

Information Assurance Enterprise Architectural Framework (IAEAF)

SABSA framework and methodology

Service-Oriented Modeling Framework (SOMF)

The Open Group Architecture Framework (TOGAF)

Zachman Framework

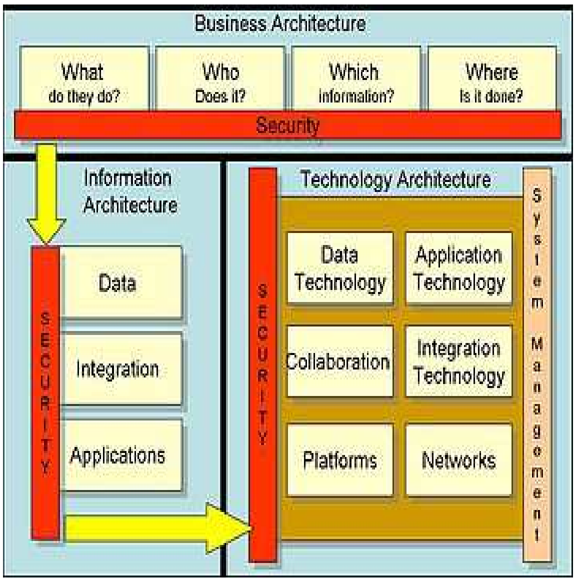

Figure 1: Architecture of Info Security

Scope

The term enterprise is used because it is generally applicable in many circumstances, including

- Public or private sector organizations
- An entire business or corporation
- A part of a larger enterprise (such as a business unit)
- A conglomerate of several organizations, such as a joint venture or partnership
- A multiply outsourced business operation
- Many collaborating public and/or private organizations in multiple countries

The term enterprise includes the whole complex, socio-technical system, including:

- people
- information
- technology
- business (e.g. operations)

Defining the boundary or scope of the enterprise to be described is an important first step in creating the enterprise architecture. Enterprise as used in enterprise architecture generally means more than the information systems employed by an organization. A pragmatic enterprise architecture provides a context and a scope. The context encompasses the (people), organizations, systems and technology out of scope that have relationships with the organization(s), systems and technology in the scope. In practice, the architect is responsible for the articulation of the scope in the context; engineers are responsible for the details of the scope (just as in the building practice). The architect remains responsible for the work of the engineers, and the implementing contractors thereafter.

Conclusion

As new technologies arise and are implemented, the benefits of enterprise architecture continue to grow. Enterprise architecture defines what an organization does; who performs individual functions within the organization, and within the market value chain; how the organizational functions are performed; and how information is used and stored. IT costs are reduced and responsiveness with IT systems is improved. However, to be successful, continual development and periodic maintenance of the enterprise architecture is essential. Building enterprise architecture could take considerable time and proper planning is essential, including phasing the project in slowly, prior to implementation. If the enterprise architecture is not kept up to date, the aforementioned benefits will become useless. Enterprise architecture is a key component of the information technology governance process in many organizations, which have implemented a formal enterprise architecture process as part of their IT management strategy. While this may imply that enterprise architecture is closely tied to IT, it should be viewed in the broader context of business optimization in that it addresses business architecture, performance management and process architecture as well as more technical subjects. Depending on the organization, enterprise architecture teams may also be responsible for some aspects of performance engineering, IT portfolio management and metadata management.
Recently, protagonists like Gartner and Forrester have stressed the important relationship of Enterprise Architecture with emerging holistic design practices such as Design Thinking and User Experience Design. Analyst firm Real Story Group went further, suggesting that Enterprise Architecture and the emerging

concept of the Digital Workplace were "two sides to the same coin.

References

[1] Carbone, J. A. (2004). IT architecture toolkit. Enterprise computing series. Upper Saddle River, NJ, Prentice Hall PTR.

[2] Cook, M. A. (1996). Building enterprise information architectures: reengineering information systems. Hewlett-Packard professional books. Upper Saddle River, NJ, Prentice Hall.

[3] Fowler, M. (2003). Patterns of enterprise application architecture. The Addison-Wesley signature series. Boston, Addison-Wesley.

[4] Togaf Guide to Security Architecture "http://www.opengroup.org/pubs/catalog/w055.htm"

[5] Groot, R., M. Smits and H. Kuipers (2005). "A Method to Redesign the IS Portfolios in Large Organizations", Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05). Track 8, p. 223a. IEEE.

[6] Steven Spewak and S. C. Hill (1993). Enterprise architecture planning: developing a blueprint for data, applications, and technology. Boston, QED Pub. Group.