Role of Security and Privacy in the Enterprise Architecture

Enterprise architecture is a discipline in world business that consist set of strategies and approaches a business uses in decision making on various circumstances, make effective changes, and adjust policies to reflect long-term goals. The purpose of enterprise architecture is to create a map of IT assets and business processes and a set of governing principle by increasing importance of information for enterprises and appearing new forms of threats such as Cyber - attacks, information warfare and terrorism. Security and privacy are hence a major blocks in Enterprise Architecture.

In the case of security, we may consider Security Architecture which is a structure of organizational, conceptual, logical, and physical components that interact in a coherent fashion in order to achieve and maintain a state of managed risk. It is an enabler/driver of secure behavior, safe behavior, resilient behavior, reliable behavior, and upholding of privacy at risk areas throughout the whole enterprise.

Security Architecture components always have a relationship with other elements in the architecture. Thus, although the Security Architecture might be *viewed* as one architecture, it can never *be* an isolated architecture.

Enterprise Architecture involves offering a flexible and powerful way of expressing the security concerns of the business owners through Information Security management (ISM) that defines the security objectives, assigns ownership of information security risks, and supports the implementation of security measures. The security management process includes risk assessment, the definition and proper implementation of security measures, reporting about security status (measures defined, in place, and working), and the handling of security incidents.

SABSA Business Attribute model, as described in the section "*Requirements Management*" allows measure of efficacy. The efficacy of a security measure is considered in relation to the risk it mitigates. To give a more down-to-earth idea of what security encompasses, some generally accepted areas of concern for the Security Architect are given:

- Asset Protection – the protection of information assets from loss or unintended disclosure, and resources from unauthorized and unintended use
- Risk Assessment – determining what risks we face, measuring them to determine their likelihood and impact, and then accepting, mitigating, or transferring the risk according to the organization's risk appetite
- Access Control – who are you and what activity are you allowed to do under which conditions?
- Audit – does the operational environment operate in accordance with the requirements?
- Availability – the ability to function without service interruption or depletion despite abnormal or malicious events

Privacy is the ability of an individual or group to seclude themselves, or information about themselves. The boundaries and content of what is considered private differ among cultures and individuals, but share common themes. The domain of privacy partially overlaps security, including, for instance, the concepts of appropriate use, as well as protection of information.

In general, directives on privacy demand that personal data should not be processed at all, except when certain conditions are met. These conditions fall into three categories: transparency, legitimate purpose, and proportionality.

In retrospect this context shows that security and privacy are highly related to Enterprise Architecture since security involves securing of information from risky areas while privacy involves maintaining the confidential information secure which describes the major role of Enterprise Architecture .