

IT Security and ITIL: A Case Study

Shay C. Colson

IST 700 - Dr. Scott A. Bernard - Spring 2009

Introduction

Having undergone a June 2007 revision, the Information Technology Infrastructure Library (ITIL) provides an up-to-date framework for an organization to conceive of, direct, and manage their information systems. ITIL is very service based, in fact - ITIL® is the most widely accepted approach to IT service management in the world. (APMGroup 2009)

The newest revision of ITIL (v3) focuses heavily on the aspect of service, working to take the corporate conception of IT from the back rooms to the forefront of corporate strategy. Where v2 talked about business and IT alignment, v3 emphasizes business and IT integration. (Greiner 2007)

ITIL is not, however, the blueprint of a perfect organization. "ITIL does not prescribe an ideal organization; instead, it describes the relationships between the activities and processes that are relevant to governing any organization. ITIL, therefore, is not a method, but a framework." (Shewmaker, Brock et al. 2006)

The strategic drivers of the ITIL v3 framework map nicely to the goals of a successful IT Security Architecture. These four points define the Primary Practices of ITIL v3:

1. **Market Definition:** Defining who the customers are for IT service.
2. **Offering Development:** Identifying services to be offered to customers and initiating projects to develop those services.
3. **Prepare for Execution:** Prepare the IT organization to be able to carry out the services strategy successfully, including identifying critical success factors, setting objectives, prioritizing initiatives, promoting growth, and differentiating the IT organization as a service provider.
4. **Strategic Asset Development:** Identifying assets that may be used as building blocks for the creation of services and initiating projects that develop those assets. (Long 2008)

It is precisely this focus on service that provides a framework well suited to an IT Security Architecture implementation. ITSA is about achieving success in a challenging, dynamic balancing act between keeping information flowing and keeping it secure. Additionally, the concept of an over-arching influence is shared between ITSA and ITIL.

Market Definition

The heart of the Market Definition practice may be better conceived of as “Customer Definition.” This redefinition allows us the needed granularity to define exactly what a “customer” is in the ITSA and who meets that definition. Defining customers in terms of IT Security Architecture is a unique challenge; often those who “buy” the service are not necessarily those who “use” the service. To overcome this challenge, and reconcile ITIL and ITSA, I offer the following definition: *Anyone who has a legitimate need for an organization’s data is a customer.*

In today’s world of multi-faceted, interconnected systems and processes, this definition of customer can encompass an enormous number of entities. Typical “customers” will include employees, contractors, customers, other companies, and the public. Non-traditional definitions of an ITSA customer may be found in unsuspecting places, as well - perhaps your paper is ordered automatically through the copy-count function on your copy machines. Your office supplies source has just become a customer; a customer with a limited demand for information, but a customer who relies on accurate, timely information nonetheless.

It is also important to note that this “customer” relationship is dynamic, ever-changing, and contextually dependent. The crucial word in the definition of customer is legitimate. For example, what one entity may legitimately access in Situation A, it may happen that the same entity in Situation B may not access the very same information. Thus, it is important that “legitimate” be clearly defined by each organization seeking to implement the ITIL framework, ensuring that this definition does not hamstring daily operations, and that it complies with the organizations rules and policies.

Applying the ITIL framework to ITSA and conceiving of IT Security Architecture in a customer-focused way allows us to gain insight from sources that previously would have been tough to connect to IT Security. One prominent example of this insight is gleaned from preeminent business strategist Peter F. Drucker. Drucker writes that “[b]usinesses are not paid to reform customers. They are paid to satisfy customers.” (Drucker 2008)

In an ITSA/ITIL context, what does that mean, exactly? Satisfying customers, as opposed to reforming customers, means meeting their needs in a timely manner, something that is often easier said than done. “ITIL is based on the need to supply high-quality services with an emphasis on customer relationships. The cross-functional nature of business services and the development of services across organizational lines can be managed only if the services are effectively governed and compliance to standards, policies and requirements is monitored.” (Shewmaker, Brock et al. 2006)

This process of governance and compliance, a strength of IT Security Architecture, is incorporated in the second pillar of ITIL v3: Offering Development.

Offering Development

Now that we have expanding our knowledge base through the ITIL framework, we can once again reference Drucker in the quest to identify services demanded by customers and initiate those projects: “High-tech innovators are least likely to be market-focused, and most likely to be technology and product-focused.” (Drucker 2008)

Assuming Drucker is correct, “offering development,” what amounts to a detailed market analysis, becomes a much more complex process when done within an IT Security Architecture context. Pitfalls are all around the IT Security Architect as they move through the ITSA/ITIL process in an attempt to service their customers. Two of the biggest obstacles on this path are diametrically opposed: *paving cowpaths* and *technology for technology’s sake*.

Because determining services to be offered to customers can be a very challenging and resource-intensive process, it is easy to fall into the trap of “paving of cowpaths.” Paving cowpaths means updating existing processes through technology, without substantially changing or enhancing the process itself. In the case of IT Security Architecture, an example is attempting to force a physical-world model for handling or processing documents into a digital context.

While there are some processes and procedures that are best left unchanged, or simply automated through technology, these are the rare exception. Often there is much value to be had in re-evaluating these processes, working towards successful integration into a larger, more technologically capable ITSA/ITIL architecture.

The other significant danger facing a Security Architect when it comes to “offering development” is technology for technology’s sake. As an example, while it may be possible to encrypt every file on every hard drive with a 2,048 bit key, and require a biometric scan to be performed before any sensitive action is taken, is this really going to increase the secure function of an organization? While it may increase the security, it will most certainly decrease the functionality - and it is important to remember Drucker’s admonition: we are not “are not paid to reform customers. [We] are paid to satisfy customers.”

The sword of technology for technology’s sake also cuts the other way. If you are a small, local, integrated technology firm, you likely do not need the latest, greatest, untested, Enterprise Resource Planning system. This could expose you to unnecessary risks, and is not focused on the needs of your customer, but rather the push towards the technological bleeding edge. Hurried implementations of untested hardware and software are only good for the companies who produce, sell, and support that hardware and software - not for your organization.

Preparing for Execution

The ITIL framework encourages security professionals to identify critical success factors, set objectives, prioritize initiatives, promote growth, and differentiate the IT organization as a service provider. (Long 2008) Perhaps Drucker says it best: To achieve success, “Goals and objectives for each area need to be set.” (Drucker 2008)

Modern research supports Drucker’s claim. Especially in a high technology context, it is vitally important to ensure that these goals are focused on the needs of the customer (business) and not fall into the above mentioned pitfalls.

Security Objectives should be defined in general from a business point of view. They serve the purpose to provide clear and understandable communication of the main security goals. In our point of view, it is important to derive these security objectives not from a technical perspective (i.e. IT perspective) but to define the goals from a professional perspective of the involved parties or stakeholders. (Hafner and Breu 2009)

This idea is so crucial to IT Security Architecture that Sherwood, Clark, and Lynas put the concept in the title of their book: *Enterprise Security Architecture, A Business-Driven Approach* [emphasis added]. (Sherwood, Clark et al. 2005) ITIL facilitates this process by allowing an IT Security Architect to work under a framework that ties together the processes and activities of their organization. In this way, ITIL is not unlike Bernard’s EA3 Cube. (Bernard 2005) Both the ITIL framework and the EA3 Cube apply to management aspects other than security, their combination of inter-related modeling serves to assess nearly all of the contingencies that are encountered within a modern organization.

Strategic Asset Development

Strategic Asset Development is listed as the fourth pillar of ITIL’s Primary Practices not because Strategic Asset Development is icing on the cake, but because the other three Primary Practices (Market Definition, Offering Development and Prepare for Execution) must be solidly in place before expanding into Strategic Asset Development. Strategic Asset Development is also the most challenging of the Primary Practices as far as IT Security Architecture is concerned.

With the Primary Practice of Strategic Asset Development, the ITIL v3 framework seeks to create processes that themselves become strategic assets and create competitive advantage and market differentiation. (Malone, Blokdijsk et al. 2008) In an exceptional iteration of an ITIL framework, a positive feedback loop is achieved where the ITIL framework itself becomes a strategic asset that is continually cultivated and fed back into the organization. Strategic Asset Development can also offer many other benefits on the road to ITIL’s self-fulfilling prophecy.

For the IT Security Architect, opportunities to develop strategic assets abound. It is once again beneficial to look outside of the traditional technology realm to draw development strategies. One particularly well-suited case study is “Human Resources as Strategic Assets.” (Mueller 1996) In this case study, the author develops the concept that a true strategic asset does not develop from senior level policies, but rather from “the 'social architecture' that results from ongoing skill formation activities, forms of spontaneous co-operation, the tacit knowledge that accumulates as the unplanned side-effect of intentional corporate behaviour [sic].” These unplanned side-effects of spontaneous co-operation are exactly what an IT Security Architect should be looking to both facilitate and capitalize upon.

As Bernard’s EA3 cube illustrates, both security and technology cut across all Lines of Business and EA components of an organization. These intersections are frequent, and often insignificant. However, some of these intersections produce the “spontaneous cooperation” that Muller discusses. A well designed IT Security Architecture should be able to allow for experimentation and the evolution of processes and procedures without placing the organization and its data at undue risk. Conversely, when “spontaneous cooperation” produces unforeseen consequences, the underlying IT Security Architecture should facilitate the detection of anomalies and take appropriate action (either preventative or reactive).

ITSA and ITIL, Conclusions

By incorporating the many strengths of the ITIL framework, an IT Security Architecture becomes better able to facilitate inevitable organizational progressions by focusing on the needs of the customers. This customer-centric mentality encourages innovation within the organization by meeting the needs of customers as they arise. It also allows for innovation by not restricting the strategic assets of an organization (often the employees themselves) to a set path of action. The combined strength of ITIL and IT Security Architecture ensure that as these changes take place, either organically or through targeted initiatives, the information required is stored, accessed, and delivered securely.

Sources Cited

- APMGroup. (2009). "ITIL® Home." Retrieved 29 March, 2009, from <http://www.itil-officialsite.com/home/home.asp>.
- Bernard, S. A. (2005). An introduction to enterprise architecture. [Bloomington, Ind.], AuthorHouse.
- Drucker, P. F. (2008). The Essential Drucker: The Best of Sixty Years of Peter Drucker's Essential Writings on Management, Collins Business.
- Greiner, L. (2007). "ITIL: the international repository of IT wisdom." netWorker **11**(4): 9-11.
- Hafner, M. and R. Breu (2009). Security Engineering for Service-Oriented Architectures.
- Long, J. (2008). ITIL Version 3 at a Glance: Information Quick Reference, Springer.
- Malone, T., G. Blokdijk, et al. (2008). ITIL V3 Foundation Complete Certification Kit - Study Guide Book and Online.
- Mueller, F. (1996). "HUMAN RESOURCES AS STRATEGIC ASSETS: AN EVOLUTIONARY RESOURCE-BASED THEORY*." Journal of Management Studies **33**(6): 757-785.
- Sherwood, J., A. Clark, et al. (2005). Enterprise security architecture : a business-driven approach. San Francisco, CMP Books.
- Shewmaker, R., D. Brock, et al. (2006). SOA Management Landscape - Achieving Enterprise Service Management within the Modern IT Architecture.