

IT Security Governance in Existing and Emerging Organizations: A Case Study

Shay C. Colson

6 March 2009

IST 700 - Spring 2009 - Dr. Bernard

Introduction

Implementing effective IT Security Governance poses unique challenges in every organization. In an established organization, implementation can be easier because an overarching governance structure exists, and management and employees alike are used to working under this framework. However, it can also be more difficult: envisioning IT Security as a core component may require a sea change for those who create and enforce governance policies, not to mention the rest of the organization who is subject to these policies.

In an emerging organization, effective IT Security Governance can be interwoven into the initial set of governing policies, providing a great advantage to both the business and security interests of the organization. One of the greatest challenges, however, is the fact that because the organization is new, their business process or model may not be well established, and may change frequently. How can you create and implement effective IT Security Governance in such a dynamic, young organization?

In this case study, I will examine these two scenarios and offer suggestions for implementing effective IT Security Governance in both an established and an emerging organization. Effective IT Security Governance is indispensable; organizations need to protect themselves against the risks inherent in the use of information systems while simultaneously recognizing the benefits and the value that can accrue from having secure information systems. (Williams 2001) Realizing these risks and value, however, is a much different challenge for an emerging organization than it is for an established organization - and it is not easy for either. The side-by-side comparison model of this case study will help to illustrate this contrast.

IT Governance Defined

Before we can begin our discussion in earnest, it is important that IT Security Governance be accurately and clearly defined. Sherwood offers the following definition:

[IT Security Governance should] provide a road map to be followed by individual projects serving individual business initiatives. The [governance document] provides the overall strategic direction across the enterprise, and the projects follow that direction. They are also the vehicles by which certain pieces of strategic infrastructure get constructed. (Sherwood, Clark et al. 2005)

I prefer to combine this definition with an addition from Dr. Bernard's book, specifically that "IT security is most effective when it is integral to the enterprise's strategic initiatives business services, information flows, applications, and infrastructure. [It is] best described as an all-encompassing security solution." (Bernard 2005) From this definition, we can begin to work out towards applying IT Security Governance in both emerging and established organizations.

The Buck Stops At The Top

No matter how IT security governance is defined, one thing that has become clear in today’s business environment is that information security is a corporate governance responsibility :the buck stops right at the top, and there can be legal consequences. (von Solms and von Solms 2004) Leading scholars suggest that the formation of effective IT Security Governance requires “greater involvement of boards of directors, executive management and business process owners,” (Williams 2001) This requirement plays out very differently in the two types of organizations we are examining.

Established Organization	Emerging Organization
<p>Problem: Implementing effective IT security governance will require serious effort from a high-level leader in the organization. If there isn’t a “C-level” officer who both believes in the value of effective IT security governance and possesses the necessary vision to create and implement it successfully, the organization’s governance structure is sure to remain lacking.</p>	<p>Problem: In a newly formed organization, the board of directors, executive management, and business process owners are likely to be the same group of people. Additionally, except for very few rare cases, the core competencies of the organization are not likely to be IT Governance or Enterprise Architecture/Design. Lacking in this expertise can prove disastrous at this nascent stage.</p>

Solution: To overcome these challenges, an Enterprise Architect can be an enormous asset. For the established organization, an Enterprise Architect can assist the CTO or CIO in determining the impact of IT in their organization and help the board realize the value that an effective IT security policy can add. For an emerging organization, an Enterprise Architect will help the organization define and refine their structure, incorporating IT security governance as a core concept. After all, information security is a multi-dimensional discipline, and all dimensions must be taken into account to ensure a proper and secure environment for a company's information assets. (von Solms and von Solms 2004)

Policy Creation: Not Just 1, 2, 3

In their 2004 book, IT Governance, Weill and Ross suggest that effective governance can be created from the answers to three simple questions:

1. What decisions must be made?
2. Who should make these decisions?
3. How will we make and monitor these decisions? (Weill and Ross 2004)

Although admittedly over-simplified, this basic framework does provide a solid jumping-off point, but is not enough by itself. Other vital considerations include strategic alignment with organizational direction, value delivery, risk management, and performance measures. (Williams 2001) With these additional aspects included, an organization can begin to codify such a policy.

Established Organization	Emerging Organization
<p>Problem: Developing a well-written, robust new policy in an existing organization can be an enormous expenditure of resources. Moreover, a newly formed security policy may mandate revisions to existing policies, practices, and procedures in order to bring them into compliance with this newly instituted IT Security Governance document.</p>	<p>Problem: In a newly formed organization, the business process itself is likely to be in a state of flux, still adapting to market requirements and experiencing the growing pains that all organizations initially encounter. Without an established process from which to draw inspiration, creating these high-level policy documents may seem like an exercise in compiling “best practices” from industry magazines, or simply the luck of the draw.</p>

Solution: Refer back to our definition of IT Security Governance: “integral to the enterprise’s strategic initiatives business services, information flows, applications, and infrastructure.” (Bernard 2005) Once an organization understands that this thread runs throughout - and pays dividends throughout - it is much easier to justify the resource expenditure required for creating a well-constructed policy document. Incorporating all of the aspects mentioned by both Weill and Ross and Williams will lead to a robust, effective IT Security Governance document and policy. Next, the organization must ensure that this policy is presented clearly and effectively.

Top to Bottom: User Focused

An IT Security policy or governance document must be presented in such a way that the users - those who are both subject and subjected to the aforementioned document - can access, interpret, and apply the document. (Höne and Eloff 2002) Otherwise, the policy becomes a formality - something that is not only ineffective, but potentially damaging to the organization. It is vitally important to remember that these policy documents are no longer a kind of corporate insurance policy. (Williams 2001)

Established Organization	Emerging Organization
<p>Problem: Especially for large organizations, the list of policy documents is cumbersome by sheer volume alone. Aside from making the policy document available, users need to know where to look to find the document when needed - or perhaps be made aware what type of situations mandate that they reference the document.</p>	<p>Problem: Depending on the size of the organization, many emerging organizations are more concerned with juggling the business requirements of taking and meeting orders, creating project proposals, and other bottom-line oriented activities. For maximum benefit, users must be made aware of policies in such a way as that it informs these business activities.</p>

Solution: Not only must the document be created and presented in an accessible format, but it must be updated regularly to remain relevant and coherent. The actual wording of principle statements is also critical to the effectiveness of the information security policy, as a misinterpreted statement can damage an organization’s information security arrangements. (Höne and Eloff 2002)

For emphasis, or in an organization where IT Security is of paramount importance (perhaps a Department of Defense agency, or technology corporation that deals with highly sensitive research), the policy can be presented in person, typically as a training. For additional impact, training can be conducted by high-level executives of the organization. Users will not believe in the information security policy if they do not see their leaders conforming to, and living by, it. In fact, for the policy to be truly effective, it needs buy-in from all levels of the organization. (Höne and Eloff 2002)

It’s Alive! The Evolution of IT Security Policies:

As I have already established, the creation, distribution, and implementation of IT Security Governance is a very important, expensive, and time consuming undertaking for any organization. This does not, however, mean that it is a one-time process, or that an organization can simply review their policy documents every *X* number of years (2, 5, 10, etc.). This mentality will almost certainly guarantee that the organization is not getting the most out of their policies, employees, or technological investments.

Established Organization	Emerging Organization
<p>Problem: When a large, latticed policy structure is established, changes and reviews can certainly be a burdensome process. Moreover, many of an organizations policies do not require frequent review or updating. Convincing leadership that an IT Security policy review is required more often than other policies can be a difficult pitch to make, even for a CIO/CTO/CISO.</p>	<p>Problem: Because an emerging organization will face an accelerated pace of change, it is perhaps even more imperative that IT Security Policies be reviewed and changed as needed. Opening new offices, using off-site data storage or processing facilities, the implementation of a CRM or ERP system, any public-facing web applications, and other business tools mandate a review of IT Security policies.</p>

Solution: It is vital to realize that these policies should be considered “living” documents - it is acceptable to review and change them as business and organizational needs dictate. In fact, and organization who views their IT Security Governance as a “set it and forget it” part of their business is deserving of what comes from that mentality. Thorough policy reviews, while not inexpensive, are nowhere near the investment of creating the policy properly in the first place. With a thorough, robust policy in place, reviews should be relatively straightforward, and can often highlight other areas of the business process that may be lacking.

Conclusion

Interestingly, the challenges for creating and implementing effective IT Security Governance vary greatly between established organizations and emerging organizations, but solutions are similar, if not identical. This is a clear indication that each organization, emerging or established, global or domestic, will face unique challenges. These differences, however, are overcome by solid execution of the basic tenants of IT Security Governance discussed here:

1. *Effective involvement from organizational leadership.* Not only must policies be created and set by the “C-level” of an organization, leadership must walk the walk, as it were. “Do as I say, not as I do” will not result in a secure organization. If needed, bring in the required expertise of an Enterprise Architect or other consultant.
2. *Successful IT Security Governance is not cheap or easy.* Investing a sufficient amount of time and resources is critical to establishing a functioning, robust set of policies such that organizations protect themselves against the risks inherent in the use of information systems while simultaneously recognizing the benefits and the value that can accrue from having secure information systems. (Williams 2001)
3. *Focus on the users.* The document must be created in such a way that employees can access, interpret, and apply the policies contained therein. If this means additional training, then either the policy should be reviewed for clarity and accessibility, or the investment in training should be approved.
4. *Establish, review, adapt, succeed.* Especially with today’s break-neck pace of technological changes, it is absolutely essential that an IT Security Governance policy be reviewed on a regular basis with the intent that any needed changes can be made, distributed, and enforced with the backing of senior management.

Following these basic tenants of effective IT Security Governance will go a long way towards helping any organization, emerging or established, implement policies in the best possible way. Despite their unique challenges, solutions remain similar, allowing these organizations to draw on existing best-practices, and learn from mistakes made by other organizations. An effective IT Security Governance structure is the most effective way for today’s organizations to realize the value of effective policies in order to both protect themselves from technological downfalls and reap the benefits that technology can offer.

Bibliography

Bernard, S. A. (2005). An introduction to enterprise architecture. [Bloomington, Ind.],

AuthorHouse.

Höne, K. and J. H. P. Eloff (2002). "What Makes an Effective Information Security Policy?"

Network Security **2002**(6): 14-16.

Sherwood, J., A. Clark, et al. (2005). Enterprise security architecture : a business-driven approach. San Francisco, CMP Books.

von Solms, B. and R. von Solms (2004). "The 10 deadly sins of information security management." Computers & Security **23**(5): 371-376.

Weill, P. and J. W. Ross (2004). IT Governance.

Williams, P. (2001). "Information Security Governance." Information Security Technical Report **6**(3): 60-70.