Developing a framework for understanding Security Governance

INTRODUCTION

Organisations

- rely more and more on computers for multitude of tasks
- but are badly prepared to cope with the increased risks in their IT environment
- most are simply doing "what everyone else is doing."

These problems lead to a need to improve Corporate Governance by including guidelines for decision making about, and accountability for, information security. By improving Security Governance it is not only expected that organizations will be more effective in securing their systems, but should in effect also assist incident handlers, and other people involved, to make more appropriate decisions when dealing with incidents and other security related matters.

In order to better understand Security Governance, a Security Governance framework was developed by investigating the literature on Corporate and IT Governance, and then by undertaking an initial case study based on this framework.

WHY SECURITY GOVERNANCE?

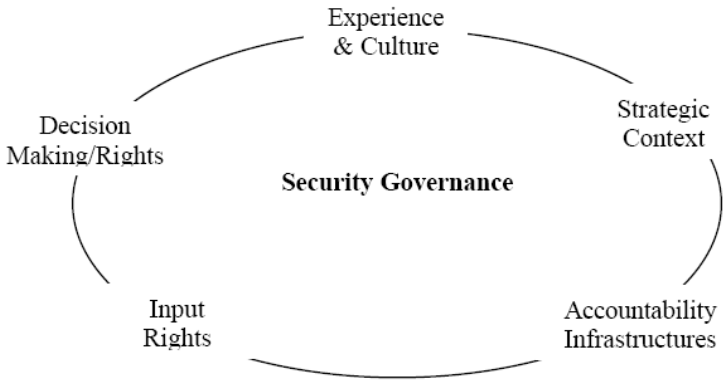
IT Governance stipulates that because enterprise IT investments are often large, the decision-making process and the chain of authority that concerns spending must be documented and managed well. Security Governance is not only important to minimize the occurrence of security incidents, but also to limit the damage from any incidents that could not be prevented.

THE ESSENCE OF SECURITY GOVERNANCE

Governance is about effective coordination in a dynamic environment where both knowledge and power are distributed. Security Governance is a subset of Corporate or Enterprise Governance and includes:

- Security responsibilities and practices
- Strategies/objectives for security
- Risk assessment and management
- Resource management for security
- Compliance with legislation, regulations, security policies and rules
- Investor relations and communications activity (in relation to security)

The framework adopted the "success traits" or best practices from Corporate and IT Governance to Security Governance and has shown to provide an adequate and interesting description of the Security Governance process and to allow a structured analysis of that process in an organization. The framework consists of the following interrelated areas: Strategic Context, Decision Making Rights, Accountability Infrastructures, Input Rights, and Experience and Culture.



Strategic context

Creating effective Security Governance involves a series of decision points based on a sound understanding of the firm's strategic context. This understanding is best expressed and hence communicated through mission statements.

Decision Making Rights & Accountability Infrastructures

Security Governance is about the arrangements with regard to who (can) make(s) critical decisions and who is accountable for them. Accountability includes the essence of good decision making including feedback loops, documentation, etc.

Input Rights

Effective governance relies on the arrangements of thoughtfully and purposefully combined decision making about major security domains, by the right group of people, using appropriate mechanisms. Organizations need to understand that for the 'right' decisions to be made it must be clear who has input rights into that decision.

Experience & Culture

While the right decision making processes may be in place, they are of no use if there is a culture of ignoring them. While decision making in a particular area may officially be delegated to a lower level, that is of no use if every decision needs to be approved by the level above. Hence, culture is important in Security Governance.

THE UWL CASE

After discussion with two security professionals at the firm the following conclusions were drawn according to the framework previously described.

Strategic context

At UWL, ineffective Corporate Governance at the top management level results in little guidance being given to the decision makers. What emanates is a rather informal security structure and a very narrow outlook and understanding of security (strategy).

Decision Making Rights & Accountability Infrastructures

There was little evidence of feedback loops and no measuring of decisions nor the history of decisions. Decisions and the reasons for the decisions are not documented. Neither input rights nor the inputs given are documented. Decision rights appear to be documented, but the decisions are not. Policies pertaining to security (usage policies, incident handling documentation, etc.) are available but fall short in terms of providing help or guide to the participants in their decision making.

Input Rights

Input rights are similarly unclear and highly unstructured. However, participation in decision making appears fairly high even if one person, the Systems manager, makes all the decisions. There was evidence of limited input rights but there was evidence of active ‘social’ participation too.

Experience & Culture

If the decision to be made were important, authorisation would have to come from the top.

Conclusion

The previous points of the framework applied to the UWL case clearly lead to a sub optimisation of the decisions concerning security.