Margaretha Eriksson
Irbis Konsult AB and DSV/KTH
SWITS Workshop Report 2009

My Licentiate thesis Work is aiming at creating *"A map of key factors for secure information systems seen from an organizational perspective"*. My research question is “How can organizations (enterprises/companies) ensure that the information systems they are developing have a sufficient level of information security?”

I explore the key factors affecting information security during the life cycle of a system, from the analysis phase to design, implementation, use, and maintenance up to the point in time when the system is closed or replaced by a new system. What is appropriate to do in order to retain a secure system?

My hypothesis is that there are a number of processes that must be in place for building secure systems: processes for controlling IT security and information security during the development of the system, as well as guidelines and resources for the education of the users of the system when in use. There might also exist more key factors apart from those involved in the life cycle and the education of users. Are these processes depending on each other? If so, how?

The key factors can be pictured as checkpoints which must be visited once or more during the life cycle of the system. How important is the organizational support for these key factors? Are top managers awarded for compliance, or are other factors as time to market assumed more important? Can system development be halted due to non-compliance to information security requirements on the system? Who are the key agents in these essential processes?

The research methodology and approach used is a Systemic-Holistic Approach blended with anthropological and interpretative components.

The final result is a map of the key organizational factors for developing and maintaining secure information systems, including their dependencies.

My findings so far

As an Industrial PhD student, I have had the opportunity to observe system development in about 20 big, as well as small, system development projects since 2005. I have noticed one big threat to security being stress due to lack of time to make it right. Another source of security threats is lack of knowledge among the everybody, from sales people, to manager of different levels, and down to developers of what to do, and who to ask. Tight time schedules and shortage of resources are inducing flaws, which may cause security threats to the system.

It is obvious that security need to be considered from the very conception of any system, starting from the design phase and even before that, i.e. a total life cycle view. During sales, the sales people need to know about security from a sales and customer perspective, in order to sell a proper security solution to the customer. It is also important that the customer agrees with the solution and its security mechanisms. Seen from above, the security policies of both the supplier and the customer need to align. Applying the 14 layer model (14L2C6T5QM2) presented by Yngve Monfeldt 2008, in the Social layers of the model the upper management and Project Managers need to agree on the solution, and in the Technical layers the technical solution also must be aligned, down to the least bit in an IP address of a firewall, in order to create a secure system.