SCHOOL OF ECONOMICS AND MANAGEMENT
Lund University

Lusax Security Informatics

www.lusax.ehl.lu.se

LXM-TK2-Knowledge & Innovation

Author: Thomas Kalling
Subject: **Knowledge & Innovation**
Date: 5 November 2007
Pages: 2
Recipients: Lusax
Email: thomas.kalling@ics.lu.se

Knowledge & Innovation in the Security Industry

Executive Summary

- There are two major knowledge gaps in the convergent security industry, both of which give certain players competitive advantages.
  - Strong skills in the management of businesses providing new IP, IT and IS-based products and services
  - Strong customer relations
- In this memo we discuss the character and importance of these knowledge gaps, and how different actors, particularly so traditional system integrators, could act to increase their knowledge base while maintaining and leveraging their unique customer relations.
- We argue that mergers and acquisitions, by traditional integrators of new "IP integrators", are imperative in the mid to long term, since organic growth and learning through classroom training and recruitment are too slow, given that we believe the penetration and adoption of new technology in the security industry is non-linear, progressive and incident-driven.

The converging security industry displays many different kinds of knowledge gaps. This memo deals with two of them, and how these knowledge gaps force different renewal strategies, particularly for traditional security integrators. One knowledge gap centres upon knowledge of new technology, typically IP and IT/IS products and systems. The other centres upon the knowledge related to customer relations with end users.

- A traditional security integrator typically faces a knowledge gap in relation to being able to offer qualitative, competitive offerings of new IP- and IT-based products and services. The gap emanates from complexity relating to technology, functionality, sales logics, new purchasing functions (often IP and IT knowledgeable procurement), and operational/installation and maintenance issues. This piece of knowledge will be referred to as "IP knowledge" below.

- A traditional security integrator typically has a competitive advantage in its strong and often personal customer relations. This knowledge often rests on long term experiences of relation-building and years of delivery meeting or exceeding customer expectations and requirements. This will be referred to as "Customer relations" below.

These two pieces of knowledge have highly different properties, and the two gaps require asymmetrically different strategies. We argue that *IP knowledge*, albeit being relatively novel, is easier to obtain than strong customer relations. The entire requisite understanding of how a business based on new IT and IP products and services should be managed is complex (particularly so organisation, marketing, capability base, customer interaction, offering bundling), but *the technical understanding of content and functionality is not tacit but rather explicit* – at least more so than building sustainable customer relations. IP knowledge, at least the technical aspects just mentioned, is also more of a *multi-individual and generic skill* for which there is a common language and well-known theories and standards. An even more crucial aspect is, however, that IP knowledge is about to become absolutely imperative to any player in the security industry. It will be a basic requirement, a *hygiene factor*, within 2-3 years, we believe, for anyone interested in above-industry performance. Other skills sets are needed too, of course, but not being able to offer products and services using IP, IT and IS technology will require aggressive niche marketing strategies or lower expectations on profitability.