SCHOOL OF ECONOMICS AND MANAGEMENT
Lund University

Lusax Security Informatics

www.lusax.ehl.lu.se

LXM-TK3-IP Excellence.doc

Author: Thomas Kalling
Subject: **IP Excellence**
Date: 2 March 2009
Pages: 3
Recipients: Lusax
Email: thomas.kalling@fek.lu.se

IP Excellence

Executive Summary

Competence in IP-based video surveillance business in a broader sense is imperative for security integrators and installers across the world. This memo discusses the results of a global survey distributed to integrators both from the security and IP sides. We focus on the factors that drive IP competence and excellence. Two knowledge obstacles, or phases were identified:

- *Obtaining technical knowledge*: this is explicit, theory-based knowledge that offers an option to enter the IP business, a necessity, but not necessarily advantages.

- *Applying and continuously generating knowledge*: this is experience- and practice-based knowledge that offers potential advantages. It grows with experience and requires experimentation and trial-and-error processes.

The key success factors, i.e. the factors that separate the excellent from the less excellent, are primarily organisational, even if both formal education and experience are clear factors. The more excellent integrators are better at the basic managerial and organisational tasks:

- *Top management involvement*
- *Strategic plans for IP*
- M*easuring and monitoring*
- *Managerial agendas*
- *Culture*
- *Incentives*

The findings lead us to conclude that getting started with IP surveillance is not primarily a knowledge challenge. Rather it requires a declaration of will from corporate, a communicated strategic intent, action plans, measuring and monitoring, and addressing IP business by putting on the management agenda. Creating an "IP culture" is also a significant success factor. Implementing an IP surveillance strategy will probably benefit if it includes acquiring IP talent as a complement to training and recruitment.

Background

Becoming good at selling, installing, managing and operating IP-based video surveillance solutions is difficult yet a strategic challenge to global security integrators. IP surveillance growth has been and is strong, and will continue to take share from analogue solutions. An approximate 15-20% share currently might grow into an 80%+ share in the next five to six years, meaning substantial growth depending of course upon changes in general demand for surveillance products. Being able to compete for this growth poses, however, some significant challenges. This memo focuses on *competence* and how competence needs to be managed to excel in IP. It is based on a survey of 1,736 respondents from across the world, representing both more traditional security integrators (approx. 52%) and pure play IP integrators (approx. 48%). The survey included questions revealing to what degree 1) competence and skills, 2) institutional forces, and 3) organisation and management

impact IP performance. Findings suggest that 1) competence and skills matter, and that 2) they are the product of and can be managed by means of organisation-internal institutional pressure and management.

Two Phases in Competence Development

Firstly, the study suggests that becoming excellent on IP surveillance is a two-step process including:

- *Obtaining knowledge*: formal education surfaces as a strong key success factor. The higher the general degree of education, the stronger the company is at IP surveillance. By education we mean formal education, not necessarily job education and training, even if such efforts might compensate for lack of formal of education. The knowledge we include here is the explicit knowledge of technical conditions, including electronics, cabling, network, systems management and so on. It is knowledge that is explicit in character and which can be learned by means of theory understanding, such as classroom training and book-reading, not necessarily practical experience (even if this will be beneficial). This explicit technical competence however, is primarily a *ticket to the dance-floor*, a basic requirement and a hygiene factor, that will allow players into the market. It does not provide immediate advantages or price premiums.

- *Applying knowledge*: experience of IP surveillance, in the form of number of years a person has worked with IP in different parts of the value chain, also turns out to be a success factor. In contrast to the explicit and technical knowledge discussed above, IP experience is implicit and tacit, and based on practice, not classroom training or studies of theory. It includes all the competence and skills required from the point of approaching customers first time, throughout design, specification, installation, and after sales activities such as service and systems management. Experience generates knowledge by means of the trial-error-correction-trial loop, and so requires reflective practice, where experimentation is supported (and first failures accepted). This implicit and personal knowledge is a logical extension to technical competence, and a potential source of *competitive advantage*, as it is subject to increasing returns (the more knowledge you have, the more you want and get) and time compression diseconomy (knowledge cannot be imitated rapidly without significant costs).

These two steps are sequential, meaning the former generally is a precondition for the latter. Our study reveals that pure play IP integrators are ahead in this race towards IP excellence, but that overcoming the first technical knowledge threshold could open up for advantages to security integrators as they have established customer relations and stronger awareness about operative security issues.

What Drives Learning?

Apart from underlining the importance of education and experience, the findings imply that what separates the excellent from the less excellent, primarily is related to basic *managerial and organisational matters*. It turns out that institutional forces, such as the degree to which integrators are driven by customers, suppliers, competitors, legislation and standards, and general media, do not create differences in performance: i.e. all players basically understand and interpret similarly the need and urgency for IP competence. The factors that explain IP performance differences all centre upon clearly interlinked organisational and managerial issues:

- *Top management involvement*
- *Strategic plans for IP*
- M*easuring and monitoring*
- *Managerial agendas*
- *Culture*
- *Incentives*

The ones who are good at these management features also are better at IP business. They drive both the first and second steps of obtaining and applying IP knowledge. The implications based on this is that IP performance starts with a *declaration of will and intent*, including the *pace of change* (e.g. "X% growth in IP business per year", "outcompete rival MNO", or "Y% increase in IP profits per year"), and whether to be a first-mover, a fast follower or a laggard. The intent must be formulated in a *strategic plan* and broken down into *specific targets*, all the way down to individuals (e.g. salesmen, general managers) if necessary, and they should be attached by *action items* needed to achieve the targets. Progress should be *monitored and measured* regularly, typically in conjunction with regular performance reviews, and there should be actions to exception to targets. Furthermore, softer matters such as *talking about IP*, putting it on the management meeting *agendas*, and *incentivising and rewarding* those who improve their skills, be it in sales, installation, service or any part of the value chain, are important too.

As it turns out, and this might be good news for those who have not yet acted, is that there are no major institutional obstacles to progress and learning. In fact, it is perhaps a matter of will rather than ability, and it does not necessarily imply hefty investments. It starts with will and motivation, and the implementation of rather normal management principles and actions.

Implications

As a conclusion, we suggest that there is only one "path" to IP excellence, and that different players have made different achievements along this path. This path has two major steps: creating/obtaining technological competence and applying it to business continuously in order to increase business IP competence by experience. These two steps require formal education as well as job training, and, as firms proceed, experience by trial-and-error learning. Fairly basic management features will determine to what extent players succeed, and it all starts with a declaration of will by corporate management, which is then broken down into plans that are measured and monitored and incentivised.

Depending on the background of the integrator and the achievements made, it will face slightly different challenges. In general, for integrators making a fresh start towards IP excellence, solutions to the following four implications are imperative:

- You *must* learn technology to pass the first threshold including implications throughout the entire value-chain: sales, installation, service, operations and management. This can be done via *education*, *training*, *recruitment*, but also through *M&A* and *alliances*. We argue that many integrators should aim to catch up not only by training – M&A and inter-firm cooperation could speed up the process.

- You need to strive for *experience* as a complement to formal education. This includes being prepared to *experiment* in a trial-and-error fashion (but in a controlled environment), and to accept failures as you venture in to new territories.

- You need to make *new contacts at the end-user* (e.g. CIO and IT department). Established contacts with security directors are important, but IP surveillance is as much a bandwidth and storage question. There are many ways to "get to" the CIO and IT department, but it involves absorbing the typical IT industry way of doing business, and among other things aiming for volume not margin, large batches rather than one-offs, problem-solving relations, and assisting end-users with business cases and ROI and TCO assessments. It involves, naturally, a change of not only competence but also *culture* and *perceptions of how business is done*.

- You should leverage advantages associated with *scale*, *presence/footprint*, *recognition*, *operative security skills*, and *customer relations*. These are assets that many IP integrators lack, and that can be sources of competitive advantage and price premiums for security integrators.