SCHOOL OF ECONOMICS AND MANAGEMENT
Lund University

Lusax Security Informatics

www.lusax.ehl.lu.se

**LXM-TK1-IP Integration**

**Author:** Thomas Kalling
**Subject:** **Learning IP Integration**
**Date:** 26 June 2007
**Pages:** 5
**Recipients:** Lusax

## Leads to a Successful IP Integration Business

### Executive Summary


- Significant knowledge gap in the industry (not visible to all yet)
  - IP knowledge "correlates" with the vertical: stronger at the top, increasingly weaker downstream
  - Tacit knowledge, requiring practice and documented success cases. Not rhetoric, fad or theory
  - Suppliers are a strong influence
  - Educational differences: IP generally more educated
  - All functions a challenge for traditional security players; Sales only for IP integrators
- Experience & Volume are absolutely imperative
  - M&A or volume-generating partnering – organic growth and classroom training not fast enough
  - Price cuts, new revenue models could be an alternative to win market fast
  - To institutionalise operations a must, including the culture of the operation
- Specialist and Differentiated Organisations required, at least temporarily in early phases
- Driven by market (customers, suppliers, competition) demands, not trends, regulation or standards
- Dense Cultures in successful companies:
  - Heart and brains and on paper
  - Peer to peer & Principal to agent


This memo reports the findings from a study aimed at increasing the understanding of the factors that drive or hamper successful business change within the security sector, particularly so the critical success factors behind change towards becoming an integrator of IP surveillance products.

### Background and Theory

The security systems integration sector is undergoing significant changes, as is the entire security industry, following the introduction of new information technology and the IP protocol, which substantially alter the ability to expand the functionality and quality of security services such as, in this case, surveillance. Analogue CCTV systems still make up a larger proportion of the surveillance camera market, but network cameras are growing faster. The selling properties of network cameras include functionality, storage, analytical possibilities, and better economy (at least for larger installations). What supports analogue cameras is primarily legacy: already having an infrastructure built up around analogue surveillance TV means the marginal investment typically needs to build on what you have.

The surge in demand for IP surveillance solutions has initiated an "invasion" of players. Both traditional security integrators as well as companies supplying network services or integration of IT services now compete over the growing market. This shift in technology forces players to modify their operations and change their business practices. This can be viewed as a radical organisational learning exercise (e.g. March, 1991), whereby routines, structures and the view on the business are changed. Typically, the forces that impact or hinder this process can be structured into three different factors:

- *Cognitive* (implying that change is related to the nature of the knowledge behind the new operation and business, and how that knowledge is related to the knowledge that individual subjects have)
- *Normative* (implying that change is also related to the will of individuals to change as well as the institutional forces internally in the organisation and externally)

- *Organisational context* (meaning the way the immediate context of the subject is impacting learning, through structure and control)

These theoretical constructs serve as the basis for this study, trying to identify leads to the important learning factors behind becoming an IP integration operation (see Appendix for questionnaire).

## Method

This is a case study of one IP surveillance education event in Chicago, IL, in June 2007, where a network camera supplier presented its company and products and services. Some 34 participants from around the Chicago area partook, of which 60% were IP/IT integrators, 30% were more traditional security integrators, and 10% were distributors of IT, IS and IP related products. The data collection method included:

- *Questionnaire survey*. A questionnaire was handed out at the start of the first day, and collected at lunchtime the same day. This was exclusively a deductive, hypothesis-testing exercise. Some 33 of 34 participants responded.
- *Interviews*. Ten people were singled out for further interviews. These interviews allowed for more unstructured and inductive discussion where respondents were asked to explain freely their view on the obstacles to developing a successful IP integration operation.
- *Observation.* Two researchers partook throughout the entire education session, and observed concerns and discussions among the audience and the teachers. Several observations hinted about questions to discuss in interviews, and observations also helped us interpret the data collected.

## Results

The data included three analyses: 1) general concerns of participants, 2) the role of demographics such as belonging primarily to IT/IP or security, age, industry experience and level of education, and 3) critical success factors.

Starting with **general concerns**, the data suggests among other things:

- A *significant knowledge threshold*, visible to some actors but not all. The knowledge about purchasing, installation, service and maintenance is something IP and IT savvy players already have, while they would like to know more about the customer. IP players claim they are considering partnering with traditional security players.
- Logically, respondents find the IP knowledge required to be *stronger upstream*, then *continuously weaker downstream*. Many claim that end-users are not driving the change, and that they know more than customers.
- The knowledge threshold is also emphasised by *perceived tacitness* of IP integration knowledge.
- IP change is thus *practice-driven* and most respondents claim that change is no longer driven by fad, regulation, standards or trend but by visible success cases that show the cost/benefits more clearly. In that respect, *market institutions* are currently the most important, not regulation or law.
- This puts *growth options* in focus, and we question whether organic growth can propel growth enough to win share and possibly set business standards. *M&A*, aggressive *inter-firm collaboration* as well as alternative *revenue models* (e.g. subscription, price cuts and discounts) might be the best way to compete currently.
- The change to IP is primarily *driven by top management*, not technical staff or general employees. However, successful IP integrators also involve personnel more strongly (see below).
- Among respondents, there was a general perception that the integration of traditional analogue CCTV and IP surveillance could be embodied by the individual employee, and that in consequence specific IP integration tasks need not be separated from other work. However, this was one of the factors that separated successful from less successful companies, where the former tended to separate IP from other work (see below).

Looking at **background variables**, it turned out that *respondents belonging to IP and not traditional security more strongly and more often*:

- Think IP–related tasks are more complex than traditional, analogue security work
- Think the IP introduction is slow
- Think the need to get IP knowledge is less important
- Know more than their customers about IP surveillance
- Talk more about IP with colleagues and superiors

- Have a strategic plan for IP products
- Are rewarded for learning more about IP
- Organise IP work separately from other work
- Do not need to reorganise purchasing
- Do need a specialised sales force

Furthermore, it turned out that *industry experience* was associated with less concern about IP, and with a stronger belief that purchasing can handle both IP and traditional surveillance products. *Age* was more associated with knowing less than customers, not as strongly associated with wanting more standards. It was also not as strongly associated with active control of IP operations. Interestingly, *education level* was associated with knowledge of IP, belief in the added value of IP, being perceived as a leader in IP, strong IP strategy commitment from top management, and a separate specialist organisation of IP work.

Finally, looking at the **critical success factors**, we used three questions as indicators of success, indicating how experienced and competent the organisation is. These questions are listed below.

- My company already knows enough about IP surveillance products to develop or run a business
- My company knows more about IP surveillance products than our customers
- Our competitors regard us as leading on IP surveillance products

The variables that correlated significantly (and positively) with these were:

- We organise IP surveillance work separate from other work in the company (positively)
- The pace of introduction of IP surveillance products is slow
- Our top management team is driving the work with IP
- It is the employees that trigger the effort to obtain IP surveillance knowledge
- IP surveillance is discussed in all management meetings
- My boss discusses IP surveillance with me often
- I have worked a lot with IP surveillance products in the past
- The main source of pressure comes from customers
- The main source of pressure comes from competitors
- The personnel always talks about IP surveillance
- My company has a strategic plan to develop our IP surveillance business
- We need or will need a specialised sales force to be able to sell IP surveillance products
- Partnership with traditional security companies is of strategic importance for us.

These correlations lead us to suggest the following *critical success factors*:

- Knowledge Management
  - Specialists
  - Differentiated and specialised organisation structure
  - Sales still an issue – partnering with traditional security players an opportunity
- Market Driven Development
  - Competition and Customers, not trends, buzz or regulation
- Established Business: Experience and Volume
  - Capability and Will: Heart and Brains
  - Managers *and* Employees
  - Peer to peer and principal to agent
  - Documented and understood strategies

Explaining these CSF's, we argue it is quite clear that in order to run a successful IP surveillance integration business, there are some significant knowledge gaps, thresholds, to resolve.

*Cognitively*, one has to realise that the IP business differs from traditional analogue security work. It is a novelty to most incumbents, it is technically complex, it is operationally different, and it requires different sales methods and processes, although many indicate that they will need to partner with traditional security players to utilise their good customer relations. Knowledge about IP operations is reportedly more tacit and complex, emphasising the need to quickly get experience to reach critical mass both on the cost and revenue/quality sides. We do not think organic growth will achieve this (unless revenue models are radically modified), but rather that M&A or aggressive horizontal collaboration are the right moves for an integrator.

*Organisationally*, it is also quite clear that the tacitness of IP knowledge puts pressure on organisations to specialise and separate IP work, at least initially. Statistics also indicate that successful IP integrators already do this to a higher extent than others. Believing that the individual employee can work with both IP and other issues is probably a mistake, implying that IP convergence within a company will have to be carefully thought through and organised. Among functions, purchasing and installation and service are more prepared, whereas there are stronger concerns, even among IP savvy players, that the sales function must be improved as well as differentiated from other sales.

*Institutionally*, we argue that the main source of knowledge comes from upstream, typically vendors. End users typically do not provide input as to how IP can be used effectively, or to what ends an IP solution could be used. The pressure to adopt IP products is driven by market institutions such as competitors, suppliers and customers, and not trends, regulation or fad. Internally, successful IP business requires the involvement of top management, but also among staff and between management and personnel. This separates the successful from the others. There has to be monitoring of IP work and incentives in place to make people realise the importance. A dense culture does not come without effort, and it is likely that classroom training or rhetoric alone are not enough, but that visible and understandable real life cases of IP surveillance need be used to convince people and to stimulate further learning and the pace of change.

## Appendix, Questionnaire & Respondents

1 I have worked a lot with IP surveillance products in the past
2 The knowledge required to work with IP surveillance is similar to analog surveillance products
3 My company already knows enough about IP surveillance products to develop or run a business
4 Knowledge of IP surveillance products is best learned by practising it
5 IP surveillance products are similar across different suppliers
6 There are many suppliers of IP surveillance products
7 The installing and service & maintenance of IP surveillance products is more complex than for our other products
8 Our main source of knowledge about IP surveillance products is through suppliers
9 My company knows more about IP surveillance products than our customers
10 The pace of introduction of IP surveillance products is slow
11 IP security holds the potential of offering added value beyond typical security needs for the end-users
12 I wish there were more standards for IP surveillance products
13 Applying and using knowledge of IP surveillance is easier than actually acquiring it
14 Getting knowledge about IP surveillance is the most important challenge to our company currently
15 The main source of pressure for us to acquire IP surveillance knowledge comes from laws, regulation and industry standards
16 The main source of pressure comes from customers
17 The main source of pressure comes from competitors
18 The main source of pressure comes from suppliers
19 The main source of pressure comes from consultants to end users
20 Our competitors regard us as leading on IP surveillance products
21 General media and trade press act as a significant force in pushing the IP transition ahead
22 Our top management team is driving the work with IP surveillance knowledge in our company
23 It is the employees of the organisation that trigger the effort to obtain IP surveillance knowledge
24 The personnel always talks about IP surveillance in my company
25 My company has a strategic plan to develop our IP surveillance business
26 IP surveillance is discussed in all management meetings
27 The market potential of IP surveillance products is very strong
28 In my company, anyone who works with IP surveillance also works or will work with other products
29 I am rewarded (e.g. salary, bonus) for increasing my knowledge of IP surveillance
30 In my company, we measure our performance thoroughly
31 We measure how well we perform on IP surveillance products installations and sales
32 We organise IP surveillance work separate from other work in the company
33 My boss discusses IP surveillance with me often
34 We need to reorganise our purchasing function to be able to interact with the new IP surveillance suppliers
35 We need or will need a specialised sales force to be able to sell IP surveillance products
36 Partnership with traditional security companies is of strategic importance for us.

## Respondents

- Typically SME companies, IL, WI
- Position
    - INTEGRATION IP = 60%
    - DISTRIBUTION IP = 10%
    - INTEGRATION Security = 30%
- Years in industry (Security) = 5 years
- Average age = 38 years
- Function: Purchase, install, sales primarily
- Education: high school, engineering or IS/network
- 32 male, 2 female