School of Economics and Management
Lund University

Lusax
Security Informatics

www.lusax.ehl.lu.se

LXM-TKBW-IP Challenges to Integrators

Author: Thomas Kalling & Benjamin Weaver
Subject: **IP Challenges to Integrators**
Date: 25 February 2008
Pages: 3
Recipients: Lusax
Email: thomas.kalling@fek.lu.se
benjamin.weaver@fek.lu.se

IP Challenges to Integrators

Executive Summary

This memo focuses the challenges brought upon traditional security integrators as a result of the digitalisation of services through the assimilation of IP-connectable security products. Challenges to security integrators:

- Develop an ROI thinking, including demonstrating the extended functionality, the scalability of IP networks, and being able to offer hybrid solutions.
- Being able to sell to CIOs, CFOs, CEO's and other executives.
- Being able to demonstrate real IP success cases, and not just rely on theory, logic and rhetoric.
- Develop the necessary technical, sales, sourcing and logistics competence, while at the same time being able to develop other strategic initiatives.

Background

Being able to sell IP-connectable security products, such as integrated access control and surveillance, is typically very different from selling other security products. For one thing, selling "IP and IT" is often connected with customer requirements of returns on investment (ROI), whereas "traditional" security rarely includes an ROI (or TCO) thinking, but rather a comparison of prices and if relevant also quality levels across competing bids. The ROI focus entails several other implications as well, which we shall discuss below. Secondly, it means selling to others than the traditional "security director", particularly so the IT function. Thirdly, it is a novel technology, the functionality of which is typically much broader than comparative traditional security products. Fourthly, IP and IT are multi-purpose platform technologies, allowing for many more services than mere access control and surveillance, meaning capex calculations need to take into account future and expanded usability as well. Fifthly, there are fundamental differences selling IP and IT solutions to someone who has a compatible legacy compared to one investing from a zero-base.

There are significant differences between traditional security integrators and IP integrators. Whereas traditional players have an advantage in their customer relations and detailed knowledge of operative concerns at end users, IP integrators hold the technical knowledge and experience necessary to survive in the future (whenever the IP-based functionalities dominate the security industry). To IP integrators, the digitalisation of security means these operative and strategic customer relations need to be mimicked, while still staying ahead technologically. This paper instead deals more specifically with the challenges to traditional security players, who have customer relations, but relations that might prove worthless if/when IP and IT solutions take over.

Challenges

Being a security integrator competitively capable of sourcing, selling, installing and servicing IP and IT products requires much more than simply being technically aware of the new technologies and their applications. This paper focuses on these challenges and what we find to important means to overcome these challenges.

- *"Thinking" ROI.* One of the first challenges includes actually thinking in terms of returns on investment on behalf of the customer. And whereas the I is typically not more complex, the inclusion of the R needs to be dealt with more carefully.

    - Simply comparing the IP product with the analogue will not reveal the relevant differences in overall *functionality*, which includes all sort of devices and functionality that can be added to the network once installed (e.g. computers, telephones, access points, servers, VoIP gateways etc). Furthermore, IP solutions combined with video analytics enable better image quality and analytical support, and are of course remotely accessible electronically globally. In fact, analytical support extends the functionality beyond mere surveillance, to incorporate anything associated with detection of variation, including supply chain management functionality such as keeping track of e.g. stock levels. In this respect, selling IP and IT products resembles the computer and software industry, which in comparison to security has been more associated with ROI thinking, at least for larger investments. Furthermore, considering the significant potential savings in e.g. retail, as a consequence of reduced shrinkage, the opportunities for better functionality should be very appealing.

    - Constraints to IP investments include *bandwidth and storage*, and potential conflicts with existing electronic assets. However, these challenges can be resolved with proper recording parameters, picture quality management (e.g. FPS), compression, etc. Furthermore, provided that IP networks are the way of the future, it is, we argue, risky for end users to refrain from investment on the mere premise that there is not enough capacity currently. Prices decline, and given the additional advantages *and* the fact that it is highly likely that the future includes IP networks in all areas where there are analogue solutions today, opportunities for first-mover advantages among end users may be lost. The *scalability* of IP solutions is of course a serious advantage that should be considered.

    - In conjunction with this, it is also imperative that integrators are prepared for and have a range of offerings for *hybrid solutions* (including ROI cases) at the end user, combining analogue and digital technologies. Any investment will always be guided by *legacy*, meaning the size and character of investment will reflect existing asset bases and competences as well as historical experiences and perceived uncertainty. Although it will always be more appealing to supply clean sheet zero-base solutions, this is often not attractive for end users with functional assets in place already. Furthermore, a more incremental approach will give the end user a piece-meal transformation which increases the possibilities for visible "early wins", and a smoother learning process. The hybrid strategy directs integrator attention to products as well as systemic solutions, and will force integrators to keep track of not only products based on the "latest latest" technology, but also more cost-efficient older generations of products. Paralleling hybrid and zero-based systemic strategies might also require specialisation of functions for sales, integration and services for different kinds of projects.

- *Selling to the IT and executive communities*: Due to the extended functionality and the direct use of resources typically belonging to the IT director or CIO, an integrator must find ways directly to the CIO, to be able discuss solutions with the most relevant and influential function. Approaching CIOs means that there will be tougher requirements on technical and product competence, an ROI approach including discussions of relative benefits rather than mere price/quality comparisons, and typically a greater insight and comprehension of the strategic ambitions of the end user (e.g. is it a low cost or premium player, is it international, is it technically driven, etc). Approaching CIO's may also mean integrators get closer to CFO's or even CEO's, further emphasising the need for a broader and more customised offering. This will put particular pressure on the integrator sales force, and is an area where existing customer relations might not be an obvious advantage. Getting to CIOs and others in the C suite might require using existing relations to security buyers, and finding operative reasons to meet the CIO. One overarching tactic is however to team up with IP and IT vendors or integrators of such products.

- *From logic, theory and rhetoric to real cases*: The introduction of IT and IP products, the so-called convergence of the security and IT sectors, has been hyped for several years, despite a relatively slow pace of change so far. Much of the reasoning behind the fuelling of the idea of convergence has been based on theory, common sense, logic and sometimes outright rhetoric, and has been conveyed by strong advocates, typically in a so-called evangelist fashion. The view among the advocates, that IP technology and extended functionality are unarguably *the* way of the future, has suppressed an empirically orientated discussion of the relative effect of actual cases of IP implementations. The debate is based on logic and rhetoric, not real cases, which, we believe, has deterred prospect buyers. On the contrary, a successful IP integrator is bound to approach customers using real cases rather than just talk, reason and logic. This underlines the importance of rapidly collecting data and generating business cases that compare IP and analogue solutions, and enable the integrator to fit the offering (e.g. choose between product or systemic solutions, as discussed above) to customer preferences – including being able to offer analogue or hybrid solutions too.

- *New competences*: A traditional integrator trying to manage or overcome the challenges identified above, is facing some serious knowledge gaps to bridge throughout the value chain. Technology, product, sales, installation and after-sales, are primary areas. And although the technical knowledge of IP products may be relatively explicit and easy to develop i.e. through recruitments or education, the sales, the strategic understanding, and the value of the extended functionalities are far more tacit and difficult to generate. And so although personnel education and recruitment should be made reflexive, it is also imperative to develop IP business experience quickly (we know from previous studies that IP business competence is subject to experience – on top of classroom training). And whereas experience can be generated simply by initiating IP offerings more strongly, we think a better way to generate experience fast is to buy accumulated experience, i.e. acquire and merge with IP integrators, where the competitive element is not so strong. Knowledge is subject to so-called time compression diseconomies, meaning that the only way to shortcut time is to pay for it. And a more traditional security integrator with strong customer relations could probably leverage that advantage by buying an IP integrator whose geographical scope complements the buyer (see LXM-TK2).

This memo is based on the premise that security integrators will be forced to consider developing competences necessary to include IP-based solutions. Although the timing and process of the assimilation of new technologies is difficult to forecast, it is, we believe, going to happen sooner or later. Those who act sooner, by experimenting and trying the new technology out, by building and reflecting upon experiences, by expanding the interfaces and connections at customers, by securing relations to vendors, by starting to benchmark and familiarise with pure-play IP integrators, by applying an ROI and a more strategic perspective, will probably have an advantage, when the new technology is adopted on a broader scale.

In the meantime, and notwithstanding the technological changes, integrators must consider and possibly combine other strategic moves, such as implementing total solutions, increasing and getting paid for services, enforcing certain verticals/end user segments, utilising international footprints, developing particular solutions, and teaming up with key vendors. But none of those strategic measures crowds out the importance of building a business that also includes IP and IT offerings – on the contrary, in the future, we believe IP and IT offerings will be *strategic necessities*, without which other advantages might be worthless.