# Inhibiting and driving forces for the digitalization of security systems: security officers' view on the issue

Lahtinen, Markus

2007

SCHOOL OF ECONOMICS AND MANAGEMENT
Lund University

Lusax Security Informatics

www.lusax.ehl.lu.se

**LXM-ML1-Driving Forces**

**Author:** Markus Lahtinen
**Subject:** **Driving Forces**
**Date:** 25 August 2007
**Pages:** 3
**Recipients:** Lusax
**Email:** markus.lahtinen@ics.lu.se

# Inhibiting and driving forces for the digitalization of security systems: security officers' view on the issue

## Executive summary

This memo reports on factors that drive and inhibit the digitalization of security systems. The reported factors are as follows:

*Technology-push factors*

• Need to lower costs on the end-user side, i.e. replacing labour with technology
• Perceived convenience and ease-of-use of digital systems
• Digital products can be connected to the current enterprise network; enabling an expanding set of security features
• Firms holding the IP-capability (IP=Internet Protocol) and not having offered security in the past see business opportunities in adding security solutions to their offerings

*Inhibiting factors*

• Bandwidth and storage limitation and the political 'battle of the bandwidth'
• Consultants and systems integrators are pushing "old" solutions
• Fragmented industry on the systems integrator side
• Fear of technology challenging current position, i.e. job security, of security officers
• Fear of being 'locked-in' to only one supplier of security

## Theory and background

It is "old" news in the security industry that the future security systems increasingly will run on IP-based networks. One systems integrator reports that the transition is inevitable, while at the same time suggesting that the development pattern has been different and faster than they had expected some years ago.

However, there still remains a need to qualify such a statement, and especially what is meant by the term *industry*. An industry can be described as being a value system; ranging from manufacturers all the way down to the end-users. This memo focuses on suggested factors that *drive* the technology shift and ones that *inhibit* the shift as seen from the perspective of the systems integrators and end-users.

Kalling's (2007) study within the Lusax program suggests that the technological shift mainly is technology-push driven and not market-pull driven, i.e. the industry is driving the shift towards a new technological platform for security systems and products. Still, a large portion of the

systems integrators offers products and services based on analogue, low-voltage technology to their customers.

The combination of lack of ability to work with network-based security and the convenience factor of having had the sales relationship for several years provides few incentives of offering digital integrated security solutions. In the US this is most evident due to the highly fragmented industry on the systems integrators side and serves as an obstacle for the digitalization of security systems.

## Method

The results of this study are based on interviews throughout 2006-2007 with security officers at end-user organisations; both private and public. 37 telephone interviews with security officers in Sweden were conducted between June and August 2006, 5 personal interviews in the UK in November, 2006 and March, 2007. In addition, 3 weeks were spent in the US in July, 2007 conducting interviews with and making participatory observations of sales reps and end-users at universities.

## Results

*Technology-push factors*

- Need to lower costs on the end-user side, i.e. replacing labour with technology. Security officers in Sweden, the UK and the US all reports that there are constant pressures to lower costs. Consequently, technology offers a possibility of removing a variable cost to a fixed cost.
- Perceived convenience and ease-of-use. Having all the systems running on the same network offers a cost-effective alternative since there is a minimum need for additional cabling. Also, the option plug-'n'-play and open systems are attractive in reducing the risk of 'lock-in'.
- Digital products can be connected to the current enterprise network; enabling an expanding set of security features. Larger organisations have an enterprise network which paves the way for potential global and enterprise-wide security systems. Current software offers possibilities of analysing for example video streams in ways that were not possible in the past, e.g. video analytics.
- Firms holding the IP-capability see business opportunities in adding security solutions to their offerings. An interesting follow-up question to this relates to if the IT/IP-companies will collaborate with the established security companies having the current sales relationship or if they will by-pass them in order to build up their own sales relationship.

*Inhibiting factors*

- Bandwidth and storage limitation and the political 'battle of the bandwidth'. Video streams are 'heavier' on the network than other types of data streams, which give rise to the perception that video-surveillance based on digital streams might be an unacceptable strain on the network. Ruled-based monitoring and lowered FPS (Frames per Second) offers a significant reduction to acceptable levels. However, the network might also have a symbolic power value in the organisation which gives rise to potential conflict between the IT function and the security function.
- Consultants and systems integrators are pushing "old" solutions. Similar to the way it was described above there is a short-term and mid-term incentive to offer 'copy&paste'-solutions offering higher margins than untested network-based solutions.
- Fragmented industry on the systems integrator side. The end-users do recognize that no company lives up to having a true global/national footprint; local relationships in some cases act as an inhibitor on the shift.

- Fear of technology challenging current position, i.e. job security and potential de-skilling, of security officers. On the end-user side there is also a reported fear that technology might reduce the need for security officers. This makes them reluctant to push for more advanced security system.
- Fear of being 'locked-in' to only one supplier of security. Having several suppliers of security, e.g. man-guarding, access control, network supplier might also act inhibiting due to the lack of coordination between the different areas. Having one supplier makes it possible to experiment with more holistic security approaches systems supporting this.

## References

Kalling, T. (2007): *Leads to a Successful IP Integration Business*
Lund, Sweden. LXM-TK1-IP Integration. LUSAX, Memo-series.
[Author: thomas.kalling@ics.lu.se ]