End-user challenges to security digitalisation and integration: a retail perspective

Lahtinen, Markus

2008

SCHOOL OF ECONOMICS AND MANAGEMENT
Lund University

Lusax Security Informatics

www.lusax.ehl.lu.se

LXM-ML3-End-user integration

Author: Markus Lahtinen
Subject: **End-user integration**
Date: 26 February 2008
Pages: 4
Recipients: Lusax
Email: markus.lahtinen@ics.lu.se

End-user challenges to security digitalisation and integration: a retail perspective

Executive summary

With the assumed digitalisation happening on the end-user side, progressive systems integrators stress the importance of changing the business concept from being installers to being service and solution providers. However, less is known about the details of this process on the end-user side. Based on an on-line survey of loss prevention managers it can be stated that security digitalisation and further business integration of security is a top agreement among the respondents. Integration and change efforts are often associated with challenges; it will become necessary for end-users to quantify a clear 'Return' in 'Return on Investment' calculations, bundling security and loss prevention investments with other business supporting systems, e.g. video conferencing, Voice over IP and/or HVAC etc. Of equal importance are necessary organisational changes to achieve integration, for example seeking internal sponsors and approaching departments often characterized as being 'siloed' in the past.

Background and purpose

Fighting low margins in a mature business, security systems integrators aim to move away from pure installation services to becoming a total solutions provider offering services and added value beyond mere security, to taking the full responsibility of an 'outsourcing' effort on behalf of the end-user, establishing a contractual and legal relationship. Connecting security equipment to the existing IP network offers such an opportunity throughout the system lifecycle, i.e. from specification, service and maintenance to upgrading and system termination. Consequently, the increased use of the corporate IP network drives for offerings increasingly based on being able to provide solutions and services.

Recognizing this transition effort by systems integrators as logical from the perspective of the industry, less is known about the end-user perspective of this shift. Based on a survey addressing loss prevention managers in the retail sector[1], the purpose of this paper is to discuss security digitalisation and integration and its associated challenges More specifically, the objectives of this paper are:

- Discern the end-users' view on security digitalisation and integration
- Identify rationalities associated with willingness to digitalise and integrate.
- Provide leads to how end-users can drive integration internally.

[1] End users in this case refer mainly to retail loss prevention managers. Some comments upon the material in itself: some 150 retailers were asked to participate. 20 of these responded to the survey and they represent a median value of 20 years of experience in the retail industry and 22 years of experience from the security industry. The material also has a bias towards North American and Swedish views on security.

Each of these purposes will be addressed sequentially below.

Results

Integration on the end-user side

The strongest agreements among the respondents were the following:

- Wishing to integrate security systems with other operational systems
- Video surveillance is absolutely necessary to keep shrinkage at an acceptable level
- Trying to replace man-guarding with security technology.

From these agreements it is clear that technology plays a crucial role in the security operations, all stressing the importance of technology. Addressing the first purpose of this paper; technology integration *is* a shared vision of the future and common interest among end-users; this beneficial for any systems integrator considering inclusion of integration services into their offerings. Also, the agreement reflects the replacing role of technology with regards to manual labor which is a valuable lead for constructing business cases and calculating ROI.

On the issue of integration of security systems with other operational systems, the following statistical correlations were identified:

- With higher age comes an increased likelihood of seeing integration possibilities.
- Firms giving importance to loss prevention also see integration possibilities, and
- Organizations holding a positive view towards integration are also brand aware of security equipment.

While the first two intuitively make sense, it is somewhat interesting to see that brand sensitivity is associated with a propensity to seeing integration possibilities. Service agreements do not imply a relationship where brands matter but rather that the system integrator takes responsibility in choosing a technical solution that supports the agreed service level. This might be an observation relevant for the systems integrator attempting to offer services and solutions rather than products and installation.

Summarizing the above discussion it is possible to say that integration is seen as an opportunity, not only by systems integrators but also by the end users. A purposeful design of computing hardware resources (e.g. networked cameras) combined with appropriate software (cf. different applications of video analytics) and an analytical approach offers opportunities of cost savings on manual labor and possibilities of adding value to the income side of business.

Implications for the systems integrator

Some of the implications for the systems integrators are to build on the existing relationships with the LP function. The systems integrators also have the option of finding new and parallel ways into the end user organization, i.e. offering services and solutions to other functions like operations (COO), facilities or IT (IT manager or CIO). This becomes even more evident if broader systems integration is a strategic objective of the systems integrators. Working in a network/partnership-approach with other industry players would potentially facilitate such a strategic initiative. For a more detailed reading on challenges for systems integrators please consult LXM-TKBW-IP Challenges to Integrators.

End user challenges to integration

Systems integration on the end-user side is made possible by utilizing common infrastructure and merging databases, often based on the IP-based corporate network. Seen from the perspective of the security manager this offers both an opportunity and a challenge. Opportunities lie in the potential added value offered by merging data in an ambition to refine information from 'siloed' systems.

Turning the focus to the end-users interested in driving integration from within; one of the more important challenges lies in breaking the 'siloed'[2] structure often encountered on the end user side to pave the way for a more 'integrated' approach to existing computing resources that can be run over the corporate IP network. Identifying an integrated 'business case' with an associated positive ROI then becomes of key importance.

Considering the Return on Investment (ROI) in terms of security is complicated due to the complexity of the 'R' since the return is often derived from a set of probabilities and impacts associated with different security risks. Identifying the cost (or 'I') is a much less complicated operation; mainly compiling a list of cost entries and assigning economic values to each entry.

In order to compensate for the volatile nature of the 'R' it will become necessary to 'bundle' security with other applications on to the IP network to cater for 'economies of scale', i.e. several applications can share the same investment cost. Bundling opportunities lie in constructing business cases that include clearer cost savings with VoIP[3], video conferencing[4], HVAC etc. combined with running security data through the same network[5]. Besides bundling, and as indicated above, possibilities of reducing costs on manual labor also should be included to any ROI calculation. However, the more complex the business case the more complex the calculations and its potential returns.

Acknowledging the benefits of a clear business case, complementary organizational changes are equally, and potentially even more important, than offering only a positive ROI. Hence, seeking internal sponsors and support is necessary as a reaction to often rigid organizational structures. The memo "Adding value beyond traditional security – lessons learnt from the software industry" by Lahtinen (2007) provides documented insights in critical success factors to successful implementation of data warehouses.

Conclusions

Security managers report that systems integration through IP-networks is here to stay. Not only does it save costs but potential added value is recognized. Integration poses several challenges to the end user; to prove the business supporting value of security but also technical due to the complexity of IP networking and architecture. Finally, complementary organizational changes are necessary to push integration ahead. The following recommendations are given:

- Construct integrated business case with hard numbers and clear gains, for example bundling security with other business supporting services, e.g. telephony over IP networks, information security and video conferencing etc.

[2] Siloed in this case does not necessarily mean a conflict relationship with other function. It could very well be the case that it is characterized as being a consensus. The term merely refers to departmentalization.
[3] http://www.ciscopress.com/articles/article.asp?p=336256 [verified: 20/02/2008]
[4] http://www.fvc.com/fvc/fvcweb/Files/The%20business%20case%20for%20videoconferencing.pdf [verified: 20/02/2008]
[5] http://www.axis.com/files/whitepaper/wp_axis_tco_en_0709.pdf [verified: 20/02/2008]

• Identify and seek support for associated and necessary organizational changes, e.g. initiate collaboration efforts with other business supporting functions.
• Move from thinking in terms of 'boxes and brands' to 'providing internal business support'

References

LXM-TKBW-IP Challenges to Integrators. Lusax memo, 2008, The Institute of Economic Research, Lund University, Sweden

Lahtinen, M. (2007): *Adding value beyond traditional security – lessons learnt from the software industry* The Institute of Economic Research, Lund University, Sweden
http://www.lri.lu.se/markus.lahtinen