From security system integrator to total solution provider

Weaver, Benjamin; Kalling, Thomas

2008

SCHOOL OF ECONOMICS
AND MANAGEMENT
Lund University

Lusax
Security Informatics

www.lusax.ehl.lu.se

LXM-BWTK1 - Security outsourcing

Author: Benjamin Weaver & Thomas Kalling
Subject: **Security outsourcing**
Date: 25 February 2008
Pages: 4
Recipients: Lusax
Email: benjamin.weaver@fek.lu.se
thomas.kalling@fek.lu.se

From security system integrator to total solution provider

Executive summary

As the electronic security sector converges with IT security, traditional security systems integrators are coming under pressure to redefine their business models. By not acting now, a traditional SI may see their addressable market share snapped up by aggressive IT entrants who absorb the most profitable projects and customers, leaving security SIs to fight over lower-margin work such as the installation of fire and intrusion detection. Clearly, security SIs that want to survive in a future dominated by IT and IP security technologies will have to adapt and change. This memo focuses on one of the possible strategies that security SIs could adopt – that of becoming a *total solution provider for outsourced electronic security services.*

Method

This memo is based on extensive interviews with end-users, integrators and manufacturers coming from both the traditional as well as IT side of the industry.

Security systems integrators need to redefine their business models

Traditional security systems integrators are increasingly coming under threat from a number of players. Major IT integrators and manufacturers like IBM and Cisco have made inroads into the security market, leading some of the most technologically advanced projects. Building management companies like SBT and TAC are also targeting the security sector aggressively, offering advanced IP-based integration systems, while telecom operators are starting to offer remote monitoring and ARC services. At the lower-end of the market, local niche IT and IP installers are stating to target smaller businesses and SMEs. Security SIs are thus being squeezed both at the top and the bottom by competitors that use IT and IP capabilities to gain a position in the security systems installation and integration market.

Despite facing these numerous threats, security SIs still have some major competitive advantages that they will be able to capitalize on for quite some time yet, given the slow-moving nature of the security market on the demand side. *Firstly*, security SIs have a major competitive advantage in strong, established customer relations based on trust built up over decades, focused on verticals or geographies or both. *Secondly*, security SIs are today uniquely positioned to grasp both the 'old' and 'new' ways of the security industry. Security SIs understand (and have indeed in many cases installed) the legacy systems that many customers will continue to use for years yet. Provided that they manage to bridge the knowledge gap to the IT and IP side (see LXM-BW1), they should be able to help legacy customers migrate towards the latest digital technologies, while providing integration and continued maintenance of legacy analog systems for as long as these remain operational. *Thirdly*, traditional security SIs – provided that they ramp up their IT/IP knowledge – are in a better position than any of the other types of players addressing the security market when it comes to providing a total security solution. Entrant IT and IP integrators are less likely to address legacy systems or more mundane aspects of security, such as fire and intrusion detection. Building integrators are strong competitors to

security SIs for security installations that are focused on single buildings and sites, but typically lack the specialized vertical knowledge (e.g. retail, banking) that more advanced security SIs will possess.

Drawing on these competitive advantages, security SIs will have a distinct advantage over its competitors in the security sector in offering a total solution for outsourced, managed security services. For a typical security SI – offering services in the traditional domains of fire, intrusion, access control, video surveillance – the type of services offered as part of a total solutions may include:

- Security system assessment and analysis
- Systems design
- Installation and integration with legacy systems (if applicable)
- Training of in-house staff
- Systems management
- Maintenance and service
- Remote monitoring and security operations center services
- Alarm-receiving center services
- Vehicle fleet tracking etc.

The opportunity – demand side drivers towards an outsourced business model for security services

- *Convergence of IT and security:* Outsourcing of general IT services has long been a staple of corporate strategy to enhance effectiveness and free up internal resources in order to focus on core competencies. Although data and information security may be seen as core assets for most companies, the market for managed security services (MSS) is growing. According to Gartner (August 2007), some 60% of Fortune 500 companies had used MSS, while Forrester research (October, 2007) estimates that the global MSS market totals $2 billion today. With the convergence between physical and IT security functions inside corporations, where security devices are increasingly integrated and connected to corporate IP networks, physical security management – including investment and purchasing decisions – is increasingly falling under the auspices of the IT department. One result of this process will likely be an increased demand for outsourced physical security services that complement and ties into companies' current MSS engagements.

- *IP networking:* While the trend towards IP and IT is posing a threat to security SIs who fail to bridge the knowledge gap, the same trend is also a major opportunity for those who jump on the wagon in time. Security systems based on IP and open standards software are modular and easier to adapt to customer's existing systems compared to the highly proprietary legacy systems of the past. The *de facto* standard emerging with increased usage of IP technology will help the security SI minimize development and systems design cost, and can be used to integrate most security devices, including legacy equipment. In addition, IP security systems are – by their very nature – perfectly adapted for the provision of remote surveillance and monitoring services as well as remote systems management and maintenance. Once a customer has migrated to an integrated and networked IP security system, SIs will also find it easier to be to offer future add-on services and solutions.

- *Increased complexity of threats:* In the past, the physical security function used to focus on relatively straightforward and tangible threats and issues such as perimeter and building intrusion, fire and access control. As physical security systems converge with corporate IT systems and networks, a more a holistic approach to security management is necessary to defend against increasingly sophisticated

attacks from organized crime working in tandem with the hacker community. Keeping on top of these complex risk scenarios and maintaining the necessary expertise and updated procedures in-house will be increasingly difficult for companies who might well want to turn to a specialized third party who continually updates its security capabilities.

- *Regulatory compliance and industry standards:* Penalties for not complying with regulations and standards related to areas such as information security, data protection and privacy can be significant. Maintaining in-house expertise on these issues and developing corporate-wide operating procedures and instructions is costly and time-consuming, and is obviously a service that lends itself well to outsourcing.

- *The changing role of the security manager/CSO:* The security manager (or equivalent) has traditionally been the point of contact for security SIs in the past. As a result of this development, a new breed of CSOs with a combined responsibility for physical and IT security is emerging, and the people recruited for these positions usually to possess a strong IT security background. The end-result of these trends is that physical and electronic security will increasingly be seen as an added responsibility for IT security managers. With physical security being a rather marginal and non-core business activity compared to IT and information security in most companies, these new CSOs will likely prefer to outsource the pure security aspects – such as component and software selection, systems design, monitoring and maintenance to a third party. The new-breed CSO might not have the background and experience or the necessary time and resources to acquire the knowledge needed to make an informed investment decision. Anyone who has visited a recent security trade show, for example can attest to the staggering amount of bewildering offerings available in e.g. the fields of intelligent video, video management and video recording solutions. In many cases, therefore, he will prefer to leave the design of the security system, including the choice of components, software etc. to a security SI who takes total responsibility in delivering a complete solution.

- *Cross-border services:* As a growing number of multinational corporations opt for converged and integrated security systems, there is an increased need for service providers who can deliver and duplicate security systems installations across national borders adapted to local legislation and standards. With the security industry lagging far behind the IT industry with respect to following its customers internationally, security SIs that manage to acquire a true international footprint and offer cross-border uniform service level agreements across borders, will have a powerful advantage over SIs that remain regional. The latest IP technologies enable SIs to control and manage systems worldwide remotely, thus further facilitating an outsourced business model.

Challenges

- *Ramping up internal capabilities:* Very few, if any, current security SIs have all the qualities, expertise and capabilities necessary to meet all the requirements of an ideal total solutions security provider described in this text. The main challenge for security SIs that wish to lead in this new market segment is thus to ramp up internal capabilities and skills, most importantly in the areas of IT/IP, consulting and general systems management. Over time, this will entail a radical (and necessary) shift in focus from installation and sales of 'boxes' to consulting and services for security SIs that chose to go down this path.

- *Acquiring a national and global footprint:* Clearly, the economies of scale involved in building up a total solutions business model will favor large SIs with national and international footprint. Such security

SIs will be the partners of choice for major corporations that seek to integrate security systems on a national and global scale. While consolidation among security SIs is already well underway on the national level, few are able to offer truly international services. Even for security SIs with an international scope, local operations tend to be run autonomously. Developing and managing a truly international business organization that can follow clients seamlessly around the world will be a formidable challenge for most security SIs. The latest technology and IP networking tools will facilitate the process by enabling remote management of systems globally, by minimizing the need for local offices and security operations centers.

- *Building trust:* Successful Security SIs rely on end-user relationships based on trust built up over long periods of time. As they take on even more responsibility over a corporation's security functions, trust will be even more of a critical factor, as will be the business risk if security SIs fail to live up to their promises. It will hence be crucial for security SIs to carefully assess its internal capabilities and manage its resources in order not to overpromise and underdeliver total solutions provided to end-users.

- *Competition with MSS providers and IT integrators:* A major issue for security SIs that attempt to become total solution providers for security services is the fact that their offering will eventually overlap with the services provided by current MSS providers as well as IT integrators. Ideally, a security SI would want to maintain win-win partnership relations with these players, but this may prove difficult in the longer run. In order not to fall in the familiar trap of mainly providing 'box installation' and typical low-margin work, security SIs opting for a total solutions model will want to expand their service offering to include security consulting, information security and network management, which are domains currently dominated by MSS providers and IT integrators. Security SIs will thus have to balance their ambition to offer higher-end (and higher margin) consulting and IT services against the need to maintain good relations with its MSS and IT counterparts. The upside – from the security SIs perspective – is that the risk that these players reciprocate by entering the traditional physical security domain is minimal. The physical security market is simply too marginal in relation to the IT integration and information security market to be an attractive option for IT companies.

References

Raschke, Thomas (2007), The Forrester Wave: Managed Security Services, Q4 2007, Forrester Research Inc.

Kavanagh, Kelly M. & Pescatore, John (2007), Magic Quadrant for MSSPs, North America, 1H07, Gartner.

Weaver, Benjamin (2007), Security industry convergence – bridging the knowledge divide, LXM-BW1, The Institute of Economic Research, Lund University.