Security industry convergence – bridging the knowledge divide

Weaver, Benjamin

2007

SCHOOL OF ECONOMICS AND MANAGEMENT
Lund University

Lusax Security Informatics

www.lusax.ehl.lu.se

LXM-BW1 - Knowledge Gap

Author: Benjamin Weaver
Subject: **Bridging the knowledge gap**
Date: 26 August 2007
Pages: 5
Recipients: Lusax
Email: benjamin.weaver@fek.lu.se

Security industry convergence – bridging the knowledge divide

Executive Summary

Convergence in the electronic security industry entails the meeting of two very different business cultures, which is currently manifesting itself in the form a knowledge gap. In view of this, the crucial strategic resources needed to succeed in the converged electronic security market of tomorrow will be a combination of competences, capabilities and skills sets – or *knowledge*, in short – drawn from both the security and IT industries. This knowledge can be divided into three main categories: *technological*, *business-related* and *cultural*. In terms of bridging the knowledge gap, those best positioned for success in a converging market scenario are:

- *Pure-play IP manufacturers* who are currently taking aggressive postures on the market. Close collaboration with security incumbents will provide ample access to security skills as well as provide avenues for strategic IP knowledge diffusion.
- *Security systems integrators* that rapidly acquire the necessary IT and IP skills will be in a unique position to leverage their security-specific capabilities, and will be the partner of choice for manufacturers as well as end-users.

Those less likely to bridge the knowledge gap will be:

- *Incumbent analog manufacturers*, primarily in CCTV. These players have been too slow in responding to convergence, and are strategically held up by their vested interests in legacy technology.
- *Smaller security installers,* who are faced with a daunting knowledge challenge, increasing competition from IT installers, and who cannot rely on the conservativeness of end-users to delay the migration towards IP technology.

Method

This article is based on interviews with 60+ respondents, representing all categories of industry players.

Background: security industry convergence

Having been a virtually isolated sector – in terms of technology, products, customers and industry participants – the electronic security industry is currently facing a discontinuous technological change mainly driven by the increasing pervasiveness of IP networking. As mechanical and analog security products are IT- and IP network enabled and whole product segments are shifted onto digital technology platforms, major IT players as well as smaller, innovative entrants are increasingly targeting the security sector. This convergence of two hitherto separate industries is leading to the blurring of previously clearly demarcated industry boundaries.

By radically altering the competitive landscape, convergence will have a profound effect on the electronic security sector. The risk – from the incumbent's point of view – is that when IT players enter the electronic security market, they will cherry-pick the most advanced and profitable technology segments where they are most likely to leverage their IT capabilities, leaving incumbent security players to scramble over lower margin legacy market segments and less profitable projects and customers.

At this point in time we are far from this scenario. The security industry is traditionally – by its very nature – highly conservative on both the demand and supply side, and new technology trends spread slowly, especially when compared to the IT industry. Consequently, most electronic security incumbents seem to be adopting a wait-and-see approach, perhaps hoping or betting that a full-blown IT convergence scenario will never be realized, or at least be gradual enough that they will have time to adjust. On the other hand, many entrant IT players are convinced that convergence has already gathered the momentum necessary to radically turn the industry upside down in a matter of a few years.

Convergence leading to a knowledge gap

While industry participants may debate the pace of convergence, everybody seems to agree that the shift is inevitable and that the process is already underway. From a strategic perspective, a discontinuous technological change such as the one currently affecting the electronic security creates new market opportunities, which is the reason why entrepreneurial IT players are entering the market in the first place. It also entails ambiguity and uncertainty, especially for security incumbents whose legacy asset positions are being threatened. For anyone – whether entrant or incumbent – aspiring to a leading position on the electronic security market of tomorrow, the time to strike a strategic position is undoubtedly *now,* while the window of opportunity is still there.

Industry respondents tend to agree that the crucial strategic resources needed to succeed in the converging electronic security landscape will be a combination of competences, capabilities and skills sets – or *knowledge*, in short – drawn from both the security and IT industries. At the moment, security incumbents and IT entrants face a significant knowledge gap relative to the other side. Much of the strategic positioning that will take place over the coming years will thus center around gaining access to – and controlling – the knowledge and skill sets that will be crucial for success in tomorrow's market.

Untangling the knowledge divide

Having established that convergence is opening up a knowledge gap between the security and IT industries, it will be necessary to look closer at the specific knowledge components that give each side a potential competitive advantage over the other. A broad definition of knowledge will include the competences, capabilities and skills that are held both by individual employees as well embedded within organizations and whole industries in the form of processes and routines, manuals and training programs, etc. This knowledge can be divided into three main categories: *technological*, *business*-related and *cultural*, each of which are further discussed below.

Technological knowledge lies at the heart of the convergence process. As an example, installing a basic CCTV system was once a case of running a coaxial cable from A to B between a camera, a monitor and a VCR. In contrast, installing an IP video surveillance system involves network, router and server configuration, choosing cameras and configuring a digital recording system based on features such as resolution and video compression codecs, and selecting, choosing and installing the software needed for control and operation of the system. The technological knowledge gap does however go both ways, and – in the case of video surveillance – the IT side will have to acquire traditional security skills such as video surveillance systems design, camera selection and placement, and integration with other security systems such as access control, fire and intrusion.

Business knowledge: Security industry convergence is not just about technology. It is also about the meeting of two separate business cultures, with very different go-to-market strategies. The convoluted sales processes and market mechanisms of the fragmented electronic security market – often involving a plethora of consultants, integrators, installers, sub-contractors – can be very non-transparent to an outsider. Just identifying the right target for a sales pitch, let alone devising an effective marketing and channel strategy, will be major challenges for IT players that attempt to go it alone in the security sector. Security incumbents are faced with similar challenges as they are increasingly exposed to competition from IT players. Making the business case

of a network-integrated security system to IT executives and CEOs, for example, is a much more complex undertaking than selling a stand-alone security system to a security manager.

Cultural differences: The IT and security industries come from very different traditions and backgrounds. The security industry is used to slow and incremental technological change, as new classes of equipment have to prove themselves thoroughly in actual field settings before being embraced by integrators or end-users. In contrast, the IT companies are well accustomed to rapid technological change, and have adapted their organizations to this environment. Most IT employees have experienced the "competence-destroying" effects of major technological platform shifts and are accustomed to constantly updating their skills through training and certifications. To prepare and realign their organizations for a converged industry environment, incumbents and entrants need to be aware of these and many other cultural differences between the security and IT industry.

Some of the most important knowledge-related advantages that can be identified for each side are summarized in the table below.

Convergence – security vs. IT industry knowledge advantages

Security industry (incumbent)	**IT industry (entrant)**
Technology-related knowledge	
▪ Security integration (fire, intrusion, CCTV, access control) ▪ Security systems design ▪ Security component selection, placement ▪ Security-related technical standards	▪ Network integration (data, VoIP, video) ▪ IP network design, configuration ▪ IT security, encryption etc. ▪ Digital recording and storage ▪ Software development ▪ Education, training of end-users and channel partners on new technology
Business-related knowledge	
▪ Selling to, and knowledge of, end-users/security managers ▪ Security market mechanisms, channels etc. ▪ Regulative and legislative compliance ▪ Insurance regulation and compliance	▪ Selling to IT departments, top management ▪ Selling the business case of security and data network integration ▪ Developing new applications for security, using new combinations of existing security equipment ▪ Access to efficient IT channels
Cultural knowledge	
▪ Security, risk mitigation and crime prevention permeates organizational and industry culture ▪ Quality, customer service and maintenance culture – spare parts and service is guaranteed for long periods of time ▪ Prudence and conservativeness – will only use products and technology that works ▪ Brand-agnosticism: the name on the box matters less than how well it works	▪ Learning culture, organizations adapted to near permanent technological change ▪ Superior business and work processes and organizational routines ▪ Codifying complex knowledge into manuals, training programs, certifications ▪ Innovation using existing resources, business and market development ▪ Collaboration, outsourcing, working in ad-hoc project constellations

Analysis – winners and losers in the race for knowledge

Based on the discussion in the previous section, and using knowledge as a key strategic success factor on a converging security market, it is possible to analyze the competitive potential for different categories of players in the industry.

Equipment manufacturers: In this category, the most obvious losers will likely be pure-play incumbents in the analog CCTV segment. At the moment, the convergence process is largely propelled by the technology shift in video surveillance. This shift is truly disruptive in that it involves the substitution of one class of products (analog) for another (digital) and thus creates the potential for *creative destruction* – the process whereby industries and markets are radically transformed by the introduction of new innovations and technology. It is an irrefutable fact that although analog CCTV cameras will be around for many years yet, they will eventually be completely superseded by digital IP cameras. In view of this, many of the leading analog incumbents have been exceedingly slow in reacting to the shift towards IP, and their heavily vested analog interests make them poorly prepared for bridging the knowledge gap. Their main advantage in the current market – superior security-related knowledge – will continue to erode as convergence presses on, and will eventually not be able to offset a lack of IT/IP skills that can be translated in to market offerings.

On the other side of the coin, future winners are likely to be found among the entrant IP manufacturers that are striking aggressive positions on the market today. The main advantage of these players is that without the burden of an analog legacy, they are able to concentrate wholeheartedly on pushing IP. This can clearly be seen in the way these players are persistently educating the market and channels on the benefits of migrating to IP. In effect, they are using an aggressive knowledge diffusion strategy as a Trojan horse with which to conquer important segments of the market. The pure-play IP entrants still lack some security-specific knowledge, but through collaboration with security integrators, installers and distributors, they will be able to catch up quickly. Moreover, in reaction to the slow response from sections of the traditional security industry, IP manufacturers are expanding their addressable market by developing new, innovative applications. This allows entire segments that have been outside the radar of the incumbents – such as small retail businesses – to leapfrog straight into IP technology.

The large diversified electronic giants manufacturing analog and IP cameras and other equipment for the security industry are likely to be less affected as they have substantial IT and IP knowledge embedded in their organizations, ready to be leveraged on a converging market.

While the shift towards IP and IT affects all areas of the electronic security industry, the change will likely be less dramatic for manufacturers and vendors of access control and fire and intrusion equipment. In these product segments, the advent of IP represents more of an incremental or *sustaining* technological shift that will provide new ways to integrate and extend the application of current systems. For this reason, a radical shakeout among the players in these product segments is unlikely.

Software developers: Stand-alone software players are another group that will benefit from convergence in the security market. In contrast to the substitutive aspect of analog-to-digital equipment migration, software represents a *complementary* class of technology and products that will be increasingly important in all sectors of the security industry. Software developers – especially those that focus on open standards – are needed to achieve seamless integration and will be able to partner with all types of equipment vendors and integrators.

These types of collaborations will enable software developers to gain access to key security-related capabilities. However, many software entrants developing cutting edge solutions such as video analytics, are currently overshooting market demand, and will have to come to terms with the real-world needs of security end-users.

Systems integrators: Of all the players in the industry, incumbent security systems integrators are probably faced with the most daunting knowledge challenge over the coming years. Being at the forefront of security technology and integration, they will quickly have to absorb IT- and IP-related capabilities, while at the same time retaining the competence needed to serve customers with legacy installations for many years yet. This will be a difficult balancing act for many incumbent integrators, especially as they are faced with increasing competition from IT integrators that are going after the most profitable high-profile contracts and customers.

Collaboration with IT integrators and dividing up the market is not a realistic option, as they both want to take the lead in providing video surveillance systems, which is the most profitable and fastest growing product segment. Instead, close collaboration with entrant IP and IT equipment and software vendors, will be an important avenue for incumbent integrators to access relevant IT-side knowledge. Although the challenges posed by convergence are many, the incumbent security integrators that get it right will have everything to gain. Although they might not be able to acquire the leading-edge capabilities of some of their IT competitors, the incumbents' firm grasp of all aspects of traditional security, their unique ability to integrate different types of security systems, and perhaps most importantly, their knowledge of the security market and its end-users, will give them a unique knowledge advantage on a converged market.

As with entrant equipment vendors, IT integrators have an inherent advantage in that they are able to focus wholly on IP technology and associated software development. However, IT integrators will face difficulties acquiring security capabilities. Indeed, it appears that many IT integrators have underestimated the need for security-specific knowledge when entering the security market and are now facing the consequences as security integrators are called in to finish the job. This is part of the IT integrators' learning curve, and given their sheer size advantage they may well decide to acquire some of the leading security integrators to gain quick access to specialized security skills and end-customers.

Even so, IT integrators cannot be expected to go to any lengths to penetrate the security market. For some of the larger players, it may just turn out that the market is too small and fragmented to be worth pursuing – at least at the moment.

Smaller installers: In the fragmented security industry, a substantial portion of the lower-end of the incumbent market is addressed by constellations of regional and local installers, consultants and resellers, which are often supported by national security distributors. Smaller security installers – who do not have the advanced security integration expertise held by the large integrators – will increasingly see that local IT and network companies are taking over significant parts of their market. Even though larger security distributors, who are themselves under threat by IT distributors, are investing in major education programs to prepare their key customers for the future, taking on IT and IP knowledge will be very difficult for these smaller incumbents.

Another problem for the incumbents – and a significant opportunity for IT entrants – is the fact that end-users in this segment lack the security knowledge and conservativeness that is inherent among security managers in larger companies, and will consequently be quick to embrace the elegance and simplicity of the latest IP offerings. This is thus another part of the security market that is likely to experience the full force of *creative destruction*.