SCHOOL OF ECONOMICS AND MANAGEMENT
Lund University

Lusax Security Informatics

www.lusax.ehl.lu.se

LXM-BW2 – Convergence

Author: Benjamin Weaver
Subject: **Convergence in the security industry**
Date: 10 December 2008
Pages: 6
Recipients: Lusax
Email: benjamin.weaver@fek.lu.se

'Convergence' in the security industry – definitions, drivers and consequences

Executive Summary

Drawing on a combination of empirical industry observations and management literature, this document attempts to shed some light on the usage of the term 'convergence' that can be identified within the security sector. The aim is to provide both a typology of definitions and a discussion of some of the strategic implications of different types of convergence. A basic distinction is made between convergence on the demand-side (inside enterprise organizations) and the supply-side (technology and products and services). Demand-side convergence is identified as a unified approach to security that entails tearing down the organizational walls that separate the physical security, IT and information security functions. This notion of convergence is focused on the organization of security work in terms of people, processes and technology. On the supply side, technological convergence is identified as a set of concurrent trends that have enabled the shift towards intelligent network devices. At the product (and service offering) level, a distinction is made between convergence in substitutes (e.g. IP cameras replacing analog cameras) and convergence in complements (e.g. bundling of software, hardware and services). Seen from an industry perspective, these two types of convergence have different consequences. The former potentially leads to an industry shakeout, where entrant companies challenge incumbents' dominant positions, while the latter may lead to alliance seeking and vertical integration.

Introduction

The use of the term *convergence* in the security industry can be confusing, as it is used to describe two overarching issues: *(1)* how security work and processes in enterprises should ideally be organized and; *(2)* the technology, systems and solutions needed to achieve these goals. At the same time, convergence can have a number of very specific connotations depending on the context where it is used.

For most security industry participants and observers, convergence generally refers to the functional merger of traditional physical security and IT and information security. While it is true that a major technological paradigm shift towards digital platforms is reshaping the security industry, technology is just one part of the many drivers behind security convergence.

Applying a perspective on the security industry as a whole, a basic distinction can be made between convergence on the demand-side and the supply-side. *Demand-side convergence* refers to security end-users increasing need for converged solutions, which in itself is a reflection of an underlying trend towards convergence of security organization, functions and processes.

Supply-side convergence, meanwhile, refers to how manufacturers, vendors and service providers in the security industry attempts to innovate and align their product offerings to meet the needs of end-users as well as the underlying technological platform changes that makes this possible.

Demand-side convergence

Organizational convergence

The physical security function has traditionally been isolated and organizationally siloed off within firms. In the face of increasingly complex threats and risks, many organizations are taking a more holistic approach to security. As an example, criminals targeting banks and retail outlets today often employ converged methods, in the sense that physical intrusion and modification of ATMs or cash register terminals is used to extract credit card and customer information that can be used to commit cyber-fraud. A well-circulated 2005 white paper commissioned by ASIS proposes that to meet these new challenges, firms must unify their security organization and processes:

> This situation highlights and reinforces the need to bring together – in fact, converge – all components of an organization's security through an integrated and deliberate approach. To be effective, this converged approach should reach across people, processes, and technology, and enable enterprises to prevent, detect, respond to, and recover from any type of security incident. Failure to adopt a unified approach can result in catastrophic consequences.[1]

For most enterprises, the adoption of this 'unified approach' entails tearing down the organizational walls that separate the physical security, IT and information security functions. As security systems become increasingly advanced and integrated, the information they generate become ever more rich and sophisticated. Security data, such as access control logs and video recordings, have largely been kept discrete in the past. Leveraged by IT and IP convergence, this data can now be integrated with an organization's other information and HR systems. This trend is further promoted by the advent of higher-level standards that define common event reporting, message headers and for data generated by security systems. Such standards will enable information exchange between many types of security components irrespective of manufacturer, further facilitating and enhancing the value proposition of IT and security convergence.

In larger corporations, this process has also led to the proliferation of a new managerial role – the Chief Security Officer (CSO). Often reporting directly to the CEO, the CSO – or the equivalent manager with security responsibilities – should ideally oversee all aspects of security in a way that strategically supports and adds value to the firm's core business.

In addition to the overriding goal of responding to and being prepared for complex threat scenarios, security convergence – often in tandem with general building automation and integration – also has the potential to bring about general business efficiencies that help enterprises cut costs and comply with insurance and government regulations. For many organizations, the trend described above has led to the realization that unified security work is a complex task that may preferably be outsourced to specialists, partly or even entirely.

International convergence

Over the past few decades, socio-economic development and globalization has created a cross-border convergence – or homogenization – of needs and customer preferences across markets and groups of end-users. From a demand perspective, the physical component of security work has traditionally been treated as a local matter, even within large corporations with multiple national or international sites. This has contributed to the fragmentation and local and national idiosyncrasy that characterizes much of the security industry, especially in the areas of installation and systems integration services.

As physical security systems are integrated with central information systems, multinational corporations are increasingly demanding security solutions that can seamlessly integrated and perform to the same standards across national borders.

---

[1] Convergence of Enterprise Security Organizations (2005). Booz Allen Hamilton, Report commissioned by The Alliance for Enterprise Security Risk Management (AESRM). Popularly know as the 'ASIS Report' it is available at: http://www.asisonline.org/newsroom/alliance.pdf

Public-private stakeholder convergence

As security technologies such as public video surveillance become more widespread, the lines between public and private interests begin to blur. Authorities are routinely using video surveillance data collected by private enterprises to investigate crime and identify potential perpetrators. With digital video and enhanced picture quality, it is becoming possible to apply analytics software that can drastically reduce the time needed to investigate the material.

Although personal integrity and data protection issues will have to be addressed, it is possible to conceive a future where biometric data (e.g. facial recognition) of international criminals is stored in central databases, and where networked public and private surveillance cameras are used in tandem to identify and track these individuals in near real-time. To makes such a scenario possible, however, security systems will to converge by means of standardization and common communication interfaces. Early steps towards such publicly imposed security convergence initiatives can already be seen, particularly in Europe.

Supply-side convergence

Technological convergence

Technological innovation and development is clearly one of main drivers of convergence in the security industry today. While the demand-side drivers identified above are specific to the security industry and its end-users, the convergence affecting the supply-side of the industry largely follows the same pattern as many industries affected by convergence in the recent past. In management literature and business press, examples of convergence have primarily focused on industries that have been directly affected by advancements in ICT or exposed to the Internet as a game changing production and distribution platform, i.e. primarily the electronics, entertainment and media sectors.

Integrative technological platforms: Breakthroughs in the production of semiconductors and microprocessors (following 'Moore's law') and concurrent advances in bandwidth-expansion technologies have lead to the emergence of an integrative technological platform in the past few decades that have had profound effects on all electronic equipment industries. More concretely, Moore's law facilitates technological convergence by letting manufacturers combine more functions on a single silicon chip. It is such advances in circuit complexity that allows e.g. mobile phone manufacturers to bundle an increasing number of features in small 'converged' handsets. Moore's law also lowers the cost of adding processing power, facilitating the development towards ubiquitous computing where 'dumb' pieces of passive equipment become intelligent network peripherals.

Standards: The setting and adoption of technological standards is integral in many cases of technological convergence. As proven by the emergence of the Internet, open standards can play a significant role in opening up industries to technological change and convergence. The ubiquity of the Internet – more specifically TCP/IP running over Ethernet – has provided the security industry with a *de facto* standard and communications platform through which security equipment can be networked and integrated. However, open standards are not necessarily in the interest of incumbents who have decided upon the dominant designs of their industries in the past, and their collusion to continue to influence and impose proprietary standards may act as barriers to convergence.

Product convergence in substitutes and complements

In a book dedicated to "Competing in the Age of Digital Convergence" (Yoffie [ed.], 1997), Greenstein & Khanna (1997) put forth an influential treatment of convergence. While addressing the computer and communications industries, Greenstein & Khanna's discussion is not limited to a specific industry context. One of the central features in Greenstein & Khanna's framework is that technological innovation may lead to two main types of technological convergence at the product (or service) level.

Firstly, *convergence in substitutes* occurs when separate classes of products become interchangeable in the sense that they share features and provide the same function for end-users (e.g. portable CD players being substituted by iPods). In the security industry, the clearest example of convergence in substitutes can be found in video surveillance, where traditional analog cameras and VCRs are being replaced with IP cameras and digital recording solutions. The term 'convergence' may seem inappropriate in a context where classes of products are substituted by others. However, the notion is that these different products come to perform similar functions and tasks, leading to suppliers and manufacturers from previously unrelated industries converging onto the same end-user markets. In the case of video surveillance, the move towards digital platforms have unleashed an invasion of IT companies that have identified a strategic opportunity to leverage their expertise in digital imaging, networking, storage and software in the security sector.

Secondly, *convergence in complements* occurs when previously unrelated classes of products are bundled together to form new combinations, creating an integrated product with added value for end-users. The trend towards 'meta-integration' of physical and IT security, building control systems etc., is of course the most important example of convergence in complements in the security industry, and has lead to an influx of IT, software and integrator companies. Software plays a particularly important complementary role, in the form of the 'glue' with which security systems are managed, integrated and networked. Through e.g. video analytics, software can also add entirely new features to existing systems, e.g. people counting and inventory control in the retail sector. Combining two or more distinct technologies for increased security – e.g. using both biometric data and digital tokens for physical or network access control – is another example of convergence in complements at the product level.

Consequences of industry convergence

Shifting the level of analysis from technology and products to markets, it is clear that the security sector is currently experiencing a major convergence of industries that have hitherto been more or less unrelated. In the change towards digital platforms, the IT industry is clearly the most important influence. However, building and facility management companies are seeing potential in the demand for integrated and outsourced security systems, while telecom operators are beginning to see an opportunity to leverage their communications resources in the provision of wireless security systems, remote monitoring and alarm receiving centers. Fledgling industries such as biometrics and next-gen contactless technologies (e.g. NFC) will soon start to have a major impact on the security industry.

Following Greenstein & Khanna's account, the effects of industry convergence can be analyzed according to the type of product convergence observed as discussed above. *Convergence in substitutes* at the product level typically results in an expansion of technological opportunities, leading to lower barriers of entry to a market, with increasing competitiveness as a result. This has clearly been seen in the video surveillance sector, where analog incumbents where very slow to introduce digital solutions, leaving the market wide-open for a number of innovative IP camera start-ups.

Convergence in substitutes at the product stage results from the introduction of radically new technology platforms and business models that have competence-destroying effects for incumbents. This means that resource-sharing incentives to collaboration between entrants and incumbents are low, potentially leading to a competitive situation that changes the foundations of an industry's structure:

> Convergence in substitutes represents one of the most celebrated aspects of creative destruction: the unanticipated invention of entirely new ways of achieving a product of economic value.[2]

[2] Greenstein, Shane and Khanna, Tarun (1997) "What does industry convergence mean", in Yoffie, David (ed.) (1997) *Competing in the age of digital convergence*, Boston, MA, Harvard Business School Press, p. 215).

Convergence in complements at the production stage, meanwhile, leads to a different scenario where industry boundaries are blurred due to uncertainties on standards, interfaces, systems integration and the general direction of technological change. In the case of convergence in complements, firms face a number of incentives for cooperation, as sharing of resources is mutually advantageous in terms of developing and expanding the market for new products and services. Collaboration may occur to influence the development of standards and firms may turn to strategic alliances to minimize perceived uncertainties about the direction of technology product design and standards. Reasons for vertical integration also exist, as firms may want to secure access to a new (scarce) factor product that complements its own resources.

In the case of the security industry, convergence in complements has created an opportunity for new types of competitors, in particular systems integrators that combine expertise from both the security and IT field. The increasing importance of using software to provide complementary features to security systems has so far led to the emergence of a number of successful independent software companies, e.g. in the video management field. These companies are very dependent on close cooperation with hardware vendors whose products they support.

Wary of succumbing to a Microsoft scenario – i.e. relinquishing power to dominant software companies – entrant and incumbent hardware manufacturers alike are certain to keep a close eye on the software aspect of their business model. While vertical integration and proprietary closed systems may seem a thing of the past, completely open standards and APIs could lead to an escalation of commoditization and a shift in market value and power towards the software part of the industry. One strategy employed by the hardware side to counter this trend involves putting 'intelligence at the edge' – i.e. embedding software directly in controllers and devices that operate at the edge of the network, thereby reducing the need for centralized server software.

Demand-side and supply-side convergence in the security industry

Demand-side	Supply-side
Organizational security convergence ▪ Unified security approach spanning people, processes and technology ▪ Tearing down silos between physical and information security and IT ▪ Introduction of a C-level management position (e.g. CSO) overseeing both IT and physical security ▪ Integration of physical security and migration onto IP network platforms *International convergence* ▪ Internationalization leads to a homogenization of needs and customer preferences across markets ▪ Increasing demand for cross-border security services *Public-private convergence* ▪ Blurring of lines between public and private security – e.g. public video surveillance ▪ Convergence of public and private databases and information interfaces	*Technological convergence* ▪ Integrative technological platforms: Moore's law, miniaturization, intelligent devices, software ▪ Internet (TCP/IP on Ethernet) as a *de facto* communications standard *Product convergence* ▪ Convergence in substitutes: Separate classes of products become interchangeable (substitutes), e.g. digital and analog cameras ▪ Convergence in complements: Previously unrelated products are bundled together to form new, value-added class of products, e.g. integrated security systems *Industry Convergence* ▪ The merger of two or several hitherto separate, industries, e.g. physical security, IT, building automation ▪ Convergence in substitutes may lead to 'creative destruction' where innovative entrants replace dominant incumbents ▪ Convergence in complements may lead to a blurring of industry boundaries; alliance seeking; vertical integration

Conclusion

As has been outlined in this document, 'convergence' in the security industry is a multi-faceted phenomenon. The term convergence has little meaning if it is not put into a specific context or applied to a particular level of analysis, e.g. those proposed in the table above. None of the types of convergence described in this document are mutually exclusive, and they can certainly all be seen as part of meta-trend currently sweeping the security industry. However, using a sweeping definition of convergence is often problematic.

As an example on the demand-side, a company may well decide to take a unified approach to security from an organizational point of view, but may decide – for various reasons – not to integrate physical security and IT on the corporate network. Conversely, another organization may decide to migrate its security systems onto the corporate IT network, but otherwise maintain a non-unified approach to security, keeping the organizational silos between security and IT intact. Both these cases could be described as examples of convergence or non-convergence depending on the perspective chosen, illustrating the futility of using the term without a pre-determined definition or context in mind.

In a similar fashion, supply-side convergence benefits from a more detailed analysis. While it is no doubt correct to assume that the security industry is converging with the IT industry, the consequences from different types of industry convergence may be very different. In this respect, using the perspectives of convergence in substitutes and complements as a starting point, may help explain the roles of different player categories and some of the contradictory trends that can be observed in the security industry today – from Best-of-Breed sourcing and 'ecosystem' partnering approaches to M&A and vertical integration.

References

Convergence of Enterprise Security Organizations (2005). Booz Allen Hamilton, Report commissioned by The Alliance for Enterprise Security Risk Management (AESRM).

Greenstein, Shane and Khanna, Tarun (1997) "What does industry convergence mean", in Yoffie, David (ed.) (1997) *Competing in the age of digital convergence*, Boston, MA, Harvard Business School Press.

Yoffie, David (ed.) (1997) *Competing in the age of digital convergence,* Boston, MA, Harvard Business School Press.