IP security – a disruptive or sustaining technology shift?

Weaver, Benjamin

2009

SCHOOL OF ECONOMICS AND MANAGEMENT
Lund University

Lusax Security Informatics

www.lusax.ehl.lu.se

LXM-BW3 – IP Disruptive

Author: Benjamin Weaver
Subject: **IP security technology: A disruptive or sustaining technology shift?**
Date: 18 June 2009
Pages: 8
Email: benjamin.weaver@fek.lu.se

IP security – a disruptive or sustaining technology shift?

Executive Summary

The shift towards IP-based security products and systems is often touted as an example of a *disruptive technology* that have had – and will continue to have – profound consequences for the electronic security industry as a whole. Based on Clayton Christensen's theories on disruptive innovation, this document argues that the introduction of IP-based technology has different effects depending on the product segment observed. In the case of video surveillance, it is argued that IP has brought about a *disruptive* change, whereas the effect on access control is found to be more of an incremental, or *sustaining* character. These conclusions are based partly on an analysis of the impact of IP technology on product platforms, and partly on observations of changes in industry structure that can be observed in the video surveillance and access control sectors.

The wider effects on security industry dynamics are also discussed. It is argued that despite the apparently disruptive changes seen so far in the video surveillance sector, the unique characteristics of the security industry (e.g. end-user and channel conservatism, slow technology replacement cycles) may lead to a different scenario than that prescribed by Christensen. Hence, analog CCTV incumbents may still have time to catch up with the entrants that currently dominate the IP video surveillance market. In access control, the dominant incumbents are leading the change towards IP-based solutions, leading to less dramatic effects on industry dynamics. Viewed from an overall security industry perspective, these conclusions indicate that the shift towards the digital technology has not happened – and will likely not happen – through a disruptive change, but rather gradually and incrementally, in a sustaining fashion. Finally, emerging technologies with disruptive potential are briefly discussed.

Introduction

As the electronic security industry is migrating digital and networked technology platforms, many industry commentators have been keen to point out the radical and *disruptive* nature of this change. Among proponents on the IT and IP side of the industry, this disruptiveness is seen as creating no less than a major upheaval of the structure and business logic of the industry. In contrast, some security sector veterans point out that the industry has seen it all before and that the current wave of change is not necessarily more significant than many previous technological shifts. To these observers, the move towards IT and IP represents more of an incremental change that is likely to happen slowly enough that most of the incumbent firms in the security industry will have time to adapt.

In economics and management science, it is widely acknowledged that industries often face radical change and that firms need specific strategies to cope with these situations. The discussion goes back to Austrian economist Joseph Schumpeter (1934; 1942) who believed that all economic development emanates from a continuous process of strategic innovation, generated by the entrepreneurial activity of individuals and firms within the capitalist system. 'Schumpeterian innovations' are difficult to predict and, if successful, tend to lead to radical, discontinuous change, where incumbent firms that are not able to adapt to the new conditions are unceremoniously swept away in what Schumpeter (1942) dubbed 'the process of creative destruction'.

Christensen's disruptive innovation context

Since Schumpeter, research on radical change has focused mainly on the management of technology and innovation. In this field, it is the theories of Clayton Christensen that has garnered most interest. Originally based on longitudinal data from the disk drive industry, the quest of Christensen's research has been to examine why established leaders in a particular industry often fail in periods of radical technological change. While incumbents are usually great at improving the technologies and products that gave them their initial success in the market, they often fail to recognize and embrace the dominant technologies of the future, paving the way for innovative entrant companies.

In a series of articles and books aimed at both practitioners and academia Christensen and his co-authors (Bower & Christensen, 1995; Christensen, 1997; Christensen and Raynor, 2003) have identified two types of *innovation contexts*[1] that determine whether incumbents are likely to fail or not. In a *sustaining* innovation context, already dominant companies refine and improve their products – and the technology base used to manufacture them – to satisfy the demands of their most important customers. In contrast, a *disruptive* innovation context sees the emergence of a new technology base that generates a new class of products. At the outset, these products are more basic, lower performing, (often) cheaper and exhibit new and different set of features or performance attributes that are initially not valued by the majority of existing end-users.

This leads incumbents to misjudge the market potential of disruptive technologies, assuming the profit margins will be too low in relation to the effort needed to reach new customer segments. Instead, it is innovative entrant companies – unencumbered by legacy technology and old ways of doing business – that are successful in commercializing disruptive products. Once the critical product performance attributes valued by the majority of customers segments are improved, entrants are able to use their early lead in the disruptive technology to conquer mainstream customers. While incumbents' R&D and engineering departments often develop and champion products based on disruptive technology, incumbents typically fail to move these products through their internal organization and onto the market as quickly and efficiently as the entrants. Thus, the short answer to why incumbents fail in the face of disruptive innovation, is that incumbents listen *too much* to the needs of their most valued customers.

In *The Innovator's Solution,* Christensen & Raynor (2003) refined the original theory of disruptiveness with two further distinctions. A *low-end disruption* occurs when the disruptive innovation takes place at the low end of the market in the original value network. As incumbents continue to refine technology through sustaining innovation, products eventually become so advanced or high-performing that they overshoot the needs of customers at the lower end of the market. In this case, a cheaper and simpler new technology may be 'good enough' for the low-end customer segments, allowing a disruption to occur. *New-market disruption* entails a different scenario, where simple and cheap disruptive innovation makes it possible for entirely new customer groups to acquire and own the product in question. In this case, the disruption does not compete with existing markets and customers segments, allowing entrants to gain market traction unnoticed by the incumbents.

Disruptive technology in the security sector

Applying Christensen's theories to the electronic security industry as whole is difficult, as the model presumes a level of analysis at the product level. For this reason, the focus here will be on two of the most important security product segments: video surveillance and access control.

Video surveillance

From a product perspective, a video surveillance system can be said to comprise three distinct components: cameras, a video transmission system, and a monitoring and recording system. Apart from the introduction of color, the basic technology of a fully analog video surveillance system has changed little since it first appeared about half a century ago: A camera outputting a standard PAL or NTSC video signal is connected through coaxial

[1] Intially referring mainly to *disruptive technology*, Christensen changed the term to *disruptive innovation* in *The Innovator's Solution* (Christensen and Raynor, 2003). This is in reflection of the fact that few technologies are inherently disruptive – they only become so when they are successfully commercialized.

cable to a monitor and a VCR. An analog video surveillance system is by nature a closed system, delimited by the physical cabling needed to interconnect all the components (hence the traditional moniker Closed Circuit TV).

Less than a decade ago, a first wave of digital technology disruption occurred with the advent of digital signal processing through the introduction of digital video multiplexers and – more importantly – Digital Video Recorders (DVRs). The obvious benefits of replacing VCRs with hard drive based digital recorders created a major disruption to the recording side of the industry, which rather closely followed Christensen's predictions. Although not a low-end disruption in terms of price, the increased performance of DVR was so obvious to end users that VCRs are all but extinct in the security industry today. For incumbent VCR vendors, the security industry was never more than a peripheral niche. Thus, in the video surveillance value network as a whole, the DVR simply substituted the VCR, with little impact on the business models of security distributors, systems integrators, installers and resellers. Representing the bridgehead to digital technology, the successful entrant DVR firms did however shift the power structure of the industry over time. Today, DVR companies play a leading role in the video surveillance industry, often driving important projects at the forefront of surveillance technology.

The current shift towards fully IP-based video systems can be seen as the second wave of digitalization of the video surveillance segment. Driven by the replacement of analog cameras by digital network cameras, this disruption extends the digitalization of video surveillance through networking technology, in essence replacing the closed, proprietary nature of traditional CCTV with an open IP architecture. The benefits of shifting to an all-digital IP network video system are manifold (see the table below) but arguably the most disruptive feature of IP video is the possibility to remotely monitor and control cameras through the Internet or any corporate network. Although this feature can also partly be accomplished through hybrid solutions – where analog cameras are connected to a DVR or encoder with IP connectivity – an end-to-end IP system brings additional benefits in terms of cabling efficiencies, flexibility and scalability.

Network video surveillance – a disruptive technology?

The adoption of network video has largely followed Christensen's formula for disruptive technological innovations. The first network cameras (or 'webcams') were treated as novelties and initially underperformed in all product attributes valued by traditional security end-users. Nonetheless, entrant network video companies managed to find a niche among early adopters that valued the remote monitoring possibilities of the new technology. Since their introduction in the late 1990s, network cameras have today largely bridged both the feature and price gaps to analog CCTV, while the additional benefits of converging all of an organization's security and data communication on a single network have become increasingly evident.

Most tellingly, perhaps, is the fact that the push toward IP cameras has been almost exclusively driven by pure-play entrants without any analog CCTV background. Faced with initial skepticism and hesitation from traditional security customers, the IP entrants carefully built up their business through a *new market disruption*, e.g. by focusing on customer segments – such as retail, transport and education – that valued the specific benefits and new functionally offered by network video solutions. When traditional security channels initially appeared skeptical of the new technology, the IP entrants pushed their products through IT channels and IT value networks instead. And just as predicted by Christensen, most of the dominant CCTV incumbents have been very slow to respond to the shift towards IP cameras. Focused on the needs and preferences of their most important customers they initially failed to recognize the benefits of network video and underestimated the early market potential and pace of migration. The result today is that pure-play IP entrants dominate the network video segment of the video surveillance industry. Thus, while the incumbents hesitated and procrastinated, the IP entrants have managed to build a level of brand recognition and reputation that will be hard for the incumbents to catch up to, at least in the shorter term.

Access control

An access control system can be said to consist of three main components: an access control point (e.g. a door) with a locking mechanism, a reader and a controller unit containing access information. In a typical set-up, a non-intelligent reader is connected to a control panel in proximity to an

access point, such as a door. In this case, the credential data entered into the reader is checked against an access control list contained in the control panel, and if the request is granted the door is opened. Intelligent readers can also be used, in which case the reader performs the same function as the control panel and is able to make access decisions independently. Depending on the setup, control panels or intelligent readers may be connected to a central host PC, enabling remote management of access privileges as well as monitoring of events and alarms.

As in the case of video surveillance, the shift to digital technology has come in two waves. The first wave occurred in the early 1990s, with the introduction of IP-enabled control panels that could be connected to a central host through any corporate LAN or WAN, eliminating the need to install separate communication lines to a central host. Being able to leverage the corporate IT network for access control communication was thus an attractive option. As the amount of data traffic generated in an access control system is small, the bandwidth problem experienced during the introduction of IP video surveillance a decade later was never an issue.

The second wave of IP-based access control – concurrent with the introduction of IP video – extends the network all the way to the door by using intelligent, network-addressable IP readers that eliminate the need for control panels and additional cabling. IP readers have the potential to simplify installations, further optimize network utilization and enable flexible scalability of the system. As in the case of IP video, this second wave of IP access control can be seen as a part of a wider trend towards security systems integration based on software unification and the convergence of all components of a security system onto the same IP network.

IP access control – a sustaining technology?

Although IP-based access control provides a number of benefits, it is hard to identify any specific product feature that is disruptive. Looking at all the functions performed by an access control system, IP networking almost exclusively addresses how the communication between the reader or control panel and the host takes place. Most of the tangible performance metrics that are valued by access control end-users are related to the specifications of the complete system as such, and the focus is usually put on the reader component, what type of credentials that can be used, tamper resistance etc.

Thus the attractiveness of end-to-end IP-based access control boils down to two main benefits: The first is the fact that unnecessary cabling can be avoided. This benefit is largely erased if the corporate IT network does not extend to access points such as doors, or if traditional cabling (e.g. RS485) is already in place. The other main benefit of IP-based access control – remote management and control – can be attained by using intelligent IP control panels that connect to the corporate network. As mentioned earlier, this alternative was introduced nearly two decades ago and has since become widely adopted in the industry.

Given the points above, the introduction of IP networking to access control is arguably what Christensen would describe as a *sustaining* technology innovation – i.e. the type of incremental product improvement and feature updates that incumbents are always working on. Adding IP does not, by itself, revolutionize an access control system as a whole, in the same way that IP does to video surveillance. Rather, IP is a convenient, but not crucial, option.[2]

Another strong indicator of a sustaining change is the fact that dominant access control incumbents have fully embraced IP access control and are the ones seen driving this technology platform forward. A few pure-play IP access control companies have emerged, but these remain niche players. Moreover, while IP video entrants have been successful in using the IT channel to market their products, the same scenario has not played out in IP access control. Part of the reason for this is likely due to the fact that incumbents are marketing IP-based products through the same security-specific distribution channels as before. Another reason is that, in comparison to video surveillance, access control is an inherently more esoteric and regulated security technology, and as such fits less well with the competences held by the IT channel.

[2] The same reasoning also holds for intrusion detection and fire alarm systems, where IP connectivity is still trailing, partly due to regulatory issues.

IP as driver of disruptive vs. sustaining technological shifts

	IP video surveillance (disruptive)	IP access control (sustaining)
Disruptive or sustaining tech	▪ IP-networked digital cameras ▪ Video management and analytics software ▪ Network video recording (NVR)	▪ Access control and door solutions with end-to-end TCP/IP over Ethernet network connectivity ▪ IP access control software solutions
Main benefits	▪ Remote monitoring and management ▪ Network integration and scalability ▪ Cabling efficiencies, PoE ▪ Megapixel resolution/picture quality ▪ Network video recording ▪ Embedded video analytics ▪ Optional wireless IP networking	▪ Remote monitoring and management ▪ Network integration and scalability ▪ Intelligent IP reader replaces control panels ▪ Cabling efficiencies by using existing LAN/WAN networks and PoE ▪ Optional wireless IP networking
Replaced technology	▪ Analog CCTV cameras ▪ Coaxial cabling ▪ VCR recording	▪ Offline and non-IP online access control solutions ▪ Intelligent control panels ▪ RS485 (or equivalent) cabling and proprietary communications protocols
Intermediate technology	▪ Analog cameras in combination with digital video recorders (DVR) with IP network capability	▪ Control panels or central unit with IP networking capability
Entrants	▪ Pure-play IP companies with no analog legacy have become market leaders in hardware as well as software	▪ Pure-play IP entrants mainly in software, (smaller hardware IP entrants exist)
Incumbents	▪ Pure-play analog incumbents slow to react or failing in IP. ▪ Large diversified electronics incumbents adopting IP but not leading market.	▪ Dominant incumbents lead the push towards IP. Most access control hardware companies are offering IP solutions. Fragmented market.

Implications for security industry dynamics

In the above, it has been argued that the introduction of IP-based technology to electronic security systems has different effects depending on the class of product analyzed. In the case of video surveillance, it has been argued that IP has brought about a *disruptive* change, whereas the impact on access control is of a more incremental, or *sustaining* character. In this final section, the effects and implications of these findings on security industry dynamics will be discussed.

Effects on video surveillance sector

As described earlier, the digitalization of video surveillance has come in two disruptive waves:
1) the introduction of the DVR a decade ago and;
2) through the current migration towards digital cameras and end-to-end IP networking. A few years into this second disruptive change, the scenario has largely followed Christensen's recipe for disruptive innovations, as pure-play entrants have quickly established themselves as market leaders in the IP segment of the video surveillance sector. In most high-tech industries, this scenario would indicate long-term defeat for those analog incumbents that were late, let alone those that have still not embraced the shift towards digital technology. However, the security industry is unique in many aspects. When put into the context of the security industry as a whole, the long-term effects of this disruption may not follow the typical disruptive patterns (i.e. displacement of incumbents by entrants) that Christensen and others describe. With its inherently conservative end-users demanding solutions that have been rigorously tried and tested, security is one of the few technology industries where a wait-and-see approach can be a win-

ning strategy. Product replacement cycles for CCTV equipment can run up to a decade, explaining why 80% of globally installed video surveillance systems are still analog. In this context, two important disruption 'blockers' can be highlighted.

First, IP camera systems are rarely sold stand-alone, but as a part of larger security projects and installations, making it difficult for IP camera vendors to decouple from traditional, conservative security channels and 'go it alone' using IT distribution business models. This interdependence between IP vendors and traditional security channels slows down the pace of migration, allowing incumbents further time to adapt. [3]

A second disruption blocker is price vs. product performance attributes. While Christensen suggest that disruption will occur as a result of the introduction of radical, new performance attributes (e.g. IP connectivity, digital imaging), some technology disruption researchers believe this underestimates the importance of absolute price on end-user demand, or, as stated by Adner: *"Consumers with sufficiently satisfied functional requirements are more concerned with differences in absolute price than with differences in price/performance points"* (Adner, 2002, p. 684). This reflects an often repeated argument from security end-users and incumbents, that while network cameras are as good as or better than their analog counterparts, their higher price (per unit) makes them hard to justify in many installations where digital and IP functionality is less important.[4]

The overall effect of these disruption blockers is a slow pace of change that makes it difficult for IP video entrants to leverage their initial market lead, to the extent needed to gain control over the market. Incumbents may well be able to catch up, and even gain a second-mover advantage as they follow their end-customer's replacement cycles. The result in the near future could be a video surveillance industry that is even more fragmented than in the past, with entrants and incumbents fighting hard over market share. And to fend off commoditization and cheap Far East alternatives, entrants and incumbents alike will have to retain their innovative edge and superior after-sales service capabilities.

Effects on access control sector

Identified as a sustaining innovation at the product level, the effects of IP on the access control industry are not likely to be dramatic. Leading incumbents will continue to dominate and channel structures will largely remain intact. However, as access control is very much affected by the general trend towards integration and convergence, the deployment of IP-based access control will undoubtedly accelerate in the coming years.

Eventually, driven by their ventures into network video technology, some IT players, notably integrators and installers, are likely to enter the access control market in order to be able to offer fully integrated security systems solutions. As this happens, IP access control may increasingly start to move through IT channels, alongside network video systems. But these changes will happen slowly and gradually, giving industry incumbents time to adapt and consolidate their market leadership.

Effects of IP technology shift on security industry as a whole

So far, at the level of specific products segments, we have found IP technology to have both disruptive and sustaining effects, with correspondingly different consequences for industry dynamics. However, many security commentators take a more holistic view of the industry, arguing that the true disruption lies not at the level of individual security components, but at an aggregate level, where IP enables a level of systems integration and remote management that was not possible before.

Similarly, the increasingly important role played by software in security systems could be seen as a potential disruption driver for the industry as whole. While IP undoubtedly provides a unifying communications platform, systems integration is ultimately achieved through software. Software – whether embedded in edge devices or run on network servers – will also be key to leverage the near limitless possibilities offered by all-digital and networked security hardware platforms. Over time, there is no doubt that this will increas-

[3] The need for an increased understanding of the industry and value network context in which a disruption occurs (or not) has been put forward by critics of Christensen's model (e.g. Danneels, 2004)

[4] Such claims have been vigorously contested by IP camera vendors. The point here is that as long as end-users and incumbent integrators and installers *perceive* that the absolute price/unit for IP cameras is higher, they may postone investment.

ingly shift market value and power to software developers in the security industry.

However, identifying disruptive technology shifts from an aggregate security industry perspective is problematic. Integrated security systems have been around for decades and most real-world integrated systems are in any case based on a mix of legacy components and newer IP-enabled equipment. Likewise, software has been an integral part of security solutions for decades, making it difficult to argue that we are seeing is a disruption, rather than gradual (sustaining) evolution of technology and products.

There is no doubt that the high degree of systems integration made possible by the combination of networked IP hardware and software, is quite radical compared to what was possible a decade ago. But the point here is that from an *overall industry perspective*, the shift towards the digital state-of-the-art has not happened – and will likely not happen – through a disruptive change, but rather gradually and incrementally, in a sustaining fashion. The fact that disruptions have occurred in some underlying product segments (DVRs, IP network cameras) does not change this overall conclusion at the industry level.[5]

Future disruptive innovations in video surveillance and access control

Looking forward, it might be interesting to speculate on potentially disruptive technologies and innovations that are already in the early stages of development. With IP video becoming a subset of the IT industry, product development cycles are now counted in months, rather than years (or even decades), as was the case with analog CCTV. Hence, there is currently a race towards higher-resolution (megapixel and HD) video as well as continuous improvements in video compression and analytics software. These are examples of sustaining technology improvements that will likely drive the feature sets and performance of digital video products to 'overshoot' the needs of most security applications. When this happens, the hardware side of the industry will likely face increasing price pressure and commoditization. As the power and performance of digital hardware is taken for granted, the pressing issue will be how to manage, analyze and leverage all the surveillance information generated. This, in turn, opens up the possibility that future disruptions will shift market power away from the hardware side of the industry to innovators within software and managed services.

In access control, truly disruptive technologies tend to emerge at the credential-reader interface. The most recent disruption of this kind was the introduction (by innovative entrants) of contactless proximity cards and readers, which over a short period of time displaced the then ubiquitous magnetic stripe and wiegand systems. One emerging access control technology with a disruptive potential is Near Field Communication or NFC – an extension of the proximity card standard that allows enabled mobile handsets to act not only as intelligent credentials but also as readers/writers and peer-to-peer devices. Combining this flexibility with the possibility of sending credential data through mobile networks, NFC opens up almost endless possibilities in terms of converging access control and electronic keys with mobile payment and commerce.

[5] An analogy can be made with Christensen's original account of disruption in the disk drive industry. While disk drive technology disruptions had major impact for the disk drive manufacturing sector, these specific disruptions did not have an impact on the computer industry at large.

References

Adner, R. (2002) When are technologies disruptive? A demand-based view of the emergence of competition. *Strategic Management Journal,* 23, 667-688.

Bower, Joseph L. and Christensen, Clayton M. (1995) Disruptive Technologies: Catching The Wave, *Harvard Business Review*, Jan-Feb 1995.

Christensen, C. (1997) *The Innovator's Dilemma,* Harvard Business School Press, Cambridge, MA.

Christensen, C. and Raynor, M. (2003) *The Innovator's Solution: Creating and Sustaining Successful Growth*, Harvard Business School Press, Cambridge, MA.

Danneels, E. (2004) Disruptive Technology Reconsidered: A Critique and Research Agenda, *Journal of Product Innovation Management,* 21, 246-52.

Schumpeter, Joseph A. (1934) *The Theory of Economic Development,* Transaction Pub-lishers, London.

Schumpter, Joseph A. (1942) *Capitalism, Socialism & Democracy,* Routledge, London.