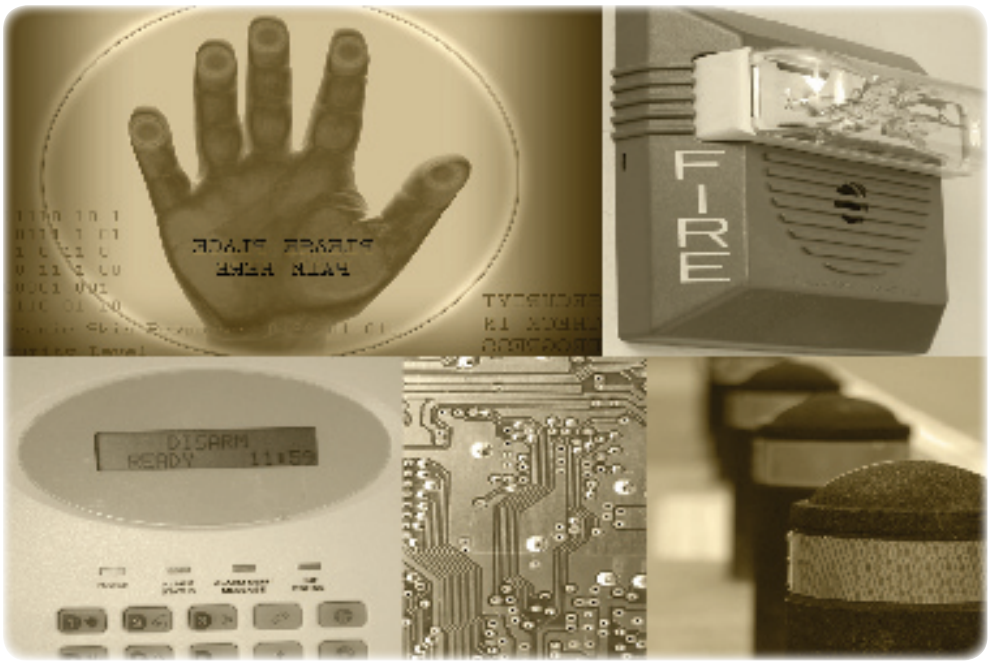


Physical Security Information Management

May 2008

John E. Mack III
Managing Director
(310) 246-3705
jmack@imperialcapital.com

Gavin Long
Vice President, Industry Monitoring Group
(212) 351-9766
glong@imperialcapital.com

PLEASE SEE IMPORTANT DISCLOSURE ON PAGE 18

Imperial Capital

Table of Contents

Section I:

The Security Environment & the Need for PSIM

Introduction

A large, established industry is in the midst of a sea change. The Physical Security Industry, with a total market size in excess of $150 billion, is both mature and complex. Vendors ranging from one of the largest corporations in the world (General Electric) to numerous niche technology players with less than $2.0 million in revenues serve this Industry. In fact, Imperial Capital tracks more than 500 companies in this Industry. In many respects, the Industry is reasonably mature and developed, but with respect to information management the Industry is highly underdeveloped and even myopic. Most software vendors in the Physical Security Industry, to date, have created closed, proprietary systems. Hardware vendors have been reticent to share application programming interfaces (APIs). In turn, the Industry has functioned in a territorial manner and end users are communicating that the Industry must change.

In an attempt to protect their hardware sales, larger players have used a closed approach to keep the competition from penetrating their market share. The victims of this closed approach, however, are not just the smaller players who get locked out from the larger player's channel. The true victims are the end users who continue to add data into the security information reservoirs, but have little means to manage and use that data. As the information reservoirs get bigger and more diverse, the security departments get larger and more inefficient. Organizations have to employ more human resources to keep up with the data and the value proposition for security infrastructure is increasingly more difficult to justify. For instance, one of the world's largest oil companies employs thousands of security professionals, including more than 250 vice president or director level professionals that focus solely on security. Security information is inundating its users.

Put simply, managing security information is critical to the next phase of the Industry. With increasing amounts of rich data available from ever larger investments in physical security systems, the need for better information management is much greater and the rewards for maximized use of this information can not only enhance security, but also translate into increased business productivity. The advent of the physical security information management category is integral to the next phase of growth for the Security Industry.

The Need for Physical Security Information Management (PSIM)

In large enterprises and government organizations, a host of security devices comprise the physical security infrastructure. Below is a working list of disparate systems that exists in one of the largest financial services companies of the world:

- Access Control System
- Biometric Scanners
- CCTV, Video Analytics and Video Software
- Geographical Information Systems
- Communications Systems
- Automated Bollards
- Alarm Systems
- Panic/Duress Alarms
- Fire Alarm Systems
- Building Management Systems
- Elevator Controls
- Air Purge Systems
- CBRN Sensors
- Radio Frequency Identification (RFID) Tags

Each of these systems operates within its own ***intra-textual*** environments. In other words, these systems work within their own confines to perform a defined task - surveillance, authentication, emergency notification, etc. These systems, however, are not ***inter-textual.*** They do not have a working knowledge of each other and have limited ***inter-activity*** with each other. The result is a completely piecemeal approach to security, which, in many respects, actually creates inefficiency. No doubt the security infrastructure does help secure an organization in many fashions, but within large organizations the inability to manage the technology and the information flow actually translates into organizational inefficiency. Not only is security compromised, but the deployment of existing security systems with no ability to manage the security information translates into a false sense of security, which is an even larger problem with larger liability. In a recent interview with a Fortune 25 company who is evaluating a PSIM platform they stated, "We are placing a hold on all security technology purchases, except for PSIM. We simply cannot afford to move forward without a physical security information management platform.

As expansive as our organization is, we must find a way to manage the volumes of data that often paralyze our enterprise. We need PSIM for operational efficiency and for our own compliance concerns. Improved security is obviously a benefit, but PSIM moves beyond security for us and deals directly with the day-to-day activities of our organization." In the later pages, this piece will touch on some of these themes. But the point of this quote is to highlight how end users are thinking about security information within the context of the entire organization, not just a department or a technology.

A Physical Security Information Case Study: The Video Analytics Phenomenon

The industry has tried to deal with this central concern of information management, but has done so on a limited basis. The most recognizable information management innovation of the last decade is video analytics. Yet, after all the hype, little has come of the intelligent video phenomenon. In retrospect, this lack of development makes sense. We have interviewed more than 30 intelligent video companies. Of the 30 companies fewer than 5 are greater than $10 million in revenues. No want of clever technology exists. In 2006 more than $100 million of venture money was invested into the space, so investment has been sufficient. Yet, almost all of these these companies have yet to scale. Why is that the case?

The reason that video analytics space has not taken off is not because of the cost or the difficulty in creating or tuning the analytics. The root cause is much simpler than those reasons. End users are already inundated with data. Though the premise of video analytics centers around alerting users to anomalous activities or events, in reality an analytic trigger is just another noise in the cacophony of security alerts. In one global financial services company more than 100,000 false alarms occur daily. The video analytics information may be helpful, but quite simply end users do not have the mechanisms to make sense of the data. Video analytics is just a feature and is not an information management platform. Like an alarm, analytics are just another piece of the solution, but is not the solution itself. Without an information management platform intelligent video analytics are rendered largely ineffectual. Within the context of an information management platform analytics are a powerful tool that can help manage video data and security personnel bandwidth in an efficient manner.

What we see in PSIM is a fundamental shift in an information management philosophy. "Analytics" has largely been used for forensic data evaluation. There has been little to no ability to manage events and situations. PSIM spans the entire scope of security data, and translates data into real-time knowledge and situation management. PSIM incorporates, but also transcends video alerts. PSIM takes the large volumes of security data and translates them into actionable intelligence.

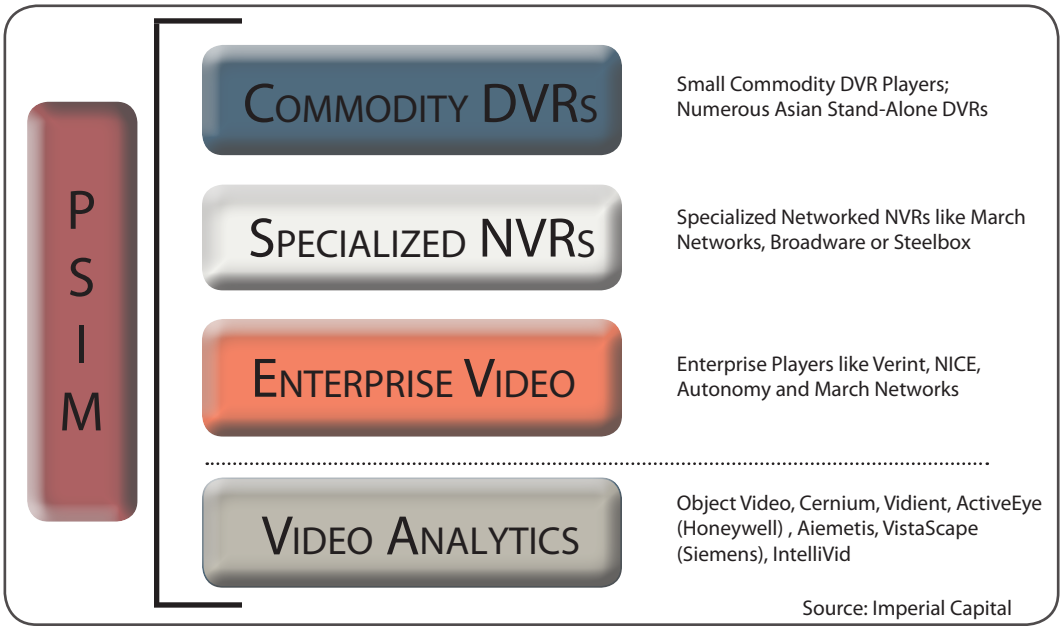
Beyond Intelligent Video — Managing the Entire Security Spectrum

As we have discovered, video analytics was the industry's first attempt at sorting through data and making security information more usable and efficient. But the flaw of video analytics was the lack of true security information platform capabilites. One could argue that video analytics has failed because of its lack of channel and therefore has been unable to generate growth; however, the rest of the industry — even some of the largest, most established players — are beginning to experience the difficulty of getting analytics to market and the negative ramifications of proprietary thinking. So, if channel is not the problem, there must be something more critical to the concern of information management. We believe that the problem is in its fundamental architecture.

Though PSIM spans well beyond video, incorporating video into the total security information continuum may be most difficult. Video players, in many respects, have been the hurdle to a complete PSIM solution. Video players have had difficulties dealing with the concept of sharing information and allowing a software platform to manage video data. Below we breakdown how the current video landscape.

Each of these video players house and manage video in different ways. Yet, they are largely ineffectual at integrating that information into a broader security context and translating that video information into real-time intelligence. Enterprises and Governments will not be able to overhaul their video infrastructures to create universal information management solutions. Therefore, a security information management platform is necessary to unify video data and integrate it into the broader security context to create a total physical security solution. That idea is the essence of PSIM. This is one reason that we argue why PSIM is not video management, but a complete PSIM solution must be able to manage video and integrate it within the broader physical security domain. PSIM translates data into intelligence and helps users make sense of the information within their enterprise.

Figure X: Video Information Management Landscape



An example of this phenomenon within the Security Industry is a recent safe city project for one of the largest cities in the Western Hemisphere. This past year the initiative launched a city-wide security infrastructure overhaul. In this initiative (funded by the federal government) a new city-wide security system is being developed. The goal of the initiative is to create an intelligent security information sharing and management environment that enables multiple agencies, jurisdictions and even large private enterprises to pool and manage security information and effectively respond to incidents. A multi-billion security player lost a very large NVR/DVR order (again, keep in mind this is a city-wide initiative) because they could not (or possibly would not) provide an API for their system. End users quite simply cannot afford the myopia of traditional thinking. Not only end users, but also equipment suppliers suffer the consequences and are forced to try to put the pieces together of a highly fragmented puzzle. Larger players are beginning to experience the impact of an evolving industry.

At the core of this evolution is a demand for a physical security information management platform. Without a platform, large and small players alike are floundering. As we have argued before, a security information management (SIM) platform is not only essential for the industry, a SIM for physical security is the killer application for the industry. In other words, a SIM platform is the application that justifies and redeems the existing security infrastructure and actually generates the need for new applications (like intelligent video software). Put more simply, the catalyst for the next phase of the Industry's growth rests on the migration to a PSIM platform.

The First Enterprise-Class Physical Security Software

Few people think of physical security within the context of enterprise-class software. Physical security has been provincially minded and the sales processes have not focused on C-Level professionals, but rather director level decision-makers who have not had the mandate of thinking about the entire enterprise. Now, Chief Security Officers (CSOs) and Chief Information Officers (CIOs) are sharing the burden of thinking through physical security and are ultimately responsible for helping CFOs and CEOs in making decisions. Again, this is a radical shift for the Physical Security Industry. Even enterprise software behemoths recognize the value of physical security. Companies like Oracle are openly investing and advocating the necessity for physical security information. The problem, however, is even though large enterprise software vendors are seeing the opportunity, traditional physical security players are unable to respond to the demand. Most physical security companies are engineering and manufacturing companies. These companies understand how to make devices and engineer a system for that particular device, for a particular application. Traditional security players, however, do not naturally understand enterprise-class software and have difficulties thinking about solutions in this broader context.

PSIM, in our opinion, is the first enterprise-class software category for physical security. This development is pivotal for the Security Industry, as security and compliance concerns continue to elevate in status. The size and nature of the opportunity is massive and is nothing short of introducing a new brand of software that belongs to the enterprise suite. Software investors and vendors, alike, are always looking for the next enterprise software opportunity, but few new opportunities of this stature exist. We believe that the PSIM category is one of those rare exceptions where a new category is actually being created in the enterprise suite and we are already seeing the opportunity develop quickly.

How Big is the Disparate Physical Security Infrastructure Problem?

In the course of this report, we have talked about disparate systems within the physical security infrastructure. But to communicate the severity of the problem, we'd like to give a few examples. In another Fortune 50 environment, a company has 54 access control systems. Not one of those access control systems interoperate with each other. No one in the organization has a universal purview of the access control systems. None of the credentialing systems work with the larger enterprise HR databases. The company manually runs 54 different access control systems and has no centralized, over arching security management or compliance reporting.

The company did try to standardize on its DVRs; however, the software and the DVR, though made from the same manufacturer, did not interoperate. Even infrastructure made from the same vendors has problems communicating with each other. So creating a seamless system is by no means an easy task.

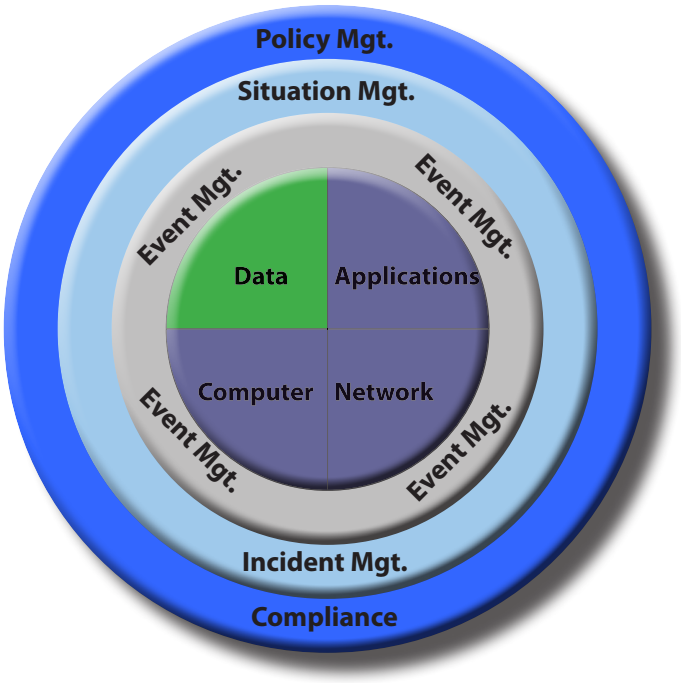
The video surveillance market is highly fragmented with DVR manufactures ranging from $multi-billion Honeywell to leading stand alone players like Nice, Verint, DVTel and March to small vertical market specific players like Comtrak. There are literally hundreds of DVR and NVR players. Some are robust and highly advanced with real network IP integration, like Broadware and SteelBox; others are simple stand alone systems. From large government projects like SBINet to large, global Fortune 50 enterprises complex physical security systems are underscoring the need for security information management systems. The two mainstays of physical security, access control and video, are exceptionally difficult to unify. But beyond video and access control are other sensor networks and software applications. In short, Physical Security is a highly complex environment that needs a information management platform to simplify life for end users. For all types of organizations, PSIM provides them to shift their focus beyond technology and data and allows these organizations to focus on knowledge and action. In other words, the PSIM goal is not about managing technology or data, it is about managing the situation.

Section II:
Defining PSIM

Defining PSIM Part One - The Network SIM Analogy

The SIM concept is not new. Though the network infrastructure world is much younger than physical security infrastructure, the network arena was quick to adopt a SIM concept. Intrusion detection and prevention systems (IDS/IPS), along with firewalls, vulnerability assessment tools, IAM software, and behavior anomaly detection applications were too much for a network administrator to manage. The SIM concept was essential for the health of the overall IT security industry. Several major players Cisco, EMC, Novell, Symantec, and IBM acquired and/or developed SIMs to manage network security infrastructure. Fortunately for this industry, open standards and information sharing were assumed modes of operation. In turn, the SIM became the central dashboard for all security management.

Figure 1: The SIM Concept

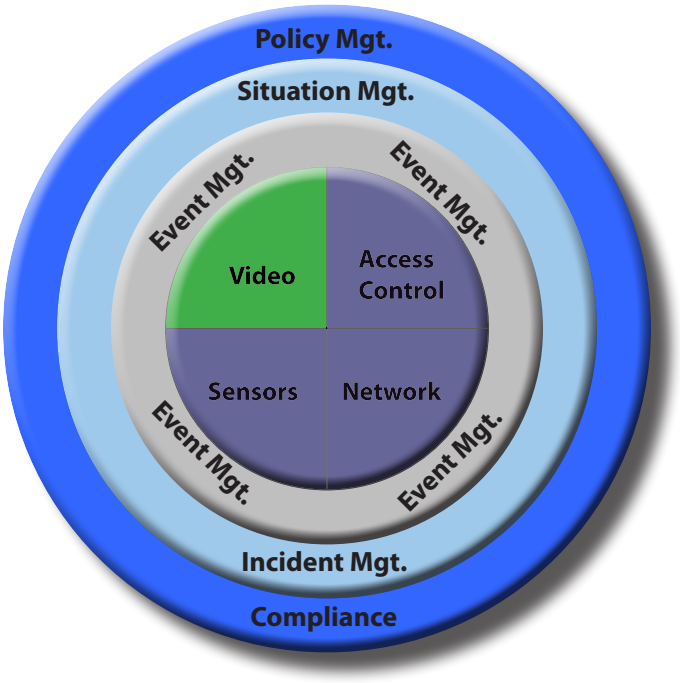


The SIM platform extends from event & incident management into policy and role management systems for security and compliance applications. The way in which information is shared, access is controlled and polices are managed hits at the very core of how an organization operates.

Defining PSIM Part Two - Translating into Physical Security

The PSIM concept mirrors network SIM. But rather than gathering security data from IDS/IPS, firewall, vulnerability assessment, IAM and other network security infrastructures, PSIM is taking data from physical security infrastructure. (Notice: Both PSIM and SIM intersect with IAM technologies.)

Figure 2: The PSIM Concept



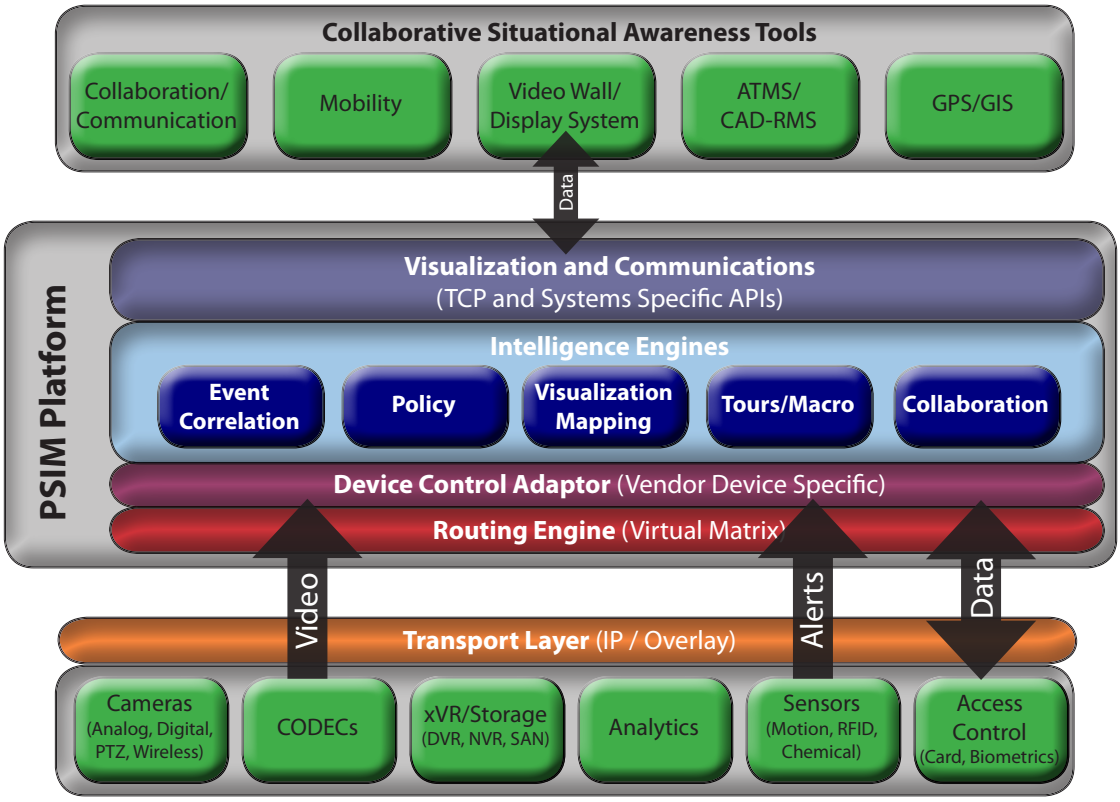
Rather than monitoring countless devices and applications with security professionals, SIM platforms help security groups sort through the data, elevating that which is important and filtering that which is not important. Operational efficiencies are dramatically improved and security processes are properly integrated within the organization's ontology. In the same way, PSIM sorts through volumes of physical security information feeds and alerts to determine that which is important and that which is not. Also, PSIM creates operational efficiencies and dramatically increases the security infrastructure's efficacy. So, the use of PSIM translates into saving time and organizational bandwidth, which translates into saved dollars (see example on page 14, correlating saving time and money). Appropriately, PSIM integrates physical security data back into the organization's overall ontology, creating agile responses that correspond to the organization's policies and procedures. Without PSIM, an organization has to combat the high volumes of security information with more professionals and therefore more operational challenges.

As successful as SIM has been, we believe PSIM could actually represent a larger market. PSIM, however, does have the hurdle of dealing with slower moving players who could be adverse to change. Ultimately, end users must reconstitute the landscape by pushing incumbents to open standards so that the Industry can move to an information management platform.

Understanding the PSIM Architecture

To integrate these disparate systems and create organizational efficiency, the PSIM platform takes data feeds through various protocols and APIs to create a "common language" for security information. In turn, the software uses intelligent analytics and correlation engines to sort through volumes of security information across numerous data sources to create a unified security risk management lens. (Remember this platform helps redeem legacy infrastructure and make it more effective - it is the killer app.) Keep in mind that in each of the major categories listed below (analog cameras, digital cameras, CODECs, NVRs, DVRs, Storage Area Networks, analytics, sensors and access control systems, including biometrics) there are numerous vendors. So with each category, the difficultly of unifying the information is exponentially increased because of its proprietary nature.

Figure 3: The PSIM Architecture



Source: Vidsys

Section III:

Making Security Technology Accretive to the Enterprise

Using PSIM to Manage Important Situations and Events

Unifying information across a common platform not only redeems legacy security infrastructure, it translates security data into usable information to respond and manage a situation. Organizations are faced with a host of situations that pose challenges or threats to everyday operations. PSIM platforms help shift the focus from the technology and move it directly to managing the situation. Because the software creates a unified platform, professionals can spend time and energy on managing the needs of the situation, not dealing with patchwork information and problems associated with the technology.

The ability to use security information to manage situations is highly accretive to the productivity and efficiency of the organization. For example, if a car were to jump a barrier at an airport, or if a security breach were to take place, a terminal would have to be shut down. Each minute that a terminal is shut down costs each airline approximately $25,000 ($1.5 million per hour, with the average cycle time ranging from 3 - 4 hours). When managing these situations, every minute counts. If the video data cannot be retrieved and the subject (or subjects) cannot be tracked, and if the responders do not have the proper information to respond the situation can be elongated exponentially.

Airports are not the only example. Enterprises are at risk of deploying resources inefficiently or facing grave liability when deploying resources in a negligent manner. If numerous false alarms are not automatically filtered, the time demands for security professionals can rise exponentially. In turn, more professionals are needed and efficiency is compromised. Also, amidst the inundation of alarms and alerts, one of them may be critical. Without proper analysis, an organization can ignore urgent situations and face liability exposure of large proportions.

One idea that we feel is important to note within the situation management discussion is that video should provide a context for all security data. In other words, it is not enough to say that security information is unified on a common platform. The data must be contextualized. We believe that video is the context that give security data "meaning". The video context provides for appropriate correlations of security information to the situation at hand. For example, if a fire alarm goes off the event may be connected to burnt popcorn in a microwave or a fire generated from a bomb explosion. The fire alarm provides an alert, but very little context. Only when the video is queued, however, can the severity of the situation (and the necessary response) be ascertained. In another example, a suspicious car in the parking lot late at night may not set off an alarm but in tandem with a motion detection alarm near a rear door could trigger a live video of the suspect and recorded video of car's driver to see if they are related.

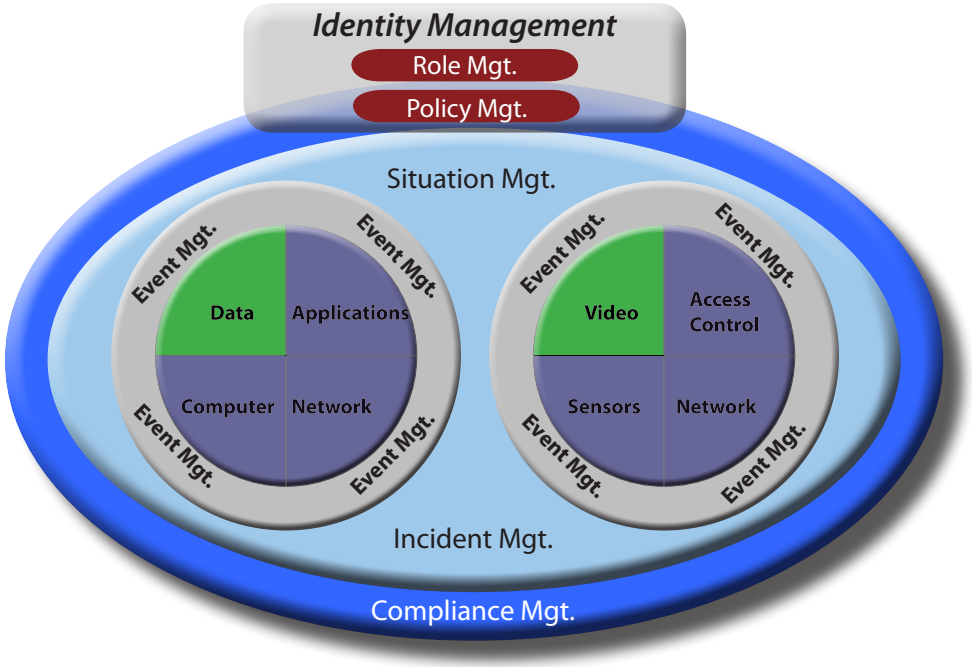
In addition to ascertaining the event, video enables the security professionals to respond in an informed manner. Correlating the event to a place enables professionals to map devices and alarms to determine where activities are happening and to automate displaying the appropriate cameras. The relevant video information is then routed from any video source to any device, independent of hardware and without regard for whether it is live or recorded. A responder or security monitoring professional can properly assess the situation and understand the barriers, the obstacles and the requirements for an appropriate response. For a first responder in the field, this could save their life and the life of others.

Using PSIM for Compliance, Governance and Business Intelligence

The scope of PSIM transcends the security domain. Because of the data extracted from physical security apparatus, the data is effective for compliance, governance and business intelligence purposes. Physical security data intersects with identity and access management software and corresponding directories which provide access and authorization to users. In addition, corresponding roles apply to particular identities. For instance, a person may be associated with certain devices that consistently request network access. In addition, that person may be associated with certain credentials that authorize that person with both physical and logical access. This person may have a particular role within a department. He may access certain areas, but not others. His physical authentication (stand-alone biometrics, smart cards & tokens, and video-enabled biometrics) and his logical authentication (stand-alone biometrics, smart cards & tokens and directory service identity) must confirm each other. From that point, a person's physical identity and physical behavior may be matched with his virtual identity and virtual behavior. With the intersection of physical security data and logical data, enterprises can express (with a high degree of certainty) who accessed what data or department. In addition, enterprises can report what they did and if they acted in correspondence with their role. Finally, enterprises can not only report how that verified person acted with respect to his authority, enterprises can also evaluate with what degree of efficiency and effectiveness the person performed. Because physical security data and logical security roles can corroborate an identity, enterprises can measure the effectiveness of that person within the organization with a high degree of certainty and veracity. For example, in a day where identities are often borrowed or stolen, PSIM solutions can actually correlate access control to data within an IT system with video of the person who was using that Identity. PSIM can actually help authenticate that the person is who the systems says that he/she is and help enforce and evaluate processes and policies within the enterprise.

When physical security and logical security data intersect in situation and policy management, the enterprise is able to leverage volumes of previously unused data to help the organization run in correspondence with its own internal governance and respond quickly to emergencies or catastrophic events. PSIM is therefore useful for both the day-to-day operations and the emergency situation. Quite simply, this is the definition of business ontology - the basic roles and relationships that define the existence of the enterprise and how it functions. Once an organization is able to define, enforce and evaluate these roles and policies, the organization can operate more efficiently, more effectively, more profitably, more ethically and more securely.

Figure 4: Physical and Logical Security Convergence



Section IV:

The Current State of Security Convergence and PSIM

How Convergence is Currently Working

The term "convergence" has been somewhat loosely used and defined. Many define convergence by moving physical security infrastructure over to the IP backbone an act of convergence. In reality, that move is a helpful step for convergence, but not convergence itself. In reality, digital data or data that travels over IP networks can be just as disparate as analog data. The concern is not the state of the data or the protocol upon which the data resides, but rather what the data does. Convergence is about the unity of disparate devices and data working together harmoniously. In other words, getting devices and data on common operating protocols is essential. That is like getting two musicians singing the same song in the same key. But if those musicians are not singing at the same time in the same location, there is still no music being made. Moving data to common operating protocols gets those musicians singing the same song in the same key. Intersecting physical security information with roles and policies and with the data of the enterprise is the act of making music. PSIM, SIM, IAM (and particularly role and policy management) are able to synchronize the devices and the data (even beyond security data) to enable the enterprise to work harmoniously.

Currently, many vendors are making moves to provide converged solutions. In the SBINet project, Intergraph, the premier Computer Aided Dispatch (CAD) and Records Management System (RMS) software provider and Broadware have teamed to provide an integrated video management and incident management solution. The combination, however, is not able to unify video feeds from multiple sources and distribute that video agnostic to the hardware. In addition, the combination is not able to use video to contextualize the multiple alarms and alerts and manage situations with a holistic understanding of the event and the situation. Other access control software providers are taking feeds from multiple sensors, including fire alarms and motion sensors, but video management capabilities are absent. The lack of a true, interoperable platform is hindering many federal projects and enterprise security concerns alike. We feel that a new breed of platform is necessary to provide a solution to these physical and logical security issues.

Finally, a new group of converged security software providers is emerging. Quantum Secure has emerged as a platform play in physical access control interoperability. The company is creating interoperability between multiple access control devices and intersecting physical access control with an enterprises' IAM and ERP suites. Also, several PSIM vendors are attempting to bring to market PSIM solutions, although most today lack some core capabilities to function as a complete application and platform solution. VidSys, by far, has the most mature offering with respect to its open platform, common operating picture for situation management, and video management services. These capabilities enable it to manage situations using contextualized security information from multiple security and video systems in a compelling way. As we argued earlier, we believe that a strong multivendor video management solution is a key component to the overall PSIM solution as it provides the appropriate context for real time situation awareness and management.

Concluding Thoughts

This relatively new category, PSIM, is developing quickly and has demonstrable market traction in several large verticals. Many end users have come to a stalemate position with their security infrastructure. Given the heightened visibility an concerns that surround security, compliance and governance, end users are looking for new solutions. No longer is physical security relegated to the facilities manager. Physical security is a concern for the entire enterprise (starting with the CEO and CFO) and is requiring enterprise-class software to manage terribly fragmented security infrastructure environments. Enterprises cannot afford to replace their legacy infrastructure and yet, they cannot afford to remain in their current, high-overhead situations. Though this category is in its early stages, we believe that the market is pointing to rapid development. We continue to monitor the progress of the emerging converged security software and more particularly, PSIM vendors. We believe they will be crucial to the progress of the overall Physical Security Industry and will make a material impact within the enterprise software domain.

Important Disclosure

The information contained herein represents a summary of public information. Imperial Capital, LLC neither makes any projections with regard to outcome nor makes any recommendation with respect to investment in or transferability of the securities discussed herein. The information contained herein does not necessarily reflect the views of the research department of Imperial Capital, LLC and any research analyst may have contrary views or opinions.

This summary is for information purposes only. Under no circumstances is it to be used or considered as an offer to sell, or a solicitation of an offer to buy any security. While the information contained in this report has been obtained from sources believed to be reliable, we do not represent or guarantee that the summary is accurate or complete, and it should not be relied upon as such. Based on information available to us, prices and opinions expressed in this report reflect judgments as of the date hereof and are subject to change without notice. The securities covered by or mentioned in this report involve substantial risk and should generally be purchased only by investors able to accept such risk. Any opinions expressed assume that this type of investment is suitable for the investor. While this is in circulation, Imperial Capital, LLC or its affiliates may, from time to time, make or quote a market in or make purchases or sales for their own accounts of securities of the issuers described herein. Imperial Capital, LLC or its affiliates may from time to time perform investment banking or other services for, or solicit investment banking or other business from, any company mentioned in this report, and therefore Imperial Capital, LLC may have a conflict of interest that could effect the objectivity of this monitor report.

Imperial Capital

LOS ANGELES

2000 Avenue of the Stars
9th Floor, South Tower
Los Angeles, CA 90067
(310) 246-3700 / (800) 929-2299

NEW YORK

485 Lexington Avenue
28th Floor
New York, NY 10017
(212) 490-0004 / (800) 371-7087

SAN FRANCISCO

55 2nd Street
Suite 1950
San Francisco, CA 94105
(415) 615-7700 / (888) 350-7878