

Will Physical Security Information Management (PSIM) Systems change the Global Security World?

A look at this important emerging security technology to
aid decision making and deployment planning

February 2011

By
Jon Roadnight, Director
CornerStone GRG Ltd
jon@cornerstonegrg.co.uk

This White Paper has been prepared to help Security Professionals understand the Physical Security Information Management arena. It provides the historic context and background of PSIM along with some practical advice on how to make the most of a newly proposed deployment and how to avoid some of the pitfalls, ensuring maximum Return on Investment.

CornerStone © 2011

Will PSIM change the Global Security World

Contents

Introduction3

So what is Physical Security Information Management (PSIM)?.....3

PSIM or not PSIM, that is the question5

History of PSIM.....6

How to guard against disappointment.....7

Conclusion8

About the Author9

About CornerStone.....9

Will PSIM change the Global Security World

Introduction

For anyone that is close to the global security arena, it is unlikely that you would have missed the increasing profile of one subject in particular; Physical Security Information Management or PSIM for short.

Whether its via the industry blogs, on-line forums, social networking sites, Linked-in or just talking to security system manufacturers, the profile of PSIM is increasing at a rate of knots and that generally suggests one thing; a significant industry development is underway.

The purpose of this White Paper is to inform both end-clients and industry professionals what PSIM actually is and how it may impact a security operation. We'll look at the development of this new technology, we'll explain the differences that exist along with the benefits and the pit-falls of the available options.

So what is Physical Security Information Management (PSIM)?

Whilst on the face of it this is a simple question, the answer you receive may depend upon a range of factors including market knowledge and technical understanding. Before agreeing on a universally accepted definition, the security market is currently experiencing a 'jockeying for position' which has involved some, attempting to jump aboard the PSIM band wagon by adding the PSIM tag to their existing product offering. This has been true of some Video Management System (VMS) providers as well as some Access Control System (ACS) Manufacturers. But beware of imitations as these 'lite' or 'part PSIM' products lack some key functionality and threaten to not only disappoint but also undermine the market development of the true PSIM product vendors.

To fully explain the 'true' verses 'lite' or 'part' PSIM tag we must look at the key elements that make up a Physical Security Information Management System. It is our contention that the 'true' PSIM System should incorporate at least the following 5 elements:

Data Gathering: Device level information gathered from a broad range of disparate security systems that incorporate products produced by an array of independent manufacturers for reporting real time status updates.

Data Evaluation: The PSIM software should have the ability to evaluate the information that is gathered and based upon analytical algorithms, identify and prioritise, real incidents or situations.

Will PSIM change the Global Security World

Confirmation: The monitored 'situation' should be presented to a system operator in a clear, concise, yet comprehensive format, enabling an accurate and speedy response to a 'confirmed' security incident.

Resolution: The PSIM system software should facilitate the presentation of logically displayed and clearly communicated actions that the Security Operators should carry out when managing a real time incident or situation. These instructions will have been developed from a range of references including the Standard Operating Procedures, Assignment Instructions, the prevailing policies and standards imposed by national or international regulations and which will adapt dependent upon the present Threat Profile. There should also be a range of tools available to enable the resolution of the situation to be managed effectively.

Reporting: All activity should be monitored and 'recorded', including all Operator actions, to aid compliance management, provide training scenarios and as an auditable record of activity subsequent to a security incident.

Whilst there seems to be a consensus amongst the 'true' PSIM vendors that these elements are necessarily included within their software solutions, others, generally with an existing offering within the Video Management or Access Control arena, appear determined to blur the lines of delineation in an attempt to broaden the market scope of their own products.

Generally, with the continued convergence of security and IT systems, quicker processing, greater network speed & bandwidth and more efficient transmission algorithms, the humble VMS or ACS have developed quickly in recent years. There are some very capable and feature rich examples of these system types that can offer very powerful security solutions. But whilst they serve a very important role in today's Physical Security market place it is important to draw the distinction between these and the PSIM systems.

The use of enterprise level databases has helped elevate 'physical security' to become another 'business service' supported within the same environment as the ERM (Enterprise Resource Management), Accounts and Payroll systems. As the technical platform has developed so has the additional functionality.

The introduction of shared databases (video and alarm monitoring), video analytics, improved graphical user interfaces and logical & physical security integration to name but a few, has improved the VMS/ACS system offering. At the same time there has been a market shift towards more open protocols and interoperability. However, whilst all of these elements could be expected as part of a PSIM solution it doesn't mean that these systems have become 'true' Physical Security Information Management Systems.

Will PSIM change the Global Security World

The area of differentiation and in reality, what separates the PSIM solution from a Video Management or Access Control System is the ability to analyse the data from disparate, interconnected systems and then assess, based upon a range of factors including chronology, location, priority and prevailing threat, the correct response procedure which will conform to not only the regulatory requirements but also the procedural and operational needs of the enterprise.

It's this analysis and intuitive 'decision' making along with the communication of the necessary response actions and the comprehensive auditability that do not exist within a VMS or ACS. Therefore to align a Video Management or Access Control System with PSIM, when these fundamental elements are not present, is disingenuous on the part of the VMS and ACS manufacturers. There is a distinct risk that ill informed or poorly advised clients may be persuaded to commit to a product that doesn't fully meet their aspirations or even worse, having made their investment, find out that the systems limitations preclude the continued system development required in large enterprises resulting in missed opportunity and wasted investment.

PSIM or not PSIM, that is the question

As already defined, there is a range of PSIM 'flavours' available in the market today. It is important to identify the differences, in general terms, between a 'true' or 'Tier 1' PSIM solution and the 'part' PSIM or 'lite' options, sometimes known as 'Tier 2 or 3'. The Tier 1 products have one important determining factor. Within the system architecture, the Tier 1 product sits above all the other systems and devices, receiving constant status updates from the field. It's supervisory, command and control status and its lack of proprietary product options means it can be considered truly product agnostic in the sense that it is reliant upon the integration with independent system and product manufactures for its own existence.

This symbiotic dependency ensures the benefits of 'open' system architecture and interoperability are fully realised as there is no reason that a developer of a particular product will be resistant to share some potentially unique or unusual features of their product. Indeed, the Tier 1 PSIM provider potentially offers the system or product manufacturer a new, untapped route to market, so the restrictions and barriers to further development are removed.

The 'part' or 'lite' Tier 2 & 3 options should therefore come with a health warning. Whilst the solution may be right for some scenarios and certain elements of the overall system functionality might appear similar, there is a risk that clients select one of these options with the expectation of being able to develop and build on their investment in years to come. If the PSIM system is not independent of proprietary products or to put it another way, if the product that is purchased is based on a

Will PSIM change the Global Security World

VMS/ACS System with the ability to integrate other independently manufactured products and systems, it's shelf life may become substantially reduced.

It might become difficult for a product/system manufacturer to share commercially sensitive information, such as the introduction of a unique feature, with a company that also produces competitive products. If the Tier 2 or 3 PSIM vendor also provides a range of their own video cameras for example, the third party provider is going to be reluctant to share their latest Research & Development that has the potential of reducing the competitive advantage that they may have established.

The risk is that subsequent to the original implementation, Tier 2 and 3 systems start to become isolated from the latest market developments and clients lose out on the interoperability benefits that they believed they could achieve. This ultimately leads to disappointment, wasted investment and recriminations, which could have been avoided.

One other key differentiator is the reduction or loss of data analysis. Without this powerful and important feature the onus is returned to the operator to make the key decisions and decide upon the correct course of action in every scenario. The speed and improvement in decision-making and the subsequent ability to accurately audit a past incident was one of the driving factors for the development of PSIM solutions in the first place. It therefore seems perverse in many ways to not have this addressed if you have decided that Physical Security Information Management is an important tool in your security armoury.

Finally, there is the issue of resilience and redundancy in the system design as a key area for business continuity and recovery/crisis management. Most non PSIM, Video and Access Control systems don't scale across a global enterprise to provide true resilience and in most cases don't even feature as part of business continuity and recovery plans. PSIM solutions provide extensive enterprise capabilities to ensure continuous operational 'up' time.

History of PSIM

Isn't PSIM simply a new name for an Integrated Security System? This is a question regularly posed and easily answered although we believe indicative of the current market perception and misunderstanding surrounding PSIM. We have already defined what differentiates a PSIM System from a Video Management, Access Control or indeed other Integrated System. To fully appreciate why PSIM has become such an important development it is helpful to look at it's short history.

Subsequent to the terrorist attack on the World Trade Centre in New York on the 11th September 2001, it became apparent that emergency response systems needed

Will PSIM change the Global Security World

to change. No longer could it be acceptable that critical information from numerous sources was left to system operators to interpret and act upon consistently and correctly. In the analysis that took place in the months and years following the attack, a belief emerged that Security System Management and the emergency response could be improved.

By approximately 2005 the PSIM acronym was born and the development of the early solutions was well underway. The emphasis was no longer simply on gathering and presenting device status information for the human resource to assimilate and act upon. By using a range of relatively new software based concepts that were being applied to other industries, the notion of 'analysis' and 'automated decision making' in conjunction with the association with an agreed set of actions/procedures to be undertaken dependant upon pre-conceived priorities and threat level, users could experience a significantly faster and improved continuity of response.

As PSIM solutions have developed, with the backdrop of interoperability and the willingness of system manufacturers to develop 'open' system architecture, the proliferation of the range of interconnected systems has continued. Whilst adding complexity, the additional reference information available at the initiation of an incident helps refine and improve the accuracy of the prescribed emergency response and adds other value-added functionality.

This can include identity management, credential management, logical/physical integration and facilities management in addition to improved analytics. It's these types of features and services that will deliver improved Return on Investment opportunities and help Heads of Security develop not only their broader Security measures but also the integration of Security with other mainstream Business Services. This climb up the corporate influence ladder can only improve the chances of being able to deliver more comprehensive and better aligned security solutions and help guard against a diminishing physical security influence as departments become homogenised with the likes of the IT or Facilities functions.

How to guard against disappointment

Whilst the objective of a PSIM System is to simplify and enhance the way 'situations' are managed, PSIM is not a simple solution to implement. Before a system can be deployed it is essential that the business operational requirement is fully understood. The business consultation process undertaken with all identified stakeholders will provide the platform for a successful PSIM implementation. A poorly defined operational requirement will nearly always result in badly conceived system integration and the incorporation of inaccurate emergency procedures.

Will PSIM change the Global Security World

That's not to say that a well delivered, comprehensively undertaken consultation process will guarantee a completely successful PSIM implementation. Deployment is complex and requires a well developed and executed Project Management process. Low level, Cause and Effect and Rules and Permission matrices should be produced and agreed to permit accurate system programming. Once deployed, extensive scenario testing should be utilised to fine tune and complete the PSIM system and it is important that this is carried out by an Independent, subject matter expert as opposed to the software vender. This ensures the requisite checks and measures are applied and each and every cause and effect is checked and verified.

Conclusion

Will Physical Security Information Management change the Global Security World? Well, to some extent it already has. New levels of system integration and the facilitation of a faster emergency response is a benchmark that is only going to become more demanding.

As products and expertise develop and the Return on Investment models are refined, more and more organisations will consider PSIM and the potential benefits that can be attained. It is essential throughout this development phase that clients are properly informed and advised, as there is a risk that poorly deployed PSIM Systems will hamper the potential PSIM market growth.

Clear and concise subject definitions are required to prevent client confusion and remove the potential for manufacturers to blur the lines between true PSIM solutions and other types of integrated system.

Of most significance is the methodology utilised to establish if PSIM is the solution to a clients operational requirement. This in-depth consultation process must be designed to focus upon the key system deliverables. It should be carefully managed, and constantly monitored and result in a comprehensive Cause and Effect matrix that defines the precise software structure required. Within the coming 3 to 5 years it is inevitable that the penetration of the multi-national organisation market will have had a 'spill over' effect into other medium and large enterprises. This will substantially increase the total market size but during the same period cost models will have developed and market prices will have reduced.

The combination of a range of factors including client demand, IT convergence, improved technology and external industry involvement have all conspired to ensure that Physical Security Information Management System will flourish within the coming years and probably be considered as a 'mainstream' solution within the next 3.

Will PSIM change the Global Security World

About the Author

Jon Roadnight has been in the Security Industry for over 20 years. His broad experience encompasses Manufacturing, Installation and Consultancy Services and for the last 11 years he has sat on the Board of some of the UK's most successful Security Companies.

Since 2007 he has been an Executive Director of CornerStone GRG, a leading Independent Security Consultancy firm with Headquarters in London, UK. He has extensive International experience having been involved in projects throughout Europe, Africa and Asia. He has actively helped shape Security Industry opinion and recently took part in a live television debate about Video Analytics on the BBC's "The Politics Show". He is a member of the Security Institute's Academic Board and is also a Fellow of the Institute of Leadership and Management.

For further information contact: jon@cornerstonegrg.co.uk

About CornerStone

CornerStone provides a range of Consultancy Services aimed at assisting organisations and individuals deliver their corporate security and risk management objectives.

In recent years they have developed a range of tools to aid the complex consultation and Project Management phases of a PSIM implementation project. This experience has been built whilst delivering a range of PSIM project solutions. Their unequalled knowledge and experience has added tangible value to client relationships and has made them one of the worlds leading Consultancy Practices in this emerging technology.

The quality of the service that CornerStone provides has been recognised by the broader security industry as they have been named finalists in the Security Excellence Awards 'Best Security Consultancy' category in 2008, 2009 and 2010 as well as the 'International Achievement' category 2009.

For more information please visit them at www.cornerstonegrg.co.uk

Integrated Security Solutions inc. Physical Security Information Management Solutions (PSIM) Perimeter Protection, CCTV, Access Control, Visitor Management, Counter Terrorism, Hostile Vehicle Mitigation, Crowded Places Strategy, Security Strategy, Security Policies and Procedures, Vulnerability, Threat & Risk Assessments, Audits, Consulting, Specifications, Project Management, Training.