

Integrated Situation Management – More than Just Physical Security Information Management

A new sector is emerging within the security industry. A number of products have been released into the market in the last few years which are designed to integrate all security systems devices, applications and systems, providing a more holistic approach to security. This creates a challenge for organisations, as it is confusing for them to identify a product which will give them the features they need to enhance their security and provide compliance to evolving security policies, whilst actually giving them a tangible return on what is often quite a large investment.

As with any emerging market, a host of new terms and acronyms have been created making it difficult to define exactly what an individual product does and more importantly doesn't do. Some of these terms are;

- *PSIM – Physical Security Information Management*
- *CMS – Central Management Software*
- *ISMS – Information Security Management Software*
- *Situation Management*
- *Enterprise Command and Control software*

One thing for sure is the security integration software market is growing. According to IMS Research, the CMS market is set to grow to \$728 million by 2011. This is a fairly conservative number compared to other analysts, such as Frost and Sullivan who see the global market place for Enterprise Command and Control software reaching \$2bn within the same time frame. Again a perfect example of different terminology covering the same space; either way the rate of growth is set to be rapid.

The Security Integration Landscape

These systems fall into two categories. Firstly, proprietary systems which lean towards technology from their manufacturer and require costly wholesale rip and replace implementations, whilst limiting the

choice of compatible products for any future upgrades. The reason for this is simple; manufacturers of security devices are not likely to provide sensitive information in the form SDKs and APIs to competitors.

The second category is created by middleware developers and tends to be more open with compatibility with a larger number of other manufacturers. These products offer more opportunities for expansion and can reduce implementation cost through greater use of existing equipment. These systems manage all of the information produced by the various security applications to help security operations to better understand what is taking place in the security environment.

Whilst in principle the idea has its merits, namely centralising information from disparate systems into one application, in practice its usefulness is fairly limited. This is mainly due to its focus on the security information rather than adding value through better situation management.

Business Value

Most enterprise security departments have reduced the number of security guards over the years, replacing them with better technology, such as CCTV, access control and communications systems. This has happened to a point where many are running at a minimum number of guards, so don't have much room to make savings here. There is a flip side to running a tight ship.

What organisations often fail to see is what could happen if an inexperienced guard, who probably is a contractor, is left to their own devices. Understanding all of the alarms, alerts, video and other communications which are created in a modern control room can be overwhelming. With the limited amount of time which circumstances often only permit, following a blow out for example, training on all of the possible scenarios is just not possible.

So suddenly rock solid security has a huge whole in it.

If they have considered this, organisations often try to overcome it by stipulating a minimal amount of guard training in their contracts with outsourced security providers. How many of these providers actually deliver to these contracts? Examples of security breaches and their consequences are well documented, and ultimately they taint the reputation of the organisation rather than that of the security guard provider.

So in short, these open platform products do add value, but is it enough to warrant the initial expense? The main stream is still not convinced; this is demonstrated by the slower uptake than initially expected. There generally seems to be an "it won't happen to me" attitude in corporate organisations when it comes to spending on security. They can not be blamed, up to now what other benefits could the security operation fulfil?

Integrated Situation Management

There is third category of products that are available today, which offer broader benefits than just enhancing security.



Adlan Hussain is the Marketing Communications Executive with Computer Network Limited. He has over a decade of technical experience Adlan has first hand knowledge of what is needed to provide enterprise wide security in this technology driven age.

Integrated Situation Management offers greater business value by providing greater communications possibilities with other business systems coupled with workflow engines which guide operators at each stage. The below life cycle shows where industry analysts see the future of security systems.

Life Cycle of Security Integration

Rather than trying to reduce the number of guards, and using integration as an ROI piece, these systems go the other way and increase the functionality of security departments. They connect with building management systems, marketing systems, IT Systems and other business systems; creating new possibilities, which help bring security back into the core of an organisation.

Organisation Benefits

The practical benefits are virtually unlimited, from reducing energy consumption to physically verifying identity to IT infrastructure. Other than these operational benefits, they can help reduce costs through bringing in services which have traditionally been outsourced at great expense to organisations, such as alarm monitoring of equipment, replenishing of office/vending machinery and remote camera monitoring of satellite offices. Some of these benefits are detailed below;

Improved Security

Compliance - Transferring security policies to a software-controlled workflow ensures optimized decision-making and policy compliance. In addition, consistent and dependable evidence of compliance is auditable and automated – protecting organizations from threats, risks, and litigation. Additionally security data accumulated in these systems can be used to predict future trends and allow organisations to plan.

Auditable and Automated – These systems allow organizations to enforce security policies and standard operating procedures, even in crisis

situations. They allow more control by utilising on-screen operator guidance to ensure execution and record all procedures automatically. All data and information on device or operator activities is stored in a central database. Following an event or incident, evidence can be collated whilst maintaining the integrity of the original source material.

Future-proof – As previously mentioned, security applications and systems aid organisations to maintain the high levels of security required today, so integration of new technology is essential. These systems remove vendor dependency, allowing greater choice and lower cost of upgrades. This way, enterprises get to choose from the best technology available and deploy it in a controlled and effective manner.

Improved Efficiencies and Cost Reductions

Single Sign On (SSO) – Taking the SSO principal to the next level by incorporating physical security. Aided by the integration of biometric technology, SSO can now help fortify both physical and logical security to a level not previously possible. A single biometric scan is enough to reliably verify an individual’s identity, who could then be given permissions based access to the network. So, no need for multiple easily forgettable passwords and therefore less time wasted by IT Support as a result.

Reduced Carbon Foot-Print – The energy savings of combining physical environment data with BMS can ensure facilities are run as frugal as possible. Which not only reduces the carbon foot print, but reduces energy costs as well.

Alarm Monitoring - Organisations have for years relied on outside contractors to provide out of hours alarm monitoring of equipment on sites. These organisations have a range of key holders to contact on a prioritised list; at the time of need these list are often found to be out of date. This leaves these companies to contact the head office’s security function to get up to date information.

If the security team could see all alarms from the control room, they would quickly be able to contact the relevant key holders, saving time and money.

Remote Monitoring of Satellite Offices -Traditionally the large number of cameras which multiple satellite offices require has made it prohibitive to bring in house, due to small security teams. Integrating the latest generation of video analytics ensures guards only see video when something happens. This dramatically reduces the number of operatives required to perform this function. Interactive maps and plans give detailed local site information, allowing faster responses. This could also be used to convert single guard sites in to remotely monitored sites, again providing significant tangible benefits.

Operator Guidance

You would be forgiven for thinking all of this sounds a little too easy. How can guards be expected to manage all of this technology? This is the real advantage of this technology. Workflows can be carefully planned and easily implemented, so if a certain alarm is triggered the on screen guidance can instruct a guard where and how to carry out a physical check. If it is a real activation, it can provide contact numbers for the right service provider, and automatically escalate incident via SMS, email or pager to the right level internally.

In summary, today’s security needs, require organisations to adopt technology to aid relatively small security teams with the sophisticated threats they are open to. In doing so, they risk overloading, what can undeniably be described as low paid security staff, with too much information from too many isolated systems. They have a great opportunity to convert this challenge into a real business advantage by adopting an Integrated Situation Management solution, which is much more than just physical security information management.