

Smarter Response to Threats

What makes a physical security information management platform good or bad? Reliability and cost-effectiveness are key issues, as well as an intuitive user interface suited for different operators.

BY LING-MEI WONG

Physical security information management (PSIM) expressly exists for situational awareness. A good platform has the potential to prevent situations from getting worse. In the event of a fire or other life-threatening scenarios, an integrated response may save countless lives.

However, a PSIM solution with a complicated user interface can create problems for operators to navigate and respond quickly, said Alf Chang, Senior Consultant for *A&S* magazines.

Good PSIM should unite systems into a holistic platform. "PSIM needs to have the ability to seamlessly fetch all data and then translate that in a single, analytical presentation and archival form," said Bhaskar Ganguly, Global Marketing Director for Critical Infrastructure Protection, Automation and Control Solutions, Honeywell International

PSIM systems must account for human psychology, especially in crises. "During an incident, it's imperative that the operators get all of the information they need in a way that is easily understood, without being overwhelmed with noncritical data," Ganguly said.

Any platform for convergence should be simple to operate. "A system that requires less interaction with the operator is normally the best solution," said Ken Pereira, CEO of OneBerry Technologies. "Automation is the main ingredient that makes or breaks a solid PSIM solution."

Ease of use is achieved through intuitive features and extensive automated processes. "Workflows for operators on one GUI

◀ PSIM solutions should account for future growth and be scalable.

are essential, combined with the flexibility of portable communication integration," said Stephen Moody, Security Development Manager, ViS Security Solutions. "This allows for incident control and the efficient deployment of operatives on the ground."

A good solution should meet user needs and apply the most simple and efficient architecture, said Daniel Kok, Business Development Manager for ADC Technologies International. Conversely, a bad solution would include too many components from multiple vendors, which system integrators have no control over.

SYSTEM STABILITY

A good PSIM platform should keep running, even if one of its subsystems goes down. "There have been a number of instances when a certain module or component did not meet the requirements of the project during actual usage," Pereira said. "And when this particular module failed, the whole system was affected. It is advised that clients should go with a complete system that has been extensively tested. The key to a reliable system is decentralization."

A modular approach can prevent installations from coming to a grinding halt, such as offline operation of building and security systems at certain times, Chang said.

Good networking practices can keep systems from crashing. "While system availability can never be 100-percent guaranteed, the risk of failure can be significantly reduced by incorporating standard IT redundancy and failover architectures," said Brandon Arcement, Manager of Global Security Technology, Building Efficiency, Johnson Controls.

Along with network redundancy, users can use secondary verification techniques. "For example, an alarm can be validated through secondary sensing like video or access details," Ganguly said. "In cases when a particular subsystem fails, there is always another sensing point available to the user."

CUSTOMIZED SOLUTIONS

PSIM offers powerful functions, which are not required by every user. Providers need to design customizable but flexible solutions that are tailored to users or applications. A network infrastructure capable of supporting communications across a wide range of verticals would be optimum, said John Moss, CEO of S2 Security.

Computer Network Limited (CNL) uses template modules for specific vertical markets, enabling flexibility and reduced cost. "The advantage of this is the end user only pays for what they want," said Matthew Kushner, President of the Americas for CNL. "If they need additional functionality in the future, they just need to add modules."

Modules or business logic

templates save administrators time. "These templates repurpose common actions and responses, and are also fully customizable," said Larry Lien, VP of Product Management, Proximex. "Administrators and integrators can reuse these standard templates or create their own as necessary."

As there are currently no PSIM standards, some providers make connectors for specific interfaces so systems can communicate. "As we build these connectors, they become part of a library of capability that is part of the commercial-off-the-shelf products," said Bob Scott, Executive Director of Security Solutions Strategy for Intergraph.

Customers often bring their experience with hardware-based systems, which are notorious for underachieving. "With these software-based systems, we encourage people not to overspecify the system since this can result in unnecessary costs," said Kevin Daly, CEO of Maxxess Systems. "Once they understand how the system works, they can change it with little or no penalty. With software, you're better off undershooting requirements, getting used to the system and then getting additional functionality."

Site-specific solutions are best addressed with flexible programming options, said Anand Mecheri, CMO of Siemens Building Technologies. "A rule engine is essential, to avoid proprietary customizations that become very hard to support over the life cycle of the solution."

A set of rules and workflows can be programmed for one customer and sold to another user with similar needs. However, the client can claim exclusive rights to the solution, said Holger Maier, Product Manager for Building Integration System, Bosch Security Systems.

MULTIPLE STAKEHOLDERS

PSIM platforms will be used by administrators and guards, who have unique needs. Authorization levels will also differ for sites with several stakeholders, such as airports with customs officials and law enforcement.

One system may be deployed, but use different GUIs. "You have to enable many protocol transfers in the system," Chang said.

Administration and access rights are normally based on a hierarchical system, depending on the user's job function and needs, Ganguly said. A good system allows management



Ken Pereira, CEO of OneBerry Technologies



John Moss, CEO of S2 Security



Bob Scott, Executive Director of Security Solutions Strategy for Intergraph

to assign authorization to individual users. "The system must be dynamic to the extent of being able to customize access rights for each operator, specifying what can be viewed and controlled, depending on the level of security privileges," Pereira said. "This feature will allow management to determine the scope of responsibility and monitor the performance of each operator."

BETWEEN OLD AND NEW

As PSIM must suit each project's needs, it requires careful planning and implementation. Most PSIM deployments are at new sites, as it is easier to put PSIM into a new site with nothing there, compared to a building with legacy systems. "If the owner wanted to substitute the original system with our system, this is in general more time-consuming," Maier said.

Newer sites can select best-of-breed products, making PSIM easier to integrate, Moss said. However, the cost of switching out subsystems may be prohibitive. The existing cable infrastructure, such as analog video lines, can limit upgrades as well.

Greenfield projects can include security in the planning phase. "All aspects concerning data management and integration among different devices must be discussed in detail to ensure that the security requirements are met," Pereira said. "Locations of the different security devices like cameras and access controls must be part of the structural and electrical plans of new buildings."

However, increasingly older buildings go through refurbishment for integration, Kok said. Arcement agreed, saying, "In fact, PSIM is often most valuable in facilities and

organizations where an owner wants to leverage existing investment in disparate building and security technologies while still enhancing security operations through system integration."

Regardless of whether the project is old or new, users will deal with stand-alone systems. "In today's world, it's all about sharing better information among systems and providing security operators and related stakeholders with an improved means of collaboration," Lien said. "PSIM solutions bridge the gap between different technologies, improve processes, enhance security and save costs."

PRICE CONSIDERATIONS

The powerful performance of PSIM requires an initial investment, on top of existing equipment and subsystems. Most providers sell in modular packages, depending on the number of systems, features and licenses. Maintenance is usually charged separately.

Bosch sells by license, with several options. "The more doors, detectors, cardholders and cameras, the more the end customer pays," Maier said. "With additional or customized features, you pay an additional price for it. And for the years after the warranty period, customized service maintenance agreements and service level agreements can be purchased to keep the system up and running for years."

Pricing factors involved include systems, devices and how many manufacturers there are to

support. Some installations could have three different ACS vendors, requiring additional integration. "This is largely dependent on the type of customer, as PSIM deployments vary a great deal, so different pricing structures are in place to suit different verticals," Kushner said.

Going with one PSIM vendor can be cost-effective. "Normally, if the system requires more components to be integrated and the purchase is made under one contract, the cost savings may range from 10 to 30 percent, depending on the size of the project," Pereira said.

Recurring support needs to be budgeted for. "We do have software support, with access to the help desk, updates and training, at an annual fee of 10 to 15 percent of software cost," Daly said.

Intergraph combines licenses, maintenance and training in its pricing. "Our software is sold via a perpetual license fee — one time charge for licensed software, which is typically server-side and client-side software modules — with annual maintenance along with implementation services to configure, integrate, train and commission the system," Scott said.

Users can decide what payment plans fit their needs. "Life cycle cost



Kevin Daly, CEO of Maxxess Systems



Anand Mecheri, CMO of Siemens Building Technologies



▲ Airports have multiple stakeholders, who require different authorization levels and customized GUIs for PSIM access.

is always an important consideration when evaluating the purchase of a technology," Arcement said. "As such, it's important that end users communicate which payment schemes and licensing structures work best for their organizations during the design process."

TRAINING OPERATORS

PSIM is not plug-and-play and requires training to become familiar with its features. Training for operators can take two days up to two weeks, depending on the platform's complexity.

The system's complexity depends on the site's scale. "To get operators familiarized with the operational aspect of the entire system would depend on an individual's approach," Kok said. "On the whole, we believe it will offer significant operational cost savings to the organization."

While PSIM offers increased functionality, it should be straightforward to operate. "The interface and workflow of the platform should provide an intuitive user experience

when designed and commissioned properly," Arcement said. "It helps to have operators who are comfortable with a mouse and keyboard, but they certainly don't have to be programmers to be effective in the control room."

EVALUATION CRITERIA

PSIM providers usually look for experienced partners and integrators that are familiar with both electronic security and networking. "It is key to have long-term, stable partners when it comes to deployment of high-level, integrated solutions such as PSIM," Mecheri said.

CNL's criteria include how long the company has been in business, average deal size and how many employees have relevant certifications, such as Microsoft and Cisco, Kushner said.

Maxxess offers training to partners but does not request third-party certifications from them. However, it can be helpful in some situations. "Networking issues are very significant, both in how they affect the performance of our system and how

it integrates with other systems," Daly said.

The integrator should also have a close relationship with the owner and understand the organization's business operations and security processes, Arcement said.

Along with networking skills, installers or integrators should have experience with the connected subsystems. "Many years ago, it was getting wires in a wall, then getting wires to the controller and some keystrokes. Today, this is the easiest part," Maier said. "The challenging part is to design the optimal system and subsequently to program the functionality according to the customer's organization and requirements."

System integrators should also evaluate PSIM providers. Irish integrator ViS Security Solutions partnered with Proximex after analyzing its system architecture, flexibility, cost and unique approach. "Proximex has taken significant steps in the U.K. and European region, which provides commitment and quality reassurance," Moody said.

"We have also found the Proximex team to be proactive and contribute significantly to client requirements and system designs."

LEGACY CHALLENGES

PSIM is undergoing growing pains, ranging from bringing systems together, keeping data manageable and planning for tomorrow. These challenges require time and effort.

Hybrid systems are a hallmark of PSIM for sites with existing equipment. "In an upgrade project, challenges tend to focus around the compatibility of integrating new technology with legacy systems," Ganguly said.

Older systems can be thorny. "An end user asked CNL to integrate a system which does not have open SDKs or APIs. The manufacturer had developed its product in complete isolation of IT standards, to the point of anti-Microsoft," Kushner said. "We managed to work around it, but it's the lack of standards that is the biggest challenge we are dealing with."

A dearth of standards means interoperability is still a long way off.

"The challenges relate to evolving standards, evolving concepts of operations that support the use of integrated technology like PSIM, and the fact this is still an early market, so we are dealing with innovators and early adopters," Scott said.

HUMAN TOUCH

A PSIM platform may have countless slick functions, but still must be accessible to humans. Having the highest specifications will do no good if the interface is too overwhelming for practical use. "The challenge for Bosch is to bring a solution that connects to any subsystem and that can be customized to any user's needs, but can still be handled by our certified VARs and integrators," Maier said.

As projects get bigger, the scope of PSIM becomes more complex. "The big challenge going forward is efficient use of people," Daly said. "Organizations now are more distributed. It's not just one building or campus, but 40 to 50 sites being centrally managed, often with at least some information sent back to a central point. What you do locally

and centrally can be a critical design consideration for these systems."

It is important for machines to do what they do best — crunch data from multiple sources — while human operators decide on the most appropriate response. This frees up operators from tedious tasks and helps them work smarter.

FUTURE-PROOFING

Growth can be difficult to plan for in large projects. "A technical challenge facing PSIM vendors is enterprise scalability," Kushner said. "Some systems have been designed without enterprise-level scalability in mind, and trying to add this capability is proving very difficult for some companies in the marketplace."

The future is murky at best, throwing off the best-laid plans. "In a greenfield system, the challenge is to accurately predict and define customer requirements at an earlier stage," Ganguly said.

A more abstract problem is proving futuristic PSIM systems are real solutions already in use. "Unfortunately, integration is something which has been put in front of end users many times before, and their expectations have been high, only to find very limited integrations," Kushner said. "Thankfully, PSIM is changing this, and more end users understand that they can build systems that give them exactly what they want."

Regardless of how the future pans out, integration will be the wave of the future. PSIM harnesses existing technology and networking capabilities, enabling better use of data in a timely fashion. With increased automation of tasks, security operators can see more and respond faster to threats.



▲ Good PSIM should factor in human psychology, especially during critical situations.