PROXIMEX CORPORATION—WHITE PAPER

Experience the ROI Rewards of Risk Management with PSIM

By Jack Smith

Experience the ROI Rewards of Risk Management with PSIM

Most organizations today agree that an increase in situational awareness is necessary, whether it's for internal or external protection. But due to consolidated operations, M&A activities and expansion of security infrastructures to include new technologies, many security directors experience frustration when trying to create a unified security environment. In an ideal world, "rip and replace" would provide new systems and the latest technologies for a completely new security environment, however, for most organizations, budget constraints and practicality eliminate this option. Other challenges include how to integrate disparate systems, perform real-time analysis of events and report incidents in a timely fashion to upper management.

Enter the world of Physical Security Information Management (PSIM), the ability to integrate multiple disparate physical security systems, then connect and correlate relevant information from these systems into one centralized environment. Since its inception several years ago, PSIM has proven to be a viable solution for organizations of all sizes that need to better manage and/or reduce risk. These organizations want to ensure regulatory compliance, enforce policies and procedures, provide a holistic concept of operations and manage security with a more scalable and flexible infrastructure. The PSIM trend is catching on. In a recent report, IMS Research noted that PSIM software vendors have begun to gain market traction with the entire PSIM software market forecasted to grow to more than $1B by 2014. In addition, system integrators have started to build special practices around integrated solutions and convergence and specifiers are seeing an increase in PSIM queries from customers. Finally, organizations with installed PSIM solutions are now found on every continent in nearly every market segment.

Organizations find that PSIM is necessary for a number of reasons. First, PSIM gives better visibility into security information through a centralized environment instead of viewing multiple consoles or using several individual command center locations. It provides deeper insight into security activity as it correlates information from multiple disparate systems, thus giving personnel better information from the beginning to improve their incident responses. PSIM facilitates the process to deliver consistent operations procedures to guide all levels of security management. Lastly, PSIM reduces training costs as personnel are trained on one system instead of every type of security system installed. All of these benefits help reduce security and business risk.

Now that early adopters are well down the PSIM pathway, the time is right for more organizations to explore PSIM solutions to help achieve company business objectives. However, as with any new venture, organizations must learn to calculate a realistic PSIM return on investment (ROI) to justify the expenditure. So how do organizations decide if PSIM is a financially viable business decision?

According to IMS Research, there are seven criteria that must be met in order for a solution to be considered a true PSIM solution [see sidebar "Seven Criteria for a PSIM Solution"]. These "must haves" should also deliver a realistic ROI back to the organization in short order. In essence, a true PSIM solution is always a value-add to the company by continuing to reduce cost and risk over time.

In order to calculate a realistic ROI for PSIM, security directors must first determine the project paybacks and how they are to be achieved. Project paybacks can take both quantitative and qualitative forms. Quantitative paybacks include obvious cost savings realized from avoiding a "rip & replace" scenario and reducing costs associated with manual intensive processes, such as reporting, manned guards, training, etc. Qualitative paybacks are less obvious but still critically important. For example, having a unified security environment may allow key personnel to focus on value-add functions instead of basic operational duties. This change will elevate the role security plays within the organization. Some paybacks deliver both qualitative and quantitative benefits, such as migrating separate control rooms into one centralized command and control location. One properly configured command and control center will significantly reduce the redundancy of systems, extend the life of legacy systems and make it possible for individual systems to function better together. Determining quantitative and qualitative paybacks is a critical piece to experiencing ROI rewards from a PSIM installation.

Seven Criteria for a PSIM Solution

According to an IMS Research study from November 2010, a PSIM solution must have:

- Connectivity and integration of multiple disparate security systems and capable of integrating other business systems within a corporate IT-infrastructure;
- Real-time policy/configuration management of connected devices;
- Correlation and verification of events;
- Visualization of actual situation independent of active events;
- A rules-based workflow for response;
- Availability/resilience to support continuity of business and disaster recovery;
- Post-event reporting and analysis.

Other factors will determine a PSIM solution's ability to deliver a faster ROI. These factors are often related to total cost of ownership of the solution. PSIM vendors must understand the intricate details between infrastructure and enterprise applications to help speed installation with new and existing subsystems. A PSIM solution needs to be flexible, scalable and highly available to handle high volumes of sensors and sensor information. There should be two-way or bi-directional communication with subsystems to collect information as well as control the subsystems through the PSIM interface. It must be easy to configure, quick to deploy and simple to maintain on an ongoing basis. Finally, but not the least important, a PSIM solution should provide extensive reporting capabilities to allow personnel to update upper management quickly and thoroughly about any security incidents.

The ideal PSIM solution is built on an open architecture to support new and legacy security systems of all types, makes and models. An open architecture gives organizations complete flexibility to choose equipment and technology that is best suited for their environments. No equipment refit is required in order to integrate new systems or technologies into the command center. This also means that existing systems may stay in place until budget and monies allow for the purchase of new ones.

Managing the health of subsystems is a major challenge, especially for organizations with multiple locations and/or compliance regulations that need to be met. A true PSIM solution can provide automatic alerts of disconnected or faulty equipment, such as an open door or a broken DVR, before an incident occurs. Automatic management of operations and equipment can be a huge cost savings to an organization in terms of time spent policing areas, reporting downed equipment or embarrassing publicity.

For organizations with a large staff, lots of visitor traffic and/or other assets to protect, a centralized environment can be a major cost savings with respect to personnel. With one command and control center, organizations can reduce manned guarding and onsite security personnel as well as automate barrier control. This centralized environment helps make each resource more efficient and dramatically increases the effectiveness of the company's security team.

Finally, security directors need to determine the associated costs for purchasing each hardware system and software solution as well as costs for installing, configuring and maintaining each system or solution over time. These individual costs should be requested and estimated by the system integrator, then compared with the installation, configuration and maintenance costs for a PSIM solution.

Only one PSIM solution on the market today meets the seven criteria for a PSIM solution in every respect as well as delivers impressive ROI rewards within a calculated 12 to 18 months after deployment. Proximex™ Surveillint™ was designed to be a flexible, scalable and highly available enterprise-class solution that connects and correlates information collected from both new and legacy systems and supports expansion when necessary. Proximex offers Integration Modules that enable systems to be quickly and easily integrated with "out-of-the-box" systems but without requiring any coding, thus further reducing the costs associated with system integration. Proximex can integrate core security technologies (e.g., physical access control, video and intrusion detection), advanced security systems (e.g., video analytics, radar and sonar) and communication systems (e.g., two-way radio, mass notification, intercom and digital signage) as well as IT systems (e.g., network alarms, logical identity, LDAP Active Directory) to provide bi-directional communication with Surveillent. Surveillint delivers ease of configuration and ongoing maintenance and its reporting features reduce the ongoing maintenance and operational costs related with integration projects.

Surveillint has an open architecture which allows for smooth integration with more than 90 security systems, including video surveillance, access control, intrusion, fire and life safety, perimeter protection, mass notification and building management/automation. This same architecture allows integration of future system purchases, which means that subsystems may be added to the Surveillint platform as need and budget allow. In addition, Surveillint can monitor the health of all integrated security systems, including IT, to alert personnel if systems are down or compromised. The ability to integrate new and existing security systems into one command and control center that also handles system monitoring has saved Proximex customers millions of dollars over traditional integration or rip and replace activities.

Surveillint is the most direct path to consolidated operations; putting security control back into the hands of the organization and removing the reliance on 3rd party suppliers to help meet security initiatives. Surveillint encourages and allows organizations to develop and maintain their own policies and procedures, another significant cost savings. One large U.S. corporation saves $800K annually by using Surveillint in its command center, thus reducing the number of required manned guards and streamlining operational costs.

Surveillint reduces costs associated with false alarms. Its sophisticated Business Logic Manager allows alarms to be correlated across multiple disparate systems to determine if incidents should be elevated. Surveillint eliminates the need for multiple monitors and personnel designated to watch individual systems. Business Logic Manager lets security personnel focus on execution of planned responses instead of spending time assessing and reassessing situations.

A Tale of Two PSIM Installations

Once an organization has decided to go with a true PSIM solution, it's critical that the right players be involved from the beginning in order assist a smooth implementation as well as save project time and cost. First, project organizers should evaluate the current system inventory, then conduct a census of wants versus needs with input from key stakeholders. The system integrator can be a valuable part of this process to guide organizations to the right systems for their needs and design a growth path. Only after these steps are taken and prior to any subsystem installation, should the PSIM solution be installed to ease integration of security systems and streamline training issues.

One large transportation provider installed a complete PSIM solution and underlying security systems to secure its maintenance yards from theft. Instead of installing the PSIM solution first, the company chose to install each individual physical security system before the PSIM solution. Security personnel were trained on each system as it was installed. By the conclusion of the project installation, the staff became frustrated when they learned that all the individual system training was irrelevant as the PSIM solution user interface handled all of the required information.

Alternatively, a large seaport installed Surveillint first and its subsystems second. This process eliminated much deliberation about which subsystems to select and in what order they would be installed. To Surveillint, all devices are treated as equals which means that any camera system (i.e. analog, IP or specific manufacturer) can be installed before or after other chosen subsystems. Individual camera devices can then be added to Surveillint as necessary at any time during the installation process.

For these reasons, PSIM solutions can significantly reduce planning, integration and training time.

Surveillint offers unique management reporting to help organizations ensure that key incidents are properly reported to upper management. It offers full reports that can describe on a hourly, daily, weekly and monthly

basis all alarms and incidents from different parts of the organization as well as the alarm types that generate the most alerts or false alarms. Surveillint can also track which sensor or device needs servicing to let companies better manage suppliers from a service level management perspective.

As early adopters have proven, PSIM is a real solution with real benefits for organizations of all sizes. Many companies are already reaping a true ROI from Surveillint's open architecture, comprehensive capabilities including Business Logic Manager, system health monitoring, quick deployment and robust reporting. If your company is investigating PSIM, perhaps it's time for you, too, to start enjoying the ROI rewards of risk management.

—Jack Smith is the president of Proximex and has led the company since 2006.

About Proximex

Proximex has developed innovative PSIM solutions that ensure incidents are no longer trapped within disparate systems, but brought together in context and integrated into the customers' security policies and operations for analysis and resolution. Proximex's mission is to deliver powerful, comprehensive and open physical security and surveillance solutions to enhance an organization's overall security infrastructure while improving the efficiency and effectiveness of these systems.

Headquarters
300 Santana Row, Suite 200
San Jose, CA 95128
Phone: +1 (408) 215.9000
Fax: +1 (408) 338.0806

EMEA
2nd Floor
145-157 St. John Street
London, England EC14PY
Phone: +44 (0) 845.226.4535