PROXIMEX CORPORATION—WHITE PAPER

Physical Security Information Management: A Technical Perspective

By Ken Cheng

Physical Security Information Management: A Technical Perspective

Physical security remains a top-level concern for organizations today. In both public and private sectors, the need to mitigate risk, ensure compliance and generate a quick return on investment is more important than ever before. While a past response to these business drivers has been to increase spending on physical security infrastructure, budget-conscious organizations must now change course and leverage all available intelligence to speed incident resolution while complying with new regulatory requirements and demonstrating a realistic ROI back to the organization.

Even though the need for increased physical security has elevated to the C-level within organizations, physical security operations groups still find themselves tasked with creating a 21st century security environment from 20th century systems. At the current rate of technology change, even 4 year-old systems can seem antiquated and unable to deliver the information required by all business units. Until recently, security groups were forced to accept minimal integration between subsystems or rely on manual processes and intervention in order to manage and respond to security incidents. This approach is error-prone, time-consuming and requires a high-level of familiarity with the security infrastructure which can be problematic during an immediate security threat.

In response to the complex physical security needs and business drivers, the Physical Security Information Management technology category has emerged. The goal of PSIM solutions is to provide a comprehensive and holistic view of a physical security environment through the integration of numerous physical security subsystems and the correlation of data from these subsystems. With a true PSIM solution in place, organizations can turn silos of data from individual subsystems into actionable intelligence and elevate that information across the enterprise.

The purpose of this white paper is to detail what PSIM entails from a technical perspective, discuss current and future architectural requirements for a complete PSIM solution, identify key areas for the implementation of a PSIM solution and describe the technical architecture employed by Proximex™ Surveillint™.

PSIM Concepts

The first order of PSIM is to provide a means to integrate multiple physical security subsystems. This may apply to organizations without a command and control center or to ones that need to reduce the total number of centers. The subsystem data must be correlated in a manner that provides security operators with actionable information. Most importantly, the information that is presented must be easy to comprehend and use when responding to incidents.

To easily retrieve information, the user interface must be flexible to incorporate a variety of subsystems and display the collection of various data in one centralized place. A complete PSIM solution normalizes the data produced by multiple security subsystems to permit a common analysis of different data points and moves from simple data collection to advanced correlation and reporting capabilities.

The next step is to correlate the data which is more than just combining data points. Proper correlation requires a deep understanding of the physical security environment so data can be displayed in context. For example, access control system (ACS) alert data should be combined with video and any other sensor information in the proximity of the ACS alert so all aspects of the threat can be analyzed together.

Finally, information must be clearly read, easy to view and simple to analyze in a meaningful manner. Integrating multiple data points from multiple places highlights the importance of information presentation. The user interface of a PSIM solution must present all relevant details in a single view without the need for specialized knowledge of the environment because the greater the need for specialized knowledge the greater the potential for human error and problems.

Common Architectural Requirements for a PSIM Solution

For PSIM to meet the major challenges of risk, compliance and return on investment (ROI), it must include certain tenets such as the ability to integrate multiple disparate physical security subsystems, collect and normalize data from these subsystems into a centralized database, and then correlate (connect) this data in a way that is easily interpreted by operators. In addition, workflow must be applied against the collected data in order to automate security procedures.

Security subsystems may be integrated in various ways. The most unrefined integration approach uses simple data retrieval from subsystems by creating custom interfaces to the subsystems or using standard interfaces provided by the subsystem vendor. Custom interfaces work well for simple data retrieval but can be problematic when vendors update their products. Advanced two-way communication (e.g. pushing state changes back to a subsystem) requires detailed understanding of each subsystem. This can be difficult for developers unless they are directly involved in the original product design. The ideal integration approach is to leverage the standard interfaces provided by the subsystem vendor for the orderly retrieval of data combined with a clear mechanism for sending data back into the subsystem. This two-way interface approach should be a requirement when selecting a PSIM solution for your organization.

Using a standard mechanism to create and manage interfaces is essential because it lets organizations avoid a rip and replace mentality by adding new security products and systems to an existing environment without major disruptions. Even though industry standards are in their infancy for interfaces or integration, organizations should consider using mainstream technology components that are commonly found in IT organizations, such as SOAP, XML and web services.

The next step is to address the data itself. An obvious choice is to place the data into a standard database. But before doing so, the data must be normalized in order for it to be viewed across all subsystems. Collecting and normalizing data into a database is required before applying workflow and automation.

Workflow helps organizations ensure that personnel are following procedures and complying with security policies while automation removes the need for constant manual intervention, thus leading to fewer errors and, more importantly, faster response time. While total automation isn't yet possible today, partial automation helps the organization by allowing operators to focus on threats that require a human's attention.

To move organizations toward automation, information should be presented to users in a way that requires minimal interpretation. Ideally, operators should be able to quickly view the user interface and glean relevant information without visiting multiple screens or sifting through multiple layers. The interface should be simple and highly graphical without demanding specialized training or knowledge of the security environment.
A basic implementation would display various sensors from different types of subsystems with sensor alerts overlaid onto facility or campus maps. It should also include the ability to drill down into particular alerts or points of interest.

These workflow and automation capabilities found in PSIM solutions are advanced mechanisms that are used to process collected subsystem data. There are many ways to add these capabilities, ranging from customized engines driven by script interfaces to simple point-and-click graphical interfaces. Whichever implementation is used, organization should evaluate these capabilities with an eye towards ease of use, ease of customization, and ongoing management and maintenance requirements. Because these capabilities are the foundation of a PSIM solution, organization should be comfortable in supporting and maintaining these functions.

Implementing a PSIM Solution

Implementing a PSIM solution requires a set of activities that will significantly impact the organization, including:

- Understand business drivers and how the solution should support them. Organizations need to align their security policies and response to the business drivers of risk, compliance and ROI so the PSIM solution generates value to the business.
- Examine and refine consolidated security operations policies and procedures. PSIM solutions are not autonomous; they will only be as valuable as the policies and procedures they automate.
- Identify required process and procedure changes to streamline operations and serve business needs. These changes can be implemented through workflow and automation.
- Establish performance baseline. Without a baseline for comparison, it's difficult to determine the success of a PSIM solution when addressing an organization's security requirements.
- Measure performance often. Regular ongoing performance measurement helps drive improvement and, ultimately, business value.
- Iterate processes. These steps are not a one-time endeavor but, rather, a continuous process. The feedback from consistent evaluation reduces the potential discrepancy between business needs and implementing security policy.

Each step is equally important and should be completed in order. Skipping one or more steps may cause insufficient attention to organizational needs, less efficient physical security management of policies and procedures and, potentially, higher security operations cost.

Surveillint Architecture

As the premier PSIM solution, the award-winning Surveillint provides all of the benefits of a complete PSIM solution. Surveillint is built on a modern, scalable architecture based on standardized technology components. The underlying technologies found in Surveillint will be familiar to nearly every IT organization.

Built on Microsoft® .NET framework. Proximex developed Surveillint on the industry standard Microsoft .NET platform to provide rapid development of highly scalable, secure and manageable web services-based applications.

Utilizes a Service Oriented Architecture (SOA). SOA is the key that provides easy integration between Surveillint and existing technology infrastructures. It is described as "an architectural style whose goal is to achieve loose coupling among interacting software agents."[1] An SOA architecture offers significant benefits including flexibility, agility, better scalability, higher availability and superior maintainability.

Employs a modular application design. Surveillint's modern modular design separates application components into discrete modules that can be easily modified with minimal impact. This modular approach allows new modules to be added at any time. Surveillint's physical security subsystems modules also use this approach allowing for quick development and deployment.

[1] www.xml.com

Uses a centralized Microsoft® SQL Server® database. Surveillint stores all collected data into a standard Microsoft® SQL Server® 2008 R2 database. The commonly-deployed database platform simplifies database administration and gives customers the ability to develop custom reports. It leverages advanced features of the SQL server, including clustering and replication.

Leverages common communications protocols and messaging formats. Communication between Surveillint components is through the global standard TCP/IP protocol and uses standard port definitions such as HTTP or HTTPS. This means firewalls and other networking equipment will require minimal, if any, configuration modifications. Extensible Markup Language (XML) is the industry standard used for the message format. Using XML for data interchange reduces the integration complexity of Surveillint with third-party products that are also based on SOA and XML.

Makes use of workflow engine based on Commercial off the Shelf (COTS) technology. Surveillint uses the advanced workflow engine embedded in Microsoft® .NET Framework v3.0. Originally built for Microsoft® BizTalk® Server, this engine was designed for enterprise use with its highly scalable and extremely flexible architecture.

Leveraging these powerful technologies, Proximex built Surveillint, the first enterprise-class PSIM solution. The application of modern design principles across Surveillint ensures that future technologies can augment existing capabilities in minimal time. Incorporating standardized components verify that Surveillint is easy to deploy, easy to configure and easy to manage.

Summary

The market for PSIM solutions is growing rapidly with organizations that need to mitigate risk, ensure compliance and demonstrate an ROI back to the organization. With such significant projected market growth, many vendors are beginning to offer products with wildly different capabilities. Organizations that are considering a PSIM solution should examine the core functionality and architecture of each solution to confirm they will meet current and future needs. Surveillint offers the most comprehensive, robust and enterprise-class solution today to help your organizations meet its business needs.

Information in this article is current as of August 2011, the publication date. No part of this document may be reproduced in whole or in part without the prior written permission of Proximex Corporation. License information available at www.proximex.com or by calling 1-408-215-9000.

—Ken Prayoon Cheng is co-founder and chief technology officer for Proximex.

Microsoft, SQL Server and BizTalk are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

About Proximex

Proximex is the leader in event and information management for both physical and logical security markets. The company develops innovative solutions that leverage existing and new systems and technologies that are integrated into a centralized command and control center. Proximex solutions ensure that incident information is no longer trapped within disparate systems, but brought together in context with security policies and operations for analysis and resolution.

CSOs and security teams select Proximex solutions for their ability to help mitigate risk, ensure compliance, and offer a quick return on investment with low total cost of ownership. IT organizations approve of their scalable architecture and high availability. Proximex provides companies with the solutions to support the bigger security picture, that is, the transformation of both physical and logical security into a unified holistic model.

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