This white paper is based on a presentation by **Martin Drew, CPP, President, iView Systems** *in May 2013*

Click here to view the event

A Systematic Approach to Security Information Convergence

The business press is fascinated with the concept of "Big Data" for a very good reason; the amount of data in the world is essentially exploding. Ninety percent of the data in the world was created in the past two years and data production will be 44 times greater in 2020 than it was in 2009. The challenge in the business environment is not just to capture and store these data sets, but to curate, search, synthesize, visualize, and Identify value from the underlying data.

SECURITY MANAGEMENT

iVIEWSYSTEMS
Security | Surveillance | Solutions

In the security function, big data comes in the forms of dispatches, investigations, accidents, thefts, vandalism, threats, assaults, health and safety violations, background checks, audits, and video reviews. All of that information must be collected, structured, and summarized in the forms of daily reports, monthly reports, loss reports, OSHA performance reports, and more. Managing that amount of information is challenging, but we are on also on the frontier of combining all that security data with the data that is collected by business operations and with external data sources such as social networks. This is the new world of "information convergence." It is a world in which security and operations must evolve hand in hand.

Information: Data that is (1) accurate and timely, (2) specific and organized for a purpose, (3) presented within a context that gives it meaning and relevance, and (4) can lead to an increase in understanding and a decrease in uncertainty.

In the past two decades we have witnessed a significant shift from disparate systems and entities for security and operations toward an integrated or converged environment. The benefits of this migration are significant reductions in overall cost and gains in efficiency. But like a smartphone, which combines components like camera, mobile computing, and GPS, the converged environment also becomes greater than the sum of its parts.

Principal goals of security information technology convergence:

- Extraction of useable information from collected data
- Leveraging the investment in existing security technologies and systems
- Operational cost reduction through operational efficiency
- Streamlining and unifying security operations
- Providing a common platform to facilitate collaboration
- Support for the shift from incident reaction to loss prevention strategies
- Extraction of information to make informed strategic and tactical decisions

The Security Information Management Platform.

Many elements can become part of an integrated platform, but cost, operational efficiency, and enhanced security will be the driving factors in creating value. The data elements to be considered will come from different operation silos and they will be in different forms, such as Excel spreadsheets, Word documents, etc.

The complex interrelationships between individual elements are almost impossible to manage in their natural state of independent evolution. Moving the disparate elements to a multifunctional security information management (SIM) platform brings order, structure, and control and allows users to leverage the shared resources from a single platform.

An example would be if the visitor management system were to automatically query a persons-of-interest database. When an employee requested a badge for a visitor that matched someone who had been banned from the facility, it would send an alert to the security department. Security would then be able to access a record of the banned individual, which would include the profile of the individual, the reason they were banned, a picture, and any additional information that would be helpful such as if they had a propensity to violence.

But the efficient management of internal data repositories is only the initial value proposition. The SIM also becomes a new platform in which external data sources from video management, point-of-sale, claims management, and other standards-based open architecture systems can be integrated.

The six step process here is a systemic approach to converging only that data that increases in value by bringing it into the big picture and affording the organization immediate benefits.

1) Identify data source candidates

2) Identify system candidates for convergence / integration

3) Identify related departments and stakeholders

4) Build a requirement matrix

5) Operational requirement assessment

6) Evaluate and define access level requirements

Output Requirements

The output requirements need to be identified before the system is integrated and planned as intentionally as the data gathering and management. Each stakeholder will require different elements and in different formats. Equally important is determining which stakeholders will not have access to what information. Common outputs include:

- Event notification
- Trend reports
- Compliance reports
- Claims reports
- Performance reports
- Breakdown reports

Operational requirements describe not only what information different stakeholders may need, but essentially create the narrative of an event and coordinate the roles and requirements of each. A single incident may involve a dispatcher, a security manager, an HR manager, and a risk manager. The role of the SIM is to apply rules that choreograph the event from the perspective of the enterprise, anticipating the needs of each stakeholder, the actions they will perform, their mutual dependencies, and how they interrelate. The traditional model often required staff to physically go from function to function collecting the information and distributing reports in independent transactions of information.

The diagram below illustrates how a SIM might automatically collect, synthesize, and escalate an incident from initial report to final disposition.

The Dangers of Underreporting

One of the key obstacles to the security function is underreporting of incidents relevant to the security function. Underreported events threaten or damage the organization in terms of liability, misinformation, and the inability to solve investigations. In many cases this is due to staff becoming desensitized by the frequency of events, lack of a reporting mechanism, and lack of training to recognize events. According to research from the ASIS Security Executive Council in 2007, 53% of hotline callers were anonymous and 71% did not tell management first.

A principal value of a SIM is that it creates an efficient system through which all incidents are collected and compiled in a way that informs the security function at a very granular level. Filtering takes place according to organizational needs at a database level instead of based on the intuition of front line employees.

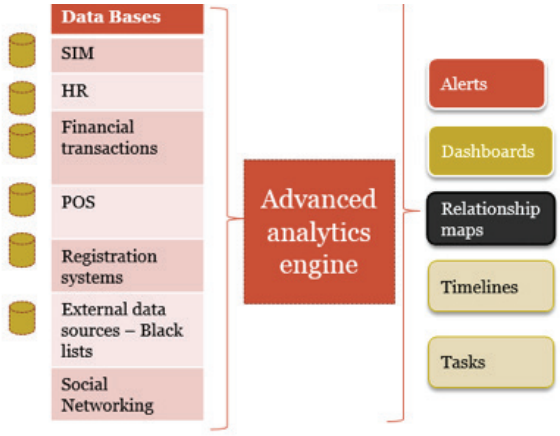
Dashboards and Visualizations

Despite all the benefits, large amounts of data can pose challenges. In its natural state, an organization's data and that of all its vendors is essentially rows and columns and tables that might spread to the horizon in the real world. From this enormous warehouse of data, reports can be constructed that routinely produce information of known value.

But such reports can generate questions of their own—questions deep in the data that would have required substantial programming work to extract as recently as 10 years ago. With such a level of effort required, many questions were never pursued. This raises liability concerns similar to underreporting, because managers actually have all the data needed to take critical decisions, but are unable to gain actionable information or to pick up on subtle trends and looming dangers that might not be obvious from pre-existing reports. In short, what could they have known and when could they have known it?

Dashboards and visualizations allow a far more nuanced method of gleaning critical insight from vast stores of data. Without resorting to time-consuming programming, these security management tools make relevant information more actionable and risks more identifiable.

This white paper is based on a presentation by **Martin Drew, CPP, President, iView Systems** *in May 2013* **Click here to view the event**



Advanced analytic tools monitor the SIM environment as well as external systems such as point-of-sale, registration systems, and social networking. The advanced analytics engine is programmed to monitor all such sources for deviations from normal behavior. When an exceptional event is observed, the engine combines the particulars of the event with nonobvious but relevant information from sources such as the HR department and passes them all up to the security function in the form of alerts and dashboards. These events can be given context with tools such as relationship maps and timelines and can assign tasks to address the event according to company policy.

In the example of casino security, an analytics engine monitors all the games on the casino floor. A blackjack table has a normal behavior of a predictable payout despite regular peaks and troughs. An advanced analytics engine can constantly monitor that table for abnormal behavior and take a snapshot to identify who was at the table at the time and compare relationships between pit boss, dealer, players, and staff in a network diagram. The engine can identify any related incident reports, known addresses, similar names, social network connections, and other data to aid investigators in real time.

The hallmarks of a systematic approach to technology convergence are

1. Start small and evolve
2. Leverage existing security technology investment
3. Use open architecture to enable integration with multiple manufactures and suppliers
4. Implement the system rapidly to quickly realize operational efficiency improvements (ROI)
5. Create a flexible environment to economically leverage new and emerging technologies

During the live event, presenters addressed many specific questions from the audience such as those below. To hear the presenters' responses to these questions and more go to the archived webinar online. If you have additional questions, please feel free to contact the presenters Martin Drew, mdrew@iviewsystems.com or Dean Correia, dcorreia@secleader.com .

- What can the security manager do to prevent white collar crime using this data?
- Would you say that an organization should own its own incident reporting system or are there benefits to having contract security own and manage this aspect?
- How do you limit or prevent the GIGO (Garbage In, Garbage Out) potential? Do you limit those with ability to input data into various systems?
- Do you see benefits or challenges with "Virtual Server" and "Cloud" Services direction. Seems many "Functions" are independently working on their own solutions. Recommendation to corral them up...IF Security led that effort, would that help?
- Please provide recommendations for team makeup to determine critical pathways for convergent software development.
- How do you take your compiled data and go one step further to put a dollar value to resource distribution in order to relate security expense to the bigger business picture?
- At what point in security program development should one begin to converge systems and then employ an analytics process?

iViewSYSTEMS
Security | Surveillance | Solutions

Request a Demonstration
http://www.iviewsystems.com/conversion-pages/request-information-demo

About iView Systems

Security and Surveillance Solutions for Loss Prevention Environments

iView Systems provides leading security software solutions, offering complete integration of your Physical Security Information Management (PSIM) reporting needs for security, surveillance and loss prevention environments. iView Systems transforms the way you report and manage incidents and events, by providing a collective knowledge centre from recording to identifying to analysis of cause, turning your incident data into actionable intelligence. iView Systems' solution suite includes; incident reporting, officer dispatch, facial and license place recognition and visitor management. These solutions are designed to increase security, improve productivity and response rates, while meeting compliance objectives and maximizing ROI. The iTrak system is one centralized platform for the global security marketplace, including the gaming, banking, corporate security and other loss prevention environments.

- Founded in 2002
- Privately-held Canadian software company specialized in the development of incident reporting; security and case management software.
- Software developed in cooperation with specialists with over 50 years' experience in the security industry.
- Worldwide customers in over 50 countries
- Winner of the 2011 Frost & Sullivan Best Practices Award for Incident Reporting & Management Systems
- Winner of the 2012 ASIS Accolades Award, Innovative Products for iDentify Face Search Module

Our Mission

To become the leading provider of innovative software solutions for the security & surveillance marketplace in the gaming and corporate security environments.

Our Team

The iView Team is comprised of individuals with many years of diverse security and surveillance experience ranging from research and development, sales/marketing, and security system engineering with specific expertise in the gaming, financial and related markets. Extensive professional and industry expertise is maintained in-house, with background checks held on file for all staff, ensuring high product and service quality.

Martin Drew, President, iView Systems has more than 30 years' experience in the security industry and is one of the original four founders of iView Systems. Martin's responsibilities include research and development; sales and marketing; product development, engineering and management.

Prior to founding iView Systems, Martin's extensive career within the security industry includes senior management positions in international markets with Racal Guardall US, Chubb PLC (Canada, US and UK) and Thorn Research laboratories.

Martin is currently a member of the ASIS CSO standard work group; Chair of the Underwriters Laboratories of Canada (ULC) S316/ S317 Surveillance Standard Subcommittee and member of ULC S 300 committee.

For sales, technical support or general information, please use the contact information below.

NORTH AMERICA
Phone (905)-829-2500
Toll Free 1-(866)-705-9671
Fax (905)-829-2528
MAILING ADDRESS
Unit B-203,
2381 Bristol Circle
Oakville, Ontario
Canada, L6H 5S9