

Big Data

Turning information
into enhanced
security

**Shrinkage
Solution**

New tools for LP pros

**Lights,
Camera ...**

Keeping video
online to capture
all the action

Insights

TECHNOLOGY

Volume 3, Issue 2
Fall 2015

Welcome

Dear Reader,

This edition of *SIA Technology Insights* is a great indicator of the exciting and valuable changes that are occurring in the security industry.

The first half of this issue is about the power of data, and this, frankly, was not intentional. It's just that five of the SIA members whom we asked to write articles about coming trends and technologies independently proposed pieces on "big data." Such is the nature of the industry now that data mining has become an important security tool, and software has multiplied the effectiveness of video surveillance cameras, access control equipment and other devices.

Who could have imagined a few years ago that a publication like this would have so much to say about data? But physical security is now as much about 0s and 1s on a network as it is about hardware. So here we are, with insightful articles about how the massive amounts of data being collected and stored can be used to identify threats, increase the effectiveness of loss prevention efforts and, generally, enhance security.

As always, we hope you'll find this publication to be informative and useful, and we encourage you to submit comments, suggestions and article proposals to the editor, Ron Hawkins, at rhawkins@securityindustry.org.

Thank you for reading *SIA Technology Insights*.



V. John Stroia
Chairman, Board of Directors
Security Industry Association

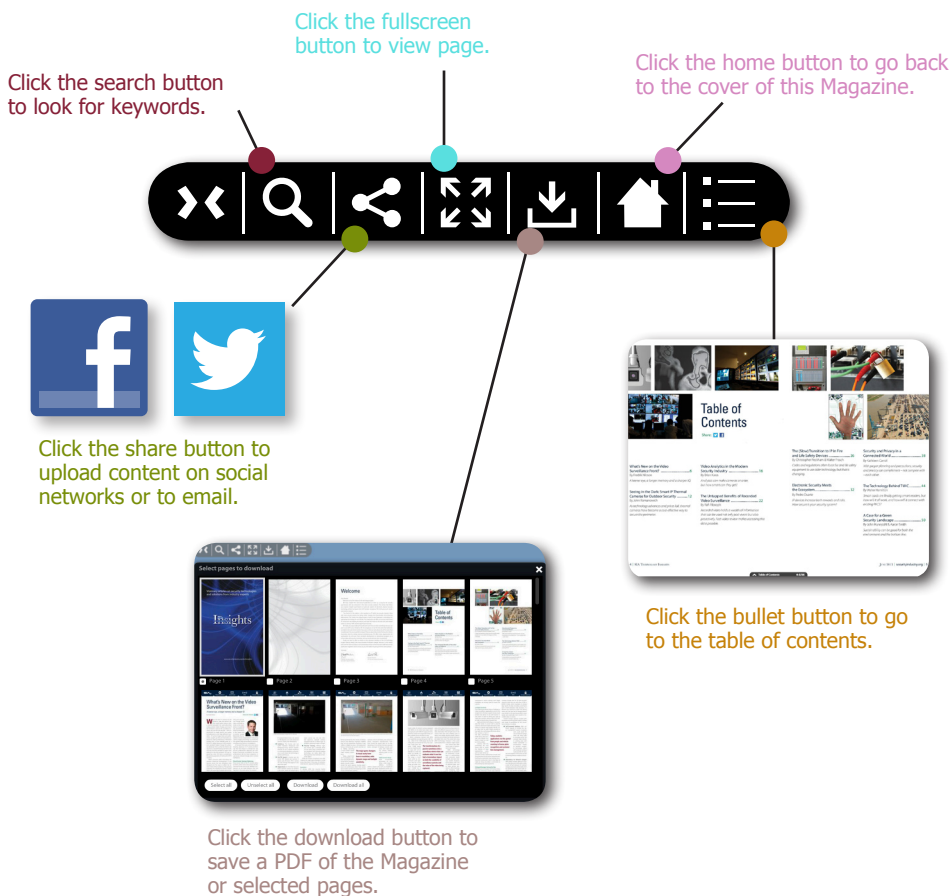


Don Erickson
CEO
Security Industry Association

How to Navigate Through the Magazine

Navigation Bar

Click the arrows button to expand or contract the navigation bar.



Topic Tabs

Click to see a list of SIA members for each topic.



Table of Contents



Transforming Data into Actionable Intelligence 6

New solutions can identify insider threats before it is too late

By Ajay Jain, Quantum Secure



The Evolution of Risk 14

Banks are using analysis of 'big data' to enhance security

By Kevin Wine, Verint Systems



Reducing Retail Shrink with Business Intelligence Software..... 22

Data mining can be a valuable new tool for loss prevention professionals

By Charlie Erickson, 3xLOGIC



Big Video Data 30

Video management systems offer a powerful platform for security and business intelligence

By Jeff Karnes, 3VR



The Public Safety Data Lake 38

Making the right decisions regarding storage and other issues can vastly increase the value of video surveillance

By Ken Mills, EMC

Keeping the Security System Secure..... 48

Ensuring that video stays online is key to managing risk

By Bud Broomhead, Viakoo



Maintaining Power 56

New network communication solutions can minimize system downtime

By Ronnie Pennington, Altronix



From Legacy Systems to Advanced Access Control 64

New solutions can offer extensive benefits to municipalities

By Robert Laughlin, Galaxy Control Systems



Unlocking the Door 72

Next-generation access control systems can offer new insights and greater security

By Scott Sieracki, Viscount Systems



Striking the Balance Between Security and Safety 80

Classroom door locks are invaluable, but they must allow quick egress

By Mark Berger, Securitech



SIA Technology Insights Article List..... 88



The actionable intelligence delivered by PIAM solutions with predictive analysis technology allows organizations to identify potential threats and opportunities in real time and apply proactive measures to guard against breaches or reap the benefits of unanticipated changes in business practices or policies.



Transforming Data into Actionable Intelligence

New solutions can identify insider threats before it is too late

In every industry, data drives decisions. This might be as simple as an organization reviewing financials to determine whether an expansion is feasible, or it could come in the form of more complex analysis, such as examining a pool of information to identify which customers might be about to defect and determine how best to retain them. Whatever form analytics may take, organizations increasingly recognize their potential to transform raw data into actionable intelligence.

With data analytics, it stands to reason that more data should equate to more insights that enable the most informed decisions and the best outcomes. And there is a growing abundance of data that is generated by and available from an expanding number of disparate sources. Access control, video surveillance, human resources, traffic control, point-of-sale and many other systems and

By **Ajay Jain**
Quantum Secure



devices all contribute to the flood of information. Unfortunately, many organizations have still not found an efficient way to deliver on the promise of “big data.”

Physical identity and access management (PIAM) solutions utilize the new science of predictive analysis to help transform the security department into a proactive strategic partner that plays an integral role in an organization's business and growth. While conventional security solutions such as alarms and video surveillance systems provide comprehensive real-time coverage and alerts, they are typically considered to be reactive rather than proactive resources. Worse yet, in some situations, the security system's own shortcomings can render it ineffective. For

example, because more than 95 percent of alarm activations turn out to be false, security officers may begin responding more slowly, or not at all, to the alarm. In essence, the alarm monitoring process itself has inadvertently trained people

not to pay attention to alerts when they occur. As a result, threats may go undetected – or by the time it becomes evident that there is a real incident in progress, it may be too late to do anything about it.

PIAM systems with predictive capability, on the other hand, are designed to analyze a wide variety of data from multiple systems and

devices to identify statistical patterns and trends. This analysis helps identify predictors for future incidents, known as indicators of compromise (IOCs), which may include changes in access or behavioral patterns, such as entering a facility at unusual hours or locations, or attempting to access unauthorized areas. This analysis allows organizations to identify potential threats or business opportunities early on. An added benefit is that these predictive analysis systems are capable of learning and improving over time, and are often able to identify patterns that were

never expected or that most likely would not have been uncovered without that level of processing and automation.

This use of metrics is a significant element of predictive analysis, allowing PIAM solutions to create a picture of what

normal looks like and, from there, extract useful information out of the mountains of data. As an example, to determine the effectiveness of security and operational policies, it might be necessary to know the number of visitors who enter a facility during specific time periods, the time it takes to process those visitors, and how that affects start-times for employees.

Given the complex psychology involved, insider threats can be incredibly difficult to understand. However, using predictive analysis, one can develop an understanding of who might be most likely to attempt an attack from the inside.



When these metrics are combined, lobby staffing levels can be understood and managed more effectively. Or, in terms of operational effectiveness, the duration of the process for new hires to receive access approval can be used to find areas where automation may have the highest return on investment.

Metrics are also proving to be vital in the fight against insider threats, which are increasingly prevalent security concerns for organizations. Given the complex psychology involved, insider threats can be incredibly difficult to understand. However, using predictive analysis, one can develop an idea of who might be most likely to attempt an attack from the inside. First, a profile can be created based on each person's current access, time of employment and time since his or her last access audit, background check or other mitigation control. The

access profile is the first element that indicates each person's inherent risk to the organization.

A triggering event, such as a bad performance review, a missed promotion or something similar is another indicator that might precede an insider breach. While this sensitive data must be properly managed and handled, it could potentially serve as a second predictive element. Information related to these events is securely stored in the human resources system and could be used by authorized individuals to generate an initial red flag that an individual might pose a rising threat.

The third element is behavioral information. This includes data such as which individuals might feel they have reason to take some kind of criminal action and have the physical access needed to do it, and who among these

individuals also has a history of activity that might indicate an imminent threat. Behavioral information can be analyzed in many ways. For instance, you may want to see a report showing every time a person entered the premises and every door he or she accessed to help establish that person's normal routine.

Each element of the insider threat risk profile provides a different perspective and builds a larger picture that can be used to reduce the danger or improve overall understanding. Access audits can be focused on individuals with high scores in multiple elements, including high levels of access, and used to remove unneeded access. Reactive alarm management can even be given new meaning. Sharing the behavioral change and risk score information with the security operations center allows them to react with real understanding instead of being forced to treat every alert the same way.

By mining the accumulated data with established metrics, security can analyze information to look at patterns across a large number of employees over a long time period to identify things that may not be

By mining the accumulated data with established metrics, security can analyze information to look at patterns across a large number of employees over a long time period to identify things that may not be obvious or intuitive.

obvious or intuitive. These patterns can then be used to develop additional metrics to indicate a potential threat. If an employee exhibits not only differentiated behavioral patterns but access patterns as well, those IOCs show that he or she is a higher risk and, as such, should be subjected to additional scrutiny. For those employees who have been flagged in

the system, future deviations from their routines, such as coming into or leaving work at an unusual hour or accessing areas of the building or information systems they have never accessed before, will generate additional red flags or even alarms, but now the

alarms will have context provided by predictive analysis.

One real-world example of the effectiveness of predictive analysis can be found in a company that was experiencing the loss of equipment over a period of time. At first, company officials were unsure who was behind the thefts, but they thought it might be the work of an insider. One factor was that the losses were mostly being reported in the morning, which would indicate that the thefts were likely occurring after hours.

Based on this initial information,

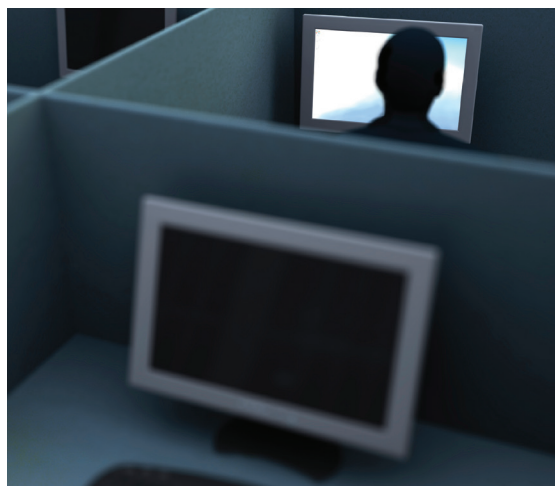


the company began to analyze data to examine employee activity, beginning with identifying any employees who were behaving outside of their normal routine. They were able to determine those routines using data that had been collected from a number of systems, including access control. This analysis led them to discover a particular employee who had started to access areas and facilities he was authorized to enter but had never previously entered. They were also able to determine that this access was regularly occurring outside of the employee's typical hours, often in the late evening. A final factor was that these abnormal behaviors correlated closely with

buildings where the equipment was disappearing. From there, the company set an alarm for any time he accessed a new area late at night, even though he was authorized to enter the area. The next time he did so, an alarm was triggered. When security staff responded, they caught the employee in the act of

disassembling and preparing to steal yet another piece of equipment.

Post-incident analysis of security breaches has repeatedly uncovered the fact that there had been enough relevant data stored in disparate sources for predictive analysis to have identified a potential breach, alerted staff and provided actionable intelligence that could have prevented the incident from occurring.



Without predictive analysis technology, the challenges related to data collection and investigation are

daunting. Most organizations have no problem identifying what they hope to learn from data analysis, but they lack the capability to collect and organize all of the data relevant to that goal. Without a comprehensive means of collecting and organizing large amounts of data – not to mention analyzing the data for insights that will help them

make smarter decisions – organizations end up with business as usual. Post-

incident analysis of security breaches has repeatedly uncovered the fact that there had been enough relevant data stored in disparate sources for predictive analysis to have identified a potential breach, alerted staff and provided actionable intelligence that could have prevented the incident from occurring.

While the idea of building an in-house custom application for predictive analysis may seem attractive, the requirements for big data analysis are often not well understood by in-house developers and business owners. Further, a professional subject matter expert can provide a better view of how to integrate company processes, business challenges and unique needs into a solution that can be developed more accurately and implemented less expensively than it could from within the organization. All of these factors underscore how important it is for organizations to seek outside assistance when considering a predictive analysis model.

Although technical at its core, predictive analysis must be integrated as a security activity, and subject matter experts who have experience in both security systems and data analytics can realize this goal for an organization. A subject matter expert can also help to ensure successful implementation and integration of predictive analysis so that organizations can benefit from the full potential of these powerful solutions. They work closely with the organization to identify and integrate all of the data-generating systems and devices – not only to ensure that data is properly collected, but also to ensure that it is high quality and will contribute to the effectiveness of the predictive analysis solution.

The outstanding value this process will ultimately deliver will be evident in the capability of the organization to develop deep insights that lead to more efficient operational decisions and that reduce its risk profile.

As the proliferation of data continues, subject matter experts





Cyber/Data Security



EAS



Fire & Life Safety



Intrusion Detection



Video Surveillance



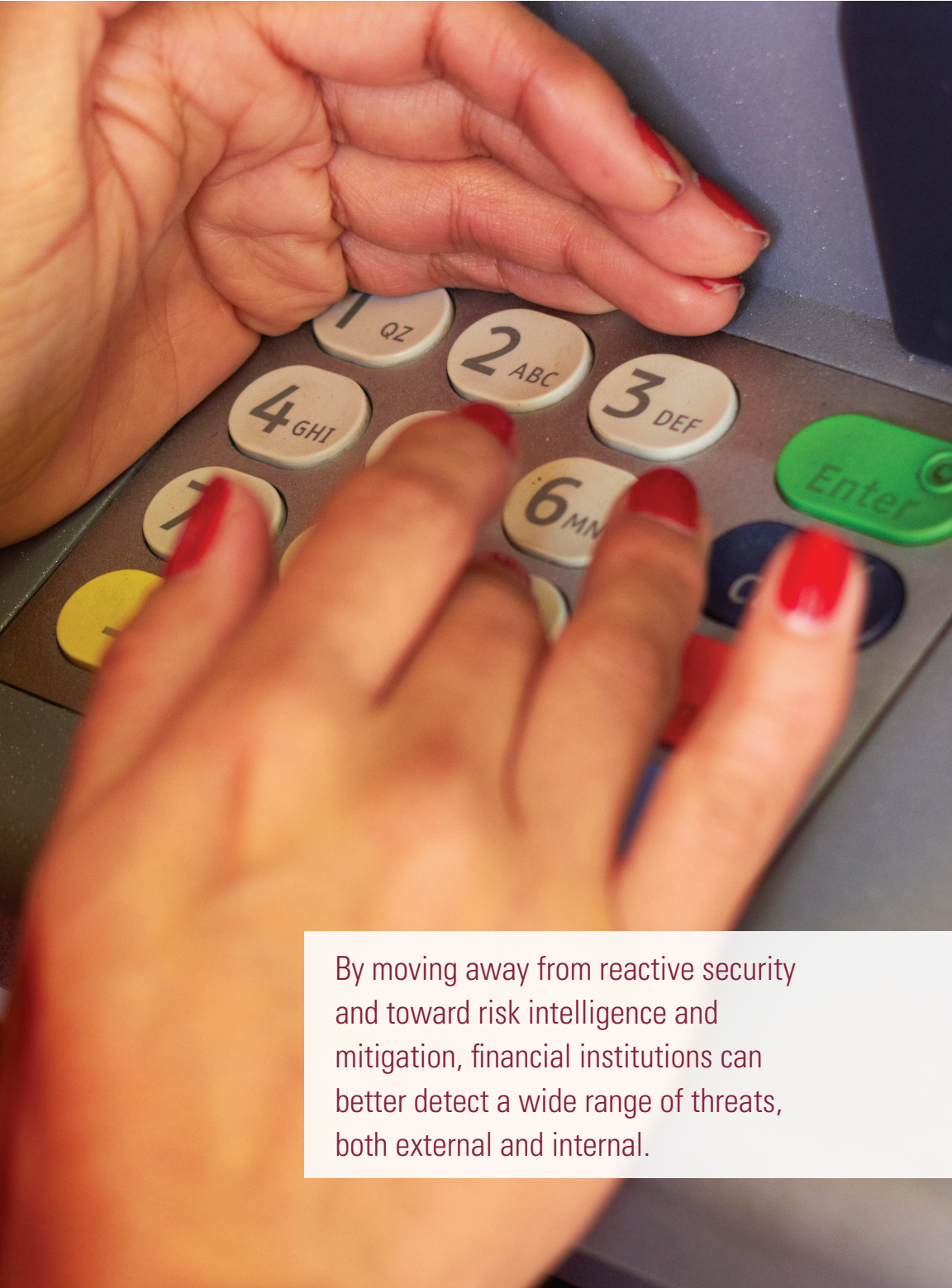
become even more necessary to organizations as they can bridge the gap between technical understanding and practical use. This ensures that identified trends or predictors are actionable and have an impact on security and business operations.

The actionable intelligence delivered by PIAM solutions with predictive analysis technology allows organizations to identify potential threats and opportunities in real time and apply proactive measures to guard against breaches or reap the benefits of unanticipated changes in business practices or policies. Lacking the means to properly collect and analyze data,

or not recognizing the opportunity for change until it is too late to be impactful, is clearly detrimental to security operations. Working with a subject matter expert to harness the full power of predictive analysis allows organizations to transform their big data into intelligence that drives more effective and efficient security practices and that creates competitive advantages for their businesses.

■ Back to TOC

Ajay Jain (ajain@quantumsecure.com)
is president and CEO of Quantum Secure
(www.quantumsecure.com).



By moving away from reactive security and toward risk intelligence and mitigation, financial institutions can better detect a wide range of threats, both external and internal.



The Evolution of Risk

Banks are using analysis of 'big data' to enhance security

The financial market is dynamic and evolving. Over time, financial institutions have transitioned significantly, reacting to demand in an effort to provide the highest level of service and convenience to customers. Banks are responding to consumer demand for faster, more flexible service by changing their branch footprint. For many companies, the branch of the future is becoming more sales focused, with virtual tellers and more customer efficiencies, and ATMs are getting advanced capabilities. For today's customers, online account access is just as important as a customer service representative at a bank branch. And for security professionals, "security" no longer means simply protecting the perimeter of a branch; it also means securing the ATM and teller systems, which requires the help of IT.

As the financial business has changed, threats have evolved as well,

By Kevin Wine
Verint Systems



challenging security and business leaders to stay one step ahead of crime and fraud trends. Years ago, the security of a bank was the responsibility of the security leader who worked to build



a robust technology infrastructure of video surveillance, access control and other systems to physically protect each location from robbery and other potential threats. Fraud investigators focused on deterring and detecting risks, working with local law enforcement and other banks to mitigate criminal activity.

Today, security and risk are larger issues, reaching far higher, into the C-suite. Banks recognize the potential for costly and damaging disruptions if risk is not appropriately controlled. As a result, IT, physical security, cybersecurity, and branch operations collaborate to manage risk. Some organizations have even begun to align risk management, security and investigations under a chief risk officer title. Other companies have created a department that oversees risk management, operating under security or IT.

It is obvious that the lines between various once-siloed departments in today's financial organizations are blurring. This is a positive change, as the trend helps promote better and stronger responses in an evolving risk environment that includes several risk drivers.

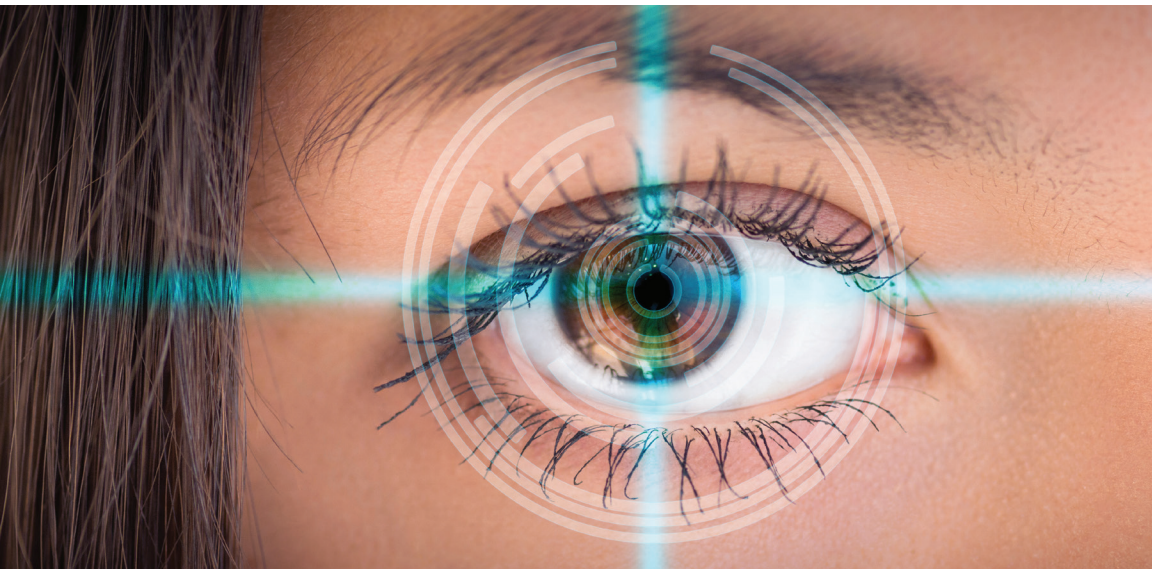
Globalization

Large financial institutions have locations around the world, as well as remote and traveling employees, which leads to a wide range of threats. To maintain a high level of security and ensure business continuity around the globe, companies need ways to predict and respond to threats, including crime, severe weather, terrorist activity, even travel delays, in real time.

Sophisticated Networks

Modern criminals are increasingly sophisticated in their tactics. Financial organizations must contend with





high-tech schemes and, in some cases, globally organized crime. This higher level of risk pushes banks to address security in a more cohesive way, with input from various departments across the organization.

Now, more than ever, executive leaders are concerned with how risk affects the entire organization.

Collaboration

Information sharing between various stakeholders, departments, law enforcement and even regulatory agencies is encouraged in today's data-driven environment, and this delivers a

Banks recognize the potential for costly and damaging disruptions if risk is not appropriately controlled. As a result, IT, physical security, cybersecurity, and branch operations collaborate to manage risk.

wide variety of benefits. For example, financial organizations are able to easily transmit information across multiple locations, helping officials detect known criminals and recognize

patterns of fraud. This collaborative approach minimizes the risks that are inherent with isolated systems and locations.

Integrated Solutions

Open systems allow users to access real-time information from multiple sources, which empowers security officials and employees to make

quick decisions that help improve safety. Following an incident, operators

Case Study: National Commercial Bank Jamaica Limited

National Commercial Bank Jamaica Limited (NCB) is completing the final part of a multi-phase implementation of its security solution. NCB is Jamaica's largest financial services provider with 36 branches and 200 ATMs, and it uses innovative technology to drive operational efficiencies and enhanced services for its customers.

In 2013, NCB decided to further align its focus on mitigating fraud, enhancing investigations and applying advanced situational awareness across its locations. The bank deployed new video surveillance solutions at its branches and ATM sites to monitor all public areas and cash-handling areas. NCB also leveraged IP cameras at its branch entrances and the head of its teller lines, using network video recorders and video encoders to capture high-quality video.

The new solution offers myriad benefits. Now, the fraud department and security personnel are able to view live and recorded video from their desktops to make real-time security decisions. A diagnostic and management application enables

NCB to manage DVR properties, passwords and firmware to help deliver superior system uptime, enhanced management control, and improved operational uniformity.

"We have embraced the latest in IP surveillance technology, while still being able to leverage our existing analog infrastructure and easily scale to meet our future needs in a cost effective way," NCB Manager of Safety, Security and Environment Glenroy Findlay said.

In addition, Findlay saves valuable time managing the distributed surveillance system through enterprise-wide health monitoring, audit reporting, firmware management and permissions management. In particular, the automated system-wide health monitoring and diagnostics maximizes system uptime and allows the security team to focus on investigations.

NCB is helping ensure its customers and employees are protected and enhancing its fraud reduction and theft prevention, while also streamlining operations, improving business efficiencies and reducing costs.

The automated system-wide health monitoring and diagnostics maximizes system uptime and allows the security team to focus on investigations.



can export video data, transaction records and other vital information to aid in a faster, more effective investigation. At the same time, an ongoing information exchange with regulatory agencies helps banks stay in compliance.

All of these factors play a significant role in moving the idea of “security” from situation management to comprehensive risk intelligence and mitigation. Another key factor is the growth of “big data.” As financial institutions gather more data from a wide range of systems, information must be analyzed and prioritized to enable operators to respond more effectively. But how can valuable data be identified and separated from non-essential information?

In a modern security operations center, hundreds of data sources are leveraged to help create a robust and

comprehensive security posture. Most times, these sources operate separately, and operators are tasked with manually identifying potential anomalies within the systems and identifying trends among them. This is a time-consuming and complex process.

Imagine a software platform that could be used to automatically fuse together multiple data points in real time and then analyze those streams to create actionable layers of data. Users could clearly visualize trends within seconds and take immediate action. Standard operating procedures would provide a guide through the correct prompts for faster responses. This software application would enable data to become actionable intelligence. Without it, the data is nothing more than noise.

Broader levels of actionable intelligence are also attainable.

Banks can fuse together information from social media, weather reports, business and IT systems, and traffic management. This comprehensive approach allows leaders to “see” what is truly important, where it is happening, how it might affect their business and what steps should be taken to mitigate risk before it emerges. By moving away from reactive security and toward risk intelligence and mitigation, financial institutions can better detect a wide range of threats, both external and internal.

Banks require technology solutions that can help identify ways to deter, detect and respond to potential risks. Situational awareness and enhanced levels of security can be gained though the use of intelligent software platforms, enabling improved information sharing and faster, more effective responses.

Situational awareness solutions combine multiple systems into one interface, enabling information to be correlated into a single easy-to-manage solution. This approach allows banks to see data in a combined format, streamlining the identification of security, service and business trends to achieve new levels of awareness

It is obvious that the lines between various once-siloed departments in today’s financial organizations are blurring. This is a positive change, as the trend helps promote better and stronger responses in an evolving risk environment.

across an organization. Further, by leveraging advanced surveillance, analytics and investigation tools, banks are better able to detect and respond to incidents in real time, no matter where they are located. And by using a centralized situational awareness platform, organizations can more effectively report incidents to other locations and branches, law enforcement and additional agencies.

Improved situational awareness enables banks to prevent internal

theft and fraud, as well. Today, most employees must use badges to physically enter a bank and passwords to log on to any computer. A situational awareness platform can fuse this type of data together to provide actionable intelligence on each user’s activities. For example, if an employee attempts to access financial information on the bank’s network,

but he or she is not actually keyed into the building, the system would raise an alert. Or, if he or she was found to have repeatedly opened new accounts for suspected fraudsters, officials could keep an eye out for potential criminal activity.

Facial recognition is one technology that, when correlated with other



data points, can help banks identify potential fraud schemes before they occur. If a bank needs to validate that

an individual is who he or she claims to be, several attributes can be used to identify the person, such as a driver's license, credit card, license plate number, etc. Add in data from facial recognition, and users can then look for connections. For

instance, facial recognition can be used to alert a bank if someone has been seen at multiple branch locations opening accounts using fake IDs. Additionally, the technology can be leveraged to monitor whether people are allowed to be in certain areas of a building.


For a growing number of financial institutions, a situational awareness

platform helps to facilitate information sharing among various locations, as well as with external authorities and

agencies. This not only improves real-time incident detection, it also helps security officials and law enforcement agencies respond to and investigate crime and fraud more efficiently and effectively than ever before. As big

data analysis continues to grow, such solutions will be key to leveraging the most critical data points to help banks increase security, reduce fraud, and ensure longevity in their respective markets. ■ **Back to TOC**

Now, more than ever, executive leaders are concerned with how risk affects the entire organization.

Kevin Wine (kevin.wine@verint.com) is vice president of marketing, Americas, video & situation intelligence solutions, at Verint Systems (www.verint.com). 



One of the benefits of using big data over the last couple of years is that the cost of creating data sets with billions of transactions is low, and adding the ability to search those transactions at an equally low cost is creating new opportunities to more effectively mine that data.



Reducing Retail Shrink with Business Intelligence Software

Data mining can be a valuable new tool for loss prevention professionals

Retailers, like most businesses, are attempting to do more with less in an effort to increase competitiveness and profitability. Hardest hit have been corporate support organizations (Target and Best Buy are recent high-profile examples), where corporate loss prevention (LP) personnel who specialize in identifying and investigating corporate shrink typically reside. These developments, combined with shrink numbers that exceeded \$128 billion in 2014, are exacerbated by decreasing employee loyalty resulting from the fact that many retailers have reduced employees' weekly hours. This has led to some employers increasing the number of their part-time employees by 30 percent or more. In fact, the Bureau of Labor Statistics estimates that the number of involuntary part-time workers nearly doubled from 2006 to 2013, and that trend seems to be continuing.

By **Charlie Erickson**
3xLOGIC



Trying to Do More with Fewer People

Retail employees now frequently have to juggle multiple jobs to earn the same income, further driving down already low employee loyalty. This has created a perfect storm: fewer people



to oversee a greater number of workers who have relatively low-wage jobs and less than stellar loyalty to their employer. Is it any wonder that upwards of 50 percent of retail shrink is internal? Employees stealing from their company – the type of theft that is not opportunistic like most shoplifting – is chronic.

The focus of retail loss prevention is on return on investment (ROI), to be sure, but, just as important, these tools must demonstrate a return on time invested (ROTI), as well. That is, if a person is going to spend an hour using a given tool, it must be more productive than

an hour using other approaches and tools. Also, the better, newer tools

Employee theft that originates at the register is a huge and persistent problem, generally making up nearly 50 percent of the loss in any retail operation, and some retailers contend theft by employees accounts for as much as 80 percent of their total loss.

must be able to capture and apply the insights of LP specialists and then make the results available to a wider audience within the company. Some retailers outsource this function to firms whose employees

have little insight into the company itself. This means the best LP tools have to be intuitive and easy enough for just about anyone to use.

Employee theft that originates at the register is a huge and persistent problem, generally making up nearly





50 percent of the loss in any retail operation, and some retailers contend theft by employees accounts for as much as 80 percent of their total loss. This means that, day in and day out, a single employee can steal from an employer using the same methods, if undetected, and losses exceeding thousands of dollars are not uncommon. Therefore, catching a single dishonest employee generally has a greater impact on shrink than catching several shoplifters who may only steal opportunistically once or twice from that retailer.

The sooner a company can identify and remove thieving employees, the greater the impact on reducing shrink. An LP manager recently talked about an employee who was doing item returns for cash and started out stealing \$8 on the first night. By the end of a month, when the employee was finally caught, he was taking more than \$600 a day, for a total loss of \$18,000. The employee is now in jail, but the retailer is out the \$18,000. Think about a company that has 1,500 stores across the country. Now, imagine only 1 percent of the stores have dishonest employees like Mr. \$18,000. Such a scenario could cost the retailer \$270,000 in just one month.

Implementing Business Intelligence Analysis

While a number of companies have specialized for some time in tools to help identify suspect transactions, the focus now needs to be not only on how to identify a suspect individual



transaction but also on how to deploy a comprehensive, data-driven method to identify employees who are the worst offenders, by company, region, division and store. All retailers have learned over time which type of point-of-sale (POS) transactions or combinations of transactions may indicate employee theft. Typically, retailers will have 20-30 types of transactions, and of these 20-30 types, some are much more likely than others to be theft.

A great way to find top offenders is to assign a weight to each type of transaction or exception (giving higher weights to transactions with higher potential for theft), so that chronic offenders visibly bubble to the top of the list for each transaction (or exception) monitored. Doing this in

combination with a straightforward and quick review of all transactions and the associated video increases the effectiveness of LP professionals and also provides a tool that regional managers and others can use to

get involved and contribute to reducing shrink. This sounds great, but what is happening in the actual stores?

A recent Aberdeen Group study indicated that 45 percent of retailers struggle to get timely data and only 26 percent have implemented any exception reporting program. Since management tools that deliver timely data are increasingly available, and there is minimal capital investment to implement a cloud-based “big data” exception reporting solution, the percentage of retailers who implement such reporting systems is expected to increase significantly over the next few years.

Business Intelligence in Action: Three Mini Retail Case Studies

Simple to Use

One company implemented a POS monitoring program for its 1,500 stores and had 8,000 employees processing more than 2.5 million transactions every day. A webinar training session was scheduled to get

the LP team started on the software, and the email invitation included a login and password that the head of loss prevention could use to access the solution’s dashboard. Five minutes after receiving the email, he replied

to the invitation, “I love it, it’s so easy to use, I just caught the first person!” The best, most effective business intelligence packages must be very easy to use and capable of finding “the needle in the haystack” without complicated maneuvers and user-written code. It must provide that all-important ROTI.

This company now projects that one of its analysts will reduce shrink by approximately \$1.2 million in one year using the software package.

Integrated Video for Instant Review

The inability to quickly review video associated with POS exceptions has traditionally been a weakness in exception-based reporting systems. Typically, systems provide the time and date of the POS exception and then the end user has to crank up the DVR software to manually input the parameters to be applied to request the relevant video. In such scenarios, the end user has to wait for the video to be uploaded from a distant store. In most retail applications, the network links to the stores are very low speed,

Catching a single dishonest employee generally has a greater impact on shrink than catching several shoplifters who may only steal opportunistically once or twice from that retailer.



and security video almost always is allocated only a portion of the network connection, so more critical store operations such as POS and credit card data can be processed. As a result, it can take more than 10 minutes to review a one-minute POS transaction. This is not very good when measuring ROTI, especially when it is repeated over and over.

The best business intelligence software utilizes a scheme in which videos of all POS exceptions that show a high probability of theft, and therefore are expected to be viewed, are uploaded to the cloud in the background, when bandwidth is available, where they can then be played in a YouTube-like format. By using such a video preload capability, one end user's corporate investigators,

who had been closing just one or two cases a month, closed 100 cases in the first full year of use. Because they could review video quickly, they were able to look at far more exceptions and close more than five times the cases on an annual basis.

Using Video for What Can and Cannot Be Seen

Tight integration with video enables LP professionals to create compound exceptions that are based not only on POS transaction data but also on who is in the camera scene. Using that capability, an exception can be created for a product return when no customer is present. Video analytics are used to determine if a customer is in the area where a customer should be standing during a return. If there is no customer, then the exception is flagged. The odds

that this type of transaction involves theft are very high. When this function was enabled for one company that had 100 stores, they caught 30 employees in the first month. Several were trusted employees in good standing who had worked for the company for more than five years, proving you often really do not know where your shrink is coming from.

What's Next in Battling Shrink?

One of the benefits of using big data over the last couple of years is that the cost of creating data sets with billions of transactions is low,

and adding the ability to search those transactions at an equally low cost is creating new opportunities to more effectively mine that data. It was customary to keep a few months of transactions per retail location, with searches possible for only one location at a time. Now, several years of transactions can be saved, and searches can be quickly performed across the enterprise.

With this much richer data set, it is possible to study employees who have been caught stealing and compare them to current employees to help spot bad behavior quickly so





it can be stopped with a conversation and disciplinary action not requiring termination. This prevents significant loss, which is the key objective of any LP specialist. This may also “save” an employee from being terminated and getting a record that will negatively affect his or her entire career, while, at the same time, saving the retailer the cost of hiring and training a replacement.

These data sets can also be used to monitor new employee performance, determine what type of training is the most effective, and identify when additional training is required. In addition, it can highlight patterns of activity where stores or regions are not conducting business according to corporate guidelines. For example, it can determine which employees are checking IDs for tobacco and alcohol purchases, rather than simply doing a date override because the customer “looks old enough.” Customer demographics are consistent over time at the same location, so checking IDs should be equally consistent for all employees.

Retailers have many other rich data sets that fit nicely into an advanced business intelligence software package. Data from alarm panels, for example, can provide many insights. Simply by


looking at opening and closing times, headquarters operations staff can quickly see which stores chronically open late or close early, and locations with higher-than-average numbers of unscheduled openings can be investigated. Monitoring phone records, meanwhile, can point to stores where employees may be spending excessive amounts of time on non-work related activity. The list goes on of data sources that may seem mundane but that provide valuable

insights into behavior that is potentially hurting productivity and reducing profits.

Retailers have only started to reap the benefits from mining all the data they are collecting across tens of thousands of locations, and

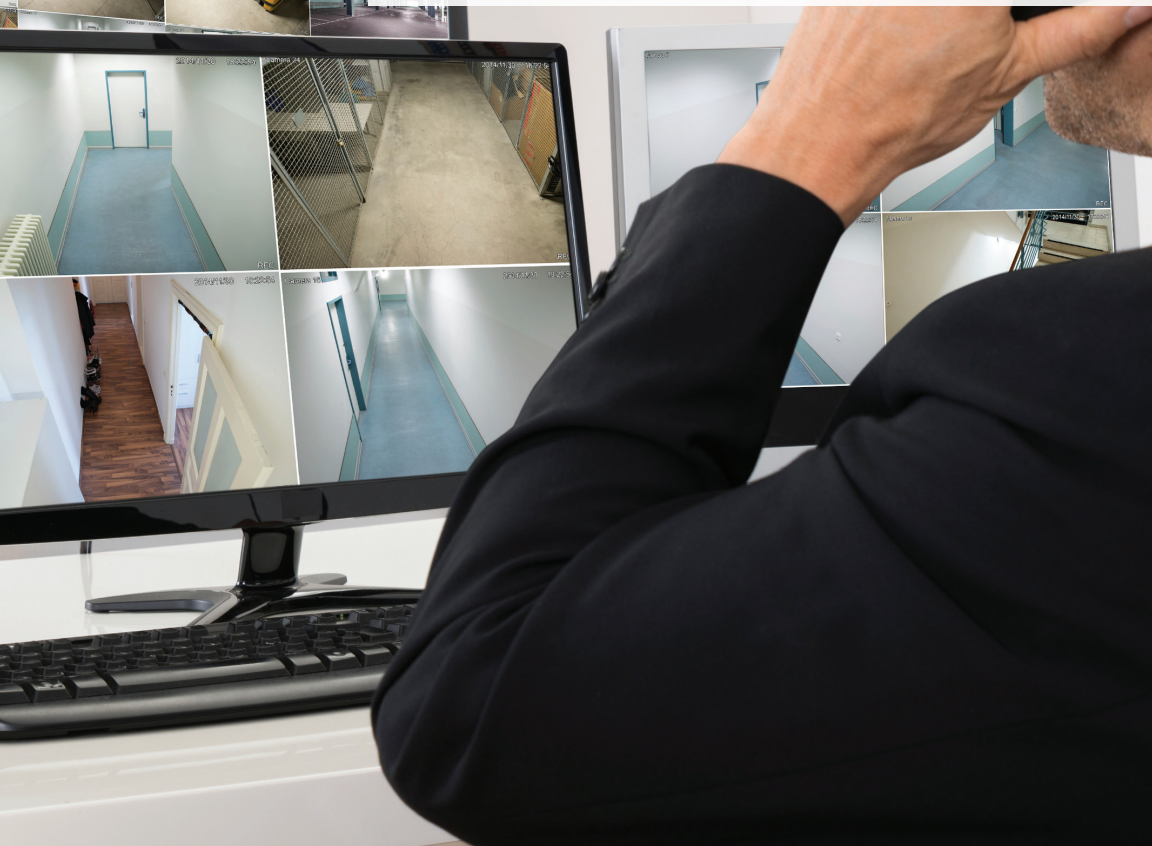
the ROI – and ROTI – will only increase as more data sets are added. When end users start asking questions about their data that would have been impossible to answer just a few years ago, they will come to understand new insights that they only dreamed of, and their wish lists for tools to further reduce shrink will really start to grow. ■ **Back to TOC**

With this much richer data set, it is possible to study employees who have been caught stealing and compare them to current employees to help spot bad behavior quickly.

Charlie Erickson (charlie@3xlogic.com) is vice president, product management, at 3xLOGIC (www.3xlogic.com). 



Video analytics may still seem like a “nice to have,” but adding analytics to a security system can help turn millions of hours of raw video footage from locations such as bank branches and retail outlets into structured, searchable data. Through the use of analytics, businesses can develop meaningful insights for decision-makers in marketing, operations and customer service.





Big Video Data

Video management systems offer a powerful platform for security and business intelligence

From a single store location to multinational enterprises, IP surveillance systems have become extremely prevalent. While the majority of these systems were originally installed to improve security, there has been a recent push by many organizations to leverage the video from surveillance systems for other business purposes. The C-suite has seen the enormous potential in doing more with all of the unstructured data being collected every day by their security systems, and IP video is now part of the “big data” trend.

This corporate hunger for business intelligence means that the traditional DVR, which simply records and stores video, is becoming obsolete. Today’s IP surveillance systems are increasingly being tasked with delivering more than improved security, and, therefore, they need to be able to analyze large numbers of videos and provide

By Jeff Karnes
3VR



actionable intelligence that can help businesses improve their bottom line.

Deploying an enterprise-wide video management system (VMS) empowers organizations to leverage a single

platform for recording, streaming, viewing and analyzing live video from any number of surveillance cameras for both security and business intelligence applications.

From a security perspective, a VMS solution that offers powerful search capabilities can help organizations find relevant information and evidence in just minutes, instead of hours, days or weeks, dramatically enhancing the ability of investigation teams to prevent or prosecute crimes. Enterprise-wide VMS solutions can also help build stronger cases for law enforcement by organizing video and documents into a centralized online case folder that can be accessed by assigned employees and law enforcement officials, significantly accelerating the investigation process. Enterprise VMS can also include centralized management features that offer the ability to manage and search videos across hundreds of locations, configure cameras remotely and receive alerts when any equipment is down.

From a business perspective, this same VMS solution can extract powerful, actionable intelligence and insights. This helps companies better understand customers and tailor business practices toward their

behaviors in order to better meet their needs.

Video analytics may still seem like a “nice to have,” but adding analytics to a security system can help turn millions of hours of raw video footage from locations such as bank branches and retail outlets into structured, searchable data. Through the use of analytics, businesses can develop meaningful insights for decision-makers in marketing, operations and customer service.

Video Analytics for Security and Business Intelligence

In general, video analytics are algorithms that take raw video feeds

from surveillance cameras and turn them into structured data that is tagged with metadata. This now-structured data is stored in a database that can be easily searched in seconds by event, person, camera, location, time, color and

keyword. Depending on security and business objectives, any number of video analytics can be used.

Facial Recognition

Facial recognition is a powerful video analytics solution for security personnel. Retail banking institutions are using this analytic to identify and track suspects and develop trends on

The C-suite has seen the enormous potential in doing more with all of the unstructured data being collected every day by their security systems, and IP video is now part of the “big data” trend.



potentially fraudulent activity across branch locations. For example, when integrated with teller transaction systems, banks can use facial recognition analytics to search for an individual associated with a fraudulent check transaction. An enterprise-wide integrated platform enables subsequent searches for similar faces across other locations, so investigators can catch criminals who travel from branch to branch, quickly connecting the dots of suspicious behavior in a way that was not possible before.

For retail organizations, facial recognition can help identify shoplifters, return fraud and employee fraud, such as internal theft and “sweethearting,” by integrating visual intelligence with point-of-sale (POS) and exception-based reporting systems. Facial recognition can also reduce employee time-clock theft and help identify employees who are not following company-mandated procedures, saving hundreds of thousands of dollars annually.

Beyond security and loss prevention, facial recognition can help businesses identify key customers. This

can be particularly beneficial in retail and hospitality settings, where staff can be alerted when a VIP enters a store or approaches the front desk. Knowing when a key customer is present can help these businesses provide prompt and personalized attention.

License Plate Recognition

License plate recognition (LPR) analytics improve general surveillance by cataloging license plate information from parking lots, drive-up windows, ATM locations and entry gates, allowing security teams to search the data quickly and find evidence on vehicle-related activity. Using this technology, banks can identify license plates that correspond to fraudulent activity at outdoor ATMs, and schools can identify vehicles that are not permitted to be on campus.

On the business intelligence front, companies that provide valet services are using LPR to provide better customer service by tracking and analyzing customers’ wait times and helping expedite evidence for damage claims.

A Canadian auto repair chain relies on LPR to track cars that come into

the service station to ensure that each vehicle has a service order assigned to it. If a car enters the service station without an order, not only is the company liable for the vehicle, but it could potentially lose money on work being completed without payment. LPR analytics enable station managers to avoid these problem areas.

Another powerful opportunity for LPR is in the parking industry. A Philadelphia-based parking management company achieved significant business efficiencies by leveraging LPR technology. Instead of requiring attendants to walk the garage nightly and manually record license plates, all plate numbers are now captured by video as cars enter the garage. If a customer loses a ticket, he or she can simply provide the vehicle's license plate number and a customer service representative can run a search using LPR analytics to determine how long the car was in the lot. In addition, if customers forget where they parked, the same tool can identify the location of their vehicles in the garage.

For the parking garage's security managers, LPR can provide valuable

evidence of criminal activity. A repeat burglar who had been breaking into vehicles in a parking garage over a six-week period was eventually caught because garage management was able to use LPR to identify the suspect's vehicle. The next time the criminal entered the garage, an email alert was sent to security personnel, who were then able to immediately notify police and catch the suspect in the act.

Motion Detection and Object Tracking

Motion detection and advanced object tracking allow organizations to search video based on specific criteria, such as motion, direction, speed, color and size. When combined with other

analytics, such as facial recognition and LPR, this information can accelerate investigation times by narrowing the search results. For example, searching for a red car going in a certain direction with a specific license plate or partial plate number will generate far

fewer video clips to review, saving investigators valuable time.

Initially, the most common use of motion detection analytics was for perimeter protection. In this case, analytics can generate an alert if there is movement across the perimeter,

Deploying an enterprise-wide VMS empowers organizations to leverage a single platform for recording, streaming, viewing and analyzing live video from any number of surveillance cameras for both security and business intelligence applications.



such as the opening of a gate, fence or doorway. If you are installing a security system to protect a business after hours, then basic motion detection may be all that is required. However, if you want to be alerted anytime someone enters a specific area, a tripwire analytic could be an alternative, since it will not interfere with the rest of the scene. Directional motion analytics can alert a security officer when a person or vehicle is going the wrong way, such as entering at an exit point.

Motion detection can also be used to create heat maps that illustrate the flow of customer traffic in retail locations. This allows merchandising teams to observe actual areas of shopper interest based on traffic density. By seeing where shoppers go most often, merchandisers can refine store layouts to maximize conversion and make it easier for shoppers to find what they are looking for. Heat maps can also identify opportunities to charge more if vendors want premier placement in high traffic areas.

Dwell Time and Loitering

One of the newer types of analytics on the market enables security

managers to monitor dwell time or loitering activity.

One example is a commercial parking management company that is using dwell analytics to protect revenue and find evidence of crimes in unmanned parking lots. These facilities have parking kiosks where customers enter their parking spot number to pay. The company discovered that criminals had started impersonating attendants, telling customers the kiosk was broken and taking their cash. Security teams used the dwell analytic to generate an alert whenever someone was seen loitering near the pay station. This allowed them to catch criminals on multiple occasions, protecting the company's revenue, as well as ensuring customer safety.

Dwell analytics can be used across a variety of industries to find evidence of loitering and secure remote or unattended areas that might be used for illegal activity. The analytics can automatically send an alert when anyone is seen loitering in these areas so that security management can examine the situation.

In retail stores, dwell time analysis can also be an extremely valuable

business intelligence tool, helping managers evaluate merchandising and promotion decisions. It can measure where people are spending time within a store to determine whether certain promotions or displays are generating the desired customer traffic. This provides key insight to the marketing department, which can then make any necessary adjustments.

People Counting

People counting video analytics are increasingly in demand as retailers try to determine conversion rates. A critical component in increasing conversions is understanding baseline conversion rates. To do this, it is essential to have accurate current customer counts. There are many solutions available to count customers. Testing is essential to ensure a particular solution is generating accurate counts. People counting can also be used to measure the number of customers that enter

areas around a promotion or to compare locations to measure store performance metrics. Some fitness studios are even using people counting

analytics to track class attendance as a measure of instructor performance.

Measuring store traffic is also valuable for security purposes as staff can receive alerts when restaurants or clubs reach capacity limits. It can also be used to measure traffic in key areas like customer service, returns or changing rooms.

Video Analytics Beyond Security

As we have seen, video analytics offer benefits beyond just security applications. Personalizing the customer experience is a top priority across many industries. Understanding

customer behavior is critical for retailers to remain competitive in today's multi-channel retail shopping environment.

In financial services, streamlining operations is critical as the industry continues to recover from the recession. Financial institutions are focused on leveraging self-service channels, such as online and mobile banking,

in order to reduce the real estate and personnel costs of physical locations. By capturing information about customer traffic patterns, video analytics can

Video analytics are most powerful when used in combination with each other. Leveraging a detailed analysis of in-store activity with people counting, dwell patterns, and heat maps, and correlating that information with POS data and transaction amounts offers managers and executives valuable insights to inform business strategy.



deliver data to inform staffing and other operational metrics, reduce wait times, optimize promotional information and improve the customer experience. Consider how the following video analytics can deliver operational benefits for an organization and provide a competitive edge by leveraging real-time insights about customers.

Demographics

For retailers, demographic data is extremely valuable in measuring promotional campaign effectiveness. Demographic video analytics can be used to capture the age and gender of customers entering a retail location to help determine which local promotions drive the desired store traffic. This type of data can directly inform marketing strategy with information about store traffic patterns, customer reaction to displays, coupon use, and similar day-to-day activity.

Queue Management

Queue management analytics capture line lengths based on a minimum threshold, time of day, or marketing event, providing real-time data on customer lines and cashier availability for a variety of industries dependent on customer service. This data can help managers identify choke points and traffic flow patterns, optimize staffing, increase store operational efficiency, and improve sales performance and customer satisfaction. Understanding traffic levels can also provide insights to store real estate teams evaluating sales per square foot. This information is enabling many businesses to gain

a competitive edge by increasing operational efficiency while delivering the best customer experience.

The Power of Analytics

Video analytics are most powerful when used in combination with each other. Leveraging a detailed analysis of in-store activity with people counting, dwell patterns, and heat maps, and correlating that information with POS data and transaction amounts, offers managers and executives valuable insights to inform business strategy.

For organizations in financial services, retail and many other industries interested in taking advantage of the potential of big data and video, finding the right VMS platform is critical. To effectively leverage the growing quantities of video data being generated for business intelligence, companies need a VMS that includes powerful search, streaming video and video analytics. Running security and business intelligence on a single platform enables enterprises to utilize surveillance data to improve the customer experience, manage staffing levels, increase conversion rates, optimize real estate usage, analyze performance across locations and, ultimately, improve the bottom line. ■ **Back to TOC**

Jeff Karnes (info@3vr.com) is senior vice president of marketing and operations for 3VR (www.3vr.com). 



The need for data is not slowing down. Keeping this data locked into individual applications and appliances only slows innovation and increases costs. It is no longer acceptable to throw an appliance in a rack and call it a day.



The Public Safety Data Lake

Making the right decisions regarding storage and other issues can vastly increase the value of video surveillance

For years, surveillance has largely been deployed either as a closed system or on an appliance. The reasons are understandable: Most customers, companies and partners come from the CCTV days where every system was closed, and that is just how it worked.

Then IP video came along and turned the surveillance market upside down, bringing in new technologies, new vendors, new partners and new challenges. The surveillance industry has finally made the turn where IP is the standard rather than the exception. But the dirty little secret of the sector is that, even though the technology is based on IP, the deployment still often looks like a closed system. The cables are different, muxes have been replaced with switches, and 150GB DVRs have been replaced with 50TB NVRs, but the way the surveillance systems are deployed still results in

By Ken Mills
EMC



closed systems. The data is locked inside the DVR or NVR. The video management applications are bound by the appliance with which they are packaged. And customers are

often forced to upgrade hardware and software together. At the end of the day, almost all of the value that surveillance can bring to a company, an institution or a government is locked inside a black box.

There is potential, though, to unlock the value of the surveillance data and make it truly portable. Once that happens, it can be shared across applications, moved across on-premise and off-premise boundaries, and ultimately bring much more value to end users.

There is no better example of the need for data to be portable than the public safety market. Today's public safety operators, offices and users require access

to many types of data above and beyond surveillance data. There is a proliferation of body-worn cameras across the country and around the world, and data from these devices can add up fast, even in medium-size police departments. Storage requirements can average as much as 1TB per camera per year, so even with only 500 cameras, a police department would need 500TB of storage annually just for this application.

Body-worn cameras are now grabbing a lot of attention in the news, forcing many police agencies to make knee-jerk decisions on a solution. And while wearable cameras

The dirty little secret of the sector is that, even though the technology is based on IP, the deployment still often looks like a closed system.

are an important part of the evidence story, they are not the only piece of the security equation. Police agencies also need to store and manage video from surveillance cameras, crime scene footage, digital evidence, interview rooms, mobile devices, unmanned aerial vehicles, and many other evidence inputs. Add in storage for license plate readers, GIS mapping, and in-car cameras, and the need for enterprise storage can be significant. And this does not take into account the addition of data coming from the

explosion of the Internet of Things.

The need for data is not slowing down. Keeping this data locked into individual applications and appliances only slows innovation

and increases costs. It is no longer acceptable to throw an appliance in a rack and call it a day.

The Public Safety Data Lake

Organizations are looking for an architecture that accommodates all of these new devices and the rapid growth of data so that they can finally realize the value that is currently locked in their closed systems. One emerging concept in the surveillance industry is the surveillance data lake. As it applies to public safety, a surveillance data lake is made up of several key pools of data feeding in from different sources, such as in-car video, video cameras,



body-worn cameras, and drones. From this pool of data, organizations can perform critical activities based on their needs, including analytics, evidence management, and anomaly detection. This data needs to be secure, reliable and available to multiple user groups across key applications.

With an estimated 54 percent of their data going unanalyzed, federal organizations are missing many opportunities for applications and insights, including crowd counting, anomaly and incident detection, face matching, safety alerts, traffic monitoring, object recognition and suspicious behavior. Data is growing so fast that these organizations simply cannot find a way to scale, let alone analyze.

But while scale is clearly a challenge here, understanding what should serve as the foundation to the data lake architecture can be even trickier. Should users go on-premise or cloud? If on-premise, do they have distributed

or centralized architectures? If they want to be in the cloud, how do they ensure easy access to the data? When they need to quickly access data for evidentiary support, will they need to dig through piles of storage to find it? How do they decide between private, public and hybrid versions of the cloud? What about a mixture of on-premise and cloud? Choosing a storage vendor alone, before even thinking of analytics, applications, etc., can be daunting and exhausting. And public safety organizations being in the public eye only heightens the pressure.

Forward-thinking public safety departments build a data platform that can collect, store and manage this data. A data lake infrastructure provides a more cost effective storage environment with the ability to seamlessly integrate new types of devices while gaining more control over the data. Finding a storage vendor that offers this type of open platform is critical to moving toward



this enterprise model, which will prove more cost effective, will be less complex to manage, and will allow for more innovation and the flexibility to add applications and gain value from surveillance data.

The Storage Layer

Storage is the foundation layer of the data lake architecture. The storage layer must support an open platform capable of managing disparate data sets from multiple devices while addressing the challenge of scale head-on. There are three major surveillance architectures out there today: distributed, centralized and cloud. Some companies have distributed-only environments. Some have only centralized environments.

Some use both on-premise and cloud architectures for different purposes, while others go cloud-only. The following section explains the differences between these storage environments.

Distributed Architectures

Distributed architectures store video and surveillance data locally and then periodically transfer the digital data set to the central platform. An example of this might be a satellite police station that stores data in the office but, from time to time, transfers the data over to headquarters. Distributed architectures often integrate the data with applications and other systems, such as access control and intrusion detection,





without engaging a central server. The resulting architecture reduces single points of failure and distributes processing requirements over many smaller sites.

Choosing the right storage vendor for distributed architectures can be made simple by answering the following questions: Is the vendor offering high bandwidth at a low cost per GB? Can the configurations be described as “plug and play,” that is, simple and straightforward to deploy? Does the vendor make virtualization easy for future growth?

Centralized Architectures

Scale is the primary consideration with centralized architectures. Centralized surveillance architectures – commonly used by police headquarters, schools, governments, airports and energy companies – host high device-count environments and are able to support large amounts of surveillance data. Storage must be made efficient in centralized architectures, and utilization rates must

be high to prevent price creep. Since retention times and pixel/resolution quality are forever changing, migration time to apply these changes must be extremely low, if not non-existent.

Some companies use a *converged* centralized architecture when they need a total, extensible solution that consolidates systems. Components of a converged surveillance infrastructure may include servers,

data storage devices, networking equipment, and video management/surveillance software for IT infrastructure management, automation and orchestration.

Converged and non-converged centralized architectures solve different storage challenges. Both are ideal options for public safety organizations that need to scale. Both also commonly exploit video monitoring and analytics to increase security

and opportunity on the same platform, which is highly attractive to companies looking to simplify their business.

Cloud Architectures

The cloud has been causing some

As it applies to public safety, a surveillance data lake is made up of several key pools of data feeding in from different sources, such as in-car video, video cameras, body-worn cameras, and drones. From this pool of data, organizations can perform critical activities based on their needs, including analytics, evidence management, and anomaly detection.

confusion lately. One example is in the case of body-worn cameras. Body-worn data in most states has very different storage requirements depending on the offense. Video of routine traffic stops may only be kept for 30-45 days, while DUIs may be kept for three-plus years, and federal crimes may need to be kept for the length of the imprisonment or, in some cases, forever. Most states have laws that require evidence used in a case to be kept a minimum of seven years. This means that, overall, video from body-worn cameras has a long shelf life, which results in big storage needs.

Organizations must consider these long-term storage and data management challenges and think beyond three-year or five-year buying cycles, or they could end up with an inflexible and costly solution. While the cloud is affordable at the start, it is important to understand the cost implications when storage exceeds 1PB, and organizations are paying monthly storage and access fees for 25-plus years.

Going the pure cloud route, therefore, is not always the best option for public safety organizations. Choosing a vendor that offers both cloud and on-premise storage options

is a better bet as it will safeguard an organization's assets and allow for future growth. Many companies opt to go on-premise first with the bulk of their "cold," or long-term, storage, and then go to the cloud for deeper storage. This approach often is more cost effective, provides greater security, and simplifies application integration.

Some vendors offer cloud storage bundled with cameras, enabling customers to go cloud first and then go on-premise to save on long-term storage. This bundled option can

be much easier for surveillance newbies as the process of purchasing is made simple. However, it may not be the best option for organizations with high retention requirements or that need to frequently move data from local to storage and back.

It is, therefore, important for organizations to

weigh all of their storage options as there is no one-size-fits-all solution. Questions to ask in considering cloud providers include:

- Who owns the data?
- Will the data be subject to the Patriot Act?
- What happens if the organization changes providers? Will the data be lost?
- What are the short-term and long-term costs?

A data lake infrastructure provides a more cost effective storage environment with the ability to seamlessly integrate new types of devices while gaining more control over the data.



Cyber/Data Security



EAS



Fire & Life Safety



Intrusion Detection



Video Surveillance

- What are the benefits of going cloud vs. on-premise?
- Will the organization have easy accessibility and/or control of the data?
- Are there long-term network costs?

Beyond Storage

Just a few years ago, the surveillance architecture conversation would have stopped at storage. Today, there are a number of ways to

protect and gain greater value from surveillance data. Having architectural storage options is crucial to scaling any surveillance solution, but, with an open platform, organizations can maximize their storage investments by partnering with video management/surveillance software providers, securing their data, virtualizing their infrastructure, and integrating applications and analytics.

Virtualization

Virtualization can be considered the “enablement player” of the surveillance





data lake. Instead of having 50 servers, organizations could have just two. When applied to the surveillance architecture, virtualization reduces physical complexity and points of failure while improving the overall system resiliency. This becomes increasingly more important with the addition of devices such as body-worn cameras and drones. It is much easier to add new devices and account for the impending “big data blast” with a virtualized infrastructure than with a non-virtualized infrastructure. Virtualization creates an open platform and future-proofs investments by giving public safety organizations access to the applications they need at the time they need them. Virtualization also helps to prevent vendor lock-in, which is critical to the idea of the data lake.

Organizations should consider virtualizing if the answer to any of the following questions is yes:

- Are our servers eating up our overhead?
- Will we be adding new types of devices in coming years?
- Will retention time requirements increase?

Security

When applying security to a data lake, it is important to consider authentication and auditing to ensure that the right people have access to the data. This can include checking who is viewing, downloading or printing certain data. Surveillance security solutions would, for instance, help a company catch an employee

who entered his or her office building and inappropriately printed documents on a weekend. The costs of a data breach (in terms of both revenue and reputation) can be easily avoided with the addition of security to the surveillance data lake.

When considering a security vendor, organizations should ask:

- How are we securing access to our data?
- Who and what do we need to protect?
- Does society have a spotlight on our organization?
- Are we willing to bet on the cost implications of a data breach?

Applications

Surveillance applications are increasingly becoming valuable assets to businesses. Applications such as transport mechanisms can seamlessly transport data from disparate devices to distributed, centralized, and even cloud storage. This mechanism becomes a critical saver of resources when an incident occurs and the organization needs to quickly find a piece of data. The transport mechanism can simplify efforts by significantly decreasing time to value and freeing up resources.

Organizations that need to access their data quickly and/or move their data in and out of storage should consider adding applications to their architecture.

Analytics

Another emerging trend is the increasing impact of enterprise analytics on surveillance data. Today's



analytics are mostly pixel-based, and they have proven to be less than 100 percent reliable. Once surveillance data is part of a data lake, organizations are able to analyze all of the data at one time using multiple analytic solutions. Software is available that can take very large surveillance files and organize them so that analytics can be applied across all the data at one time. The result is the ability to analyze large amounts of data quickly, or, at least, much faster than with pixel-based solutions. Once the data is organized, an organization can apply analytics applications and business intelligence tool sets to search for trends and anomalies, as well as integrate with other data across the enterprise.

This technology can also be applied to use cases like video indexing to enable content-based video search, traffic analysis based on trajectory analysis for optimizing city transportation, and more. Once the structured insights are extracted, adding other data can generate deeper insights from siloed data sources to, for example, help correlate retail stores' surveillance video with transaction logs.

Putting It All Together

Navigating through the new world of surveillance is not an easy task, especially considering the industry dynamics and growth trends in play. Three good general steps to follow are:

1. Commit to using an open platform via a surveillance data lake architecture.
2. Do your storage homework. Consider on-premise (distributed and centralized) and cloud offerings. A storage vendor that offers both on-premise and cloud can provide the most bang for the buck. Make sure this vendor has strong VMS relationships and a healthy partner ecosystem. A good storage vendor will provide VMS sizing guidelines, reference architectures, and implementation guides to ensure success.
3. Go beyond storage. There are many ways to realize value from data and future-proof investments. An open data lake platform will provide the flexibility needed to add security, virtualization, analytics and applications to storage solutions.

Regardless of the makeup of the architecture, an open platform, ownership of the data, better security, and the ability to integrate with other applications are all critical requirements. A surveillance data lake will help store and manage these different pools of data and protect an organization into the future.

■ Back to TOC

Ken Mills (ken.mills@emc.com) is senior manager for global business development at EMC (www.emc.com). 



With more than 165 million surveillance cameras already installed globally, and with more than a 20 percent annual growth rate expected moving forward, CSOs and their organizations are demanding better means of ensuring that their security and surveillance networks continually operate at peak performance.



Keeping the Security System Secure

Ensuring that video stays online is key to managing risk

On a Tuesday morning in 2001, it became very clear that many of our fundamental perceptions about how to conduct business would have to change, especially with regard to security. Since that day, the development of new security technologies has accelerated at a rapid pace along with our expectations that people, property and assets will be protected.

The last few years have, accordingly, seen growth in the recognition of the importance of a C-level title for security – the chief security officer, or CSO. While adding security to the C-suite demonstrates an organization's commitment to safety and protection, it also designates an individual who holds the ultimate responsibility for security and is accountable for anything that might go wrong across myriad facets of an organization.

As a result, today's CSOs carry

By Bud Broomhead
Viakoo



a heavy burden. In addition to identifying and implementing the most effective technologies, systems, policies and practices, these professionals also own the growing scope of risk their



organizations face on a daily basis. That risk could come in many forms, including liability for on-site incidents, maintenance of organizational compliance with standards and regulations, insider threats and much more. In the face of this ever-expanding range of potential issues, CSOs' need for answers to tough questions is also growing.

Since 9/11, the paradigm of professional security has changed. The Internet and the growth of IP-based networked security systems have given us access to reams of data, generated by a widening

range of advanced technologies, for situational awareness, risk management, event response, and communications.

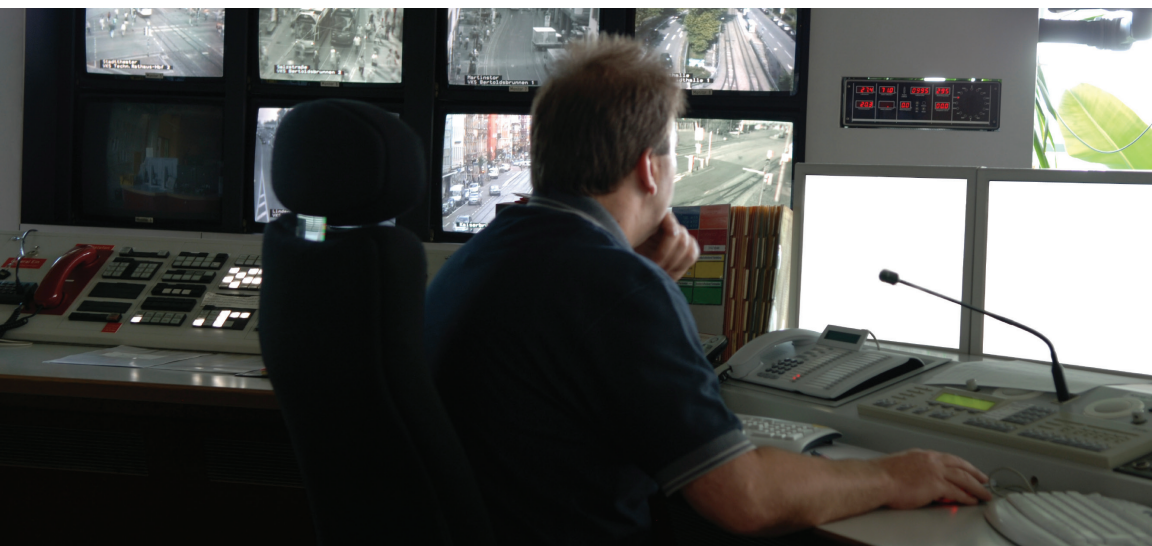
A security and surveillance network has multiple IP-connected elements – cameras, encoders, switches and storage – each of which leaves the system open to vulnerabilities. Whether the devices reside on a network of their own (a best practice) or on a larger network backbone, CSOs must ensure that the security and surveillance system itself is secure.

This flood of data is certain to continue growing, providing more reasons to look to security systems for information to which sophisticated analytics and data processing risk management algorithms can be applied.

A significant share of this data is generated in the form of video. Video surveillance has gained

tremendous traction in every type of organization and facility around the globe, and surveillance cameras





are nearly always in sight. Video is constantly being transmitted, recorded, watched, archived and analyzed, and data from video surveillance systems have become essential to identifying criminals, gaining insights into events and protecting organizations from liability.

By their nature, physical security devices are endpoints on a network, and they are attractive targets for people seeking to gain unauthorized network access. Failures in cybersecurity can allow hackers to take control of critical systems, and when it comes to video surveillance or physical access, the stakes can be especially high. Also important from a cybersecurity standpoint is detecting and preventing any tampering with these systems, especially during a retention period required for compliance.

A security and surveillance network has multiple IP-connected elements

– cameras, encoders, switches and storage – each of which leaves the system open to vulnerabilities. Whether the devices reside on a network of their own (a best practice) or on a larger network backbone, CSOs must ensure that the security and surveillance system itself is secure.

For the CSO, the owner of all risk within the organization, the importance of video to mitigating risk and managing security programs cannot be overstated. Two minutes of recorded video can save a corporation millions of dollars in a lawsuit or keep executives safe from prosecution or incarceration in a criminal investigation. Real-time video can help pinpoint the location of an active shooter and help to save lives. Sophisticated analytics can identify an individual trying to breach the perimeter of a critical infrastructure facility and send an alert to an administrator, prompting a quick response to keep people safe from a

wide range of threats. In all of these situations, it is easy to recognize the disastrous consequences that would ensue if, at the critical moment, when the video was most needed, the display screen was blank.

The conversation about video reliability and quality of service is long overdue. With more than 165 million surveillance cameras already installed globally, and with more than a 20 percent annual growth rate expected moving forward, CSOs and their organizations are demanding better means of ensuring that their security and surveillance networks continually operate at peak performance.

Missing video is a risk that CSOs simply cannot take. The most common modalities to maintain video systems – spot-checking, scheduled maintenance and environmental monitoring systems – cannot ensure that video will always be available and there will never be a

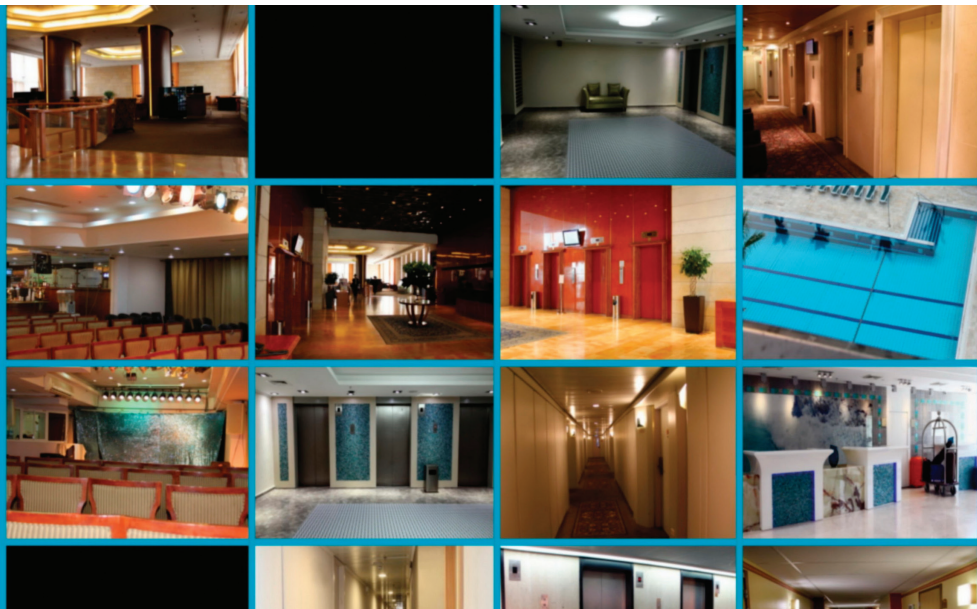
In many instances, serious issues with a video system's performance go undetected until investigators are searching for a particular event or segment of video, only to find that it is missing. As video systems grow in both physical scale and role in today's risk management and security programs, anything less than 100 percent video uptime and retention compliance is a significant brand, financial and life safety liability.

missing segment. Further, as networks continue to grow in complexity, it is becoming increasingly difficult to afford even those limited resources. Remote locations and small sites only add to the complexity. At times, even when all components appear to be working properly, there can still

be moments when the video stream is interrupted – a condition that can no longer be tolerated.

With storage costs continuing to decrease, organizations are finding it advantageous to retain data for longer periods of time, especially as the nature of threats like industrial espionage and organized retail theft can take significant

time to uncover. What is essential is making sure there are no issues, problems or interruptions in the video stream so video information will be available for review. This raises a major question: How are CSOs managing the performance of their video surveillance infrastructure?



Unfortunately, despite major advancements in video, there's a good chance a CSO has very little visibility into his or her surveillance network. Even if video is being displayed on an organization's high-definition screens, this by no means guarantees that it is being recorded properly. In many instances, serious issues with a video system's performance go undetected until investigators are searching for a particular event or segment of video, only to find that it is missing. As video systems grow in both physical scale and role in today's risk management and security programs, anything less than 100 percent video uptime and retention compliance is a significant brand, financial and life safety liability.

Beyond incident-related video, some organizations, such as hospitals, require video footage to demonstrate compliance with

industry or government standards and regulations. For health care organizations, these might include regulations or standards for ensuring patient privacy or properly managing and tracking medication. When that video is not available, the results could affect patient safety and the handling of controlled substances, potentially damaging a hospital's reputation, which not only could affect its bottom line but could also hamper the facility's ability to administer the care and treatment its patients require.

These potential negative outcomes clearly illustrate the importance of maintaining a reliable video infrastructure. As the security industry moves toward a new model of predictive analytics, the need for a consistent and dependable flow of information is only increasing.

Communication about physical

security issues has both immediate and long-term effects. The immediate impact of slow communication is increased risk to the organization; the longer-term impact is poor visibility into emerging threats and less time to plan effective strategies to counter them. Not only must data be available quickly, it also must deliver actionable intelligence and information. Physical security solutions that allow users to gather and examine data are critical to effective planning. Solutions that enable analysis of physical security network behavior across time, geography and multiple types of events are very effective in

Technology ultimately delivers solutions to the issues it creates, and, fortunately, the same accelerating research and development that is driving new security technologies across myriad platforms is also delivering a host of new solutions to secure the security systems themselves – a sort of meta-security that is gaining traction as integrated systems become more complex.

getting quickly to insights.

Technology ultimately delivers

solutions to the issues it creates, and, fortunately, the same accelerating research and development that is driving new security technologies across myriad platforms is also delivering a host of new solutions to secure the security systems themselves – a sort of meta-security that is

gaining traction as integrated systems become more complex. For CSOs, these solutions are quickly proving their return on investment (ROI) by helping to maintain a higher level of protection and safety from threats and their consequences.

As a result of these technological developments, it is now possible to bring crucial reliability to existing IP video networks and ensure that all video is available when it is needed. New solutions continuously collect thousands of points of diagnostic information from across the video system infrastructure, capturing valuable performance metrics to provide intelligent, actionable





intelligence to a command and control center. Without ever touching video content, the software analyzes the video stream. Any failures or interruptions are quickly detected, problems are diagnosed and security and/or IT personnel are alerted, mitigating or eliminating the problem of missing video. When a crime, claim or other incident needs to be investigated, the video is there. When the need to demonstrate regulatory compliance arises, the video is there. The solution is easy to implement, efficient and conveniently manageable from users' mobile devices.

For CSOs, ensuring the availability of uninterrupted video is no longer optional. There is far too much at stake, and video has become far too

important in the overall architecture of the security system to take that sort of risk. Thanks to new technology, the expectation of reliable video is now a reality – one that increases security levels and improves the effectiveness of investigations and compliance while also delivering the ROI that today's high-quality video surveillance systems should provide. Deploying a solution that can eliminate missing video relieves at least some of the burden that CSOs carry day in and day out, and ensures that the day will soon come when CSOs can shift their focus away from those concerns and reduce their organization's exposure to risk.

■ **Back to TOC**

*Bud Broomhead (bud.broomhead@viakoo.com)
is CEO of Viakoo (www.viakoo.com). *



Amid the increasing deployments of security technologies that incorporate IP communications, the need for detailed reporting and diagnostics has become more prevalent, and to ensure the performance and effectiveness of systems, those capabilities must extend to the most basic building blocks of security.



Maintaining Power

New network communication solutions can minimize system downtime

As the security industry continues its migration from analog to IP-based surveillance and security systems, there is a great deal of focus on implementing networked systems with higher levels of integration. With ongoing advancements in networking, security managers are increasingly looking to deploy improved means of achieving network communications between what had been separate systems. These interconnected systems can make possible higher levels of situational awareness and security thanks to the ability to share information and data between multiple security and non-security systems.

Given the move toward integrated, network-driven systems, it should come as no surprise that the demand for Ethernet connectivity has evolved into a need for network communication. In addition to establishing more advanced levels

By Ronnie Pennington
Altronix



of connectivity between systems, networking allows users to remotely manage a full range of security devices and report vital data and diagnostics on a single, unified platform. This



model is proving to be both highly efficient and cost effective.

To date, most resources have been spent on integrating the top-line solutions, such as IP video surveillance and access control, which have significantly benefited from the facilitation of communication between cameras, access controllers and their respective head-end solutions, including video management systems (VMSs) and access control

platforms. These solutions have come a long way in delivering remote monitoring and control capabilities,

as well as providing end users with the benefits of improved security, automation, reporting, system and device health monitoring and more.

At the same time, what has traditionally been missing from network communication solutions and tools that monitor the overall health of security systems is the ability to remotely observe, control and report diagnostics on those systems in real time from the core products

that make up their foundations: power supplies and transmission products. Amid the increasing deployments of

Network diagnostics, monitoring and communications capabilities deliver sustained integrity and operation of security systems, and organizations benefit from higher overall security while also reducing the liabilities associated with system downtime.





security technologies that incorporate IP communications, the need for detailed reporting and diagnostics has become more prevalent, and to ensure the performance and effectiveness of systems, those capabilities must extend to the most basic building blocks of security.

That important need is being addressed today, as new solutions are now available for power supply and transmission products that can fill this network communication void in mission-critical power distribution applications, allowing products at multiple sites to be easily integrated, managed and controlled remotely. These advanced components are making a significant impact on the way systems are installed and serviced,

as they allow security managers to deploy comprehensive network communication by choosing solutions that achieve the type of higher-level systems integration that has long been available in video surveillance, access control and other top-line security systems.

Among the functions these new network communication solutions enable are:

- Remote monitoring, programming and control
- Reporting of user-defined IP device parameters
- Grouping of multiple products based on user-defined parameters
- Grouping of multiple locations to delineate specific system sites and installations



- Automatic notification of system events
- Password-protected login with levels of authorization
- Event history log, which records all events and system modifications

In security, downtime is never acceptable, and Murphy's Law often applies. How many times has an organization gone through its surveillance archive to locate video of a particular event for investigation and/or prosecution, only to find that the specific camera that would have captured the event was down at that moment? In these cases, there is no investigation or potential recourse, which can end up costing a company a lot of money in litigation or other expenses.

This is why it is so vital to be able to monitor the overall health of multiple systems and devices. The most effective approach to system health is preventative maintenance, but even the most diligent preventative program will not solve every problem every time, making early intervention when an event occurs an essential part of a strong security solution. Solutions that enable fast responses for video and access control systems, for example, have long been used and have become an important part of ensuring

overall security and safety for organizations. The ability to accomplish this for the critical foundational components further strengthens the integrity and reliability of a security system.

Network diagnostics, monitoring and communication capabilities deliver sustained integrity and operation of security systems, and organizations

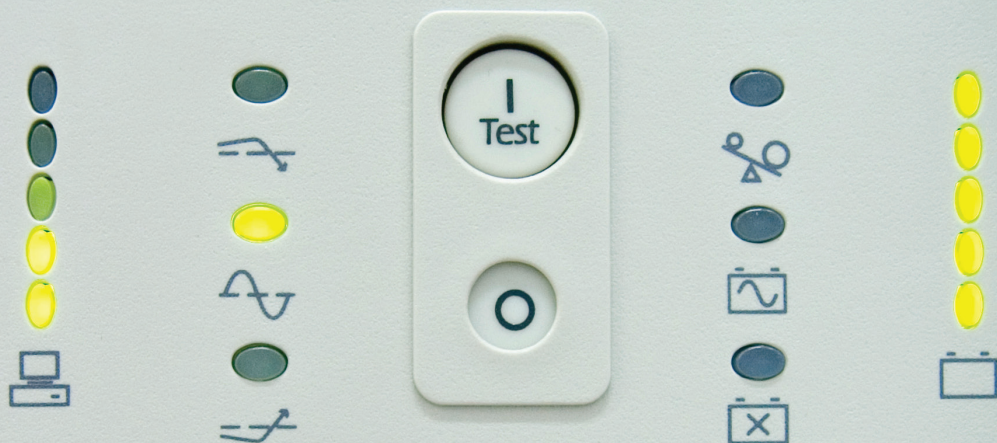
benefit from higher overall security while also reducing the liabilities associated with system downtime. As an added benefit, the ability to network, control and monitor all the core power and transmission devices completes the IP network

Real-time data from core power and transmission components allow system administrators to quickly diagnose and resolve problems that could otherwise take hours or even days just to isolate.

communication chain, thus creating a truly networked system.

Among the key communication features now available with power supplies and transmission products that allow organizations to streamline the process of diagnosing and correcting system issues are:

- Controlling and monitoring the DC voltage output to ensure that it is within range of the components being powered
- Monitoring and measuring the current draw to see if components are drawing too much power and if the peripheral device itself has



enough amperage for all the connected devices

- Verifying the actual total current draw to determine if additional devices can be added to the system.
- Monitoring temperature to determine if equipment is possibly in danger of shutting down or overheating
- Delivering the end user's preference of instant or delayed notification in the event of AC power loss
- Alerting users and/or service professionals when batteries need to be changed, ensuring system backup is up to date

From a maintenance and service perspective, real-time data from core power and transmission components allow system administrators to quickly diagnose and resolve problems that

could otherwise take hours or even days just to isolate. These advanced capabilities available in networked components allow organizations to achieve what could amount to significant cost savings by all but eliminating the need for unnecessary and often expensive service calls, while also contributing to the overall reliability of security systems.

As a result of networked communication, preventative maintenance and early intervention becomes more efficient, effective and accurate. For example, if a particular device goes offline, the diagnostics and monitoring functions immediately alert security staff, who can quickly and easily isolate the problem and determine the appropriate course of action. Should the device simply need to be rebooted, the remote access capability allows users to perform this



procedure without deploying in-house personnel or calling in an outside service technician. Better yet, because devices are networked and can be accessed remotely, network and/or security personnel, or even managers, can reset the device from anywhere over an Internet connection.

Because they can all but eliminate unnecessary service calls, networked devices deliver reduced costs, while remote control, monitoring and diagnostics also make system setup, service and maintenance much more efficient, allowing

these processes to be completed more quickly and, by extension, cost effectively. Further, some manufacturers make application program interfaces available for their networked power supply and transmission components, allowing for

customization with partnered suppliers to enable single-platform control and open up a new realm of possibilities for system design, deployment and use. This further contributes to improving overall security while also reducing the total cost of ownership for power supply and transmission products, as well as the systems they enable.

Considering how important data

communication is to a networked system's integration and reliability, it is important, when evaluating components, to research and compare the feature sets and capabilities offered by various solutions to best integrate power supply or transmission devices. At a minimum, devices should include remote monitoring, programming and control; strong diagnostic and reporting capabilities; the ability to group multiple products and locations based on user-defined goals and parameters; and automatic e-mail and/

or simple network management protocol (SNMP) notification to send trap messages to authorized personnel when exceptions in an IP device's operation or status are detected. Additionally, all status updates, event notifications and device programming

changes should be recorded in a detailed event log on a product-by-product basis.

Last, but by no means least, access to the platform and individual devices must be password-protected with user-defined administration levels – *without exception*. To ensure seamless compatibility, ease of deployment, and reliability, it is also always

Because they can all but eliminate unnecessary service calls, networked devices deliver reduced costs, while remote control, monitoring and diagnostics also make system setup, service and maintenance much more efficient.

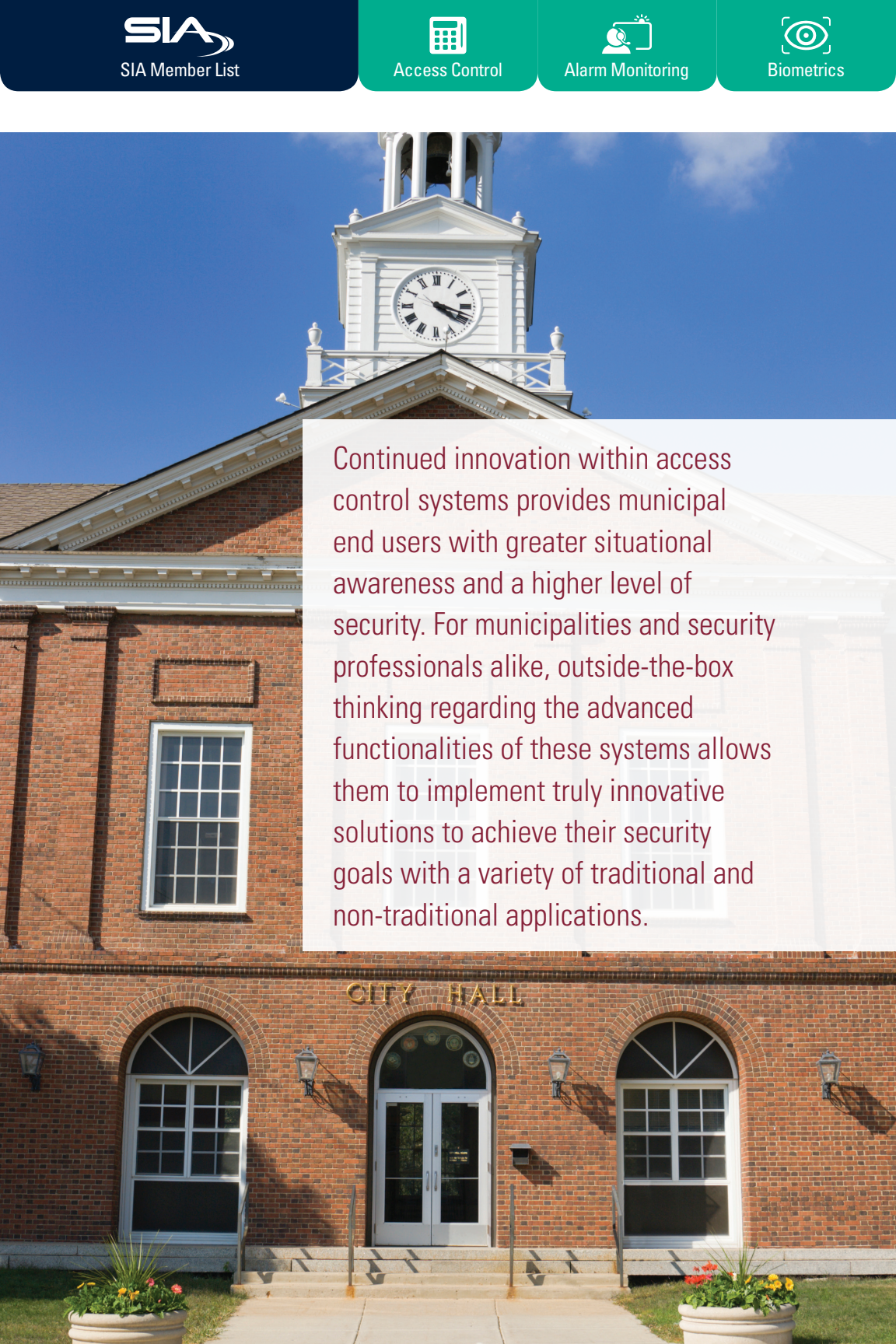


recommended that end users deploy devices from reputable manufacturers specializing in core power supply and transmission products.

Now that power supply and transmission devices are capable of networked communication, security professionals have the ability to deploy truly unified, comprehensive networked solutions. These foundational components of video surveillance, access control and other systems are raising the standard for integrated security and surveillance. Diagnostics and instant notification of issues empower end users to

correct potential problems quickly, without having to rely on costly and unnecessary truck rolls. As a result, end users benefit from knowing that the sustained integrity and reliable operation of their systems can significantly improve overall security, while reducing potential liabilities associated with system downtime. At the end of the day, that is what security is all about. ■ **Back to TOC**

*Ronnie Pennington (ronniep@altronix.com)
is national accounts manager for Altronix
(www.altronix.com). ✉*



Continued innovation within access control systems provides municipal end users with greater situational awareness and a higher level of security. For municipalities and security professionals alike, outside-the-box thinking regarding the advanced functionalities of these systems allows them to implement truly innovative solutions to achieve their security goals with a variety of traditional and non-traditional applications.



From Legacy Systems to Advanced Access Control

New solutions can offer extensive benefits to municipalities

For a variety of reasons, past technology implementations at the municipal level have tended to be fragmented with little regard for system integration or investment protection. Fortunately, this piecemeal, expensive approach is being replaced by more thoughtful, integrated solutions that offer reduced operational expenses and strengthened physical security.

Increasingly, municipalities are recognizing the potential of today's advanced access control solutions to accomplish these objectives. Across the country, local governments of all sizes are employing these new solutions over wide area networks to control, monitor and manage tenants across multiple facilities. To further enhance these solutions, many municipalities are also integrating mobile and remote devices for applications ranging from emergency

By Robert Laughlin
Galaxy Control Systems



call centers to mass transit monitoring and scheduling. These large-scale security networks are intricate but robust, and they are playing a critical role in the revitalization

of many communities and major metropolitan areas.

Continued innovation within access control systems provides municipal end users with greater situational awareness and a higher level of security. For municipalities and security professionals alike, outside-the-box thinking regarding the advanced functionalities of these systems allows them to implement truly innovative solutions to achieve their security goals with a variety of traditional and non-traditional

applications. Below are just some of the potential advantages that advanced access control systems can offer municipal government users.

Standardized Systems

Many municipalities employ multiple access control systems from multiple manufacturers. These legacy systems may not be able to communicate or integrate with each other, making management and maintenance tremendously – and needlessly – complicated. Even just a few years ago, a “rip and replace” plan would have been the most feasible option to bring uniformity to the municipality’s physical security systems – but that is not the case today.

The current availability of best-in-breed access control solutions that enable legacy systems to be upgraded and/or integrated is bringing new options to the table and, in turn, resolving many issues and eliminating the need to replace an entire system.

The current availability of best-in-breed access control solutions that

enable legacy systems to be upgraded and/or integrated is bringing new options to the table and, in turn, resolving many issues and eliminating the need to replace an entire system. By deploying an advanced access control solution, municipalities can create systems that standardize their existing array of diverse solutions into a single

interconnected system.

What makes this solution possible is new brand-agnostic software that eliminates the barrier of integrating legacy hardware, as well as deployment of any brands in the future. Installation is also made easier because, in many cases, the legacy systems are most likely running on twisted pair cabling that can be utilized by the new system, adding to the cost efficiency of the upgrade.

Compatibility

In addition to buildings that house municipal offices, many other locations must also be secured, including maintenance facilities, parking garages, transit stations and more. Every site



is different – even among facilities that have been built using the same design and construction models – and each location presents a unique set of challenges. Addressing these needs with leading access control solutions is possible because legacy systems typically comprise a series of controllers that have embedded software to control specific activities or entrances. Essentially, the intelligence in the system is distributed to the access location entry points, with data sent back to a centralized location for system control. The flexibility of today's access control systems means that, in many cases, only the controllers must be replaced and new remote interface cards installed so that all operations can be controlled centrally.

Further, when special needs are identified, advanced access control systems allow custom deployments to

meet each facility's specific needs, even when legacy systems are involved. An example of an innovative application of this capability can be seen in custom elevator interfaces that establish specific rules for each credential holder that restrict access to floors with potentially sensitive areas.

Integration

Advanced access control solutions are capable of integrating with parking, video, time and attendance, identity management and other security and non-security systems to provide more complete information that enables better management of access control, including policies and procedures. For example, municipalities can integrate human resources and access control systems to allow personnel data to be used to populate and program identity card data fields to create access



control credentials. Another potential application would be to integrate access control and video surveillance systems with facial recognition technology to verify that people using credentials to enter a facility are who they say they are. This ability to integrate software and hardware brings new capabilities to the system that can help detect and flag abnormalities and then alert key personnel to a potential problem. Intelligence of this type also changes the municipality's physical security system from a reactive model to a proactive model and allows security management to be more focused and anticipate where problems might occur.

System and Information Management

The combination of solidly built hardware with an abundance of powerful software-based capabilities

has made access control systems the focal point of a municipality's physical security system. From a single control platform, users can monitor the state of the facility as well as share data with other systems, such as video surveillance, visitor management, time and attendance, fire/safety, photo imaging, badging, elevator control, and building management.

When access control systems throughout the municipality are standardized, personnel and operator activity can be tracked and analyzed for overall procedural improvements or for forensic auditing purposes. Reports can be generated that include alarms, door and card activity, roll call and many other factors. Powerful utilities allow the administration to query data selectively and configure and save unique report filters for future use.





The functionality of the converged system is also enhanced by ease of use. A real-time log of cardholders in the building or in a designated area provides a roll call report that is easily printed or viewed, helping management determine the status of personnel. Systems with a flexible database structure can utilize personnel data to populate and program cardholder data fields, while active directory support enables real-time identity management and individualized identity-based door access. This approach significantly streamlines the process, making

operations and personnel more efficient and offering municipalities the potential to save significantly on staff costs.

Advanced access control solutions are capable of integrating with parking, video, time and attendance, identity management and other security and non-security systems to provide more complete information that enables better management of access control, including policies and procedures.

Networked System

Municipal applications involve a potentially large number of employees spread across many sites, which makes the network backbone on which advanced access control systems live crucial. Of the available network topologies, fiber optic offers the fastest and most reliable communication between devices at multiple locations and the access

control management software. While the initial planning and installation logistics of bringing these networks to fruition can be complex, the payoff

is well worth the cost and effort. In situations where video surveillance is integrated with access control, municipalities benefit from the real-time situational awareness these combined solutions can deliver.

In the future, network appliances will come pre-configured for easier and more efficient on-site system setup, application installation and customization. For example, on-board capabilities will allow users to connect to the network appliance by launching a shortcut from any LAN-connected PC. This will greatly reduce installation time by eliminating

the need to deploy or install software and servers.

Wireless Communication

The emergence of wireless readers and networks has brought further innovation and heightened

This ability to integrate software and hardware brings new capabilities to the system that can help detect and flag abnormalities and then alert key personnel to a potential problem. Intelligence of this type also changes the municipality's physical security system from a reactive model to a proactive model.

performance by expanding the capabilities of access control solutions. For example, municipalities are now able to deploy wireless access control and other solutions at remote sites and/or in mobile locations, such as transit stations, buses and trains. Innovation in wireless

technologies allows these systems to tie in with each other and with access





control software to provide real-time situational awareness when and where it is needed.

It is important to note that the term wireless can be a misnomer, as what is called a wireless access control locking system is actually not entirely wireless. Although the hub communicates wirelessly with the door locking system, the hub is still hard wired to the control panel. Hubs are usually located in every hallway or corridor and can wirelessly communicate with multiple doors, preventing the need to individually wire each door. The systems typically have a range of up to 200 feet between the door and the hub and do not need line of sight. Installation of wireless locksets is relatively simple and tends to be less disruptive and require fewer after-installation repairs, such as repainting.

The combination of solidly built hardware and a variety of robust,

software-based capabilities allows an access control system to transcend its traditional role and become the single platform that enables users to monitor facilities and share data with other systems. The many innovative applications these advanced solutions make possible have the capability to deliver heightened situational awareness and overall security, and their potential uses are seemingly limited only by the imagination. As a result, advanced access control software and solutions provide a powerful platform for municipalities and security professionals who can think creatively to identify non-traditional applications and implement truly innovative solutions. ■ **Back to TOC**

*Robert Laughlin (robert@galaxysys.com)
is president of Galaxy Control Systems
(www.galaxysys.com). ✉*



Opportunities to leverage technologies that can deliver more data on security, risk mitigation and compliance have never been greater. Security executives need to re-evaluate their organizations' use of older architecture to gain the newest security benefits.



Unlocking the Door

Next-generation access control systems can offer new insights and greater security

Today, security leaders are getting a first look at the benefits derived from next-generation, IT-centric access control and identity management applications. Such solutions unify physical and logical security by replacing siloed systems with an integrated approach that is designed to ensure the protection of critical business assets. This new system architecture is inherently flexible enough to keep up with the dynamic IT infrastructures of government and corporate organizations.

Why is now the time to move to the next evolution of physical access control solutions? Admittedly, the physical security industry has moved slowly and cautiously into the converged world. Physical security and cybersecurity professionals typically remain separate. With the advent and increasing adoption of IP-based security platforms, the data of IT and

By Scott Sieracki
Viscount Systems



physical security systems share the same networks, but that is where the “convergence” ends. Without correlating information together into one solution, there is no way



to use that information to enhance situational awareness across the enterprise.

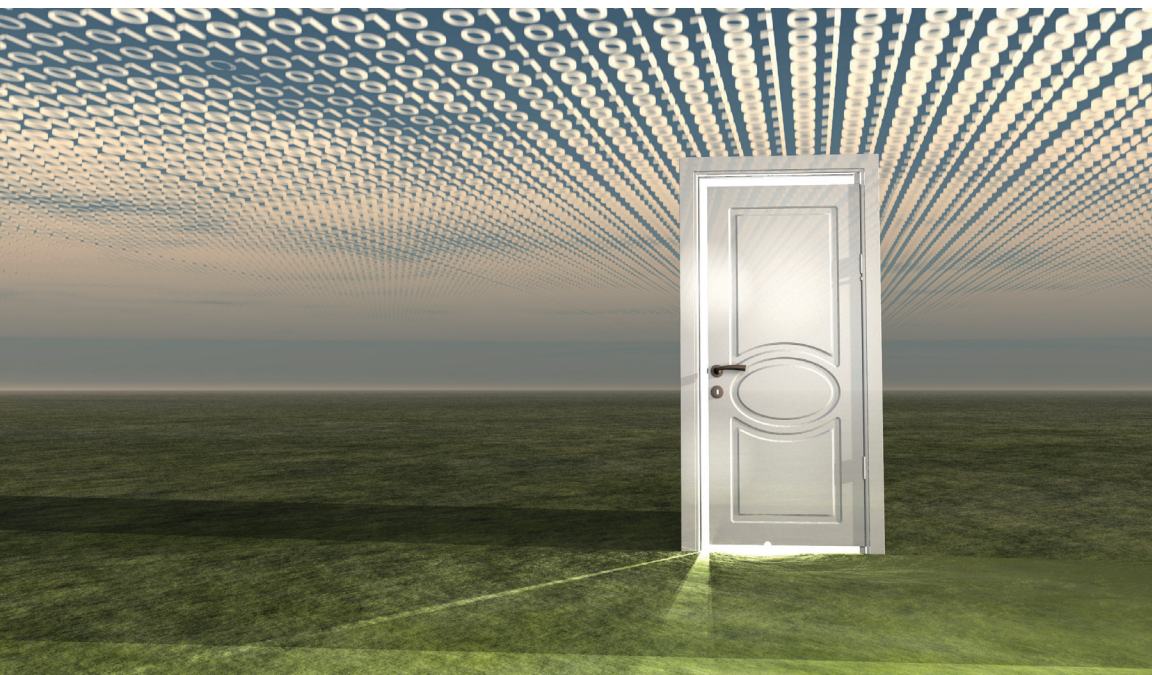
In today's risk-averse environment, security leaders need to know which individuals are accessing areas that are critical or high-risk. They need to correlate an employee's access privileges to a building in one geographic location with the same employee's logical privileges to a computer in another location to detect unauthorized entries. The combination of this data in a single, unified security

platform allows users to see trends, evaluate security protocols and identify potential breaches before they occur.

IT-centric access control solutions offer a significant reduction in upfront costs – from 20 to 40 percent less per door – because control panels and associated installation and third-party hardware are eliminated.

The risk environment has changed and legacy access control systems can no longer provide the value and benefit once promised. Opportunities to leverage technologies that can deliver more data on security, risk mitigation and compliance have never been greater. Security executives need to re-evaluate their organizations' use of older architecture to gain the newest security benefits.





Enterprises spend hundreds of millions of dollars purchasing proprietary access control systems, which are often based on 20-year-old architecture. These systems are costly to deploy and support and are not IT-friendly. Unfortunately, this type of deployment locks organizations into spending significant dollars on support and system management for siloed, ineffective security operations.

New IT-centric solutions provide a unique opportunity to move physical access control out of facilities management and into the native IT infrastructure. The idea of moving to a fundamentally different architecture may appear daunting to individuals who manage legacy deployments, but next-generation architecture actually simplifies system installation

and management by enabling it to fully leverage the enterprise's IT infrastructure.

Next-generation access control capabilities include computing and networking functionality, infrastructure management, and network and IT security. In the end, physical access control must be easily deployable throughout the enterprise, just like any other business application that utilizes networked end-point devices. At the application level, next-generation access control technology is built on adopted IT standards in order to gain synergies with identity and logical access management across the enterprise. These types of systems can easily integrate with other enterprise business systems to gain new levels of insight into critical

information and threat levels and to ensure business continuity.

IT-centric access control solutions offer a significant reduction in upfront costs – from 20 to 40 percent less per door – because control panels and associated installation and third-party hardware are eliminated. Since the application runs in any server environment (conventional servers, virtual servers, private/public cloud or on an appliance) and the entire client architecture is 100-percent web browser-based, the cost per door is significantly lower than a conventional system. This also dramatically lowers expansion costs and annual maintenance costs, driving down the total cost of ownership.

Cybersecurity is also enhanced. Cardholder databases, configuration parameters and card reader event histories exist only within the server software and are stored within robust IT security protocols to ensure data protection. Conventional access control solutions are vulnerable because information is stored on local devices and applications.

Next-generation access

Next-generation access control platforms are engineered for networking beyond internal communication among access control devices. They open doors to new levels of system intelligence by correlating real-time data from a wide variety of network devices and applications.

control platforms are engineered for networking beyond internal communication among access control devices. They open doors to new levels of system intelligence by correlating real-time data from a wide variety of network devices and applications,

including the Internet of Things, to obtain enhanced levels of situational awareness. Seamless information sharing enables more predictive capabilities and faster responses to maintain personnel safety and asset security.

A server-based solution drives real-time access decision-making based on role and policy attributes

provisioned through a common identity database. Additionally, 24/7 threat-level status, location data, access zone compromises and environmental safety updates allow users to extract valuable data from a more unified security management system.

As security evolves, system flexibility, interoperability and scalability are critical. Adding another door should be as simple as adding another end device to the network. The physical access control application



Case Study: Sun Health

Arizona-based non-profit Sun Health embarked on the next evolution of its access control infrastructure by deploying a new system to secure The Colonnade, one of its three Life Care communities.

The software-centric system allows The Colonnade's residents and staff to monitor and control entry to doors and elevators by sending commands to a central IT network, resulting in a high level of safety and security throughout the 40-acre community, which includes two recently built and two under-construction luxury villa towers, each with 36 residences. This system is also in use at the company's corporate headquarters, and plans are underway for expansion to other Sun Health senior living locations.

"The hallmark of our three Sun Health senior living communities is that we provide our more than 700 residents with safety, security and peace of mind," Sun Health President and CEO Ron Guziak said. "As we continue to grow and

upgrade our communities and the services we provide to our independent living residents and those we serve in our health and rehabilitation settings, we require a security system that is sophisticated and innovative."

The access control solution they deployed includes a software platform that allows IT personnel to manage both physical and logical security systems seamlessly. Entirely

web-based, it meets the stringent standards set by the Department of Homeland Security to protect federal facilities.

Maintaining the safety of residents, visitors and staff is a top priority for Sun Health, and today it has the same level of advanced protection that is often found in

government facilities. The complex access control needs of Sun Health are streamlined through the use of an IT-centric, next-generation physical access control solution that helps protect critical assets, staff and patients and that provides the wide array of benefits associated with operating a unified security management solution.

The access control solution they deployed includes a software platform that allows IT personnel to manage both physical and logical security systems seamlessly.



can run on a single server, but it also natively supports running in a virtual environment or in the cloud using the same deployment model the IT department uses for logical and network security solutions. This drives physical access control reliability to new levels, achieving high availability and resiliency in the same manner that Amazon, Facebook, Twitter and YouTube deploy their massively scaled, high-performance systems. Today's enterprise confronts

An IT-centric access control solution must fit into the overall enterprise identity management strategy in a more “harmonious and unified” environment, taking doors out of the realm of physical barriers and turning them into an IT asset that is provisioned based on identities, policies and attributes.

ever more complex and integrated risk levels. Finding a solution that can easily conform to an IT department's

technology roadmap, as well as its policies and practices, including Power over Ethernet, IT server redundancy, and end device auto-failover to alternate servers in the event of a server failure or network path outage, are

some of the most important qualities when identifying an IT-friendly solution.

An IT-centric access control solution



Cyber/Data Security



EAS



Fire & Life Safety



Intrusion Detection



Video Surveillance


must fit into the overall enterprise identity management strategy in a more “harmonious and unified” environment, taking doors out of the realm of physical barriers and turning them into an IT asset that is provisioned based on identities, policies and attributes. Access control solutions should be standards-based, with user configurable integration accomplished through established standards rather than custom integration through proprietary application programming interfaces and software development kits.

These next-generation access control solutions provide broad authentication technology support, accommodating a full spectrum of card readers, cards and electronic credentials, as well as native support for credential technologies with high-security features like challenge/response protocols and biometrics. This means that a migration to newer technology will be significantly

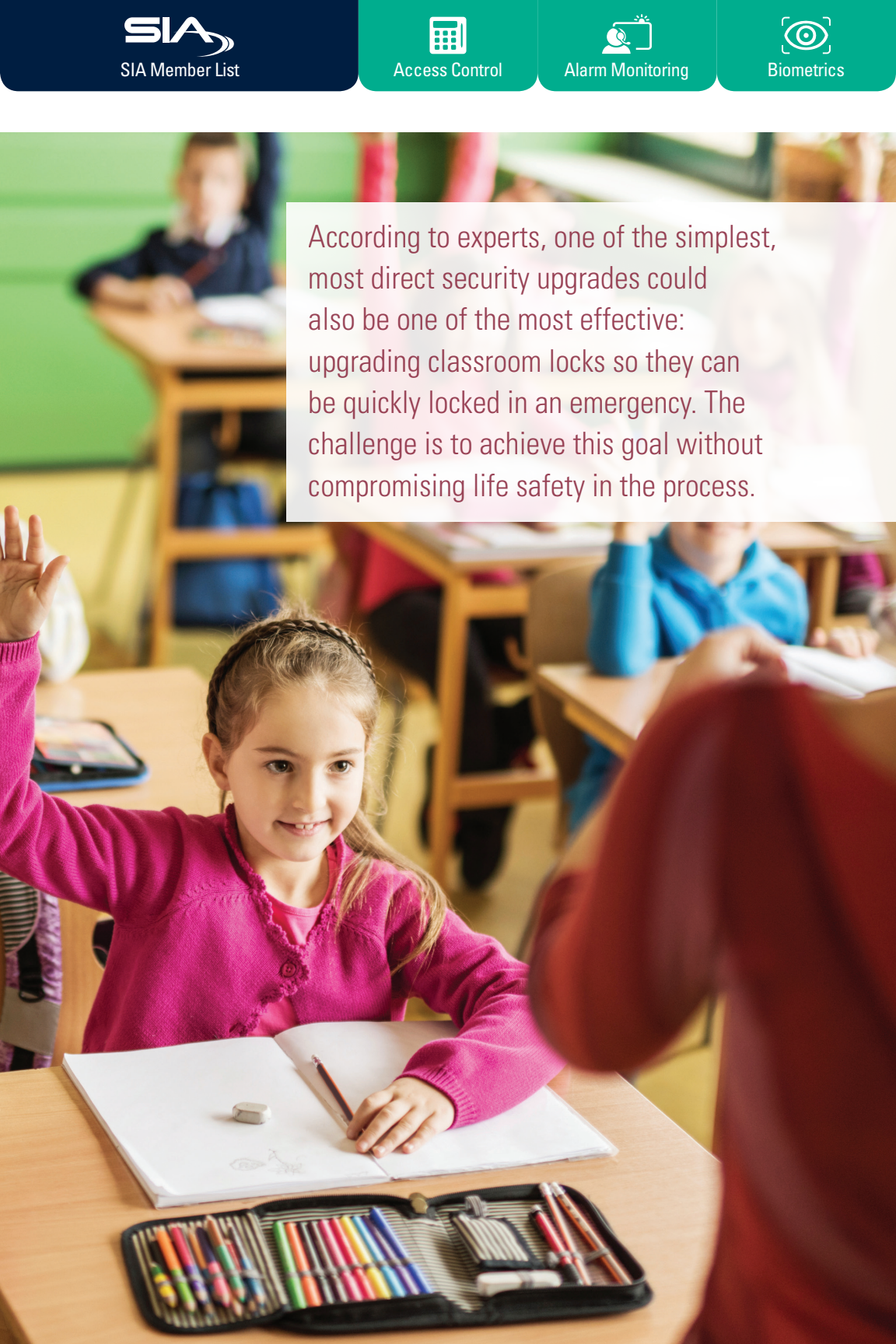
simpler to plan, execute and maintain than previous migration and integration efforts. Legacy access control systems were designed and built on decades-old network hardware technology and do not easily fit into an organization's IT infrastructure.

The implementation of next-generation access control architecture delivers many benefits. Enterprises that continue to leverage legacy deployments will continue to fall further behind, while taking on additional risks and costs. For most organizations, transitioning to next-generation physical access control solutions architecture is not a far-off future option, but a very real and immediate requirement.

■ **Back to TOC**

*Scott Sieracki (scott.sieracki@viscount.com)
is the CEO of Viscount Systems
(www.viscount.com). *





According to experts, one of the simplest, most direct security upgrades could also be one of the most effective: upgrading classroom locks so they can be quickly locked in an emergency. The challenge is to achieve this goal without compromising life safety in the process.



Striking the Balance Between Security and Safety

Classroom door locks are invaluable, but they must allow quick egress

Researchers confirm that crime rates have dropped considerably since the 1990s, and, actually, violent crime in the United States has been on a long-term decline ever since colonial times.

Nonetheless, we are living in a time when even infrequent crimes and terrorist acts strike at our core feelings of safety and security. Terrorism aims to create fear, so perpetrators look for relatively unprotected “soft” targets that will have high emotional impact. Groups of unsuspecting people have already been targeted at government facilities, business offices, movie theaters and public events. But perhaps the most shocking and painful violent acts have been directed at schools.

We may not be able to stop every attempted attack, but we can certainly take reasonable actions to secure potential targets – schools, in particular – to make it more difficult for perpetrators to achieve their goals.

By Mark Berger
Securitech



According to experts, one of the simplest, most direct security upgrades could also be one of the most effective: upgrading classroom locks so they can be quickly locked in an emergency. The challenge is to achieve this goal



without compromising life safety in the process, and that challenge can be met today with proper planning.

Note that, while this article will focus on increasing school security, these concepts are broadly applicable to other locations that might be targets. This is true whether the location is targeted for terrorist purposes or for other reasons.

The Urgent Push for Action

Whenever a violent act occurs, the conversation typically turns to some variation of how “we need to do something so this will never happen again.” Perhaps it is only natural that

we respond to horrific situations with a renewed emphasis on security, especially when children are involved.

Often, there is a lively debate about what corrective action or actions need to be taken, as a wide variety of possible solutions usually surfaces after the fact, along with a swift demand for action from the media and the public. Elected officials and others feel the urgent need for action, not only to appear properly responsive to their constituents, but also to take advantage of the heightened support for the spending or other resources required to implement solutions. It is particularly important at these times to carefully think through the proposed security actions to be sure that life safety implications are well understood.

Security and Safety

Implementing a new security procedure or tool often raises a new challenge: making sure the solution does not hamper life safety. Before discussing the case of school classroom locks, let’s see how this challenge played out in two aspects of air travel.

For the first example, consider the airport terminal building. Originally envisioned with the same design philosophy as train stations, airports were open travel terminals where a family could walk with a passenger all the way to the departing gate to see the person off. The phenomenon of airplane hijackings in the late 1960s and early 1970s led to new





policies and procedures. In the name of security, airports could no longer remain open environments, and people were required to go through security checkpoints before proceeding to the gate areas. Passengers now wait in a protected area, separated from the planes, runways and other operational areas. For security, this area is physically protected by locked, alarmed doors and windows that do not open.

These same locked doors, however, also serve a life safety purpose – as fire exits. They are fully accessible and clearly marked with signs; anyone in the terminal can open them and

exit the building without any special badges, keys or training. In some cases, the doors open directly onto the tarmac, a highly secured area.

Naturally, there are also large signs

warning that the use of these exits is restricted to real emergencies and opening the door will set off alarms. In fact, not only does a local alarm sound, but entire terminals have been evacuated, flights delayed and

airports closed when people have opened emergency exit doors. This causes a tremendous inconvenience to passengers, but it is one that is necessary in order to ensure there is safe egress in an emergency. This is an

Implementing a new security procedure or tool often raises a new challenge: making sure the solution does not hamper life safety.



example of respecting safety codes while meeting today's heightened security needs.

For the second example, consider the cockpit door aboard the airplane itself. On Sept. 11, 2001, the hijackers were able to commandeer the airplanes because the cockpit doors were not secured. As one response to that event, an electronic system was put in place on commercial airplane cockpit doors with a lockout feature that included a keypad lockout button and a toggle lock with a five-minute delayed entry. This system was meant to ensure that pilots could lock terrorists out of the cockpit, and it served the security need.

The possibility of a pilot going rogue and locking out other crew members was evidently not a high enough concern, and this lapse allowed the chain of events that led to the horrific March 2015 crash of a Germanwings flight. The very same security protocols that were put into place to prevent planes from being hijacked directly enabled the copilot to hijack the plane by preventing the captain from returning to the cockpit.

Life safety professionals and security professionals both look at doors and methods of operation, but each group asks different "what if" questions. Because the question, "What if someone in the cockpit wants to lock all others out" was not considered during the design process, a system was created that allowed this to occur.

Locking Classroom Doors

We are all too aware of the need to protect schoolchildren and teachers. While some providers have developed solutions for prevention and response, some of these address only the goal of preventing access to the classroom by a would-be assailant. As important as this goal is, as seen in the example above, securing classroom doors must never be considered from only one point of view.

Schools and classrooms are occupied on a daily basis by students and teachers. At times, a classroom may be unattended by an adult, allowing anyone inside to control the door and any locking devices. For years, this was the reason classroom door



Cyber/Data Security



EAS



Fire & Life Safety



Intrusion Detection



Video Surveillance

locking was regarded as an action to be controlled by a key, similar to a public restroom.

However, we now recognize the need to secure classrooms more quickly when an assailant is in a school.

Protecting students and teachers from an assailant, however, cannot sacrifice the critical role that doors and single-motion exiting play in life safety. Similarly, the ability of school officials and first responders to have speedy access into classrooms is critical at all times.

We can never tolerate a potential “cockpit door” situation in which someone in a classroom has the ability to prevent entry of authorized personnel. Products that may be effective in preventing forced entry

or “blockading” a door must never be installed if they prevent

authorized entry. The unintended risks and potential consequences of such devices are too great.

As one example, imagine the harm that could be inflicted upon a student imprisoned in a classroom by a bully. Certainly, this is not a situation any responsible school or public safety official would want to create, nor is it a liability any student, parent or school district should have as a consequence

of providing a door blocking device in the classroom.

Protecting students and teachers from an assailant, however, cannot sacrifice the critical role that doors and single-motion exiting play in life safety. Similarly, the ability of school officials and first responders to have speedy access into classrooms is critical at all times.

Recommendations from the Experts

There is no single federal agency that can dictate specific actions and



compliance for schools. Instead, decisions on what steps to take, and how quickly to take them, rest with local and regional school boards and superintendents.

Fortunately, there are highly qualified groups that have studied recent incidents of school violence and have prepared expert security and safety recommendations. Two excellent examples are the Department of Homeland Security (DHS) primer on safe school design, and the Final Report of the Sandy Hook Advisory Commission. The DHS publication provides specific recommendations for classroom door locks intended to keep occupants safe in the event of terrorist or criminal attack. In particular, DHS recommends door locks that can quickly be locked from the inside with a “simple locking mechanism, such as a button,” that “can always be opened from the inside for emergency egress,” and that can be opened from the outside with master keys. This guidance was published almost a year *before* the Sandy Hook incident.

Among the recommendations in the Sandy Hook Advisory Commission report, the very first one could be considered the strongest and most urgent. Referencing a report from

the Connecticut School Safety Infrastructure Council (SSIC), it states:

“The SSIC Report includes a standard requiring classroom and other safe-haven areas to have doors that can be locked from the inside. The Commission cannot emphasize enough the importance of this recommendation. *The testimony and other evidence presented to the Commission reveals that there has never been an event in which an active shooter breached a locked classroom door.*”

Products that may be effective in preventing forced entry or “blockading” a door must never be installed if they prevent authorized entry. The unintended risks and potential consequences of such devices are too great.

Clearly, experts agree that installing fast, strong locks on classroom doors is a highly effective means of creating a safe haven and saving lives. This makes them a very sensible first step to improve school

safety. The good news about this recommendation is that, among the many security modalities available for schools, physical door locks may be the most simple to implement.

Choosing the Best Locks for Schools

The following guidelines should help school officials make the best lock choice for their facilities:

- Locks designed for classrooms should comply with the intent



and specifics of the DHS primer on safe school design and the Connecticut SSIC recommendations. Installation should be easy, without the need to replace existing doors.

- The teacher or student closest to the classroom door in an emergency should be able to instantly lock the door from the inside.
- Speed and effectiveness are both important. The best solution is both fast and strong.
- It must also be possible to quickly exit the locked room. The best locks provide a single-action exit. This exit action is critical to protecting the safety of occupants.

- Authorized individuals with keys should be able to enter the room from the exterior. Some door blockers offered for classroom use prevent even authorized entry, putting occupants at risk.

School safety experts have spoken. With code compliant, cost effective products available, administrators everywhere can take immediate action to make their school systems more secure without compromising safety.

■ **Back to TOC**

Mark Berger (mberger@securitech.com) is the president and chief product officer of Securitech (www.securitech.com). 

SIA Technology Insights Article List

All of the articles published by *SIA Technology Insights* since it was launched in 2013 are listed below by subject. The edition in which an article was published is noted after the title:

F15: Fall 2015

S14: Spring 2014

S15: Spring 2015

W13: Winter 2013-14

F14: Fall 2014

J13: June 2013

All editions are available at www.securityindustry.org/techinsights.

Access Control/Identity Management

From Legacy Systems to Advanced Access Control (F15)

New solutions can offer extensive benefits to municipalities

By Robert Laughlin, Galaxy Control Systems

Unlocking the Door (F15)

Next-generation access control systems can offer new insights and greater security

By Scott Sieracki, Viscount Systems

Striking the Balance Between Security and Safety (F15)

Classroom door locks are invaluable, but they must allow quick egress

By Mark Berger, Securitech

Get Up and Bar the Door (F14)

Access management and door hardware play a critical role in school security

By April Dalton-Noblitt, Allegion

Who Is Entering Your Facility? (F14)

Verifying identities is challenging; partnerships can help

By Daniel Krantz, Real-Time Technology Group



Say Hello to Social Spaces (S14)

Social Applications will transform the security experience

By Steve Van Till, Brivo Systems

Fingerprint Biometrics for Secure Access Control (S14)

Moving beyond passwords and tokens can enhance security while decreasing costs

By Consuelo Bangs, MorphoTrak

Integrating Card Access with Interlocking Door Controls (S14)

While there may be implementation challenges, interlocks can greatly enhance portal security

By Bryan Sanderford, Dortronics Systems

Frictionless Access Control: A Look over the Horizon (S14)

New uses of biometric and RFID technologies could make access badges obsolete

By Henry Hoyne, Northland Controls

More Security, From Bottom to Top (S14)

Buildings are increasing entrance controls on the main floor and upstairs

By Tracie Thomas, Boon Edam

Hardware Security, Today and Tomorrow (W13)

Advances in door technology are enhancing both safety and convenience

By Will VandeWiel, DORMA Americas

Secure Authentication without the Cost and Complexity (W13)

New technologies are narrowing the gap between passwords and stronger authentication solutions

By Ken Kotowich, It's Me! Security

From Access Control to Building Control to Total Control (W13)

How innovation drives the need to update product standards – and ways of thinking

By Michael Kremer, Intertek

The Technology Behind TWIC (J13)

Smart cards are finally getting smart readers, but how will it all work, and how will it connect with existing PACS?

By Walter Hamilton, Identification Technology Partners

Big Data

Transforming Data into Actionable Intelligence (F15)

New solutions can identify insider threats before it is too late

By Ajay Jain, Quantum Secure

The Evolution of Risk (F15)

Banks are using analysis of 'big data' to enhance security

By Kevin Wine, Verint Systems

Reducing Retail Shrink with Business Intelligence Software (F15)

Data mining can be a valuable new tool for loss prevention professionals

By Charlie Erickson, 3xLOGIC

Cybersecurity

Keeping the Security System Secure (F15)

Ensuring that video stays online is key to managing risk

By Bud Broomhead, Viakoo

Target, eBay ... and You? (F14)

Cybersecurity threats are real, even for small businesses

By Hank Goldberg, Secure Global Solutions

Electronic Security Meets the Ecosystem (J13)

IP devices increase both rewards and risks. How secure is your system?

By Pedro Duarte, Samsung Techwin

Fire and Life Safety

Removing the Barriers: The Wireless Side of Fire Protection and Life Safety (S15)

The industry's wireless movement is fueling innovation

By Richard Conner, Fire-Lite Alarms and Silent Knight

The (Slow) Transition to IP in Fire and Life Safety Devices (J13)

Codes and regulations often force fire and life safety equipment to use older technology, but that is changing

By Christopher Peckham & Walter Frasch, Kratos Public Safety and Security Solutions



Integration

Commanding the Enterprise (S15)

New software platforms enable security leaders to ensure awareness, manage risk

By Rob Hile, SureView Systems

Tying It All Together (S15)

Integrating video surveillance, access control, building management and other systems can enhance security and reduce costs

By Mitchell Kane, Vanderbilt Industries

Safe on the Water (S15)

Integrated solutions secure the nation's largest independently owned commuter ferry operation

By Kostas Mellos, Interlogix

Broken Promises: The Current State of PSIM (F14)

Physical security information management solutions have so far fallen short of expectations, but next-generation systems could change that

By David Daxenbichler, Network Harbor

Enhancing Continuity Planning through Improved Security (F14)

Web-based systems can tie everything together

By Kim Rahfaldt, AMAG Technology

Technology-Enabled Collaboration Builds Safe Cities (S14)

Better management of more information can enhance the protection of people and property

By Itai Elata, Verint Systems

Solving a Big Problem for Small Businesses (W13)

New security technologies offer integrated solutions for small and medium enterprises

By Scott McNulty, Kantech

Intrusion Detection/Alarms

Integrating Intrusion (S15)

Video and access have converged on the network; the time has come for intrusion detection to join them

By Mark Jarman, Inovonics

Integrating Technology with Telephone Service at Central Stations (W13)

IVR implementation can be challenging, but when done well, it can significantly increase capacity and customer satisfaction

By Jens Kolind, Innovative Business Software

Related Issues

Maintaining Power (F15)

New network communication solutions can minimize system downtime

By Ronnie Pennington, Altronix

Do You Hear What I Hear? (S15)

Audio technology is redefining the surveillance industry and has become an essential component of security systems

By Richard Brent, Louroe Electronics

Enabling Safe Learning Environments (F14)

Securing schools demands a layered approach

By Neil Lakomiak, UL

From Horse-Drawn Wagon to Moving Truck (F14)

Nearly a century after the first VBIED was detonated in the U.S., what can be done to mitigate the risk of car bombs?

By Laurie Aaron, Building Intelligence

What Is in Store for the Physical Security Community (S14)

New technologies will open up great opportunities for the industry

By Bill Bozeman, PSA Security Network

Security and Privacy in a Connected World (J13)

With proper planning and precautions, security and privacy can complement – not compete with – each other

By Kathleen Carroll, HID Global

A Case for a Green Security Landscape (J13)

Sustainability can be good for both the environment and the bottom line

By John Hunepohl & Aaron Smith, ASSA ABLOY



Video Surveillance

Big Video Data (F15)

Video management systems offer a powerful platform for security and business intelligence

By Jeff Karnes, 3VR

The Public Safety Data Lake (F15)

Making the right decisions regarding storage and other issues can vastly increase the value of video surveillance

By Ken Mills, EMC

The Sun Shines on Surveillance (S15)

Solar power enables wireless video solutions in remote locations

By Dave Tynan, MicroPower Technologies

Surveillance in the 21st Century (S15)

Smart, 3-D, 360-degree cameras that see in the dark are on the way

By Jumbi Edulbehram, Oncam Grandeye

10.7 Billion Security Challenges (S15)

As transit ridership increases, so must security

By Steve Cruz, Panasonic

The Future of Video Surveillance (S15)

A rapidly changing security landscape will provide new ways to meet end users' needs

By Alex Asnovich, Hikvision USA

Making Campuses Safer with Innovative IP Technologies (S14)

Networked systems mean more information, more collaboration and more security

By Kim Loy, DVTEL

Harnessing the Increasing Power of Video (S14)

New functionalities and greater ease of use enhance the value of video in both security and non-security applications

Megapixel Cameras Go Mainstream (W13)

Functionality, versatility, clarity make megapixel video the future of surveillance

By Scott Schafer, Arecont Vision

Seeing the Big Picture: 360-Degree Camera Technology (W13)

High-resolution panoramic video overcomes the limits of PTZ cameras

By Steve Malia, North American Video

Achieving IP Video Management System Scalability through Aggregation (W13)

Video isn't just about security anymore

By Jonathan Lewit, Pelco by Schneider Electric

What's New on the Video Surveillance Front? (J13)

A keener eye, a longer memory and a sharper IQ

By Fredrik Nilsson, Axis Communications

Seeing in the Dark: Smart IP Thermal Cameras for Outdoor Security (J13)

As technology advances and prices fall, thermal cameras have become a cost-effective way to secure the perimeter

By John Romanowich, SightLogix

Video Analytics in the Modern Security Industry (J13)

Analytics can make cameras smarter, but how smart can they get?

By Brian Karas, VideoIQ

The Untapped Benefits of Recorded Video Surveillance (J13)

Recorded video holds a wealth of information that can be used not only post-event but also proactively. Fast video review makes accessing this data possible

By Rafi Pilosoph, BriefCam

SIA Technology Insights is published twice a year, in the spring and fall, by the Security Industry Association in Silver Spring, MD. All editions are available at no charge at www.securityindustry.org/techinsights. Questions, comments and article proposals may be submitted to the editor, Ron Hawkins, at rhawkins@securityindustry.org.



Cyber/Data Security



EAS



Fire & Life Safety



Intrusion Detection



Video Surveillance



securityindustry.org/techinsights

Security Industry Association
8405 Colesville Road, Suite 500
Silver Spring, MD 20910
301.804.4700

