LPM SPECIAL REPORT

Retail Safety and Security

CCTV Surveillance Systems, Retail Alarm Systems, and Security Training

Retail security is a term with two very different and distinct meanings in the retail environment. In one aspect, retail security is an outdated and understated term for a critical sales support function. In the early years of the profession, most companies called this aspect of the workforce the "Security" or "Protection" department. Programs typically assumed a reactive and one-dimensional approach, responding to issues as they occurred and working to keep the stores safe and secure.

Over the years, responsibilities increased, and these departments were looked at in a different way. It became increasingly apparent that in order to benefit the overall organization the industry would have to evolve, embracing the concepts of retail shrink reduction. The term loss prevention evolved to reflect our broader strategies to prevent all types of losses while enhancing the retail business plan.

Today, retail security more appropriately identifies a form of protection that creates a separation or dissuades vulnerability between retail assets and potential threats to those assets. These separations are generally the various tools, controls, and approaches used to protect vulnerable and valuable retail assets—whether our merchandise, customers, employees, facilities or other assets—by deterring harmful or malicious behavior and/or increasing customer and employee safety.

There are many different types of precautions that retail organizations will take to guard against crimes, losses, and other threats to the business. For example, this might include physical tools such as locks, EAS tags, fire exits, or security caches. It may also include a particular strategy or approach such as the hardening of our facilities, executive protection plans, information protection, or certain aspects of a crisis management strategy.

The resource report focuses on two retail security tools—CCTV/video surveillance and retail alarm systems. It provides insights into enhancing the safety and security of retail establishments through the use of these two technologies, as well as offering tips on the security training that should accompany their use.

CCTV Surveillance Systems

Closed-circuit television (CCTV) is a television transmission system applied with the use of video cameras to transmit a signal to a specific, limited set of monitors. As the name implies, it is a system in which the circuit is closed and all the elements are directly connected. Signals are sent to a specific group of receivers, either using coaxial cable or wirelessly through scrambled radio waves that are unscrambled at the point of reception. This is unlike broadcast television, where any receiver that is correctly tuned can pick up the signal from the airwaves.

CCTV cameras are most often used in retail stores in areas that are determined to need special attention in order to protect customers, associates, and store assets. These security systems can be used to monitor customer behaviors and suspected shoplifters, more conspicuously when used in accord with public view monitors to deter theft and provide increased safety and security, or more covertly when investigating internal theft issues. When used appropriately, such devices provide a valuable weapon in deterring theft and other undesirable activities. However, CCTV systems may also be used to monitor customer behavior to assist with marketing, sales, and customer service needs.

Today, most CCTV systems use small, high-definition digital camera systems. Advances in digital technology have made video surveillance more user friendly than ever before. Digital surveillance is now coupled with computer technology, compressing images into a format that allows the images to be stored on a computer hard drive. Images can be stored in computers, transferred to DVD equipment, or transmitted to a computer monitor thousands of miles away. Security systems using IP cameras are easy to install and maintain, and can be customized to meet the ever-changing needs of the retail environment. There are countless systems available utilizing different schemes and different technologies, and the available recording options are growing almost daily.

Research

The ubiquitous deployment of CCTV in commercial environments has occurred despite limited hard evidence documenting its effectiveness. Indeed, most research conducted on the issue has suggested that CCTV can be effective in retail environments, but also that value is not guaranteed, that best practices must be followed, and that video surveillance programs must be dynamic to sustain value.

For example, in a study of retail stores equipped with interactive CCTV (allowing communication between clerk and personnel watching a monitor in a remote location), researchers found a 31 percent decrease in crime in the first year following the installations. By the second year, however, crime reduction had shrunk to below a statistically significant level (*Preventing Crime: What Works, What Doesn't and What's Promising*, a report to the US Congress prepared for the National Institute of Justice).

In another study of CCTV in fashion retail environments, high-level systems were found to "pay for themselves" by reducing loss sufficiently to cover the capital expense of the systems ("Context-Specific Measures of CCTV Effectiveness," *Crime Prevention Studies*, vol. 10; Criminal Justice Press). After 3 months, stores with high-level systems were experiencing an average $590 dip in losses each week. That made for a payback estimate of 1.2 years for $38,000 CCTV systems. After 6 months, because savings had slowed, the payback estimate adjusted to 2.6 years.

However, high-level systems in the study were the *only* ones to break the cost-benefit barrier. After 3 months, both low- and medium-level CCTV systems were cutting losses at a rate that indicated a good return-on-investment, but neither sustained loss reductions. After 6 months, all the stores in the medium- and low- categories experienced weekly average losses at levels at or higher than pre-CCTV installation levels. Subsequently, medium- and low-level systems did not seem on track to ever pay for themselves.

According to research, the impact of CCTV hinges more on a would-be offender's risk perception than it does on the actual rates of conviction and detection. Additionally, CCTV appears most effective at combating opportunistic offenses, in which items are small, easily portable, and of relatively high value. In such cases of "high" enticement, CCTV acts as a situational prompt that encourages individuals to be more rational in their decision whether or not to steal. (Of course, they still may rationally decide they want to steal.)

There have been many studies of the impact of CCTV on retail crime and most have reached similar conclusions. Essentially, that a well-designed CCTV surveillance system often makes good business sense, but that the benefits of CCTV often diminish over time. CCTV is most effective as a deterrent, and that impact has been found to wane in as little as three months.

Here are common conclusions from research conducted into the effectiveness of CCTV in retail environments:

- *CCTV schemes need clear objectives.* The pervasive attitude that CCTV 'is a good thing' can reduce critical thinking surrounding its deployment. So, too, can the feeling that 'we need CCTV because everyone else has it.'
- *CCTV deployments need an active, competent project manager.* Without technical expertise in-house, users are too easily swayed by sales pitches and make it likely an organization will invest more than they need in systems that are a poor fit for the operation.
- *There has to be a structured, comprehensive plan* to accompany the positioning and objective for each camera in the system and how these will be fulfilled. In the absence of a formal planning process, systems rarely have cameras that provide their maximum potential benefit. Planning failures also lead to technical troubles, such as cameras that have trouble in different lighting situations.
- *CCTV strategy should be designed in combination with other crime prevention measures that will support it.* CCTV operates most effectively in conjunction with other crime-reduction measures. Unfortunately, in many deployments, the way in which CCTV is integrated with other security measures is insufficiently thought trough, which leads to poor overall results.

Traditional CCTV System Controls

The most important requirement for a traditional CCTV system to be effective is the most basic: it needs to be working. Regardless of the existence of service contracts, companies have work to do. They need to audit maintenance companies to ensure they meet schedules, follow guidelines to ensure the integrity of CCTV images, and check that each location has responsible employees conducting daily monitoring of CCTV systems, immediately reporting problems, and following-up to ensure that problems receive immediate attention.

Consider these goals at the corporate level for operating a traditional CCTV system:

- We conduct an annual operational review of all aspects of CCTV operation and management. Our review includes CCTV operation, image storage, and equipment maintenance.
- We conduct spot audits of CCTV systems at several store locations. Out audit includes checks of picture quality and picture content and a random review to ensure that image quality is to the required standard in both daylight and darkness.
- To ensure faulty recording is discovered, we verify that staff, at the end of each recording period,

directs a designated staff person to carry out random spot replays to ensure the recording is of a reasonable quality.

Image Quality

"The resolution of the camera is only as good as the weakest link in your system," warns Charlie Pierce, a leading CCTV expert and president at LeapFrog Training & Consulting. If you don't understand your weakest link, you may invest in technology that provides no benefit, be a sitting duck for CCTV salespeople, and have a false sense that you're improving security when you're only wasting precious resources. He recommends that you:

- *Learn the technical stuff.* At least understand it well enough that you know what questions to ask. "If you're afraid to ask questions, they'll be able to sell you anything." And if you know the basics, salespeople won't be able to bluff you with technical talk.
- *Understand the weakest link in your system.* For example, a high-res camera with a high-res monitor won't yield a quality picture if the signal also passes through a multiplexer that doesn't have the capacity to make use of it.
- *Take the time to learn the math before shopping.* Despite the dizzying number of product offerings, "If you do the math, you can always find the best camera for the application," Pierce said.
- *Don't be afraid to ask for a demonstration.* Everything looks good on the trade show floor, ask dealers to "let me see how it works in my application."
- *Provide every camera you have with a written purpose.* You may only have a few different purposes, but you need to identify—for each camera—why it is there. Only by identifying the camera's purpose can you know whether your system is providing a sufficient quality picture to meet your goal.

Privacy & Archiving

Collecting better quality video more cost efficiently may be at the heart of video surveillance, but ignoring how it's collected and managed can create problems for retail security operations.

How video is collected—meaning where to place cameras—is often the focus of privacy concerns, but attention needs to be extended to what happens after video is collected. Companies generally have authority to capture video in areas that aren't sensitive (like bathrooms), but what they do with the video can potentially cause problems. "Controlling access to captured video is an important way to mitigate privacy impacts," according to Donald Zoufal, an executive with SDI, a national systems integrator. For example, a loss prevention agent who is a live operator may not need access to an archive of video incidents, he said.

It's also important to build audit functions into the system. Loss prevention executives should set them up so that they can tell "who is looking at what," said Zoufal. Related to that, departments should have surveillance policies that outline what is and is not authorized, "so operators aren't following good looking girls with the cameras."

Retailers that desire a CCTV surveillance system that steers clear of most privacy concerns should:

- Conduct an annual assessment or audit to ensure that the system is being operated correctly, used for its express purposes, and that CCTV remains the correct security tool for the job.
- Conduct operator training on privacy aspects of the system and expectations.
- Keep relevant video secure through appropriate technical and organizational measures and retain it no longer than necessary. Companies should align their video retention policies to where the law is "and also where you think the law is going," warned Zoufal.

Although the retention of security video for use as evidence is a separate issue, addressing it will make it easier for the system to also meet privacy best practices because it requires identifying how video is handled and who can access it. Without it, not only are video clips less useful as evidence but more likely to find their way on YouTube and cause potential harm to a company's reputation.

Unfortunately, although commercial video management platforms do a good job of organizing and identifying video, they sometimes do a poor job of helping users manage incidents for which companies need to maintain video. Many systems approach it like, "It's your incident, it's yours to manage."

Without proper software prompts, some retail security operations may do an incomplete job of managing incident footage. They may have no way of validating the chain of custody of video, audio, or still images, and lack a structured process for determining how long to keep files, where to keep them, or what level of backup is required based on the severity of the incident.

When developing a CCTV system, retailers need to be as careful planning video incident storage as surveillance coverage. When looking for a video management solution, executives—in addition to considerations about live video management—need to look for how incidents are treated.

- Systems should be open so that all types of evidence can be collectively managed (still pictures, audio clips, incident report, etc.).

- Systems should authenticate clips, maintain an audit trail, and validate that a clip transferred from one location to another is unaltered.
- You should be able to create a protocol for keeping and backing up clips based on type of incident (suspicious, criminal, or legal, for example).

Analog vs. IP Video

As technology evolves and business needs grow more complex, loss prevention leaders are looking for video surveillance solutions that are both affordable and capable of meeting the escalating demands of the business. Mike Dunn, vice president of strategic services for BSI, shared some of the primary considerations when choosing between an analog versus an Internet protocol (IP) camera system.

"The primary difference is in the way the video signal is delivered," Dunn explained. "Analog cameras turn video signals into a format that can be transferred over coaxial cable and received by a television or other receiver, such as a digital video recorder (DVR) where the image is digitized and stored. IP camera technology is much more advanced. It captures an image, immediately digitizes the video signal inside the camera and keeps the image digital throughout the entire transportation and viewing process. This process allows the IP camera to keep a higher base-level image over analog."

Dunn described some primary considerations:

1. *Image Quality*—This would depend on how the system is being used. Resolution limits on analog cameras make them best suited for placement close to the area being monitored, whereas the advanced capabilities of IP cameras allow millions of additional colors at a higher resolution with crisper picture quality.

2. *Scalability*—The ability of a system to handle a growing number of cameras in a capable manner will factor in many decisions. For example, most analog systems require DVRs that manage 16 or 32 channels, which may work well with smaller systems. But what if you have 17 or 33 cameras? This would require adding additional equipment at substantial costs. IP systems provide greater flexibility, allowing you to construct the system based specifically on what you need and offering more options if you wish to expand later.

3. *Intelligence*—Today we want our systems to do much more than capture images. Some analog and most IP systems offer options that can add intelligence to live and recorded video. However, analog systems require additional hardware to accomplish many of these functions. Conversely, an IP camera is as much a camera as a smartphone is just a telephone, providing higher intelligence capabilities that can be built into the device.

4. *Edge Storage/Serverless Solutions*—This would also depend on the size and use of the system. Analog systems require digital conversion and a method to store the video outside the camera, which requires the use of an encoder or a DVR. Smaller IP systems don't necessarily require DVR equipment for 4-16 cameras, providing the flexibility to break free from the traditional setup of cameras and a DVR. Some IP cameras today can use their own built-in CPU and storage, recording the images directly on the camera. The customer can view HDTV recordings or live viewing from his smart phone or tablet leaving no physical "box" on site. Costs of software and additional equipment to manage the solution must then be factored in.

5. Total Cost of Ownership—Analog systems are typically less expensive when initially installed. However, it is important to consider the total cost of owning your system. The size of the system, expansion costs, maintenance, intelligence solutions, and other advantages may provide direct ROI and substantially lower the break-even costs on IP systems, which should definitely be factored into any design.

"Hybrid systems (part analog and part IP) can also be designed that allow companies to migrate existing analog components into a modern IP-based system," explained Dunn.

Evolving Video Technology

Video has traditionally been seen as just a piece of equipment for the stores, heavily reliant on available resources to either monitor live footage in dark rooms in the backs of stores or to manually review huge quantities of footage to build a case or identify incidents. This has limited its value and relevance to the broader organization beyond loss prevention.

However, even just in the last few years, video technology and the other technologies it enables have been transformed. For example:

- Digital technology enables material for case management to be collected and collated much more quickly. Further, by setting up alerts that look for exceptions, incidents can be acted on in near real time and reviews can be speeded up, which has been seen as a significant change transforming the perceived value of this technology.
- Smaller, higher-resolution security video cameras provide sharper images and fewer blind spots at increasingly lower costs.
- Networking, video compression, cloud technologies, and improved broadband speeds have enabled greater remote monitoring by field managers, allowing real-time interventions while central hubs with two-way communications can provide local reassurance through "virtual" visibility and the opportunity to see, send alerts to, and talk to those in many stores, all from one location.
- The integration of cameras into store infrastructures, including doors, store alarm systems, refrigeration, point-of-sale registers, EAS gates, lighting, and more, generate new opportunities for value creation. For example, one big-box retailer in the US is exploring the potential energy savings of being able to remotely turn off the lights the store managers forget to switch off when they lock up and leave the store after closing.
- Complex data analysis and algorithms made possible by technology advances enable pattern and image recognition, creating new capabilities such as scan avoidance and facial recognition.

While these big changes—moving video from being seen as just a uni-functional piece of store equipment to a technology with enormous potential—are increasingly evident, it is not wholly clear that these new capabilities are being fully appreciated by either store staff or retail executives. As one loss prevention director recently shared, the video loss prevention technology now available to stores is, in car terms, like a Ferrari, yet we are asking it to be driven by novice drivers.

It is not uncommon for retail security guards and store associates to use but a small fraction of the potential capability of the video systems installed. And, in the end, a system is reliant on those who have the time, skills, or inclination to use it. For example, video can be set up to deliver alerts via text message to security guards or other staff in the stores as and when high-theft items are selected from shelves. This is a terrific capability, one that can deliver the great customer service that thieves hate, but it is reliant on the response of the increasingly scarce and often under-trained security guard or store associate.

To address potential gaps in current and future video capability and capacity, loss prevention leaders could start by defining and aligning their organizations to a five-year strategy and business case for video. This exercise can help identify the many different drivers of value to the organization and the financial benefits they deliver. Some will be hard to quantify, such as staff feeling safer or the marketing department knowing the number of shoppers turning left or right on entering the store. However, others will be easier to quantify, such as productivity savings from moving to remote monitoring or reducing energy bills by turning off the lights store managers forget to switch off.

With the use cases identified, the capabilities required to execute and the head count needed to deliver can then be calculated. Without doubt, a broad range of skills will be needed to manage video. For example, there will be a need for highly skilled individuals who know how to fully leverage video for monitoring purposes. There will be those that know how to organize and deliver an efficient and effective remote monitoring center, and there will be those who can sell and promote video as a capability to other functions in the organization.

Some organizations may consider some of these competencies, shopper insights being one example, as ones they believe their organizations can uniquely develop and deliver themselves for competitive advantage, while other competencies such as the remote video monitoring of stores by security guards may be viewed as a task that could be outsourced.

Once inescapable conclusion about video today is that it is now an advanced technology and not simply a piece of store equipment, and as such it needs managing, and most importantly, a strategy needs developing to build capability and capacity so that its potential is fully exploited.

Remote Video Surveillance

Remote video surveillance enables the reallocation of loss prevention personnel from low-activity locations without the elimination of loss prevention coverage and oversight. This not only increases the effectiveness of LP associates, but also increases overall job satisfaction, which reduces turnover, lost time, and recruiting, hiring, and training costs.

Loss prevention personnel productivity can increase five to ten times, depending upon the current coverage model and activity levels. This increase in productivity is partially due to the fact that low levels of activity lull loss prevention personnel into a false sense of security, resulting in missed observations and apprehensions. Maintaining a video monitoring "sweet spot" improves their effectiveness.

Remote video monitoring enhances loss prevention's business value to the organization by raising overall productivity of loss prevention personnel while simultaneously increasing coverage and oversight—without increasing the loss prevention budget.

It also increases deterrence. Sophisticated external and internal threats are aware of the physical presence of loss prevention personnel and, in local monitoring locations, focus their efforts when LP personnel are physically present. When remote security cameras are used, it is more difficult for sophisticated external and internal threats to determine if they are being monitored, increasing the deterrence effect. This technology also positively impacts district, regional, and corporate loss prevention management by providing the capability to observe remote locations without having to be physically present. This improves management's effectiveness by reducing both the time and costs of travel.

Coupled with the integration of additional key data elements, such as POS, alarm, and EAS data, remote video monitoring enables loss prevention professionals to investigate and resolve threat events quicker and more accurately. This data integration also enables store and retail management to better understand the nature and volume of threat events by store and departments within the store, improving management and loss prevention program targeting and effectiveness. For those locations with proprietary retail alarm systems, remote video monitoring can dramatically reduce the costs associated with false alarms.

In addition to its loss prevention uses, establishing a remote video surveillance capability enables cross-functional corporate executives to obtain real-time feedback on customer traffic, customer service execution, merchandising presentation, and in- and out-of-stock conditions.

This extension of the use of remote video surveillance systems beyond LP adds significant value to the retail organization both in a functional as well as bottom-line basis. For example, retailers are using remote video to conduct ongoing audits that effectively help reduce shortage and increase sales, safety, and productivity.

Negatives. While there are many positive aspects of remote monitoring, there are several issues to consider that can reduce the impact of this technology in the retail environment.

- Remote video monitoring works most effectively for activity that is clearly discernible or detectable, versus fine or complex activities. It is also less effective when observed activities require immediate on-site response.
- Remote monitoring can prove difficult in environments where existing camera angles create zones where activity can't be observed or the environment is complex, requiring detailed first-hand knowledge.
- Remote video monitoring can be fatiguing. Associates performing only remote video monitoring duties become increasingly less effective without regular breaks or additional work assignments that don't require video monitoring. Care is needed when evaluating the costs of digital video for remote monitoring.
- While digital recording systems are comparable in cost to tape recording systems, maintenance and storage costs can be higher, depending upon how maintenance is performed and the retention period for the digital records.

Decision Framework. Three variables establish the viability of remote video monitoring for a retail location, including the best times and locations. These variables are:

- The level of activity,
- The response time needed to respond to threat events, and
- The need for independent verification of threat events.

When evaluating this decision framework, consider threat events to include shoplifting, robbery during store open hours, burglary during store closed hours, internal theft of merchandise or cash, and thefts by outsiders but enabled by employees.

Locations are candidates for remote video monitoring when their activity level does not warrant full-time loss prevention coverage or when their activity level does not require an immediate threat response from an internal loss prevention associate, such as in most cases of internal thefts.

Locations are not candidates for remote video monitoring if the video system requires independent verification of a threat event due to insufficient camera coverage, such as the continuous observation of shoplifting suspects.

Case Study: Remote/Interactive Video

When jewelry chain Zale Corporation installed interactive video in troublesome stores with consistent problems in shrinkage it cut some store losses in half.

Zale took its standard CCTV surveillance system and added ceiling mounted microphones and a video transmission unit. The bonded video and audio were transmitted to a central station monitored by a contractor.

The equipped Zale stores were then checked randomly, giving security monitoring personnel the ability to look in and listen "live" to the stores. Store

clerks were given the ability to press an alert button to ask the monitoring station to look in, e.g., if the store was over crowded or if they felt threatened. The interactive nature of the system allowed monitoring personnel to talk over a speaker and address anyone causing a problem (instructing them to leave the store, for example).

Following are some of the lessons learned:

1. Training. For interactive video to cut shrinkage and make employees feel safer, you will likely have to increase training, especially if you utilize a contract company to conduct the monitoring. The first requirement is clearly written policies and procedures that are shared with the security monitoring team, according to George Slicho, former senior vice president for loss prevention, security, and physical inventory and now a security consultant (Slicho LP, LLC). All employees who are working where the system is in use need a complete indoctrination in how the system is designed to help and what they can rely on it to do. "We went over every single scenario that we could imagine," says Slicho. "We sat down and wrote everything from a robbery in progress to just a suspicious person."

2. False Alarms. Because security can both hear and see an area, remote monitoring can cut down on the number of dispatches needed to respond to an alarm. Often times security staff can tell it's a false alarm. That is especially cost-effective for companies that pay a private guard company to check out every alarm and for businesses that have many remote sites that need monitoring.

3. Observing worker habits. With the addition of interactive video, Slicho says Zale was able to address staff violations of company policies before they become losses. Security monitoring revealed staff who worked from open show cases, left their keys unattended, showed more than two pieces at a time, and never asked for identification.

4. Leveraging value. To justify the expense of remote monitoring equipment, security departments may want to partner with other departments, such as marketing or customer service, who can utilize the same technology to improve training, conduct merchandising research, and review store operations.

Stress the safety aspect to workers. Some retail staff will quit rather than submit to being watched or listened to. But those workers are most likely the ones who are taking from the till, says Slicho. But to make the surveillance more palatable, companies should stress security monitoring as an employee benefit purchased for their protection. Explain how the video allows security to help in emergencies, assist in handling irate customers, and is always available for workers to call at any time for any reason.

5. Legal Issues. If utilizing interactive video, establishments need to notify employees and customers of the presence of the monitoring. A sign such as "Notice: audio and video activity in this store may be monitored," is typically sufficient. The sign is also part of the preventative benefit of the surveillance.

6. Manpower. Slicho says his experience with interactive video was a quick upturn in turnover for the first month the system is use, followed by a much higher retention rate. In one store, turnover fell 28.5 percent. Plus, having security watch the store live—with the ability to interact with clerks—provides them support, and important consideration in light of OSHA guidelines for retail establishments that recommend that clerks not be made to work alone late at night.

7. Employee escorts. An added benefit of interactive video is that it can give employees who feel at risk the safety of having another pair of eyes looking on. Employees can call or buzz the monitoring station and have security watch as they leave the store. It also lets security monitor stores during closing and openings.

Assessing Value of CCTV

How do you know if your CCTV system is paying off? Taking a statistical "before and after" measure of crime is the standard methodology. Is crime up or down since implementation? By how much? You can then use the data to help decide about future video surveillance investments.

However, this is not the only input available for making strategic management decisions. One addition to a "by-the-numbers" evaluation of CCTV is to take a "realistic" approach. A realistic model evaluates crime prevention measures within their context, and encourages you to ask what "mechanisms" are acting to produce which "outcomes." For example, one mechanism related to CCTV is that its use might give staff more confidence to approach offenders. The context in which this mechanism would be triggered is one where store personnel feel intimidated by shoplifters and are not currently confronting them. Such a mechanism would not be triggered—and the corresponding reduction in theft not expected—in instances where staff already felt confident to confront thieves; or in situations where they believe it is not their responsibility to do so.

This type of realistic approach to CCTV assessment acknowledges that many factors can influence the value of video surveillance. It encourages loss prevention executives to acknowledge that staff attitudes and management involvement is critical. For example, a CCTV system

introduced to a store where staff welcomes its arrival may create the right "context" to cut crime. A store where staff resents the system may increase crime—by reducing staff concern or vigilance.

Retail Alarm Systems

Protecting retail locations with an alarm system is a basic—and vital—protection measure. Interviews with commercial burglars have repeatedly found that they avoid targets that have point-of-entry protection, such as technologically advanced alarms.

But an alarm system can be used as more than just an electronic tool designed to keep bad guys from getting into your buildings. While that's important, it's also possible to use an alarm system to identify internal problems. With the ability to monitor alarm systems over the Internet, a retailer can have realtime event status on every location, on who goes in and out, when, how long a door was held open, and whether or not a store has even set their system.

Maintenance

Here are some suggestions to improve the likelihood that preventative maintenance on retail alarm systems is completed when and how they should be.

- Issue guidance to all locations on tracking and monitoring preventative maintenance actions.
- Do not rely on self-reported data provided by maintenance contractors (validate the data to confirm that preventative maintenance has been completed).
- Require company personnel to verify and "sign off" on all corrective maintenance actions to ensure work was completed and that equipment is ready for service.
- Review contractor-provided reports to ensure that data is complete.
- Comprehensively track maintenance inspections (via spreadsheet or other recordkeeping mechanisms) with the work frequency and inspection requirement identified. Example: "Monthly: Conduct function test to monitoring service."
- To help ensure inspections are performed regularly, capture them within a performance measurement system (e.g., percentage of timely preventative maintenance checks performed on alarm units.)

Finally, it is important—every time a vendor comes to service an alarm system—to record what they did, how long it took, how many repair staff they needed to do the job, etc. Analyzing these logs before yearly maintenance negotiations can inform the best business choice—such as going with "hourly," or to self-insure some components, or to assume the risk of preventative maintenance. Having detailed data of past maintenance permits more cost-effective decisions regarding features of future maintenance agreements.

Testing

Regular inspections and testing of alarm systems and equipment is a critical component of an intrusion detection program. Retailers can use testing to evaluate performance, reveal weaknesses or flaws, and identify problems that may otherwise go undetected.

A review of alarm system testing may include:

- A review of the existing security test procedures, if any.
- What tests are being conducted under the current program, who conducts them, when and where.
- An analysis of whether current tests are cost-effective and successfully eliminate elements of risk.
- How records of past tests are maintained for future use.
- A determination of whether or not less expensive test methods can be used as effectively as current methods.
- A review of all high-risk locations and a determination if there are any that are not receiving necessary testing or auditing.
- A suggested testing program for all locations where tests are not, but should be, conducted.
- An analysis and determination as to whether outside consultants would be able to more effectively perform necessary testing.
- A review and analysis of the current organizational structure to determine whether individuals are properly authorized to implement tests when it is determined it is necessary to conduct them.

Alarm Monitoring: Who Should Do It?

Every company has a unique set of conditions under which it operates. This uniqueness is often the primary driver behind the decision to bring an alarm program in-house. Management churn, schedule adjustments, administrative reporting demands, and custom loss prevention needs can all be significant components of the decision process; a decision process that must also consider how an in-house program will integrate with the total loss prevention approach.

1. Management Churn. Have you ever called an alarm company to verify dispatch data only to find that none of the account information in their database was correct? How about deletion of old access codes? No matter how much effort and time is invested in getting things straight again, it only lasts until the next personnel shuffle by operations.

But what if the retail alarm center had access to the same systems and information used by human resources and operations? What if this information could be automatically updated in a way that could prevent widespread inaccuracies? By teaming up with IT and HR partners, an in-house retail alarm program has an opportunity to develop systems and procedures that can greatly reduce this exposure.

2. Inadequate Resources. Supervised openings and closings can be the bane of any alarm monitoring center. Effective supervision is dependent upon the monitoring center having accurate entry/exit schedules and adequate communication infrastructure. This is especially true for alarm centers monitoring accounts that are concentrated in the same time zone and have identical opening and closing schedules. Just picture 3,000 facilities all opening within 5 minutes of each other and what it might take to ensure all signals (read phone calls) are received and processed. It is a tough challenge that many alarm companies are unable to effectively meet. Unless adequate resources are dedicated to the issue, the client is vulnerable during two of the most critical time frames of the business day.

An in-house program can overcome this challenge by sizing infrastructure and staffing to meet this critical peak time frame. A partnership with the IT group can provide opportunities to explore alternative communication options, such as LAN or Internet, which can greatly enhance capabilities. Further improvement can often be realized by forming partnerships with additional in-house support groups to assist in developing creative methods of obtaining accurate entry/exit times.

3. Focused Reporting. Retail alarm activity reporting can be a useful tool if offered in an efficient format and in a way that doesn't smother the end user. Alarm companies that blindly send out reams of paper to their clients are doing little more than depleting valuable forest products. Internet-based access to alarm information is a better alternative, but can still be problematic for users that are unsure what they need and when they need it.

An in-house program can provide the means to custom fit reports to individual needs. Email of real-time events and integration of alarm activity with data mining applications are alternative methods that also provide efficiencies not easily duplicated with an outside alarm company.

A well-designed, in-house alarm program can be a valuable tool for the field loss prevention manager. Real-time notification of alarm zone trips, after-hour entries for overt installations, and alarm event analysis are just a few of the things a typical in-house program can offer. Although outside alarm companies excel at providing "canned" products, they rarely have the resources required for "one off" activities that are needed in many loss prevention investigations.

4. Comparing the Costs. "Is it cost-effective for us to have an in-house alarm program?" Current monitoring costs and ownership status of existing retail alarm equipment must be weighed against in-house start-up costs and operating expenses. This typically dictates that the in-house program be clearly defined and modeled before making comparisons. Some important questions to ask:

- *Have I exhausted the potential for service fee reductions with my current or alternative retail alarm vendors?* It is the rare alarm vendor that will refuse to consider significant cost reductions when faced with complete loss of a reoccurring revenue stream. Ever thought to ask for scheduled cost reductions instead of cost increases? It has been done.
- *Does my company have the expertise on staff to tackle the intricacies of building and running a comprehensive alarm program?* If not, what measures will be necessary to recruit the needed talent?
- *Are there any potential obstacles to obtaining assistance from IT, telecommunications, and other support groups within your company?* Outsourcing these skills and services is expensive and rarely allows for seamless integration with company systems.
- *How critical is an alarm program to my company's business model?* If even temporary loss of retail alarm monitoring cannot be endured, back-up arrangements will need to be considered. These arrangements could range from a local off-site facility with total or partial redundancy, to a contractual arrangement with another central station to transfer monitoring responsibilities.

Once the envisioned program has been defined and appears to address the critical expectations of the company and end users, the process of identifying program costs can begin. The typical components that must be considered to build a viable working budget include:

- Facility construction,
- Capital expenditures, such as alarm receivers, computer automation system, and telecommunications equipment,
- 24/7 staffing, and
- Controllable expenses.

With the budget process completed, realistic cost comparisons can then be made against the existing outside services. Additional considerations might also include any operational efficiencies that would be realized by bringing this activity in-house. These might include better control of false-alarm fines or enhanced control of sales floor environments to reduce shrink,

It is important to note that the growth requirements of an in-house retail alarm program do not directly track with the increase in monitored alarm accounts. In other words, as stores are built or facilities added to the program, it does not necessarily follow that staffing headcount or infrastructure must increase. Although there are certain "saturation" milestones that dictate additional resources, for the most part, the cost per account decreases each time an account is added. Put another way, a staff of twelve people can monitor 100 accounts or 1,000 with the same cost effectiveness.

Case Study: Third Party to In-House

A proprietary alarm monitoring program is clearly not the best approach for all companies to take, but, for some, the benefits can be significant and far outweigh the risks. This was the case when CVS evaluated the pros and cons of bringing a program in-house.

- Monitoring costs were soaring.
- There was no consistent approach to the design of new store installations.
- Repair costs and false-alarm fines were increasing year after year.

Rather than just address the monitoring opportunity, CVS opted for a complete and comprehensive approach in 2006. In addition to having a UL-certified alarm central station, the CVS Asset Protection Services group designed and coordinated the installation of alarm systems for new stores and remodels, troubleshot and coordinated alarm system repairs, and even established a proprietary lock-and-key program. The management of these activities significantly reduced costs and maximized the benefit to CVS. After all, who better can understand what a company needs than a team dedicated solely to that purpose?

Case Study: In-House to Third Party

Jeff Pepperney, Vice President, Franchise Operations and Member Experience at Sears Home and Business Franchise, described their company's transition to third-party monitoring as follows.

Sears successfully owned and operated a monitoring servicing over 4,000 accounts. Annually, the monitoring center's equipment and capabilities were evaluated to ensure the service, technology, and performance levels met or exceeded the industry's best-in-class retailers.

In 2003, we understood that our equipment was becoming outdated and would be in need of significant upgrades.

Additionally, enhancing retail alarm data integrity was necessary to ensure the highest level of security was continuously maintained. Through years of in-house monitoring functions, our monitoring center associates and store operators established relationships that began to jeopardize our security levels. Requests from stores to force-arm buildings and arm systems remotely began to increase and exceptions to our standard operating procedures were creating risk to our associates, assets, and facilities. Faced with the requirement to upgrade our systems and infrastructure, the key question was whether Sears should remain in the monitoring business or outsource to a third party. We believed that we should only continue alarm monitoring if:

- We could do it better than a third party, or
- We could do it cheaper than a third party.

If both of the answers were "No," then our decision was to outsource.

A thorough equipment and financial review was completed to position Sears with a long-term alarm monitoring solution. Our internal review concluded outsourcing alarm monitoring services to a third-party supplier was the most cost effective and provided the best solution to capitalize on state-of-the-art equipment and services.

Five critical elements served as the foundation to the conversion:

1. Transition Team. A transition team of customer-focused leaders were selected to design, analyze, and implement the alarm monitoring transition project. In addition to loss prevention, our transition team included stakeholders from the following departments: procurement, finance, business unit leaders (mall-based stores and specialty businesses), IT, real estate, legal, facilities, and operations.

Our team met regularly, defining the objectives, building success criteria, creating performance

metrics, and representing the organization to ensure a seamless transition of alarm monitoring.

The project plan included:

- Interview stakeholders,
- Establish operating procedures for supplier,
- Develop draft scope of work for review by stakeholders,
- Present sourcing strategy (scope of work, list of suppliers, and timeline),
- Develop, distribute, and analyze request for information,
- Complete supplier bid meetings and site visits,
- Present request for proposal (RFP) supplier short list recommendations to stakeholders,
- Develop, distribute, and analyze RFP,
- Negotiate with suppliers,
- Present overview to stakeholders,
- Notify suppliers and stakeholders of contract award,
- Execute contract,
- Develop performance metrics, and
- Establish quarterly performance meetings to review and track performance metrics.

2. Determining the Service Provider. Criteria for a successful service provider included the following:

- Fitness to technical and functional requirements,
- The ability to support current and emerging equipment,
- Industry reputation and experience
- Experience and qualifications of the company and resources,
- Quality assurance commitment,
- Financial strength, and
- Proven methodologies, tools, and value-added services.

Sears was sourcing the "best value/total cost" decision. While cost remained a critical decision factor, the quality of the equipment, service, and operating efficiencies that would be realized were the primary and most critical aspects.

Once the initial review was completed, Sears identified a short list of suppliers. Each of the suppliers was sent a request-for-information package to complete. The focus was to identify potential suppliers and provide more detailed data as required for the purpose of the RFP.

As a second step, Sears choose to pre-qualify the suppliers' services and products prior to issuing a RFP. The goal of pre-qualification included formal presentations, site visits to facilities, service-level assessments, testing of products, and customer referrals.

Sears' procurement department conducted the final negotiations and ADT Security Services was selected as the provider of burglar and fire alarm monitoring for the company.

3. Project Planning. The planning phase of the project was split in two specific aspects—the project team coordinated by Sears and ADT's project team. These teams identified the tasks involved in the conversion, including both established tasks from the process flow and additional tasks that are outside or not included in the current scope of work.

A project task list was created to identify key issues that can affect the overall project and allowed assignment of tasks such that primary and secondary owners can be established. Tasks were assigned milestones in the project file to help balance workload for project planning. Both project teams established a plan for transition.

Sears' transition plan involved collecting the proper information in order to assess what relevant information and services needed to be provided by our organization. Clear communication, precise operating procedures, and partnership with our selected solutions provider were the building blocks of our transition plan.

ADT's transition plan was formed from data retrieved from Sears concerning the current standard operating procedure, current database, and service information concerning the current customer base. Data included: number of locations and systems (panels) per location; manufacturer and model number of panels; breakdown of panels per location, manner of systems communication, type of receiving equipment, type of automation, and notification plan.

Our teams worked closely together on an effective transition plan to ensure our target dates and success criteria would be achieved. A test plan was created consisting of a documented test procedure to test current monitoring methods and the ability for ADT to monitor the same methods during the transition.

4. Implementation. Converting retail alarm system monitoring, whether from in-house to third party or third party to in-house, requires absolute understanding of a defined scope of work. Sears and ADT partnered together to develop a scope of work to ensure all systems were transitioned without interruption and end users were aware of their facility's signal transfers.

The initial goal described in the introduction was to perform alarm monitoring better and more cost effective. To achieve this goal, ADT's mission was to fully understand the standard operating procedures of Sears, replicate these standards, and enhance the integrity of data and services prior to the conversion.

To implement the alarm system monitoring change, the data from the existing Sears monitoring facility was gathered and scrubbed to determine its

accuracy and freshness. The data was then formatted in order to be inserted into ADT's monitoring systems and reviewed again for accuracy.

Once all data for each Sears location was in place in ADT's monitoring systems, the stage was set to develop the schedule for the change over. Backup plans were developed and notification of the change in monitoring was sent out to all locations.

5. Continuous Improvement. The retail alarm monitoring conversion from Sears' proprietary monitoring platform to the ADT National Monitoring Center was a seamless, successful event.

During the conversion, all 4,000 account signals were transitioned without interruption and when each panel was activated to arm for the close of business, signals were transmitted and building protection was achieved. Day one of a new solutions provider of alarm monitoring was completed and our focus turned to ensuring performance metrics were achieved and capitalizing on ADT's value-added services.

Meeting and exceeding performance metrics was ADT's new goal. Performance metrics included:

- Alpha service levels (fire, hold-up, burglar alarms)
- Beta service levels (supervisory signals)
- Gamma service levels (scheduled related alarms)
- Inbound service levels (alarm-related calls)
- Activity reduction efforts

Each metric was assigned a target goal. For example, 90 percent of burglar alarms within 60 seconds. To ensure continuous improvement, Sears and ADT developed quarterly performance business reviews to assess performance metrics, identify opportunities to strengthen our partnership, and continue to focus on achieving both companies' internal and external goals. Business unit leaders from inside and outside our transition team participated in the business reviews.

Case Study: Alarm System Conversion

When Rite Aid set out to convert its outdated intrusion retail alarm systems in all of its locations, Rite Aid's Group Vice President of Asset Protection Bob Oberosler and his team knew it would be a challenging project.

"We recognized the fact that over the footprint of our organization, we had as many as ten to twelve different alarm panels, many of which were obsolete and no longer supported by the manufacturer and at risk of not being actively monitored," stated Oberosler. "Because we are a highly regulated industry, if the alarm systems failed, that would mean we could not operate our pharmacies without deploying guard services. We knew we had to upgrade and standardize our approach, and we needed to do it soon."

With the objective of undertaking this nationwide conversion program to suit both immediate and long-term needs, Rite Aid engaged Protection 1 Security Services. Prior to executing the contract, Oberosler and his team held numerous meetings with the solution provider's executive staff and team members from all parts of the organization to fully vet the project and agree on an execution plan.

While the immediate concern was ensuring all retail alarm systems were operable and current, the security team also considered future needs. If they could stretch the operating budget expenditure to provide future scalability and the capability to integrate other systems, that would be an important incremental benefit.

The first step in the process was to categorize the conversion into three parts:

- Those stores that could be reprogrammed electronically,
- Those that needed their keypads and panels changed out by an on-site technician, and
- Those locations that needed a total replacement.

Adding to the first set of complexities, due to the age of some of the retail alarm systems, the master codes to reprogram the panels were no longer available. This required a more complex approach.

The next priority was to upgrade approximately 500 stores that were running on an outdated server that was at risk of failure. If the servers failed, those locations would not have a working security system and would not be able to operate without a manned guard service. The installation team had a forty-five-day window to complete the conversion in these stores.

Protection 1 decided to train a designated group of experienced technicians to execute the Rite Aid project. It recognized that in order to accomplish the installation in nearly 4,600 locations in a six-month window and, more importantly, convert the approximately 500 at-risk locations in 45 days, a different approach would be required to be successful.

This group was given the name "Seal Team" in recognition of the need to be quick, efficient, and

mobile to accomplish the task. The installation team was brought together and trained specifically on all Rite Aid profiles so it could deliver an installation experience that was uniform across Rite Aid's footprint. This unique operation essentially gave Rite Aid a dedicated installation technician team, tailored to meet the needs of the project.

Implementation

Customization became a common recurring theme during every step of the project. Rite Aid required a comprehensive strategic plan for the conversion that included constant communication and personalized execution to ensure the project would be completed on time and within budget.

1. Training. Once the Seal Team was chosen, it traveled to Detroit where a high concentration of Rite Aid stores existed, to undergo intensive training and preparation for the project. The team learned about every existing legacy alarm model that it would encounter, how to reprogram the systems, and how to ensure they would integrate with other existing systems, such as lighting, HVAC, and fire systems.

At the same time the conversions would be taking place, Rite Aid was remodeling several stores to feature its new Wellness Stores format, which included investments in new technology that would have to integrate with the retail alarm systems. This would require the Seal Team to have a good grasp of the dynamics of each location so that the end result was a fully integrated system. Hands-on training allowed the team members to model the work that would be required to be performed in the stores.

2. Conversion. A test team was deployed to Kentucky to complete 28 sites. After a successful run, the remainder of the team was initiated, and over 500 sites were converted in the first month.

During the inspection process, the Seal Team found that some stores' systems did not require replacement as initially presumed. Some existing panels had the capability to be reprogrammed, so only a fraction of the alarm systems required full replacement. At these sites, the installation technicians performed the reprogramming work, helping Rite Aid avoid unnecessary system replacement and realize cost savings to the bottom line.

3. Customization. Each system was customized to meet the needs of the individual store, requiring additional programming and technical work from the Seal Team. Some systems had multiple communication paths for the intrusion system. Because a majority of stores participate in a green program, which negotiates lower electric bills for stores that have lighting controls activated with arming and disarming of the retail alarm system, the intrusion-detection systems also required integration with the lighting systems.

"We chose a Digital Monitoring Products (DMP) solution for stores that required an alarm-panel replacement," explained. "We worked with the manufacturer to customize the panel to provide a number of personalized capabilities, including the capability of PIN-code management via an online data management portal application."

This online portal allows Rite Aid to manage security data for all of their stores, such as viewing open/close schedules and reports, viewing incidents and alarm activity, and running custom exception reports.

Rite Aid deploys separate alarm panels in its pharmacy suite. The pharmacy often operates hours independent from the store (for example, closing at an earlier time). Rite Aid needed to have the ability to activate the alarm in the pharmacy without turning off store lighting. This problem was solved by working with DMP to customize the panel software and design a system that could arm the pharmacy alarm independent from lighting controls.

As the conversions proceeded, Oberosler added additional requirements to the project. While the stores were being converted, he wanted to review the retail alarm system history at each location for false-alarm activity and fines. This information gave the installation team an opportunity to change the basic layout of the systems to improve performance. "We also found that in most locations, we lacked documentation or diagrams for the existing systems," noted Oberosler, "As the team continued with the installations, they were also generating the documentation for each location such as users guides and operating procedures for future use."

4. Constant communication. A key reason the project was successful was the constant and proactive communication. Protection 1 assigned dedicated project team members at their National Account Operations Center (NAOC) in Dallas to communicate daily with the Seal Team to receive project status updates, timely plan subsequent store conversions, and resolve issues. This center was created specifically to support large, complex deployments for national customers.

"One of my top priorities was weekly status meetings between the implementation team and the key stakeholders from Rite Aid," said Oberosler. During the calls, the two teams would go through a detailed checklist of action items that needed to be addressed.

Results

After just the first month, the installation team was able to covert over 500 sites. The peak number

of retail alarm systems converted in one month reached 740. Within four months, over 2,000 sites store conversions had been completed. The project was completed and delivered within the budget and timelines promised.

At the outset of the project, while the immediate concern for Rite Aid was ensuring all intrusion systems were operable and current, the security team also wanted the new systems to be scalable, to accommodate the retailer's future needs beyond retail alarm systems.

Jim Shepherd, Protection 1's national account manager, explained: "Because we planned for the capability of integrating with systems, such as video and access control, Rite Aid has the potential to realize further benefits, such as protection against internal theft and inventory shrinkage, as well as making progress towards thwarting organized retail crime."

Now that the conversion is complete, Rite Aid is reaping the benefits from the project. Its security systems are now up-to-date, and this has translated into lower false alarms and the resulting reduction in false alarm fees across its footprint.

Because the systems are more uniform, the data extracted can be used across a number of departments and projects. Common occurrences in the drugstore industry are audits from outside agencies, including state pharmacy boards and other government agencies. With consistent reporting capabilities, Rite Aid is able to quickly access information from the security system that provides detailed accounts of what occurred should a question arise during the review period. Administering the new security system also provides Rite Aid with cost savings through reduced labor and associated costs.

Security Training

Advancements made in loss prevention technology have provided tremendous support for the loss prevention industry. Innovations made in CCTV and alarm systems—like those described earlier in this report—have helped to help move the industry forward.

Any experienced loss prevention executive can appreciate just how much change technology has brought to our profession. But advances in security technology have hardly diminished the importance of security personnel. They still comprise the bulk of a retailer's spending on security, so squeezing as much productivity from them as possible is critical. Their action or inaction is still the primary cause of negligent security lawsuits. And regardless of technology's impressive new capabilities for spotting event anomalies, security staff is still what companies rely on to respond to trouble and resolve problems. Security officers are no less important today; their value equation has simply shifted—from mere deterrence to reacting, investigating, and managing incidents.

So despite new technology—or, rather, because of it—LP executives need to pay close attention to the training their department provides to its human element.

When viable loss prevention technology solutions are found, those solutions must be coupled with effective training programs to ensure that these tools successfully meet the needs and objectives of the organization.

Training and awareness programs are key aspects of most loss prevention strategies, in fact. We use them to show employees how loss prevention concepts can and should be embedded in their everyday responsibilities. We use them to help keep our customers and employees safe. We engage our employees with strategies that reduce losses and enhance profits. We also build upon fundamental training and awareness strategies to develop our loss prevention teams.

In today's retail world, loss prevention technology has become a primary force behind many of our strategic plans, driving many loss prevention initiatives and fueling new solutions in an omni-channel retail environment. With shoplifting and retail theft causing retailers tens of billions of dollars each year, retail loss prevention leadership and retail management teams are continuously looking for ways to find solutions to deter theft incidents and other forms of retail losses. But every technology tool still must be coupled with a thoughtful program designed to train employees on using and maximizing value from it.

Obstacles

Paper-based and on-the-job training is the norm among many retailers across the US. In such instances, retailers may not allocate a large budget for a corporate training staff and instead rely on the experience of the people hired at the store and district levels to provide the proper guidance and training for new associates. Often, it is left to fellow associates to teach the new associate "the ropes" and get them acclimated to store policy and procedure.

Other retailers choose to rely on corporate trainers to provide support to regions and individual stores for classroom and seminar training. Corporate directives may be initiated by the corporate loss prevention department and then communicated through the corporate manager of training, who delivers the message, policies, procedures, and necessary training materials to the stores.

Both strategies have barriers to success that loss prevention leaders must work to address. For example, the use of a training manual and paper test alone introduces a margin of error based on interpretation. Written procedures are subject to the interpretation and level of understanding of the reader. If not properly explained or demonstrated, this in itself may lead to a misunderstanding and failure in communication. This failure then leads to improper execution of the directive…a mistake that could cost the associate his or her job and the company a large sum of money.

The use of store and district managers as trainers leaves another opportunity for inconsistency, both in the varying levels of experience, the existence of pre-existing habits in approach to loss prevention, and the interpretation of company policy. This process also relies on the training skills of the managers, which may not always be the best.

Carelessness and turnover are also potential obstacles, resulting in test results falling through the cracks and never making it back to the corporate office.

In all instances, communication in training is often problematic. Communication is critical in both directions. First, the message has to go out from the corporate office and reach the designated audience within the stores. Then feedback and results must be communicated back to the corporate office.

E-Learning

There are many different ways to prepare individuals for security assignments, from push-and-play videotapes to detailed simulation exercises. One common element for improving any aspect of a training program—be it a computer simulation or a knowledge test—is to have it mimic or simulate as closely as possible the actual environment in which staff will be working. Test questions should reflect actual scenarios, videos should be directly applicable to the officers watching them, and trainers should use lessons learned to create realistic scenarios in classroom training and simulation exercises. More than younger students, adults learn by doing and need to perceive a direct relevance between the training material and their actual job duties.

Using an online learning management system is one strategy that can be employed to address some of the challenges identified above. Such systems typically utilize dynamic video scenarios to teach and train by visual example. Additional scenarios are then utilized to test the comprehension and retention of the training material.

The most immediate benefit of an interactive training strategy is typically cost savings realized from the elimination of the paper-based system. A retailer may allocate an enormous amount of money and resources to initiate, maintain, and update the paper training manuals within the stores and the paper tests taken by the associates. Considering this, combined with the amount of postage and shipping costs associated with communicating results back to the corporate office, return on investment for implementing an interactive strategy can be realized within the first year. Further savings may be achieved in the elimination of travel and facilities costs associated with seminar and classroom training.

Among the more intangible savings may be availability, consistency, liability, and accountability.

- A computer-based curriculum can permit access to training seven days a week on a schedule convenient to the associate, department, and store.
- Consistency is virtually guaranteed as the same message is seen and heard by each associate in exactly the same way, every time.
- Results can be tracked and every answer documented for review or for administrative action, enhancing accountability.
- Liability is reduced, as better trained associates make fewer mistakes, and because the training method permits associates to learn from their mistakes in a virtual environment.

The final benefit offers both a tangible and intangible savings of money and of time in the collection and analysis of training progress and results. Results can be measured on a particular individual or a comparison may be made between compliance results and adherence to company standards within districts or regions. This not only provides better tracking of progress and results, but better productivity and performance of the training objective. This allows focus on key areas of concern, individual weaknesses, career development, and the development of additional training programs.

Systems Training

Regardless of the sophistication of an electronic security system, it won't prevent incidents without the appropriate response of those managing it. Just like technology, the human element of security—which relates to decision making, common sense, and awareness—must be upgraded.

This can only be effected through education, training, and drilling of personnel. It's not rare for organizations invest in million-dollar security equipment systems but fail to invest in educating personnel on how to use it or assessing whether everything possible has been done to prevent security staff from making mistakes regarding the use of it.

Gerald Becker, vice president for physical security at USS, a leading integrator of IP video and access control systems, has worked with LP departments to upgrade their old analog systems to modern IP-based systems, like video and access control—and training is one of the most common challenge he's seen them face. "Training is always at the top of [the] list. You can deploy the most advanced system in the world with all the bells and whistles, but if your employees don't know how to use it to its fullest extent, that system is useless to you. As a result, your ROI can go right out the window."

Becker notes that the capabilities of new IP video systems are a primary reason why training is critical. "[They're] not necessarily more complicated [than old analog systems], but they certainly have a lot more options and features. In the old days of analog, there were just a few buttons—Record, Play, Rewind, Fast Forward. But with a software-based enterprise system, you can have dozens of features and settings. That's really why modern companies are deploying IP systems in the first place—better analytics, better insight, more capabilities, quicker decision making. The challenge is to go from having employees who are used to a few simple commands to having them understand and grow comfortable with a system that is feature-rich."

The starting point, according to Becker, is to determine what kind of training is available for the platform you are considering. "Nowadays there's a myriad of solutions and devices with lots of different ways to set up an enterprise system. If you are interviewing several integrators—your deployment partners—quiz them about what they will do after the system has been installed." Some questions to ask:

- Will they train your employees?
- How?
- How long before employees will be fully comfortable with their new system?

"When you are investing a lot of money into something, you want to see the ROI as quickly as you can," said Becker. "But there is no ROI if your employees are only capable of pushing the handful of buttons they already know—Record, Play, Rewind, Fast Forward."

When purchasing a solution, a company can decide to do the training on its own. But Becker notes that this can chew up valuable time. "Besides, the people that know your system the best are those that are selling it to you and installing it for you." USS puts a great deal of emphasis on training "because your whole ROI really depends on that," said Becker.

To identify training needs and decide who should provide it, Becker identified some key questions to ask solution providers:

- What will it take for my employees to be able to fully take advantage of the solution?
- What does your training program look like; is it portal, module, online, on-site?
- Do you provide different levels of training; for example LP folks, marketing, security, operations, et cetera?
- What kind of service or training agreements are available to us?

"Really, the ultimate question is, after you've purchased the systems, will you still have the help you need? And of course, the answer you are looking for is a firm and unequivocal, 'Yes,'" Becker noted.

Contributors to this special report include Nathaniel Fry, Robert Rice, Colin Peacock, Lee Pernice, Jeff Pepperney, and James Lee