



Evolution: A Comprehensive Solution for Retail Loss and Security

Retail loss control, the driving force behind security applications, is a complex and vital component of retail operations. However, today's most innovative loss control approach is based on a relatively simple idea—integration. Learn how thoughtful assimilation of access control, intrusion detection, and video surveillance technologies can bolster the effectiveness of each system, allowing them to work together as a powerful, streamlined security technology process.

Table of Contents

I.	Executive Summary	3
II.	Retail Security Concerns Today	4
	Shoplifting	
	Employee Theft and Abuse	
	Commercial Burglary and Robbery	
	ORC	
	Supply-Chain and Cargo Theft	
	Return/Refund Fraud	
III.	Moving Beyond Basic Security Technology	6
	Detection Systems	
	Access Control	
	Video Surveillance and Analytics	
IV.	Benefits of Integration	11
V.	Conclusion	12
VI.	References	13

I. Executive Summary

Successful asset protection is an integral building block in the success of any retail operation. However, the challenge of controlling loss and theft continues to frustrate retailers worldwide, with merchandise losses still averaging over \$40 billion a year (Hollinger and Adams).

Peripheral and cash losses from crime and theft incidents add to this already crippling figure. The money and time retailers invest in investigating and reacting to merchandise loss, as well as the growing civil liability surrounding theft events all add to the financial impact (Hayes, 1997).

Today, theft and loss pose the following multi-dimensional threats for retailers:

- increasing and costlier losses
- inability to easily pass on or absorb these financial losses
- increasing legal risk for inept crime and loss control efforts
- an unending supply of savvy, adaptive criminals

Additionally, numerous alternative shopping formats, such as e-commerce, catalogs, and home shopping networks, are now vying for consumers' attention, thus challenging the traditional retail store format to remain relevant and profitable in this technological age.

In an increasingly aggressive retail market, protecting assets and ensuring a safe, comfortable consumer experience is more imperative than ever for maintaining profits and a competitive edge. It is no surprise then, to learn retailers invest over \$4 billion annually (Hollinger and Adams) on loss prevention (LP) technologies. But what *is* surprising is that despite this heavy investment, and despite the broad arsenal of security products on the market, industry-wide loss levels have remained relatively consistent over the last decade (Hollinger and Adams).

Consequently, companies aiming to mitigate the risks involved in retail crime, and improve their bottom line, must maximize their security technology return on investments. One way to boost ROI is integration.

As any leader, coach, manager, or trainer knows, a team approach is stronger than that of an individual. The team-based approach to LP is a growing trend in retail operations, and for good reason. Forward-thinking retailers understand successful company-wide loss prevention is predicated on a comprehensive LP program that integrates deterrent, detection, and documentation capacity. Brad Dykes, Director of LP Analysis and Process Improvement for AutoZone, states "Ideally, we hope to integrate all technological and reporting components into one strategic platform. Our exposure to negative or at-risk events can be greatly reduced by the seamless transition from actual event to data to resolution."

Similarly, sound asset protection combines individual store efforts, security technologies, employee awareness and training, strict policies, ongoing monitoring and measurement, focused investigations, and support from the topmost tiers of the corporation. Just as a well-integrated LP program benefits the corporation overall, a well-integrated security system benefits and simplifies the LP program.

*Retailers invest over
\$4 billion annually
on loss prevention
(LP) technologies.*

Source: Hollinger and Adams

In this paper, we will review current challenges in retail loss control and asset protection, and discuss the various security technologies retailers employ to combat those challenges. We will go on to illustrate how integration increases the effectiveness and efficiency of each security technology, thus strengthening the LP program overall.

II. Retail Security Concerns Today

Shoplifting, employee theft and abuse, return/refund fraud, Organized Retail Crime (ORC), burglary, violence, and cargo theft comprise many of the most significant concerns in today's retail industry, and remain the most serious threats to profitability and store safety.

SHOPLIFTING

Accounting for over 40% of retail losses, shoplifting continues to frustrate retailers. Each year, the US retail industry suffers approximately \$15 billion in losses due to shoplifting alone (Hollinger and Adams). Ultimately, all types of shoplifting affect retail profitability, but most damaging are the professional shoplifters, or "boosters." These career criminals steal large quantities of valuable merchandise and convert it to cash via fences, flea markets, online auctions, and street vendors. Boosters are often well aware of stores' security systems and will use a variety of tactics to circumvent or counter these protective efforts.

While there is no "typical" shoplifter (the behavior crosses all ages, gender, race, and class strata) and types of shoplifting vary just as widely, one fact remains discouragingly constant—as anti-shoplifting strategies evolve, so too do the shoplifters. Despite advancements in anti-shoplifting security systems, the retail industry has seen little change in loss levels over the past 15 years (Hollinger and Adams). In order to truly affect shoplifting, the current security devices being used to combat it—primarily EAS, shelf guards, and CCTV—must be adapted to include the capability to better identify theft dynamics, and alert LP and store operators in a timely, accurate manner.

Larry Foster, Director of LP Forensic Analysis for CVS/Caremark, explains, "Next generation loss prevention is all about the integration of yesterday's stand-alone systems with today's transaction-monitoring information systems. Integration needs to exist at all levels (hardware with hardware, hardware with software, software with software). The critical component needed to thread each and every combination is data management."

Next generation loss prevention is all about the integration of yesterday's stand-alone systems with today's transaction-monitoring information systems.

Larry Foster, Director of LP Forensic Analysis, CVS/Caremark

EMPLOYEE THEFT AND ABUSE

Employee theft and fraud, perhaps the most insidious of retail threats, accounts for several billions more in store cash, inventory, and supply losses every year. For many retailers, internal theft can be devastating. Employees often have insider knowledge of, and access to, both products and procedures. They know where cash is stashed, and they are often able to acquire passwords, alarm codes, and combinations. They may even have copies of store keys. Store associates are intimately aware of security procedures and systems, and therefore believe they are able to accurately weigh their risk of being caught if they steal. More significantly, employees are able to accurately assess the attentiveness of coworkers. They know when alert, caring managers and colleagues are staffed,

as well as when naive or apathetic associates are in charge. According to Read Hayes (PhD, CPP), Loss Prevention Research Council and University of Florida researcher, “Employees may come to a workplace already having stolen from a previous employer. They may also be easily led by dishonest peers, have tolerant or conditional attitudes toward workplace deviance, feel overworked or ignored, sense low workplace security, and learn the best ways to steal from the store through experience.” All of these elements equip the average employee with the tools he or she needs to carry through with criminal behavior if the need or desire strikes them.

Like shoplifting, types of employee deviance range considerably, some of which include “sweethearting” (passing on low prices to friends, family, and accomplices), trading goods with other businesses’ employees, under-ringing items at the register to pass along a lower price, removing goods from the store in all manner of ways (via trash removal or storage areas, or simply hidden in bags or clothing), cash theft from registers or safes, manipulation of returns or receipts to obtain cash or store credit, embezzlement, and payroll or accounting fraud (Hayes, 2007; Hayes, 2008b).

To minimize employee theft and deviance, it is important to thoroughly screen applicants, create a workplace atmosphere that promotes honesty, and encourage and reward good behavior while making it clear dishonest behavior will not be tolerated. It is also important to develop an LP program that employees acknowledge as being thorough, accurate, and well-monitored. If dishonest employees perceive a store’s security systems as weak or spotty, they will take advantage of the situation. Control procedures, reporting hotlines, and access control and detection technologies signal employees their productivity is appreciated, and reinforce that dishonesty will be quickly detected and punished. Like all commercial threats, employee deviance should also be addressed with integrated policies and technologies. CCTV provides particular advantages to retailers, especially when tied into other systems as made clear by Kevin Ach, Director Loss Prevention Operations for Office Depot, “Integration is critical. We would like to link CCTV with our POS Exception Reporting system for example. We believe this would assist on our case development. . . .”

COMMERCIAL BURGLERY AND ROBBERY

Research indicates retail stores are nearly four times more likely to be a target of burglary than other commercial institutions such as wholesale, service, or manufacturing establishments. The



Research indicates retail stores are nearly four times more likely to be a target of burglary than other commercial institutions such as wholesale, service, or manufacturing establishments.

reason for this is simple—the merchandise is visible, providing the burglar with a clear goal and knowledge of exactly what’s available. Also, most burglars are well aware it takes most police officers an average of 4 - 20 minutes to respond to an alarm—enough time to allow for an escape before authorities arrive on the scene (Cromwell, Olson, and Avary).

Burglary and robbery present a particularly dangerous form of retail theft, as they can result not only in major financial losses, but also workplace violence and even fatalities (Tyler). Smash-and-grabs, hold-ups, “Ram-raids” (crashing vehicles through doors or windows), and after-hours break-ins also contribute to an overall perception of an “unsafe” store, which can in turn lead to

consumer fear of crime, a drop in sales as legitimate shoppers limit purchasing to daylight hours, and consumers choosing alternative shopping formats or seeking out different retailers altogether (also called “avoidance behavior”).

Typically, retailers employ alarms (usually remotely-monitored) to address burglary and robbery. However, false alarms, delayed response times, and in some cases, failures to respond at all, are all drawbacks to traditional burglar alarms. To successfully respond to a break-in, and more ideally, to deter it, retailers should implement more “intelligent” alarm systems to clearly convey to would-be offenders that burglary will be detected, and will also quickly be followed by apprehension and sanction. Access control systems can limit theft and violence in workplaces by keeping everyone but current employees out of restricted areas.

ORC

Organized retail crime is serious, widespread, and multi-faceted, creating between \$12 - \$35 billion in annual losses (Hayes and Rogers). Criminal groups of varying sophistication including “boosters”, fraudsters, and fences steal from or fraudulently attack retailers, as well as their manufacturing and cargo partners (Hayes and Rogers). With the inherent violence, contamination dangers involved, and steady influx of knowledgeable criminals into the US, ORC takes on a larger priority within the context of retail security and safety.

Unfortunately ORC shows no sign of abating, so retailers must take a targeted and proactive approach to disrupting these determined offenders and reducing demand for illicit goods. While a vital part of improving anti-ORC strategies involves strengthening state and federal laws, retailers have also begun to employ several systems-based tactics to fight ORC, some of which present much promise. Greater intelligence gathering by retailers and law enforcement, focusing of store detectives in high-loss locations, and active, multi-jurisdiction investigations of ORC networks all need to be improved and expanded. The ORC coalition and LERPNet show promise as new industry and nationwide efforts.

SUPPLY-CHAIN AND CARGO THEFT

Theft of merchandise as it travels from manufacturer to distributor to retail outlet is another source of large-scale loss, and a focus of LP efforts. In the US, annual direct losses from cargo theft are estimated at \$10 - \$20 billion per year (Boyd).

Truckload theft ranges from colluding dishonest drivers, to drivers losing trucks or loads when decoys distract or drug them, to armed hijacking in truck stops, or remote or urban areas. Groups also use other dishonest employees such as loaders, dispatchers or guards, and contracted loaders or drivers to assist with or steal quantities of product from distribution centers, warehouses, trailer drop-off points, slow-moving trains in urban areas, and staged or parked trucks. Loss prevention professionals are tackling supply-chain and cargo theft, using new advances in detection systems including radio frequency identification (RFID) and global positioning software (GPS).

*In the US, annual direct losses from cargo theft are estimated at **\$10 - \$20 billion per year***

Source: Boyd

RETURN/REFUND FRAUD

Approximately 9% of all returns are fraudulent, costing retailers billions each year—a cost, of course, that is inevitably passed on to the consumer. In a recent survey of LP executives, over 70%

indicated return fraud and abuse (RFA) as an important issue for their companies, and about half of those survey stated that reducing fraudulent and abusive returns is a “very high” priority for their companies in the current year (Johns and Hayes, 2003; Hayes, 2008a).

Abusive refund schemes have expanded at an alarming rate. Many of newest types of RFA are computer-assisted, involving phony or altered receipts, computer-generated UPCs affixed atop actual UPCs to generate more refund dollars, and gift card fraud. These sophisticated techniques present an ongoing challenge for retailers—how to minimize RFA without creating restrictive policies for legitimate consumers. Because types of RFA vary so much, solutions for it are also wide-ranging. One systematic solution many retailers employ is POS exception reporting, which can identify illicit activity occurring at cash registers. Retailers and providers also use software to track chronic or known return fraudsters and abusers, common phone numbers and addresses. Others use serial numbering and tracking systems on electronics, while some retailers use special receipt paper and ink, or check digits.

Return abuse is a very large and costly problem, in which customers “borrow” and return products rather than purchase them. To stem their losses, many companies are requiring re-stocking fees and even denying frequent returnees.

III. Moving Beyond Basic Security Technology

Historically, LP strategies often focused on “body counts”; that is, the more criminals apprehended, the more successful the asset protection program was considered (Hayes, 1997; 2003). Today, LP is more focused on proactive approaches to crime and loss control. Shoplifting, internal theft, burglary, ORC, cargo theft, and return fraud and abuse continue to generate large annual losses, and so retailers have been forced to move beyond traditional, singular LP strategies and turn to new methods for decreasing retail crime, such as technology-based electronic security systems. The ongoing development of enhanced protective procedures and technologies (RFID tags/readers, unique inks, dyes, isotopes, holographics, and biocodes), as well as enhanced GPS/cell-satellite tracking, pattern recognition software to profile point of sales, reordering, shipping and receiving, ORC investigative software, evolving CCTV analytics software, and computerized and web-based store and truck locking/seal systems all hold promise in the fight against retail shrinkage. To be most effective, however, these new technologies must be tied into intelligence, investigations, R&D efforts, and law-enforcement facilities—again reiterating the need for sophisticated integration within the retail security systems.

DETECTION SYSTEMS

In the retail industry, several types of alarmed detection systems assist security professionals with minimizing theft and loss. Intrusion detection systems sense, report, record, and pattern all entries, break-ins, and burglaries. Theft detection systems handle illegitimate removal of merchandise during operating hours; and fraud detection systems (usually in the form of software or procedures) handle fraudulent receipts, returns, and internal theft.

Intrusion detection systems send an alert for any authorized, unauthorized, or forced entries into a store. Comprised of door, window, and motion detectors, these systems are generally tied into an alarm that notifies both local officials and LP staff of a security breach. Most retailers routinely include burglar alarms in their overall LP program, and like any individual LP effort, burglar-alarm systems create both challenges and opportunities.

In a recent study, over 70% of LP executives stated they use remotely monitored burglar alarms. One major drawback of remote monitoring is the prevalence of false or non-crime event alarms. Too many false alarms create issues with local authorities, who may become unresponsive, require third-party verification, or charge penalty fees if a particular store suffers numerous false alarms. Over half of the LP executives in this recent survey reported their store has suffered suspended police response due to an increased number of false alarms. Sadly, when offenders learn of a store with frequent false alarms followed by minimal response, that store may become more vulnerable to actual burglaries (Johns, Scicchitano, and Hayes, 2008a).

Over half of the surveyed LP executives reported their store has suffered suspended police response due to an increased number of false alarms.

Source: Johns, Scicchitano, and Hayes, 2008a

Another disadvantage of traditional burglar alarms is response time; seasoned thieves are undeterred by an alarm system if they know it will take a certain amount of time for authorities to react. Also, traditional alarm systems provide very little assistance to retailers in carrying through with criminal prosecution; so, unless a witness happens to see the break-in, the incident goes largely unrecorded.

A more useful form of intrusion detection involves integration with other systems such as CCTV, video analytics, and access control devices. For instance, if a CCTV system equipped with video analytics were connected to the alarm, the video analytics system could potentially recognize suspicious versus benign activities, and control the alarm system accordingly, thus minimizing false alarms. Moreover, an alarm system integrated with access control devices could provide valuable protection in the case of a legitimate security threat. For example, an employee who spots serious offender activity, such as armed robbery, could with one subtle press of a button activate the alarm system, alert authorities, and initiate automatic locking of expensive product displays.

Theft detection systems in the retail industry most often come in the form of electronically monitored tag and gate systems. To mitigate the crippling effects of both internal and external shrinkage, many retailers partially rely on electronic article surveillance (EAS) tagging systems (Hollinger and Adams). These devices work through placement of gates at the exit point which are able to detect "live" tags attached to items. Visible EAS hard or soft tags and source-tagged soft tags differ in that source tags are placed inside packaging or even inside the items during manufacture. Visible EAS tags are added to merchandise after the fact, usually once the merchandise is in the store. Unless removed or deactivated at the point of purchase, these tags activate an alarm when passed through the gates.

In theory, store employees will react to the alarm sound and either reconcile a faulty tag with a receipt, or apprehend a shoplifter. Unfortunately, the reality is most alarm activations are not theft related, and are either live tags not deactivated by employees, or that came into the store from other retail stores. Likewise, few accurate alarm activations actually elicit a proactive response from staff (Hayes and Blackwood, 2005). In addition, motivated criminals can easily avoid both EAS and source-tagging systems, usually by removing or altering the tags, creating foil-lined "booster bags" to thwart the alarm systems, running when approached, or simply lifting tagged items over exit door antennas to avoid alarm activations.

Although EAS has been considered a staple in loss prevention over the past few decades, a recent survey indicated LP professionals are well aware of its shortcomings; while approximately 80% of retailers use it (Hollinger and Adams, 2007), only 44% of LP professionals describe it as effective as realistically executed (Johns, Scicchitano, and Hayes, 2008b).

LP professionals would likely see stronger results from detection systems like EAS if the devices were tied into other types of security systems. For instance, consider an intelligent tag that, when tampered with, signals for CCTV cameras to zero in on its location. The cameras could then, in turn, issue an instantaneous alert to security staff in order to direct attention to the suspicious activity. They could even issue an audible warning such as “This store is monitored by video camera surveillance.” or “Shoplifters will be prosecuted to the fullest extent of the law.” The image is also transmitted to the manager’s handheld device.

The newer forms of theft detection, using RFID and GPS, allow retailers to actually track individual merchandise or shipments of merchandise to prevent illicit access as products move from manufacturer to distributor to retail outlet. Global Positional Systems are most commonly installed in tractors or trailers as a means of tracking cargo as it travels across distances, enabling easy location of property and the ability to track a driver’s course. This technology is particularly helpful in combating supply-chain and cargo theft. RFID performs in a similar manner, though it is installed on products or containers of products. It too can be used to prevent supply-chain and cargo theft, but it can also be used on a smaller scale to track products in stores and beyond. Both of these technologies present an enormous amount of opportunity for LP professionals wishing to reduce cargo and supply-chain losses, as they allow for detailed, remote tracking of merchandise across the country and the world.

To combat return fraud and abuse, retailers use POS refund systems, either purchased from an outside vendor or developed in-house, to process returns. Half of surveyed LP executives stated they used a POS system developed in-house, while the other half reported they purchased a POS system or package from a vendor. In either case, these systems allow retailers to automatically tie receipted returns to the original receipt value, or in more sophisticated and integrated systems, allow retailers to swipe a driver’s license in order to obtain customer information such as name, address, and phone number. If a POS system is unable to perform this function, merchants usually choose to enter the information manually. In either case, retailers routinely attempt to identify “bad returnees” when they lack a receipt in order to prevent future abuse.

With the swipe of a driver’s license, automated POS systems can immediately identify an individual and determine if she/she fits the profile of an abusive returnee.

Automated POS systems are helpful in pinpointing “bad” returnees, systematically identifying those repeat offenders whose purchase/return profile is consistent with return fraud, but there is always room for improvement. Ideally, merchants would employ a computerized system programmed to identify returnees and analyze past behavior before authorizing a return. Recently, some advanced technologies have been developed that are able to perform this function with the swipe of a driver’s license or ID card. Such systems are able to immediately identify the individual and determine whether or not he/she fits the profile of an

abusive returnee. This new software uses the transaction history of the consumer or employee to identify behavior that is associated with return fraud and abuse. Only one-third of LP executives

stated they considered their return policies and system effective in deterring return fraud; this suggests an interest in development of more advanced RFA systems, and perhaps the implementation of an industry-wide shared return authorization database for tracking repeat offenders.

While these technologies are headed in the right direction, integration with other systems could also benefit them. For instance, if a POS system were to converge with video analytics, LP managers could be notified when any suspicious return or refund fraud is taking place. Cameras in the POS area would be directed to focus in on the register in question, and the incident could be intercepted or addressed before the transaction was completed. If not, video evidence of the entire incident would be readily available for review. In addition, dishonest employees would likely be deterred from this type of activity knowing a comprehensive video analysis system was being used, and that video footage could easily be used as evidence.

ACCESS CONTROL

In the retail industry, “access control” refers to the many different techniques used to keep thieves from illegally removing merchandise from a store. These include “smart” fixtures, locking cases, cords, cables, lanyards, and ink-dye tags. Historically, retailers have used access control devices to deter shoplifters, and in fact, they are usually effective in doing so. Offender research has indicated that shoplifters consider merchandise kept in locked cases, or attached to fixtures with locking cables or cords, as not worth the risk of shoplifting. However, there is an inherent drawback to using such restrictive fixtures—they decrease sales. Legitimate consumers want to touch, feel, and experience products prior to purchase, and are frustrated when merchandise is inaccessible. So these days, retailers must constantly balance between keeping customers happy and keeping products out of shoplifters’ hands.

Integrating access control devices with other security systems may be the perfect way to strike this balance. Consider, for instance, the shoplifter behavior known as “sweeping”. In a product “sweep”, a professional shoplifter quickly and systematically removes a large amount of small, expensive items from shelves or hooks. They may, in fact, remove all of a particularly desirable item (printer toner, for example). This is not only a major hit for the retailer; it has long-lasting repercussions when consumers, frustrated by the resulting out-of-stocks, turn to other retailers. Special curved “anti-sweep” hooks have been designed to make sweeping slightly more difficult and time-consuming for the offender, but outfitting these hooks with sensors and integrating them with video surveillance would provide a significantly more powerful deterrent effect. The fixture itself, or video analytics, would be able to sense when sweeping behavior occurred; it would immediately signal to CCTV cameras and alert LP staff, again, providing photo captures. The shoplifter, if not deterred, could at least be intercepted before the theft was complete. This type of multi-level security technology can deter and intercept theft without rendering products inaccessible to the customer.

VIDEO SURVEILLANCE AND ANALYTICS

Recent years have witnessed monumental advances in the field of video surveillance, so much so that a new subcategory has emerged within it—video analytics. Today, cameras are able to not only film activity, but automatically track suspicious individuals, distinguish between legitimate and illegitimate consumer behaviors, and predict paths of exit once a crime has been committed. Add to this the ability for cameras to interact with and send alerts to access control devices and intrusion detection systems, and video surveillance emerges as one of the most powerful tools a retailer can employ to identify and intercept store losses. Mike Combs, Senior Manager of Supply Chain and Asset Protection for Home Depot, states “Retailers who have begun to integrate CCTV with other

technologies realize the massive potential more advanced levels of integration present. We have successfully integrated POS exception reporting and alarm monitoring with CCTV technology. I think in the future, retail can become much more productive and proactive as we explore the uses of intelligent video solutions and apply them to internal theft and ORC activity.”



Although CCTV has been a mainstay in crime and loss prevention for several decades, until recently these systems have failed to maximize the real potential of protective technology. This is mainly due to the fact that most CCTV systems are passive, providing few ways to actively address crime. In retail LP, traditional CCTV has two uses: “real-time” mode for live monitoring, and “forensic” mode for after-the-fact investigations. However, both modes are difficult and time-consuming.

Fortunately, recent advances in video surveillance technologies have transformed CCTV into a more proactive system, allowing LP professionals to quickly and efficiently filter through useless footage in order to locate and assess key incidents. Data from CCTV cameras are now in digital format, allowing quick, easy, and comprehensive investigation management; centralization of notes, video, and still images; creation of an annotated video investigation; and easy storage, exportation, and file sharing. Considering the amount of time necessary to scroll through endless reels of traditional CCTV footage, this advance saves retailers a substantial amount of money. In

addition, the newest video surveillance systems are able to perform in a way traditional fixed cameras never could; they can pan, zoom, and rotate (either automatically or manually), thus providing greater camera coverage throughout the store and minimizing blind spots that “boosters” and thieves seek out when offending. Ultimately, the comprehensiveness of this type of coverage not only reduces loss, but also contributes to public and employee perceptions of a safe store in which to work and shop.

Additionally, the advent of video analytics allows these systems to do much more than simply record data; they can actually be programmed to identify the types of actions or behaviors LP professionals look for when pinpointing offenders. Research on video surveillance systems can now recognize moving objects and track them across multiple cameras, opening up a multitude of applications for security. With the ability to correlate streams of video data from multiple cameras, the most advanced video surveillance systems are now able to convert passive video data into useful and actionable information. Upgrading a traditional CCTV system to these more advanced iterations often does *not* require an entire system overhaul, making the transition to a more sophisticated technology relatively cost-efficient.

While these high-capacity systems provide a good means of monitoring retail space in and of themselves, their capabilities are expanded even more significantly when integrated with detection and/or access control systems. Video surveillance systems can be set up to monitor high-value assets and high-risk areas, issuing an alert with photos (via email, text, or pager) when merchandise or body movements match theft behavior patterns. Once alerted, LP professionals can then zero in

with manually-operated pan and tilt commands for the camera, and, if necessary, contact security staff on the shop floor immediately. This provides the kind of instantaneous, targeted surveillance necessary to catch professional shoplifters in the act. Cameras can also be integrated with asset control devices, lighting controls, and sound systems to issue an audible warning when a case or fixture is tampered with—activations which are likely to scare off an offender with or without LP staff intervention. In severe security situations, cameras can even detect a behavior and trigger doors, cases, or registers to automatically lock.

Because all the data captured by these video systems is so easily reviewed, categorized, and stored, LP managers are able to review theft incidents faster and in much greater detail, streamlining post-mortem evaluations and better informing subsequent LP efforts. As an added benefit, these systems also provide usable customer and employee behavior data to product marketing and store layout professionals. The video alerts can also signal when customer-entry flow increases, or lines at checkout exceed maximum levels, thus improving store operations overall.

IV. Benefits of Integration

Clearly, integrating asset control, detection, and video surveillance technologies empowers each system with a range of capabilities that would otherwise be impossible. By cross-referencing one system's intelligence with the others, more issues are handled more efficiently.

The following are specific security integration benefits retailers should consider:

- Integration allows multiple systems to be managed on a single-seat interface, enabling just one person to be trained on several systems, thus cutting hours and costs associated with the oversight of multiple systems.
- Overall LP efficiency is improved by assimilating multiple interfaces into one; data from multiple sources is streamlined into one system, and can be reviewed by a minimal amount of employees in minimal time; this cuts down on management, training, oversight time, and costs.
- System complexity is reduced; administrations, service, and maintenance of security technologies becomes simpler and easier.
- Converging multiple security systems imbues each with additional capabilities, reducing risk for crime and shrinkage in the store.
- System components previously used for one purpose alone are made capable of performing multiple functions. For example, cameras that simply recorded activity are now able to also control other systems, like lighting.
- Remote monitoring is made easier, as different groups within an organization are able to access security data from any location, sorting and categorizing it to suit individual needs. Remote monitoring reduces travel expense and inefficiencies.
- Security systems and management systems can be easily linked, allowing reciprocal information exchange.
- Integrated systems build off of existing security systems, allowing retailers to leverage existing technologies as they upgrade to an integrated system.
- Since the new integrated system is designed specifically for the retail space, it is designed to be as efficient as possible for that application, providing flexibility and economy, and making later expansion easy and cost-effective of tactics and tools each system can provide multiplies exponentially. Similar systems also work in retail company distribution and office sites.

- Because multiple security systems are connected to video surveillance, more useful information is recorded for fast, targeted review of incidents, and possible video evidence when required.
- Retailers are able to select preferred vendors for each individual security system, as integration provides a way to assimilate technologies from multiple vendors.
- Adding intelligence to existing systems makes it easier to add on even more advanced technologies in the future.

In essence, integration of retail security systems is a wise choice for any retailer aiming to reduce the expense and man-hours associated with oversight of an LP program. Each technology within the program is improved via its interconnection with other systems, and overall management of LP functions within the retail store can be accomplished through one simplified system. These systems can also be extended beyond the realm of security, and improve efficiency in overall store management, including environmental control such as lighting and temperature, and employee building-access such as swipe cards and identity-based access systems. Incorporating intelligent, integrated security systems into an overall intelligent, integrated retail space management system makes sense, as efficiency is improved on an even greater scale.

V. Conclusion

All retail security systems (asset control, detection systems, and video surveillance/analytics) are designed to reduce crime and protect assets, therefore increasing sales and margin. Why, then, are these technologies so often disjointed, unconnected, and ill-equipped to communicate with one another? The benefits of integrating asset control, detection, and video surveillance systems are obvious; each system will be stronger when supported by the others, and by interconnecting all three, LP professionals can create a web of security systems that thieves, fraudsters, and dishonest employees will find impossible to avoid.

In addition to improving security and minimizing shrink, integrated security systems are an economical way to upgrade LP technologies, because integration builds from existing devices in the store. These existing technologies are assimilated under the umbrella of one streamlined system, and retailers are able to realize a quick, direct ROI as the time and personnel necessary to operate multiple systems is reduced dramatically.

Retail shrink is an enormous and multi-faceted problem—one that is best combated with a comprehensive, holistic LP program. Security technologies are a key element in that program, but they are expensive investments. Therefore, an effective LP program integrates these technologies in such a way that maximum potential is realized. Today's offenders are savvy criminals who know all too well how to manipulate traditional security systems to their own advantage; so, to stay ahead in the perpetual struggle between criminal and retailer, LP programs must strengthen these systems with the newest and most innovative capabilities. Integration provides an efficient way to do just that, systematically targeting illicit activity in the store and protecting assets, employees, and consumers alike.

References

- Boyd, S. "Combating Cargo Loss." *Loss Prevention Magazine* 2007: 5; 68 - 74.
- Cromwell, P., Olson, J., and Avary, D. *Breaking and entering: An ethnographic analysis of burglary*. Newbury Park, CA: Sage, 1991.
- Hayes, R. "Retail Crime Control: A New Operational Strategy." *Security Journal* 1997: 8; 225 – 232.
- Hayes, R. "Loss Prevention: Senior Management Views on Current Trends and Issues." *Security Journal*, 2003: 16; 7 – 20.
- Hayes, R. and Rogers, K. "Catch Them If You Can." *Security Management* 2003: 10.
- Hayes, R. and Blackwood, R. *Electronic Articles Surveillance (EAS) Management*. Unpublished report 2005.
- Hayes, R. *Retail Security and Loss Prevention, 2nd ed.* New York: Palgrave Macmillan, 2007.
- Hayes, R. *Customer Returns in the Retail Industry*. Irvin, CA: The Retail Equation, 2008(a).
- Hayes, R. *Employee Deviance Control*. Virginia: ASIS International, 2008(b).
- Hollinger, R.C. and Adams, A. 2006 *National Retail Security Survey*. Gainesville, FL: University of Florida, 2007.
- Johns, T. and Hayes, R. "Behind the Fence: Buying and Selling Stolen Merchandise." *Security Journal* 2003: 16; 29 – 44.
- Johns, T., Hayes, R., and Scicchitano, M. *Professional and Amateur Shoplifter Perceptions: Implications for Prevention*. Submitted for publication, 2008.
- Johns, T., Scicchitano, M., and Hayes, R. *Burglar Alarm Response: A Pilot Report on Retail LP Executives Perceptions*. Gainesville, FL: Loss Prevention Research Council, 2008(a).
- Johns, T., Scicchitano, M., and Hayes, R. *LP Technology Study*. Gainesville, FL: Loss Prevention Research Council, 2008(b).
- Tyler, K. "Targets Behind the Counter." *HR Magazine* 1999: 8; 106 – 111.