

RETAIL PHARMACY GROWTH STRENGTHENS SECURITY NEED



Integrated Security Programs Protect Data, Pharmaceuticals, Merchandise and Employees

By Jack Finefrock
Vice President, Retail Solutions
Diebold Security

Armed robbery. Employee theft. Data hackers.

Today's retail pharmacies face all of these security threats and more. With pharmacy growth on the rise and a trend toward driving even more traffic into the store, security threats are becoming more prevalent. These threats are prompting the need for robust integrated security programs to protect critical pharmacy operations.

Some of the highest-value items in drugstores are located in the pharmacy. In fact, controlled substances are among the biggest targets of today's thieves. A research letter published by the *Journal of Pain and Symptom Management* stated that "every year, thousands of armed robberies and thefts from pharmacies, manufacturers and distributors result in millions of dosages of opioid pain medications being diverted into the illicit market." [1]

But external theft isn't the only threat. *Drug Store News* reports: "Front-end product can disappear through a drive-through window, and techs can plant a controlled substance prescription, do a label reprint, call a friend to

notify him there is a prescription waiting, and enter a zero co-pay for billing in the computer system.” [2] The friend simply visits the drive-through window and can drive away with a variety of items that ultimately represent loss for the store.

In addition to the pharmaceuticals they are entrusted to dispense, today’s pharmacies also need to protect a vast and ever-increasing amount of data, including patient medical records, prescription histories, credit card numbers, shopping reward program records, insurance information and more. In the wrong hands, this data could be used for identity and health insurance theft, as well as a variety of other fraudulent activities. As customer bases continue to grow, it will take much more than basic security measures to protect the modern pharmacy environment and secure its assets.

Retail pharmacy growth leads to need for integrated security solutions

Retail pharmacy growth is on the rise. A recent report from *Supermarkets & Drugstores* notes that the S&P Drug Retail index rose 5 percent in 2007 versus just a 3.6 percent gain for the S&P Composite 1500 index. [3] Factors contributing to this growth include an aging U.S. population, increased convenience of the retail pharmacy environment and a new trend of adding in-store health clinics to drugstores.

Baby boomers — the approximately 77 million Americans born between 1946 and 1964 who represent more than 25 percent of the U.S. population — began turning 60 in 2006. The aging of this generation will have a significant impact on the pharmacy business. According to *Supermarkets & Drugstores*: “Drug use increases significantly as people age – from less than five prescriptions per year for those under age 44, to 12.5 per year at age 60 and 20 per year at age 70.” [3]

With increased traffic from older Americans and other populations, *Supermarkets & Drugstores* says, “Chain drugstores remain focused on improving demand by increasing the convenience of their offerings.” Strategies

to increase convenience include adding more free-standing locations, offering drive-through pharmacy service, increasing the number of locations that are open 24 hours and offering one-hour photo service. [3]

Of these strategies, drive-through service has been one of the most successful in bringing new customers to stores. And these customers are not just staying in their vehicles. At a 1999 shareholder’s meeting, L. Daniel Jorndt, then the chief executive officer of Walgreens, said, “Drive-through pharmacy attracts lots of new customers to your store. ...First they come to you for prescriptions. After about the third prescription, we see them start showing up in the front end of the store.” [4]

Now, a new trend is emerging to drive even more traffic inside the retail pharmacy store — in-store health clinics and wellness centers. Such in-store clinics may offer basic diagnosis of minor medical conditions, including coughs, colds, strep throat, bronchitis, and sinus and ear infections. Many offer immunizations, physicals and health screenings. They are commonly staffed by nurse practitioners, clinical nurse specialists and sometimes physician assistants and/or physicians.

Drug Store News reports, “It has been about eight years since in-store clinics emerged, and in that time they have quickly grown from an industry anomaly to a viable access point for affordable, convenient, quality health care.” The publication estimates that there are approximately 1,000 retail pharmacy clinics throughout the United States as of April 2008. [5] (See the sidebar titled “The Rise of In-Store Health Care Clinics” to learn more about in-store clinic growth.)

Increased customer traffic introduces new risks into the store environment and raises the need for security solutions to protect what’s on the shelves, behind the pharmacy counter and within the infrastructure. With today’s sophisticated criminals, high-end security integration tools have become a necessity.

The best course of action is to implement a holistic security strategy that combines robust physical and logical security solutions to ensure protection of facilities, inventory, people and data. Retail pharmacies should

Baby boomers began turning 60 in 2006. The aging of this generation will have a significant impact on the pharmacy business.

consider working with a security integrator to develop and implement this sort of comprehensive strategy.

These security partners can help pharmacies:

- Identify areas in an organization that are most vulnerable
- Assess and prioritize which real-world threats would have the most significant impact on the business' physical and critical information assets
- Develop a holistic security strategy designed to integrate physical and logical tools to protect a pharmacy's assets
- Deploy efficient solutions and mitigation strategies that will keep assets safe and demonstrate an ongoing commitment to reducing risk
- Manage and monitor the overall maintenance of a security program
- Integrate, manage and monitor physical and logical security operations

To maintain the security of the pharmacy environment, inventory, counter and data, security integrators may recommend implementing a combination of some or all of the following tools:

- Logical (data) security
- Credentialing
- Access control
- Biometrics
- Video surveillance and alarm monitoring
- Drive-through security and privacy

Logical (data) security

Logical security — the protection of sensitive information and the infrastructure on which it resides — has become a necessity in all walks of life and business. The retail pharmacy market is no exception and needs robust security measures to protect sensitive customer data.

Pharmacy customer records may include personal patient identification information, medical insurance details, prescription histories, sensitive patient information, credit card numbers and other confidential data. Much of this information is regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and must be protected using physical, electronic and procedural means.

According to a study by The Ponemon Institute (www.ponemon.org), the average cost for a retailer to recover from a single logical security breach involving credit card data is \$5 million, or \$50 per customer for direct costs such as legal fees, notifications and fines. And that doesn't even take into account the blow such breaches can deliver to a retailer's brand. Ponemon's research revealed that nearly 20 percent of customers whose credit card information was compromised terminated their relationship with the respective retailer.

To protect customer data, pharmacy systems and networks must be safe, secure and compliant. Any network is an easy target for unauthorized users who are eager to steal customer identities, account information or trade secrets or those whose goal it is to remote-control programs, Trojan horses and other malicious code. Hackers may attempt to overcome firewalls and crack encryption to access personal data. With only simple protections in place, a pharmacy is vulnerable. A robust logical security system with detection software and limited user privileges can reduce vulnerability and provide a stronger likelihood of identifying unauthorized activity by:

- Preventing breaches and threats before they happen
- Protecting valuable data
- Improving information technology security and compliance
- Implementing appropriate responses in the event of a security breach
- Reducing security costs

Logical security — the protection of sensitive information and the infrastructure on which it resides — has become a necessity in all walks of life and business.

Deploying a logical security solution is a complex task. The solution will need to monitor facilities, data centers, firewalls, critical servers, applications and numerous other elements. It is advisable to work with a qualified security integrator to ensure a pharmacy's data is secure. Security integrators can provide valuable knowledge about a business' network environment to better manage risk, proactively protect against emerging threats and produce security monitoring documentation for regulatory compliance.

A security integrator may follow these five steps to develop and deploy a logical security strategy for an individual pharmacy:

- Assess
- Detect
- Remediate
- Protect
- Respond

Assess. Assessing a pharmacy's current situation is a vital first step in implementing a comprehensive data security program. A professional service assessment will help a pharmacy determine how well its critical systems are protected by providing valuable knowledge about the network environment both inside and outside the organization. Are computers and software programs up to date? Are any unapproved programs running on pharmacy computers? Is the network properly secured? Is it safe and compliant?

A firewall isn't enough of a defense to protect critical data. A single point of entry — one unpatched vulnerability, for example — can open up an entire network to outside threats. Therefore, professional data security experts may conduct simulations during which they act as unauthorized users to determine a company's vulnerability to access from outsiders. These experts may use vulnerability assessment tools to evaluate whether the system security is up to date and properly configured, as well as whether

it adheres to security standards and policies or has potential security vulnerabilities. The experts may also use penetration testing tools to assess whether they can exploit a vulnerability in the system or misconfiguration to gain access to a company's systems, as well as to determine the impact of a break in. With the use of wireless computer connections on the rise, assessors may also investigate points of vulnerability related to unauthorized use of a pharmacy's wireless network.

A full analysis of the current data security environment can help the pharmacy's security and IT teams work with a security integrator to develop an overall security strategy. Following an assessment, security integrators should deliver a comprehensive set of reports that detail testing results and provide suggestions about how to protect against potentially devastating attacks. Reports may analyze the attack vectors used, reveal key vulnerabilities and recommend next steps.

Protect. Following an assessment, security integrators will recommend systems and protocols to mitigate risks to customers, employees and the overall pharmacy enterprise. This stage involves the incorporation of customized security software into a pharmacy's computer network. It is best to implement a positive model solution at this stage to provide a high level of security.

Proactive, positive model solutions follow the opposite protocol of traditional virus programs found on home and business computers. Such virus programs mostly rely on reactive, negative model approaches to data security. The programs wait for malicious threats, such as viruses, Trojan horses or other malicious software to be identified in a system; then, they react to block, quarantine or destroy the threats. Because these programs rely first on the identification of a threat on "someone else's computer" to create a signature, they may allow new or targeted threats to reach a pharmacy system without taking action. It is better if lurking threats are not able to penetrate a firewall to reach the computer in the first place.

Positive model solutions provide such proactive protection by allowing only limited privileges to system users and applications. Positive model programs do not rely on detecting an intrusion before flagging a process. Instead,

It is advisable to work with a qualified security integrator to ensure a pharmacy's data is secure.

they create rules that define the “normal,” allowable activities that can occur within critical systems and permit nothing more. This least-privilege environment embraces the philosophy that fewer allowed privileges yield less opportunities for malicious activity. The network or a computer can be programmed to shut down access if an action falls outside the defined, normal scope of operation.

Detect. Implementing positive model solutions in a pharmacy’s data network lays the groundwork for detecting anomalous, unauthorized and malicious behaviors. “Normal” operating procedures are loaded into the system, and flags are set to trigger when behaviors fall outside those parameters. If someone purposefully or mistakenly tries to get around the set controls, the software will prevent this action.

For example, suppose a pharmacist is trying to download files containing customer credit card data to a removable memory stick. With parameters in place to detect such behavior, the system will perceive the request as “not normal” and will prevent the action from taking place without additional authorization. In this case, the proactive system may have helped to prevent a headline-worthy case of identity theft and consumer fraud.

Respond. Positive model solutions can be programmed to alert operators and system administrators that anomalous behavior has occurred. In some cases, the programs may be set to shut down the system or temporarily disable applications or data transfers until an administrator confirms that the anomaly is allowed.

Systems proactively catch threats in the act and respond by stopping the action based on what users and systems are supposed to be doing. For example, in the event that a pharmacist completed her shift three hours ago and someone tries to log into the system as that pharmacist, the system can be programmed to deny access until an administrator confirms the login attempt.

Remediate. Remediation is the final step in the continuous cycle of logical security monitoring. This step helps security system users and operators learn from the cycle to determine what areas of the system need to be stronger and more secure.

At the end of the remediation step, it is time to schedule the next assessment on a recurring basis. Proactively following this lifecycle will help businesses continually improve their logical security systems while continuing to mitigate security risks.

Credentialing

Because sensitive health-related data is a part of the day-to-day pharmacy environment, retail pharmacies are required by law to regulate data access and privacy. Therefore, they must ensure that credentials are in place to grant employees access to permission-only areas or systems. In the retail pharmacy environment, permission may be required to enter the pharmacy area, access computer systems and open safes.

A credential can be any item or token that is uniquely bound to a user’s identity. Credentials fall into four categories of personal information that can be used to establish identity:

- *Something you are:* This category covers any personal characteristic — commonly referred to as biometrics — that can be distinguished such as one’s fingerprint, iris, retina, face, voice, DNA or handwriting.
- *Something you know:* Distinct knowledge such as passwords or a mother’s maiden name qualifies as unique user knowledge.
- *Something you have:* Often referred to as a token, the identifying object is most commonly a card, but can also be a number of other items.
- *Something you are assigned:* These items include one’s name, title, Social Security number, address or other basic biographic information.

Because sensitive health-related data is a part of the day-to-day pharmacy environment, retail pharmacies are required by law to regulate data access and privacy.

The more factors used to verify and authenticate a person's identity, the more assurance a business has that a person is who he or she claims to be. Therefore, retail pharmacies should consider using more than one factor to prove identity, such as combining keycard access control with password entry systems.

In the event that employees are assigned individual passwords to access physical assets and data and information assets, pharmacies may be best served using single sign-on (SSO) and authentication solutions. Employees may have difficulty remembering multiple passwords, which may drive up information technology expenses just for password-related support. And if there are too many complex passwords to remember, employees may write them down and store them in locations that are not secure — often around their workstations — possibly compromising security.

SSO solutions allow users to complete a single login to gain access to multiple resources and software systems. That means there is only one username and password used for multiple applications. SSO systems can be tied to smartcard access and biometric systems for even higher levels of security.

Perhaps one of the best advantages of single sign-on functionality is that the software doesn't make a mistake. Suppose a pharmacist innocently miskeys his password. It's likely that he'll get it correct on a second try. Someone trying to guess a pharmacist's password will likely require several more attempts. A pattern of multiple wrong entries can trigger a system alert that there may be an unauthorized user trying to gain access.

Access control

Controlling access to critical areas of the pharmacy is one of the most basic elements of a strong security strategy. However, good locks don't necessarily equal good security. In fact, traditional key locks literally open the door for unauthorized access, as keys are easy to duplicate. And when an employee leaves a company, many or all of the business' locks may need to be rekeyed in the event he or she made a duplicate key

or did not turn in the original key he or she was assigned. Therefore, retail pharmacies should consider upgrading to more robust access control systems that incorporate higher levels of security than traditional key locks.

Integrated access control systems may incorporate the latest in biometrics and card-reader technology, integrated or stand-alone badging systems, door hardware and systems software. Door control systems provide the ability to easily limit employee access to specific areas and can even be set to allow access at certain times or on certain days.

System operators can control access by voiding key cards or changing permissions for individual users. Not only do these systems give a pharmacy greater control over its assets, they provide complete reporting of employee activity to determine when someone enters a controlled-access point.

In addition, access control systems may also be tied in with event monitoring services to provide managed access control to monitor access to critical facilities, while also alleviating the operational issues that come with managing card access and badging.

Biometrics

If a traditional photo ID or key card is stolen, the thief may be able to assume a pharmacist's identity and gain access to unauthorized medications, patient data, credit-card information or other potentially sensitive items. Advanced biometric technology is at the forefront of mitigating such foul play in the retail pharmacy environment. As a more advanced method of identifying and authenticating users, biometrics are especially useful for areas or applications in which individuals perform sensitive functions.

Biometric systems analyze specific behavioral, biological or physical traits to verify individuals' identities. Such systems offer increased security due to the inherent difficulty of mimicking one's physical identity. Behavioral biometric traits include signature and voice. Physiological biometrics are more commonly used in the retail

As a more advanced method of identifying and authenticating users, biometrics are especially useful for areas or applications in which individuals perform sensitive functions.

environment for applications like access control, log-in authentication for safes and time and attendance functions. These applications use physical traits — such as fingerprints, hand geometry, iris or retina scans, facial recognition and more — to authenticate a person's identity.

Fingerprints are a widely used biometric for subject identification. Electronic fingerprint readers develop algorithms based on the ridges found on the epidermis, or outer layer of skin, of subjects' fingers. When an employee uses a reader to gain access to a pharmacy safe, for example, his fingerprint is compared to the algorithms on file to determine access permission. More advanced readers can analyze fingerprint ridges several layers below the epidermis for a more accurate scan.

Hand geometry identifies users by the shape of their hands. Electronic readers measure multiple dimensions of a user's hand and compare the measurements to those stored as algorithms on file.

Iris recognition systems utilize pattern recognition techniques to identify users. High-resolution images of an individual's irises are converted into digital templates. These images capture the unique details and intricate structures of the iris such that the resulting template can identify an individual. More advanced retinal identification systems are also viable biometric devices; however, these technologies are not as prevalent in retail environments due to their higher cost.

Facial indexing technologies catalog or index a person based on a digital image or video frame. Indexing analytics compare selected facial features — such as the distance between one's eyes or ears — between the image and a facial database (random at first and then associated with particular faces later on). Face recognition is more accurate however, using 3D technology or readers to identify and verify.

Additional biometric technologies exist that analyze keystrokes, hand veins, odor, DNA, gait and ear canals. However, these applications may not be necessary for use in the pharmacy arena due to their increased complexity and higher cost.

While biometric applications are highly secure, combining biometrics with other forms of identification, such as ID

cards or personal identification numbers, will provide even greater system reliability.

Video surveillance and alarm monitoring

Retail alarm and intrusion detection solutions help facilities maintain proper levels of security. Such solutions can include a comprehensive range of alarm terminals, detection, annunciation and communications devices. Reliable systems are capable of transmitting alarm signals via the Internet, network and phone lines using dial-up, cellular, wireless, Internet Protocol (IP) or long-range radio frequency (RF) communications technology. But the use of such solutions can make facilities vulnerable to false alarms, which can be inconvenient and expensive.

False alarms caused by simple human error could pose as much of a threat to a retailer's bottom line as the theft the alarm system was designed to prevent. Each day, there are multiple opportunities for alarms to be triggered: in the morning when the opening staff arrives, in the evening when the cleaning crew arrives, signage that moves in the line of a passive infrared detector, outdoor disturbances causing vibrations that trigger an alarm and more.

Intelligent dispatching technologies like video and alarm verification are security monitoring enhancements that can accommodate human behavior. Security monitoring providers can use existing devices to come into a store — virtually — and verify the nature of alarms.

Here's how video and audio alarm verification work: Let's say a member of a cleaning crew reports for duty after a store is closed. That crew member likely has other retail customers and may be confused about which code will provide access to this store. If an alarm is triggered, video verification would enable the alarm company to view the activity surrounding the alarm. Once the "intruder" is identified as a member of the cleaning crew, audio verification enables communication between the security monitoring provider and the crew member. If the crew member can verbally provide an access code, the dispatcher can cancel the call, ensuring the store is not penalized for a false alarm.

Biometric systems offer increased security due to the inherent difficulty of mimicking one's physical identity.

Video Surveillance. A key component in a reliable alarm system is video technology designed to record potentially unlawful activity. It can be used for surveillance, monitoring and analytical purposes. The simple presence of video cameras may help deter people, including employees, from committing crimes. Video surveillance may help store owners catch criminals in the act, or at least capture a recording of the crime and perpetrator, which can be used as prosecuting evidence in theft cases. In fact, video surveillance yields some of the best loss-reduction results to date, especially when deployed as a vital component of a balanced and layered security program, including remote video monitoring.

A complete video surveillance system will include essential equipment, such as cameras, recorders and devices, designed to facilitate monitoring and information retrieval.

A full range of camera technology is available, including color, monochrome, wide-dynamic range, day/night IP and covert models. Security integrators can analyze each camera location at a retail pharmacy to determine the appropriate camera, lens and mount required to achieve the best possible images and field of view. Color and monochrome monitors offer varying levels of resolution and styles for flexibility with store locations.

Digital video recorders (DVRs) provide recording storage solutions that can be customized for every store. DVRs offer several advantages. After an alarm is triggered, security personnel can review and capture digital images of an incident. Digital technology also allows the images to be e-mailed to authorities or printed out. DVRs feature large-capacity hard drives, which provide plenty of room to store images.

Switching devices allow security personnel to toggle between cameras and views using bridging, manual, auto sequential or looping/terminating switching capabilities.

Remote Video Monitoring. Depending on a pharmacy's physical location, size, security staffing and other parameters, remote video monitoring solutions should be examined to provide enhanced protection for assets and employees. These customizable services provide outside expertise and intervention when security threats

arise. More importantly, they allow facilities to verify alarms before dispatching responders, helping them eliminate potentially costly fines in the event of a false alarm.

Using an interactive, video remote monitoring service, a store can set a response plan specifying that the first course of action is to remotely assess the problem prior to notifying store management and/or emergency responders. Upon receipt of an alarm trigger, remote security operators can survey the premises before dispatching a responder. For example, security experts may review a series of still images retrieved instantly from a retail pharmacy's networked DVRs. A two-way intercom may be utilized so the operator can listen to activity at the facility and speak with the individuals who triggered the alarm. When an event is verified and the need for outside response is confirmed, the monitoring service will immediately notify appropriate authorities.

Video Analytics. As a side benefit to security functionality, video can be used for more than just surveillance. It can also be used to analyze marketing, merchandising and operational functions within a store. Imagine being able to observe customer behaviors to analyze store traffic patterns, determine if point-of-purchase displays are noticed or simply gauge how busy a store is on various days of the month.

Advanced video analytics, also known as intelligent video surveillance (IVS), can be used to monitor places of interest within a store and log key data for analysis. IVS systems capture data based on algorithms that are set to detect movement or changes in live and recorded video. For example, algorithms can be set to monitor the direction, speed and duration of movements.

Sophisticated content analysis software then reviews the data to qualify it against preprogrammed parameters. Some examples include counting the number of people entering a store, determining the amount of time shoppers spend at a particular location inside the store, evaluating traffic patterns inside the store and assessing drive-through window traffic. Through IVS, store management might discover that weekly sales items are not selling well simply because customers do not spend much time in the area of the store in which these items are located.

Retail alarm and intrusion detection solutions help facilities maintain proper levels of security.

Drive-through security and privacy

Drive-through windows offer a highly secure environment for consumers — the inside of their vehicles. However, a proactive strategy can still be used to enhance customer security and privacy as an overall part of a retail pharmacy's security program.

Drive-through audio systems can be designed to offer varying levels of privacy. For simple two-way communication that does not require divulgence of sensitive information, a standard intercom speaker system can be used. However, to enhance privacy and comply with HIPAA regulations, pharmacies have begun to add private handset telephones to drive-through lanes. These handsets link the customer directly to the pharmacist or technician for a private conversation.

Two-way video can be used in the drive-through lane as well. In particular, these systems provide flexibility for in-store pharmacies or those facilities whose pharmacy windows and personnel are not visible from the drive-through lane.

Drive-throughs are also moving towards point-of-sale (POS) systems that allow customers to perform debit/credit transactions outside without sending their card inside the pharmacy. POS devices save time and also provide security for customers. Pharmacy technicians

don't see or handle customers' cards, eliminating the opportunity to steal credit card information. In addition, customers do not need to reveal their pin numbers over the intercom system for debit transactions.

Conclusion

As the retail pharmacy market grows, so does the market's need for high-end integrated security solutions to protect pharmacy facilities, inventory, data and information, employees and customers. A security integrator recognizes security threats and can help pharmacies develop the best customized plan for individual locations.

A security integrator will consider and recommend the deployment of a variety of tools to maintain security in the pharmacy environment. As part of an integrated, holistic security solution, these tools include logical (data) security, credentialing, access control, biometrics, video surveillance and alarm monitoring, and drive-through security and privacy solutions. An experienced security integrator can partner with a retail pharmacy to deliver the knowledge to integrate, manage and monitor physical and logical security operations.

For more information about high-end integrated security solutions, please call Diebold Security at **1-800-642-6827** or visit **www.diebold.com/security**.

The Rise of In-Store Health Care Clinics

According to Scripps Howard News Service, operators of in-store health care clinics "are trying to revolutionize health care by making basic services as easy to get as a gallon of milk." [6] As more retail pharmacies add such clinics to their stores, they are driving more traffic inside. Higher in-store traffic volume increases a pharmacy's need for a holistic security strategy to protect its assets.

In-store clinics — sometimes referred to as Convenient Care Clinics — are small health care facilities located in high-traffic retail outlets and chain drugstores. They can provide a variety of services such as vaccinations, health screenings, health management advice, dental services, "ask-the-pharmacist" events and health services targeted to specific segments of the population, such as the Hispanic population.

Consumer research company Iconoculture notes, "Health-care delivery increasingly is moving to the storefront. Retailers who marry their products and services with health care hand consumers more convenience, choice and access. And they create a bond with consumers by positioning themselves as a health-care partner." [7]

Supermarkets & Drugstores reports: "Drugstore operators are looking to aggressively expand in-store health clinics [which will] help drugstores target the 30 percent of the U.S. population that does not have a primary care physician or the time to visit one." [3]

According to *Supermarkets & Drugstores*, Walgreen Co. has more than 100 clinics in operation, with "plans to have about 400 open by the end of 2008." The publication also states that CVS/Caremark "plans to open almost 400 additional clinics by the end of 2008, in addition to the 350 that were open as of November 2007. CVS/Caremark intends to eventually add clinics to 2,500 of its stores." [3]

The proliferation of in-store clinics is sure to increase traffic inside stores and raise security needs. Pharmacies are implementing other programs as well.

In addition to in-store health clinics, retail pharmacies are integrating a wellness center mentality into their stores, with some even employing wellness advisors. Wellness center programs may include herbal supplement education, massages and makeovers.

Another successful program driving traffic inside stores is a "brown bag medication review." Patients are encouraged to bring in all of their current medications, over-the-counter products and herbal products in a "brown bag." Pharmacists then review the bag's contents and assess whether there is a concern for any potential problems, such as dangerous drug interactions, side effects or potential duplication of therapy.

End Notes

- [1] Joranson D.E., Gilson A.M. "Drug crime is a source of abused pain medications in the United States." *Journal of Pain and Symptom Management* 2005; 30(4):299-301.
- [2] Symons, Allene. "Drive-throughs, teens create pharmacy shrink challenges." *Drug Store News*, Nov. 23, 1998.
- [3] Agnese, Joseph. "Large Retailers Differentiation Efforts Paying Off." *Supermarkets & Drugstores*, Jan. 24, 2008.
- [4] Frederick, James. "Walgreens' Rx business roars on." *Drug Store News*, March 15, 1999.
- [5] Alexander, Antoinette. "Retail clinics take root in diverse locations." *Drug Store News*, April 21, 2008.
- [6] Davis, Joyzelle. "In-store clinics shake up health care." *Scripps Howard News Service*, June 16, 2007.
- [7] Henderson, Tim. "Walgreens brings more healthcare home." *Iconoculture*, July 12, 2007.

Call on Diebold for the latest in product, service and security solutions.
Since 1859, Diebold has put the customer first.

Contact Information:
Diebold, Incorporated
Global Security Division
818 Mulberry Rd. SE
Canton, OH 44707

E-mail: globalsecurity@diebold.com
www.dieboldsecurity.com

© Diebold, Incorporated, 2008. All rights reserved.
08.08

DIEBOLD[®]
SECURITY