○ ISSUE 1 | ○ VOLUME 4 | ○ June 2007

Security *Solutions*

ADDRESSING THE NEEDS AND SECURING THE FUTURE.

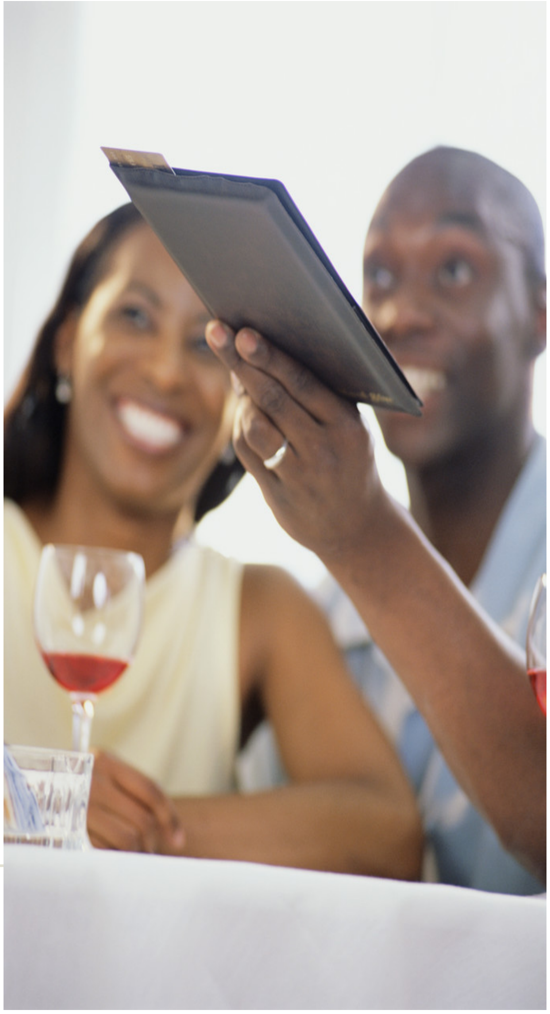
Helping secure your world

Originally when planning this fourth issue of **SECURITY SOLUTIONS** we had considered including an article on terrorism, never expecting that we would so quickly have headlines about terrorism plots in the Caribbean. **Terrorism** and its impact are major concerns for security practitioners and we believe that Caribbean corporate management must take terrorism into account when planning. The Caribbean is not immune to terrorism; a sampling of history will reveal 1976 bombing of Guyanese consulate in Trinidad, 1976 bombing of BWIA office and Cubana Airline plane in Barbados, 1987 derailing of Alcoa train in Jamaica, 1990 attempted coup in Trinidad.

We have included **Hurricane Preparedness Tips** as we are in a region that is prone to hurricanes and June is the start of the hurricane season.

Fortunately we now receive advance warning of hurricanes, such advance warning however is no reason to defer hurricane preparation. Indeed if one waits until a warning is issued you will find that all the hardware stores are filled. Plus in the rush it is easy to forget vital tasks.

If any additional persons in your organisation would like to receive this email newsletter, just send an email to **newsletter@assl.com** with the words “Subscribe Newsletter” in the subject line and the email address, name and organization in the body. To opt out of the mailing list send an email with the words “Unsubscribe Newsletter”.



Prepare for International Low Tech Terrorism

By:
Daniel L. Byman

The movies were an affront to God, encouraging vice and Western-style decadence. So in August 1978, four Shiite revolutionaries locked the doors of the Cinema Rex in the Iranian city of Abadan and set the theater on fire. The firefighters were late, and nearby hydrants did not work. The victims' shrieks could be heard while firefighters and police stood outside, watching helplessly. At least 377 people -- perhaps many more -- were burned alive.

Never heard of the Cinema Rex fire? You're not alone. But the tragedy is more than an obscure, grisly memory from the run-up to the 1979 Iranian Revolution. It's also the second-deadliest terrorist attack in modern history -- deadlier even than airline bombings such as Pan Am Flight 103 -- and one that offers many lessons about the changing threat of terrorism today. Since Sept. 11, 2001, most Americans have worried about what terrorism experts call "spectaculars": massive, ingenious and above all theatrical extravaganzas such as al-Qaida's attack on the twin towers, its simultaneous 1998 bombings of the U.S. embassies in Kenya and Tanzania, and its brazen 2000 suicide-boat assault on the USS Cole in Yemen. But perhaps we should be more worried about the Cinema Rex attack.

Although Osama bin Laden and his lieutenants still dream of spectaculars, a quick glance at the terrorist acts committed since 9/11 suggests that perpetrators are going low-tech, too. As the survivors of attacks in London, Madrid and the Russian town of Beslan will confirm, such tried-and-true terrorism methods as low-tech bombs, hostage-taking and arson have tremendous appeal to jihadists. Indeed, the State Department's annual survey on terrorism, released last week, notes that "in 2006 most attacks were perpetrated by terrorists applying conventional fighting methods that included using bombs and weapons, such as small arms." While the United States and other countries have devoted lots of attention to bracing themselves for the big one, we've spent far too little time considering what we can learn from more mundane -- and more repeatable -- terrorist attacks that can inflict mass casualties.

A look at the various suspects arrested in recent years for crimes linked to radical Islamic terrorism in the United States suggests that the immediate threat we face is angry amateurs, not poised, professional killers such as Mohamed Atta, the leader of al-Qaida's 9/11 team. Most of those arrested do appear to have meant Americans harm, whether by conducting attacks on their own or by raising money for other would-be killers. But these plots were rarely well-developed, and the operators were at best enthusiastic novices.

Consider the case of one of the few Americans actually convicted of terrorism since 9/11: Iyman Faris, an Ohio truck driver and naturalized U.S. citizen born in Kashmir who pleaded guilty in 2003, plotted to destroy the Brooklyn Bridge by severing its cables with blowtorches. Scary, sure -- but a completely absurd way to destroy the bridge, whose many cables are more than a foot in diameter.

These homegrown terrorists don't necessarily share the zeal and anonymity of a seasoned professional such as Atta. Many of those arrested on terrorism charges have a prison record and thus are known to law enforcement officials.

One of the most advanced post-9/11 plots, against the Israeli consulate in Los Angeles and U.S. military facilities in the area, involved four former inmates who began their plotting while behind bars. Former prisoners rarely make ideal comrades; many would sell their own mother for a small reward.

But it's a mistake to write off the angry amateurs. They're not terribly skilled, but it doesn't take that much skill to kill dozens of people -- as the shootings at Virginia Tech so tragically demonstrate. Attacks such as the Cinema Rex fire are easily repeated, and they don't take the years of onerous training and planning that spectaculars demand.

So how can we stop low-tech terrorism? Unfortunately, better defenses can solve only part of the problem. We should defend the White House, nuclear plants and other high-profile targets that would tempt terrorists to stage a spectacular. But we can't defend every movie theater, synagogue, local government building or shopping mall without spending hundreds of billions of dollars and turning the United States into an armed camp.

That leaves offense -- at home as well as abroad. The FBI has tried to penetrate cells of would-be terrorists, often opening itself to criticism for spending enormous resources on disrupting what seems to be a bunch of bungling blowhards. The bureau should keep at it. Of course, sometimes a ballyhooed terrorism arrest will look foolish when the media reveal the plotters' amateurish plans and backgrounds. But aggressive law enforcement can help prevent these amateurs from becoming something more deadly.

Perhaps the best way to fight low-tech terrorists is through community support. For instance, the FBI began to focus on the "Lackawanna Six," who pleaded guilty in 2003 to providing material support to al-Qaida, after receiving an anonymous letter from a member of the Yemeni community in Lackawanna, N.Y., near Buffalo. But to get these sorts of tips, Arab Americans and Muslim Americans need to see the police as protectors, not persecutors.

In this respect, Europe provides a cautionary tale. Governments there, particularly France's, have spent more time trying to shake down their Muslim communities for intelligence than they've spent reassuring and integrating them. The result? An angry, unassimilated Muslim minority whose fringes produce terrorists while its mainstream often resists police efforts to find them. The U.S. government has a fine line to walk here, too. But when in doubt, we should jettison intrusive measures in favor of those likely to win sustained support from Muslim Americans. Finally, the government needs to talk coolly and calmly to the American people. Complete protection against arson, shootings and low-level bombings is impossible. Americans will have to accept a certain amount of risk in their daily lives, recognizing that effective government policies can reduce the threat but not eliminate it. Public opinion is the fulcrum of counterterrorism. Terrorists -- high-tech and low-tech alike -- rely on overreaction from a rattled public and government to do their dirty work. We shouldn't indulge them.

About the author: Daniel L. Byman is director of Georgetown University's Center for Peace and Security Studies and a senior fellow at the Brookings Institution.

Reprinted from

China Post May 2007

Unified Asset Protection

By Sandra Kay Miller

Within the security industry, there has traditionally been a focus on asset control, but “asset” has become a broader term of late, encompassing not only tangible equipment but also business-critical data like customer databases and intellectual property. Today, organizations are looking for unified solutions to protect all their assets — from an executive's PDA that stores confidential trade data to an entire corporate division that might encompass a research and development center. Assets are now a bigger part of the picture.

Using high-tech methods to protect assets can be costly, especially when multiple and separate systems are employed to cover physical and logical assets. To save money and better manage overall security, organizations have begun integrating both physical and logical asset protection into a single entity. Thanks to this trend, encrypted tokens and fobs have increased in popularity for unified asset security.

Asset protection traditionally has held two separate realms — physical and virtual. There are keys, cards and codes for unlocking doors, gates and cabinets. On the digital side, there are encryption and passwords. Over the last few years, the two have been merging.

For medium to large organizations, the asset management and protection can demand a significant portion of a security and/or IT budget.

One system that provides both physical and virtual asset protection without the possibility of a forgotten password or lost key is biometrics. By employing a unique physical attribute, such as fingerprint, handprint, face or voice recognition, there is no longer the need to carry physical keys or remember passwords.

According to Frost and Sullivan analyst Mark Allen, the biometric market in the United States stood at $527 million dollars in 2004 and was expected to grow to $1.4 billion dollars by 2008.

Showing up in everything from secured entries to PDA authentication, biometrics has been rapidly gaining acceptance in the security marketplace. Biometrics is not a new concept, but advances in technology have made biometrics available to more organizations.

When biometric solutions to protect portable devices such as laptops, PDAs and smart phones were introduced, many organizations were not interested in adding more cost to what many considered an easily replaceable asset. However, industry giant Hewlett Packard, Palo Alto, Calif., figuring in the cost of lost productivity and information stored on the device, put an $89,000 price tag on a lost or stolen laptop. Companies realized asset value goes far beyond the cost of tangible and often inexpensive items to include the loss of data. Corporate reputations — a highly intangible asset — were also at stake.

With the need to track both physical and virtual assets to meet the explicit standards for the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley and Gramm-Leach Bliley Act, companies are willing to invest in biometric asset protection technologies like those once reserved for the government, military and Fortune 100 companies.

Although the driving factor in biometric adoption has been regulatory compliance, companies who have instituted a biometric solution are finding their overall security posture, including asset protection, has significantly improved. Today, biometrics are showing up in numerous devices such as door locks, safes, mobile devices and financial transaction technologies, thus enabling a multitude of assets to be secured using a single system.

David Jackson, IT manager for the Cumberland Medical Group, installed a biometric authentication system for its computer network to comply with HIPAA, but when he realized how much the system reduced the time spent on access management, he sought out a biometric solution for physical access as well. “I didn't realize how much money we wasted on the actual physical access to our buildings — keys for new employees, lost keys, re-keying locks when people were fired. Biometrics resolved all those issues, in addition to giving us a digital record of when anyone accessed certain areas, such as rooms in which controlled drugs were stored.”

Jackson's biometric implementation did more than just control access to critical data. The theft of physical assets, such as medical equipment, supplies and drugs, was also greatly reduced.

Although the easiest and most popular biometric identity is AFIS (Automated Fingerprint Identification System), iris, retina, face, handprint and voice recognition can also be used for identification.

Frost and Sullivan's market research puts AFIS deployments at 58 percent of the total biometric market. Besides being an affordable solution, AFIS is also easy to deploy. Jackson was able to install his AFIS biometric solution himself.

“Setting up fingerprint recognition was simple thanks to the software wizard that took me through step-by-step,” Jackson says. He was able to set up which hand and finger the system would use for identification. “We scanned the index finger of both left and right hands, so employees would only have to remember which finger to use — either hand would work," Jackson adds, noting that employees have the option to scan and save all 10 fingers into the system, so it would not matter which digit an employee used on the touch pad.

The process took less than five minutes for each employee, scanning the unique arches, loops, ridges and whorls into a database where the information was stored as an encoded character string.

Despite having a capital expenditure for the specialized biometric hardware and software, Jackson figures the entire system paid for itself in less than a year with lower management costs, reduced property theft and automated compliance auditing.

Although fingerprint identification is the most basic of biometric technologies, they are also beginning to show up in many consumer devices such as keyboards, mice and mobile phones to circumvent the use of false digits, advanced biometric systems also measure blood flow.

Protecting financial assets has also been aided with the use of biometrics. Many banks have begun testing customer acceptance by starting out with the PassVault from Diebold Inc., North Canton, Ohio, an automated system allowing bank customers to access their safe-deposit box unassisted by bank personnel.

In Santa Ana, Calif., the Orange County Credit Union scans all customer thumb-prints along with their signatures. This level of identification also ensures that customers with the same names will not be confused with each other.

The Washington, D.C.-based International Biometric Industry Association has little doubt that banks will move rapidly toward biometrics over the next several years, eliminating the need for credit cards, debit cards and ATM PINs.

Financial institutions are also banking on biometrics to raise their reputation for protecting customer assets. Pam Davis, a business owner in Carlisle, Pa., switched from her long-time bank to a local credit union because of the biometric system she witnessed while with a friend. "She just put her finger on the reader at a kiosk and had instant access to all her accounts. No waiting in line, no fumbling for ID and it's got to be so much more secure. I mean, no one is going to steal my fingerprints," Davis says.

The use of biometrics for asset protection has received a huge boost from the United States military in recent years. In addition to using biometric-based access control systems, the military has integrated complete asset protection systems into their operations in the Middle East. This includes physical security for equipment, weaponry, emergency management materials and force protection equipment. The biggest advantage is soldiers no longer need to carry numerous physical keys or remember complex passwords.

The lines between access control, identification and asset protection are blurring as the need for a unified and secure solution leads organizations to implement security measures based upon biometric technologies.

Reprinted from Security Solutions.com

January 2007

The Big Picture

By Andrew Wren

There is a bulletproof method for eliminating shoplifting in the retail environment: Assign a personal escort for each and every customer entering the store. Never let him leave the escort's sight, shadow him throughout the entire store visit and walk him to the exit.

While no one doubts the effectiveness of such an effort for preventing shoplifting, it is an obviously ridiculous proposition. Quite simply, it is diametrically opposed to the overall requirements and objectives of operating a successful retail business.

The challenge for retail security and loss prevention professionals in retail is not only controlling losses and protecting people and property, but accomplishing these objectives within the larger context of the company's strategy and culture. Retailers should strive to build security into their corporate core values, so that everyone within the organization, from top to bottom, throughout all functional departments, understands the important strategic role security should have within the company.

There are several common ideological pitfalls associated with ineffective retail security programs. The single most common is that security implementation is an afterthought. But there are several examples that demonstrate proven best practices for building effective programs to put retailers on the road to successful security planning.

The fundamental pitfall

Too often, retail security programs are planned and implemented as an afterthought to other programs already put in place. After the store is designed and built, security professionals are called in to protect the premises. After the product has been ordered, loss prevention managers are asked to implement measures to prevent shoplifting. Addressing the store's security needs after other initiatives are completed is the wrong approach. The goal should be to integrate security measures at the highest corporate levels before key decisions are made.

Consider the following example. A retail manager selects the right shelf space, the right signage and places a popular, new product on display. He steps back to admire his work and asks himself, “How can I make this display less likely to incur loss?”

Unfortunately, the real opportunity to control loss has passed. For maximum effectiveness, loss prevention measures should have been considered during the purchasing and merchandising phase. Special packaging could have been ordered to ensure the product was protected from damage and theft. Shelf space could have been selected in a high-traffic area to make shoplifting more difficult, and the product barcodes could have been checked and rechecked to ensure proper pricing. The problem is, in the vast majority of retail environments, programs are developed before security is brought in to protect goods and people. This approach not only limits the security professional's options, but also the effectiveness of the security measures taken.

Where they conflict

Implementing security programs as initiatives separate from other strategic decisions and activities in retail can result in a conflict of interest, putting two or more objectives at odds. A few common examples will bring these concerns to light.

Customer service is a major priority for retailers. Satisfied, loyal customers are essential to the long-term success of any retail business, and that means creating a satisfying customer experience in the store. Security objectives developed outside of overall customer service initiatives can easily conflict. If security is asked to protect a product against theft, it is easy to take measures to reduce the risk of shoplifting. However, if the measures are too extreme, it becomes less likely the product will be purchased. For example, it is possible to lock up a product so that an associate has to remove it in order to show it to customers. However, this may negatively impact customers' experience, leaving them uncomfortable or simply causing them to lose interest due to the extra time and effort required. If security initiatives were considered at the highest levels, retailers would recognize the importance of maintaining the customer experience by making security measures invisible to the honest customer, while still protecting the merchandise.

- **Cost control:** While effective security measures do not necessarily equate to high-dollar investments, a small investment may be required to save money down the road. To control costs and maintain already razor-thin margins, retailers often strive to procure products at the very lowest price. However, procurement managers may need to spend a few extra pennies on some products in order to protect them from loss and theft. While it may cost slightly more up-front, special packaging can protect the product from damage and theft, thus decreasing the potential for future loss.

- **Growth strategy:** Aggressive growth is a fundamental goal of most mid-sized and large retailers. One key challenge executives face is site selection and deployment of new retail stores. If security risk factors are considered after the site has been selected and designed, that particular store will rarely have the security benefits of other locations that were planned with the advice of security professionals. Helpful information might include the area and crime rates, which demonstrate that the store would likely experience high shrink. By being involved in the store design process, security professionals could also ensure the building is well-protected and designed for maximum security and minimal loss.

Developing a security-focused organization

How can a retailer develop into a security-focused organization? It is not enough to make security a priority. It must be a core value. A value is an orientation or an idea that an individual considers correct and important. Values are consistently and unilaterally applied. Priorities, on the other hand, are basically important to-do items that can always be re-prioritized. A good example of a value is the manager who treats people well — it is not a priority, but rather a constant, a part of who the manager is. Similarly, security is either a part of the culture or it's not. By making security a value, it becomes essential to every aspect of a business.

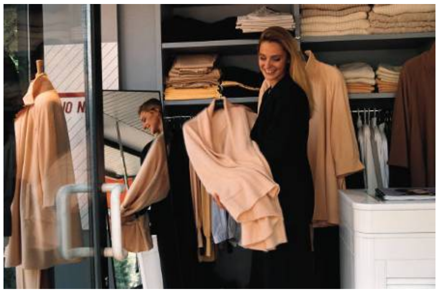
As long as security is an afterthought, retailers will never realize the full benefits of security and loss prevention programs. Rather, loss prevention should be a cornerstone of the strategic and tactical planning process. Understanding that this is easier said than done, the following recommendations can illustrate ways to incorporate security-minded strategies into the life of an organization.

‘Rifle’ rather than ‘shotgun’ approach

Security measures should take a clear, focused approach and be designed with specific objectives in mind. While the “shotgun” approach may have a broad impact, it seldom hits the right target, and the impact is often not deep enough to penetrate to the heart of the problem. On the other hand, the “rifle” approach focuses on a specific business issue and allows for a precise hit that directly addresses the problem.

Consider a shotgun security approach that is common among retailers — deterrent programs for retail associates. Organizations go to great lengths to explain the risks of stealing and the rewards for reporting. They use slogans like “Think shrink,” but simply implementing a program to build awareness and enroll associates will not lead to the desired results. These shotgun-style programs seldom provide functional information that allows employees to perform duties more effectively. If associates do not understand their specific role in controlling loss, they will be even less motivated to “Think shrink!”

A much more effective program teaches each employee about the greatest potential loss-causing risks relevant to his position. Or the employer can offer training on processes and technologies designed to eliminate loss due to errors. This type of program allows each employee to proactively minimize the individual impact on losses by helping him or her to understand the root of the problem and by providing tools that address specific challenges common to that functional area.



Work with all areas of the business

Security is relevant to all areas of the business. Therefore, security professionals must gain a broad understanding of the business and be willing and able to work with professionals in all functional areas. Security values must be integrated into all areas of the company. Security professionals who learn the specific needs of various functional areas can formulate relationships and demonstrate how strategic security measures impact each area positively.

Selecting the right tools

Today, the technology available to support security and loss prevention efforts is virtually unlimited. However, it is critical to select and implement technologies carefully that meet the specific security needs of the particular organization.

Randomly implemented technology will have minimal impact. Retailers should consider their unique security problems. Careful consideration should be given to who will use the technology and how they will use it.

Ideally, security is built into corporate values and is embraced within all levels of an organization. Successfully transforming retail security from a priority to a value may require fundamental changes in the culture of the organization. However, the payoff can be dramatic — as losses are decreased, and people and property are kept safe.

ABOUT THE AUTHOR

Andrew Wren is president of Wren Associates, Jefferson City, Mo., a manufacturer of video surveillance equipment and solutions for nearly 25 years. He serves on the *Security Industry Association's Advisory Council*.

Reprinted from

SecuritySoutions.com November 2005

HURRICANE SEASON PREPAREDNESS TIPS

June to November 2007

BASIC HURRICANE SAFETY ACTIONS

Know if you live in an evacuation area. Know your home's vulnerability to storm surge, flooding and wind. Have a written plan based on this knowledge.

At the beginning of hurricane season (June 1), check your supplies, replace batteries and use food stocks on a rotating basis.

If a storm threatens, heed the advice from local authorities. **Evacuate if ordered.**

Execute your family plan.

THINGS TO DO BEFORE A STORM OR HURRICANE

Keep your radio or television on and listen for the latest warnings and advisories.

Board up or install shutters over all windows, doors, skylights, and open vents.

Secure all doors by bolting and wedging.

Lower television and radio antennae.

Protect appliances and furniture by elevating them off the floor and covering them with plastic.

Remove loose objects from the yard and patio.

Prune dead or dying tree limbs.

Tie down any large objects that cannot be brought indoors.

Recharge appropriate equipment (such as cell phones and rechargeable flashlights).

Close all outside electrical outlets and cover with duct tape.

Turn off electricity at the main box before a storm hits.

Store as much drinking water as possible in clean, closed containers.

Prepare a hurricane disaster supplies kit. (See below)

Put personal papers and other important documents in a waterproof container and keep nearby.

Keep your vehicle filled with gas.

Get extra cash from the bank.

Have a plan in case family members are separated.

Unless advised to evacuate, stay at home. Remain indoors in the middle of the house, away from windows and doors.

Beware of the calm conditions (a lull in the wind lasting from a few minutes to about half an hour) when the eye of the storm passes over. Stay indoors until the entire storm has passed.

HURRICANE DISASTER SUPPLIES KIT

Radio and flashlight.

Extra batteries.

Adequate non-perishable food.

Adequate prescription medications.

Sufficient drinking water.

Personal hygiene items.

Special infant needs.

First aid supplies.

Fire extinguisher.

EVACUATION PROCEDURES

Follow the instructions and advice of local authorities.

Lock all windows and doors.

Turn off electricity at the main box.

Take personal papers and important documents with you in a waterproof container.

Carry as much hurricane disaster supplies as you can manage.

Arrive at the shelter as promptly as possible as and no later than the expected arrival time of tropical storm force winds.

AFTER THE STORM

Stay tuned to a radio station issuing emergency bulletins and updates with the latest information.

Avoid driving unless necessary, as roads may be blocked.

Stay away from fallen or damaged electricity wires.

Do not turn the power on at your home if there is flooding or water present.
Ensure that all electrical appliances are dry before turning on the main power switch.

Check your food and water supplies before using them. For cooking and drinking purposes, use only safely stored water, or boil your tap water.

To avoid overloading the system, use a phone only for emergencies.

Report any damage to your insurance broker as soon as possible. If possible, use a camera to take pictures of damage done to your home, before any repairs are attempted.

(N.B. The above information is supplied courtesy Risk Management Services Limited.)

USEFUL WEBSITES

http://www.nhc.noaa.gov/index.shtml
(National Hurricane Centre)

http://www.sba.gov/disaster_recov/prepared/getready.html
(Business Specific Information)

http://www.fema.gov/hazards/hurricanes/
(What to do Before, During & After)

http://www.nhc.noaa.gov/HAW2/english/disaster_prevention.shtml
(Developing a family plan, assembling a disaster preparedness kit etc.)

Amalgamated Security provides a full range of security services, which include:
Cash Services
Electronic Security
Access Control
Data Storage
Courier Services
Guarding Services
Alarm Monitoring
Response Services

If you are interested in having First Aid Training or Defensive Driving Training for your staff, contact Amalgamated Security