Issue 26 Volume 2 September 2017

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Helping secure your world

Security Solutions

Editor's Note

Within the business setting, business owners along with their employees should be aware of external elements that can cause harmful issues for a company's operations and employees both physically and mentally. The September 2017 edition of the Amalgamated Security Services newsletter explores the various ways persons may try to create havoc in your life and the lives of others in your inner circle. This issue focuses on mental health, fraud, security, and security policies.

The first article written by ASSL Regional Director Mr. Brian Ramsey highlights the issue of suicide and whether businesses have a responsibility to help prevent such an act from occurring. Within the article an imperative point is made by the writer "Any suicide prevention strategies for a business must include staff awareness through education. Staff have to be taught what are the potential signs to look for and then what action to take".

Scams and fraudulent acts are committed by persons with bad intentions who want to gain an upper hand on your company and/or your personal data. This can be done through scams such as search engine optimization scams and even your router, this topic is further discussed in the second and third article.

With the reality of crime of all types being ever present we must protect ourselves from these acts by remaining vigilant at all times, one method is outlined in article four titled 'Advanced VMS features for Heightened Security'. In the world of security we learn never be lenient, never procrastinate, never take the easy way out when it comes to protecting yourself and your assets, and in order to efficiently do this a security policy outlining the what should and should not be done has to be created, article five discusses what a well-crafted Physical Security Policy includes.

Securing your physical property from burglary and other hidden dangers is of highest priority and article six deals with gate locks, both electronic and traditional gate locks.

In wrapping up, knowledge of scams, along with the knowhow on how to protect one's self and keep danger at bay is an important life skill. Additionally persons within the workplace should always look out for each other as mental health and the issues surrounding it is one of utmost importance. We hope that you find these articles worthwhile and that the information presented here is put to good use.

Regards
ASSL Marketing Team

Suicide: Do Caribbean Businesses have a Responsibility for Prevention

By Brian Ramsey – Amalgamated Security Services Limited

Last year in Guyana there were news reports of two separate women who had committed suicide by jumping into the waterfall at Kaituer Falls. Periodically throughout the Caribbean we read about other persons who have committed suicide. There is a common belief throughout the region that if someone wants to commit suicide they will find a way to do it. Is it possible however that at some future date a bereaved family member will sue a business on the basis that they could have prevented the person from committing suicide?

Even without the possibility of a lawsuit, which business wants the negative publicity attendant with someone committing suicide on their premises? In addition dealing with the aftermath of a suicide can be considerable and would involve; blocking off the area where the suicide occurred, dealing with the police, having to clean up the affected area, providing counseling for employees or other persons on the premises who witnessed the suicide, providing medical assistance to anyone who might have been injured during the suicide, maybe having to go to court if there is coroner's inquest and if in a hotel possibly having to provide rebates to guests who witnessed the suicide, along with the negative publicity.

Suicide on a Company's premises is therefore clearly a potential issue that all businesses should address, with the focus being on suicide prevention. Within the overall issue of suicide prevention there are however two issues to address; persons who use a business place to commit their act of suicide and employees who commit suicide and the claim that they were driven to it by their job. The first issue is clearly a security issue and dealing with this begins with a security assessment that recognizes that suicide on premises is a potential risk.

There are several means by which people commit suicide with the most common in the Caribbean being the ingestion of a poisonous substance, by hanging or by jumping from a high location. Other methods used, though less common in the Caribbean, include willful drug overdose, carbon monoxide poisoning from car exhausts, purposely inhaling fumes from an oven that is on, slitting of wrists and shooting one's self.

According to the National Suicide Prevention Strategy for England 2006, "research has indicated that the likelihood of taking one's life will depend to some extent on the ease of access to, and knowledge of, effective means. One reason is that suicidal behavior is sometimes impulsive so that if a lethal method is not immediately available a suicidal act can be prevented". Consequently any suicide prevention strategy for a business in the Caribbean must take cognizance of the methods used for committing suicide and then identify systems to prevent it without impairing the overall operation of the business.

Clearly where a business uses poisonous substances in their daily operation, the business must have operational procedures in place that ensure that access to these substances are controlled and only allowed to persons to who have a legitimate need to use these substances. The procedures must however go beyond simply being written procedures but be actively enforced.

Too often in the Caribbean we see where an area is supposed to be kept locked and instead the area is left open sometimes with the keys hanging in the lock simply because the person in

charge finds it too onerous to have to repeatedly get up and open then close the area. The excuse that is sometimes given is that "I am sitting here near to the entrance so I can see who goes to the entrance". While that may sound plausible is the person really looking at the entrance all the time or are they periodically distracted by telephone calls or persons coming to speak with them.

Recognizing that jumping from high places is another common method of suicide; businesses need to consider how they can limit the access to these high places. The most obvious conclusion would be to simply ensure that the doors leading to rooftops or high ledges are always kept locked. However while it might seem both obvious and suicide-preventative to lock exits to high ledges or seal doors to some hallways, it may not be allowable under certain fire and safety codes. As a result other options should be explored.

Many years ago, the writer was staying in a hotel in Germany and noticed that outside all the windows was mesh netting. Upon enquiry I was told it was to stop persons from jumping out the windows in a suicide attempt. Now this netting gave the hotel exterior an appearance of being encased in a giant fish net. Since that time hotel designers have developed more aesthetically pleasing suicide prevention devices. Among these are artistic metal bars and also angled nets below windows that are based on the premises that you cannot jump far enough outward to escape being caught by the net. Some international hotels now seal the windows to all guest rooms so that they cannot be opened or only allow windows to be opened by several inches so fresh air can enter but a person cannot jump out.

Any suicide prevention strategies for a business must include staff awareness through education. Staff have to be taught what are the potential signs to look for and then what action to take. Very often companies train their staff to alert for various things and then tell them to inform their supervisor. The poor supervisor however has no idea of what to do when staff come to them with the concern. Any training therefore must also extend to providing supervisors and managers with clear guidelines on actions to take.

About the Author

Brian Ramsey has a B.A. in Accounting & Management, along with an M.B.A. in Finance and over 30 years in the Caribbean security field. He is the Regional Development Director for Amalgamated Security Services Limited which operates in Trinidad and Tobago, Grenada, Antigua, Barbados, St Lucia, and Guyana. He can be contacted at bramsey@assl.com.

Search Engine Optimization (SEO) Scams and More Tricks Targeting Small Firms

Are you a small business looking to improve your showing on Internet searches? Who isn't these days?

But watch out for scammers making promises that they'll get you to the top of a Google (or Bing, etc.) search. They can't -- or at least they can't guarantee it. In fact, it's highly likely they won't get you anywhere near even the first page of a search.

As you likely know, the technique for achieving a high ranking on Google et al. is known as search engine optimization (SEO). In the early days of the Internet, using a few simple SEO "tricks," like cramming a page with content and keywords, and linking with other websites, were generally enough to score an SEO hit.

That doesn't work today. Search

engines like Google are much more sophisticated in the way they rank items.

But it doesn't stop scammers from employing these ancient (in Internet terms) tactics.

A recent report on Forbes magazine website, for instance, notes that "scammers from all over the world insist on selling the same old bag of tricks to unsuspecting victims." But how can you spot the scam?

First, simply ignore their claims that they can take you to the top.

"Steer clear of those who make specific promises," Forbes advises. "Search giants don't deliver on cue and are not interested in catering to anyone in particular, other than the general masses. That's not you."

Another warning sign is when a so-called SEO specialist claims to have some kind of special arrangement or partnership with the search engine operators. These sorts of arrangements simply don't exist -- except where advertisers actually pay big bucks for prominence alongside or at the top of a search (where they're clearly marked as ads).

In fact, experts suggest that using old-style SEO techniques, such as links in otherwise meaningless online directories and forums, can actually harm search engine rankings, effectively penalizing the very organizations they're supposed to be promoting. Forbes adds: "SEO scammers typically target small businesses that have sparse resources as they offer little-to-no threat when they discover that they have been taken advantage of.

"They bought into outlandish promises, hoping to write a novel on their unlikely surge to the top, only to find out that they wasted their resources on something that may have been toxic to their business."

The bottom line is that if you want to increase your search engine showing, you'll likely have to employ a real expert. Expect to spend a lot of money. Even then, there are no guarantees.

Scam Advice for Small Firms

In the meanwhile, the U.S. Federal Trade Commission has announced the launch of a new campaign aimed specifically at helping small businesses avoid fraud, cyber-attacks and other scams. A new website page includes links to videos and downloadable reports listing the most common small business scams, plus advice on franchising scams and protecting customer data.

Find the site at https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/small-business

It's worth bookmarking and signing up for regular reports. And it couldn't be more timely.

Most Firms Hit by Fraud

A recent survey report from risk management specialists Kroll says that 82% of companies it polled were fraud victims last year. But contrary to expectations, the majority of attacks didn't come from overseas or even outside the business. Sixty percent of all illegal access and data theft came from inside the organizations -- employees, contract workers, and freelancers.

"With fraud, cyber, and security incidents becoming the new normal for companies all over the world, it's clear that organizations need to have systemic processes in place to prevent, detect, and respond to these risks if they are to avoid reputational and financial damage," Kroll says.

Facebook Scam

Scammers have also started targeting small businesses; especially solo operators or firms with just a couple of employees via Facebook.

The main tactic is to offer business loans or even grants.

This is more or less the same as fake "free money" offers that are sent out to individual consumers, usually pretending to come from a government agency. But government grant programs don't work this way and certainly don't offer money via Facebook. Nor do they request recipients to pay a fee upfront or provide bank details, as the scammers do.

So give these "offers" a miss.

High Speed Trickery

Another trick that is passing from consumers to small firms and other organizations is a scam we reported on a few weeks back in which victims receive a product they haven't ordered. It's a high-speed piece of trickery that goes something like this:

A company receives a product, usually an expensive electronics item from a well-known retailer via a shipping service or tracked mail. (In other words, the scammer knows when it has been delivered by checking the tracking number.)

Immediately, the firm receives a call from the scammer posing as the retailer, saying the item has been sent out in error and will be collected by a courier service. The courier, of course, is the crook or an associate. The victim hands over the item, meaning it's no longer traceable.

But as far as the real retailer is concerned, the item has been delivered to the correct address and the victim company faces having to pay the bill. Indeed, the bill may already have been paid via a stolen credit card or a hacked company account.

If your business receives something it didn't order, contact the retailer yourself immediately and deal only with them in arranging the return of the item.

Reprinted from scambusters.org

5 Easy Steps to Router Security

If you have a home network, you almost certainly have a router, the device that connects all of your various devices -- PCs, laptops, mobiles, security systems, webcams, etc. -- to the Internet and to each other. It's the hub at the center of your network, so it's also the gateway that hackers can use to access, and even hijack, your system.

Yet, remarkably, most people don't know how their router works or how to control the security settings to make it tougher for criminals to break in. That's partly because the people who make routers haven't yet gotten around to making them easy to manage. They're stuffed with technical jargon and bewildering controls that don't mean a lot to the average user -- with the result that many people leave themselves dangerously exposed to outside interference.

In fact, the whole world of networking is a no-go area for

most of us.

However, even with limited knowledge or expertise, there are a few things you can do to make your router more secure. Your most valuable weapon is the manual that came with the device, which likely explains how to access the settings via your PC and how to make key changes to things like security settings and passwords.

Don't have the manual? Fear not. You can probably download it from the web. All you need is the name and model of the device. The name will probably be on the front but you may have to look at the back or underneath for the model number. Then just do a search using this info plus the word "manual" and you should be in business. But even without this information, all is not lost. Let's take a look...

Accessing Your Router's Management Page

Assuming your router is already connected to your network, you can use your web browser -- like Internet Explorer, Microsoft Edge, Google Chrome, Firefox or Safari -- to view its management page. How? Your router, like everything else on your network, has an "IP address," a series of four numbers that look something like this: 192.168.1.01. If you have the manual, you'll find the address there. If not, again you can probably find it online by searching on the name and the term "IP address."

You can find the number by visiting your PC's "network and sharing center" in the control panel (or via "network" in Windows 10 settings). We don't have the space to explain the steps here, but it's fairly simple and you'll find the details, with helpful illustrations, here:

https://www.howtogeek.com/168379/10-useful-options-you-can-configure-in-your-routers-web-interface/

Once you have that number, simply key it in the address bar of your browser and hit "enter" on your keyboard.

The Password Challenge

Now, you'll be asked for a username and password. Again, you may find these in the manual or on a sticker on the back or bottom of the router. (Note, the password is not the same one you use to log onto your network.)

If you've never changed this info in the past, there's a high chance the default username will be "admin" or "administrator" and the password will be "password." You can see straightaway why it will be important to change these -- those words are the first ones a hacker will try!

If those words don't work and you don't know the correct ones, you may get an option to recover the password by keying in the serial number of the router (again, it's on the bottom or back). If that fails, you can return the router to its factory settings by finding and pressing a tiny "reset" button on the device. Then you'll have to go online to find the default username and password by searching the manufacturer's website. Do a search on the name and the words "default password" -- e.g., "Netgear R6100 default password."

What to Change

Whew! That was actually the tough bit. Because now, you should have open in front of you a page that gives you access to all your router's controls. Every router's home page settings look different from the others so we can only offer general guidance on what to change rather than how to change it. It's possible your router may have some kind of "Wizard" that will walk you through security changes. If not, read on...

The first thing to do is to make sure you keep a note of any changes you make, so that if you screw it up you can restore the original settings. (Using the

reset button mentioned above will also do this.)

Then, as a minimum, do the following 5 key things:

1. Check for available updates to the router's "firmware." There may be an option listed on the router management page or you may have to do a separate search on the maker's website. If there's an update, select to install or run it.

Router makers often improve the security of their devices and you make this check a regular thing.

2. Now, change that darned username and password. Again, make sure you keep a note of the new ones. You're already on the way to making your router more secure!

3. Look for a setting that says something like "Security Options" or "Encryption." This usually lists different modes using letters and numbers in order of security strength -- from weakest to strongest. If you can, select at least WPA2 followed by something like "PSK" and/or "AES." But even the most basic encryption -- WEP -- is better than nothing.

4. If there's an option for a guest network, switch that on. That way, you don't need to give your password to visitors who might want to use your network.

5. If there's a setting for a built-in firewall (not all routers have this), make sure it's switched on.

It may not be called a firewall but something like "NAT filtering." Most makers leave it switched off by default. Switching on works in addition to any firewall setting you have in your Internet security software.

There are several other things you can do to make your router safer -- check the manual for this -- but, if you just do these five things, you will have taken a giant stride in the right direction!

Reprinted from scambusters.org

If you are interested visit our website at: http://esis.assl.com/alarms-electronic-products/cctv-systems

Advanced VMS Features for Heightened Security

By Toya T Peterson

Basic Features
Video management solutions seamlessly integrate all components of surveillance into an advanced turn-key solution that provides customers with extreme functionality and value. They often:

Incorporate an Intuitive UI:

VMS offers user-intuitive graphical user interface that makes user experience easier while simultaneously supporting security best practices. Users can choose from a wide selection of viewing configurations including split screens and multiple resolution options.

Enable End-to-End Management:

VMS is a power-house of intelligent features and functions that bring together network cameras, encoders, DVRs and NVRs and combine them into an extremely powerful and cost-efficient video

surveillance management tool for end-to-end security management.

Incorporate Advanced Features:

VMS enables administrators to import site maps and overlay them with icons that represent the locations of installed cameras. Operators can retrieve and view recorded video for additional intelligence.

Provide Alarm Management:

VMS has an in-built alarm management feature; icons can be set to pop-up whenever there is an alarm-related event, facilitating quick monitoring (and action) of live images from the camera nearest to the incident.

Ensure Real-time Management:

VMS offers real-time event viewer with an event log. This log can be sorted by camera (number, location or type) or event (time or type) for further analysis and as evidence proof.

Offer Easy Integration:

Operators can easily register and integrate new devices into the VMS and conduct periodic health check of all the devices in the network to ensure round-the-clock security.

Advanced Features

In an ever growing industry like security and surveillance, camera manufacturers need to radically change the way innovative security solutions are delivered. A commitment to leading industry standards, in addition to multiple integration options, a highly distributed network architecture and cloud storage options are extremely sought after. Let's look at some of the other advanced features that are transforming the video management space:

Encryption:

In an age where hackers are looming and the risk of cyber security threats is intimidating, encryption has become a major requirement. Modern VMS enables encrypted communication between surveillance cameras through a secure HTTPS connection, improving the security of content, and reducing the risk hacking.

Advanced Search:

Sifting through millions of TB of data is often a time consuming (and futile) process. Modern VMS possesses advanced search options, and that drastically reduces investigation time and help in quick identification of suspicious activity, people, objects and events. Choose from motion search, image search, or text search and retrieve the required content in no time.

Real-time Maps:

With VMS, you can achieve faster navigation to cameras using their physical location and easily view the layout of a location using the maps feature. Get a list of all the maps on the server, zoom in and out, view health indicators and show and hide cameras in different locations to get a birds-eye view of security around the premise.

Multiple Viewing:

Using VMS, you can view multiple, simultaneous video streams and effectively monitor multiple areas of interest. Set up the most critical locations on the salvo, configure basic information, add the cameras and get a complete view of your premise.

Cloud Storage:

VMS uses NVRs that are specially designed to work with cloud storage. You can store a large amount of data on the cloud and access recorded video content from anywhere using your computer, smart phone, or tablet. Since files are not stored locally, even if your equipment is damaged or stolen, the videos are still safe.

Virtual Tours: Modern

VMS offers a tour feature that enables operators to pre-define a sequence of cameras to

automatically cycle through. Create a new tour, give it a name and description, set a default dwell time, add the necessary cameras and recorders to the tour and get a virtual tour of your premise according to the camera sequence.

Safeguard Assets
Considering the rate that which video equipment are evolving, monitoring a skyrocketing quantity of high-resolution video data is becoming extremely challenging. From metro stations and airports to casinos and urban roads - operators need to view several cameras at once in order to get a complete and uninterrupted overview of a location. Modern VMS empowers security operators to effectively manage high-resolution video streams in their day-to-day work. With ultra high resolution, advanced search options, maps, virtual tours, and cloud storage - VMS is just what you need to safeguard your assets!

A graduate in technology, Toya Peterson is an avid blogger who is always interested in the recent fads and trends related to wearables, IoT and embedded technologies. A mother of two, she aspires to be a photo-blogger soon as she is honing up her skills in photography. In her leisure time, she loves to go hiking with her friends.

Article Source:
http://EzineArticles.com/expert/Toya_T_Peterson/2239251

Is Your Company Security Policy Worse Than Worthless?

By George W. Babnick

One of my earliest cases as a private investigator involved a chain of auto repair shops where managers at some shops were suspected of pocketing cash payments from customers. The owner also suspected that some employees were sneaking into some of the shops late at night after the business was closed and were using company facilities, tools, and diagnostic equipment, to work on friend's cars.

My investigation involved posing as a customer, hidden cameras, targeted surveillance, and some forensic computer analysis. At the conclusion of the investigation I was able to establish that more than one shop manager was routinely pocketing cash payments from customers and in addition to using the shop in the evenings after business hours to repair friend's vehicles, one manager was running a late night under-the-table car repair business using the company's facilities and equipment.

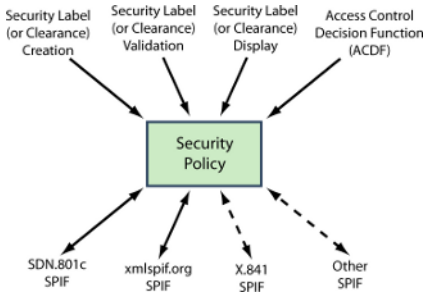
One of the suggestions I made to the owner was that he should add some protocols to the company's security policy about how managers handle cash payments from customers and also include some rules about after hours use of shop facilities and shop equipment. To my surprise, the owner said his company had no policy. At the time, I was surprised. But since then I have discovered more and more small businesses (even some medium sized-businesses) that have no written policy pertaining to security. Of those businesses that actually had a written policy, many had not reviewed or updated their policy in many years.

The importance of every business having a security policy

Very few businesses in the United States are mandated by law to have a security policy. Establishing a policy is not likely to solve security problems but it is an important starting point. A well-crafted policy provides a framework for identifying security risks and outlines how the company plans to protect those assets. It is also an unequivocal announcement from management that the company has a serious commitment to security and is a way for the company to commit to taking steps to secure assets

and keep personnel safe and secure.

Often policies are a mishmash of rules and procedures, guidelines, and maybe some standards, all rolled helter-skelter into one document and called a "Security Policy." There is a difference between policy, guidelines and rules, and procedures, and these distinctions are not just academic.



In brief, policies are overarching principles from management and are meant to establish a tone and influence behavior. Standards are levels of quality or achievement and typically involve industry "Best Practices." Guidelines are statements meant to guide behavior. Rules tell a person what to do or not to do in a specific situation. Procedures are a fixed way of doing something.

Rules and procedures are important parts of a well-crafted policy, but the policy must come first. Standards flow from the policy and guidelines and rules flow from the standards. This is followed by procedures.

Effective policies form the foundation of the company's entire approach to security and creating a practical and effective policy is not something best done on a whim or by someone who lacks the skills or motivation to do it right. Crafting an effective policy involves insightful planning and numerous sequentially layered steps. Often it is best to hire someone who has experience in security policy development to tackle the task or at least provide assistance. Good policies come in many shapes and sizes but the basis of a well-crafted Physical Security Policy includes:

*** ASSET IDENTIFICATION. Identifying the assets that need protecting**

In a physical security setting this includes buildings, parking lots & other premises, interior rooms & offices, points of entries, inventory, equipment, and many other things.

*** ASSET VULNERABILITY ASSESSMENT**

Effective asset identification should be coupled with an asset vulnerability assessment as not every asset requires the same level of protection.

*** ASSET PROTECTION STRATEGIES**

What is the plan to protect specific assets?

*** TRAINING**

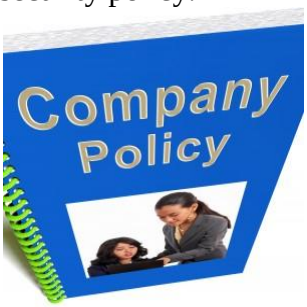
Who in the company needs security training and what type of training is best?

*** EVALUATION and REVIEW**

How will the effectiveness of the security policy be measured? How often will the security policy be reviewed and modified as needed?

Once these elements are articulated and documented in a properly structured Security Policy, then (and only then) should standards, guidelines and rules, and specific procedures be developed that support the overall Security Policy.

The elements in a physical security policy can be expanded depending on the company and business needs. Often, the physical protection of data is also addressed in a Physical Security Policy and the policy is married with an "IT" or data security policy.



Is your company security policy worse than worthless?

If a company does not develop their policy through a systematic process of asset identification, risk assessment, protection strategies, training of key personnel and provide for an evaluation and review process, the security policy ends

up just being a fancy document gathering dust on some manager's shelf. When that happens, the security policy is worse than worthless.

How can something be worse than worthless?

Having a policy that is a haphazard conglomeration of policy, standards, rules, and procedures that just "evolved" over time or was created by someone who lacked the skill or motivation to get the job done right, creates confusion among personnel. When confusion occurs, personnel are left to fend for themselves. Sometimes they get it right - sometimes they do not. And worse yet, sometimes supervisors try to enforce rules and procedures that are not consistently followed or enforced. These result in low employee morale, Human Resource type complaints, and sometimes even lawsuits.

Businesses can minimize the occurrence of all of these problems by having a skillfully constructed and effective policy followed by practical security rules and procedures.

A private investigator can find out "who done it" and a investigator who also has a background in security can also help a business improve their profitability by recognizing security issues and make practical and effective security recommendations.

Gate Locks

By George Uliano

Gate Locks could be as simple as a padlock or as secure as an electronic lock of some type. As in anything that you are trying to secure, ask yourself "What are you trying to protect and how much is that worth to you?" With gate locks you are usually talking about a fence gate of some sort. That is why padlocks are the first choice. Many times you must purchase some type of chain that secures the gate to the rest of the fence.

If using a chain, make sure that you size it up properly with the padlock. For example; if using a chain that has 3/8" diameter links you should also get a padlock with a 3/8" diameter shackle. A padlock with a 1/8" diameter shackle would not be the best choice.

Some gates have a built in latch that is made to close around the pole of the fence. It will already have a hole in it to accept a padlock. Again get a padlock with the largest diameter shackle that will fit the gate latch. Other types of gates will have a locking mechanism that will have a built in deadbolt type lock, very similar to a deadbolt lock for your front door. These types of locks have the added ability to be keyed so that a particular key will open the gate and a door to the building.

For any type of gate lock you can make a choice as to the level security that you need for that gate. Also keep in mind that most gates are outside and exposed to the elements. So choose a lock that is made for this type of environment. As stated earlier padlocks will be used as the lock for most gates. Most can be purchased at big box stores.

If you need a padlock that can be made to work with your other gates or maybe a door to the building you will have to go to a lock specialist. Someone that is able to build the lock to your exact specifications and is also capable of cutting keys. They will also be able to supply higher security locks or even electronic padlocks.

As prices come down the electronic locks will become the lock of choice. This is because of the security of electronic locks and their ability to be controlled and programmed by

smartphones.

George Uliano is a security professional with years of law enforcement and security experience. He earned a Bachelors Degree in Criminal Justice and Business graduating with honors. George holds three U.S. patents on different locking principles. This combination gives George and His Company Locking Systems International Inc the unique ability to provide its customers with the correct security at an affordable price.

For additional information or to purchase Locks go to http://www.lsidepot.com

Amalgamated Security Services offer a full range of security service solutions which are inclusive of the following:

Response Services
Alarm Monitoring
Guarding Services
Electronic Service
Courier Services
Assess Controls
Data Services
Cash Services
Investigations