



- ▶ EDITOR'S COMMENTS ... 1
- ▶ Biometric Lock Mysteries 2
- ▶ Perform Tenant Checks..... 3
- ▶ Protect Point of Sale3
- Information Security Self Assessment.....5
- Bucket Truck GPS...7
- Mailbox security risk.....8
- Security Bars.....9

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE.

Helping secure your world

The rapid pace of technological development is allowing security technology to be used in a wider array of environments. Items that a few years ago were considered science fiction are now increasingly commonplace. Our first article on **Biometric Locks** shows the variety of uses available for these devices.

There are always people looking for places to rent but you should not give your property to just anyone. So our second article on **Performing Tenant Checks** identifies some of the things you should do before renting your property.

Point of Sale Systems are computer systems and so contain valuable information. Hence the reason our third article looks at **Protecting Point of Sale Systems**.

There is a lot of work involved in doing a self-assessment of your information security maturity; however, if you follow a few basic steps it doesn't have to be difficult. The fourth article shows how you can conduct an **Information Security Self-Assessment**.

Bucket Trucks are used by a wide variety of companies including electricity providers, telephone companies and cable television companies. Each of these companies can **Improve their Effectiveness by Implementing GPS Systems**.



Most people only think about their home and property when considering home security. Just as important is the residential mailbox. Every day, there is a lot of personal information that enters your mailbox. Identity theft should be just as big of a concern as a home burglary. As a result we have included an article on **Mailbox Security**.

Security Grilles are commonly used in the Caribbean so our final article addresses **Security Screens compared to Security Grilles**.

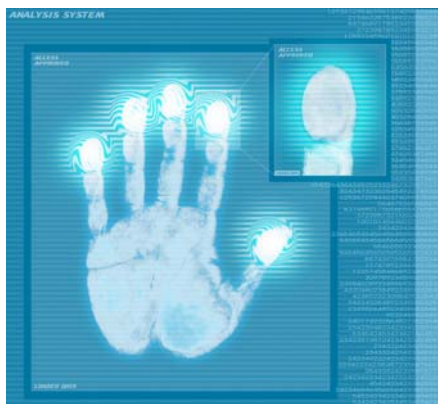
Is there anyone who you think would benefit from receiving this magazine? Just send their name and email address to newsletter@assl.com and we would be happy to add them to our mailing list.

Brian Ramsey
Editor

Biometric Lock Mysteries - What is Fingerprint Capacity?

By **Rose Li**

Biometric locks have the potential to change the face of security. For example, biometric locks use a specific human characteristic, such as a fingerprint, instead of a key. Fingerprint locks are one of the more common types which are currently available. You can even buy a biometric deadbolt for the front door of your home.



Basics of Fingerprint Locks

A fingerprint lock works by scanning your fingerprint to identify its unique structure. If it matches a print which has already been programmed into the lock, access is granted in a matter of seconds. Biometric fingerprint locks of this nature require a power source, usually batteries such as AA or 9V.

Fingerprint locks offer more reliable security over traditional keyed locks; keys can be used by anyone and are small enough to be lost. Neither is true for

fingerprints, which are completely unique and require a permitted person to be present to open a lock.

If you want several people (perhaps your family members and a trusted friend, in case of emergency) to have access to your home, multiple keys are required. With a fingerprint door locks, you can program multiple users into your biometric lock (known as enrolling). A biometric lock can replace keypads in the workplace as well.

Alternative Uses

You may find fingerprint door locks useful in other applications, besides building security. Fingerprint scanners can be used to grant access to computers - some laptop manufacturers include the technology in their systems - or to safes.

Both of these methods protect important or valuable information. Some people keep firearms or other weapons in their personal safes and a biometric lock can protect young children from these dangers.

Keyless, fingerprint locks are also used to secure storage containers such as lockers (such as in schools or gyms) or briefcases. Presently, some high end cars are also using biometric door locks as a means to enter the vehicle, instead of a keypad of traditional keyed lock.

Fingerprint Capacity

You may not realize that locks like these have a fingerprint capacity, That is, only a certain number of fingerprints (enrolled

users) can be saved into the memory. Most commercial fingerprint locks have a fingerprint capacity of 99 users. This is more than adequate for home uses or even small businesses.

Nevertheless, certain situations require a much higher fingerprint capacity. Biometric systems are sometimes used in schools in the United Kingdom, prohibiting non-students from entering. Furthermore, fingerprint locks can be a useful tool in professional environments where hundreds, if not thousands, of employees may require access.

You can choose from dozens of models of biometric door locks which are on the market right now. Rest assured that you do not need special knowledge to install a fingerprint lock. This do-it-yourself activity can offer reliable protection for your valuable items and, perhaps more importantly, your family.

Get the best **biometric locks** now. Visit [Chinavasion.com](http://www.chinavasion.com) or paste this link into <http://www.chinavasion.com/index.php/equipment-fingerprint-devices/>

Reprinted from Ezine Articles

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

Always Perform Tenant Checks Before Letting Someone Stay at Your Home

By [Chris J Anderson](#)



The tenant verification is routine procedure taken up due to security requirements worldwide. This is essential help tool to give you better information and help to screen out the tenants before hands. Here are some important points regarding the verification of tenants that you can do quite easily.

The first step for verification is designing a suitable form. The form should contain all the information to let you know what tenant history the person has and how you can deal with it. The benefit of this form is that you can easily take out the habitual absconder, and people who can leave without paying rent or are not having the financial position to rent your property.

The land lord is helped a lot with the background checks and the

information in many other ways also, it can give you the references, the contacts and other information also. It should include things like, identification of tenant, his co signer id, references, credit report, other addresses, criminal history, along with the rapid report etc.

The checks should also contain information about the other areas like their previous tenancy experiences. The information about their past experience and payment and references can guide you a lot in finding some

idea of their future conduct.

There are always people looking for places to rent but you can't give your property to just anyone. The pitfall in doing blind is that often the tenants are found to change the whole color scheme or even the paint job in the property; some are not able to maintain the garden or have some pet issues. This too can be addressed during tenant checks.

The tenant information should also contain the expected guest range and even the possible events that the property might have. This is quite handy to safeguard you from hiring your property to some one who has too many guests or even is partying almost every other day.

For more information about [Tenant Checks](#) and [Tenant Checks](#) visit my website.

Reprinted from

Ezine Articles

Can You Protect Your Point of Sale Systems?

By [Patrick Kelley](#)

Well managed point of sale systems are imperative to any business that uses a cash register. POS Systems allow for much faster processing time, better customer service and more accurate record keeping abilities.



The problem is, can all of the valuable information on there be safe? In 2007, three men managed to hack into the popular restaurant chain Dave and Busters' point of sale system and log credit card and payment card data. By doing so, the hackers were given access to about 5,000 cards and were able to make more than \$600,000 in fraudulent transactions.

Another troubling instance is when well-known computer security company McAfee had an issue with its POS system and inadvertently forced a major

Australian Supermarket to close its doors for a short while. In this case a bug incorrectly identified a legitimate operating system component as containing a virus. While the problem was dealt with swiftly, it still raised many questions and concerns with point of sale systems in general.

There are a few things that are relatively quick and easy that you can do to help protect your system that are often skipped over.

Back It Up

Simply put, POS Systems are really just a specified computer and just like any other computer system it can crash. Any time you are housing large quantities of sensitive data you want to make sure that it isn't lost in the event of a crash or power outage so it's important to back it up.

If possible it's best to back it up using a private and secure network where you have the greatest level of control. However, especially with smaller businesses, this is not only always doable so there are other options. Google's cloud network is an example of an online live server where you can store secure information and shared documents but there are concerns.

Although systems like this do offer top of the line security, they also place all of your sensitive and valuable information in one convenient place that experienced hackers may find extremely tempting. So if you can, backup up your data on your own private secure network away from the internet prowlers

looking for a hacking challenge with a huge prize.

Keep It Simple

Treat all point of sale systems like you would any other computer in your business and keep an eye on who is in and out of it. Restrict access for only those people who absolutely need it and if you can, keep it to yourself. The fewer people who have access to it the more secure and protected it will be.



Keep in mind what your POS Systems are supposed to do for your business, specifically, and keep it to those functions. Just because it might be able to perform all of the same functions your office PC does, doesn't mean that you should. So save sending e-mails and checking your fantasy teams to your secure personal computer as doing so only makes your **POS Systems** more accessible to outside hackers.

Also, keep the information traveling in one direction and not processed through every register in your business. This will help restrict the hacking options available to get to your sensitive data and can also perform damage control should a glitch of some kind occur.

Do All That You Can

There is no way to absolutely protect yourself and your POS Systems from hackers, crashes and glitches but it's important to do as much as you can. Remember, limit who has access to your system to as few people as possible. If a problem does arise you will be able to identify and fix it quickly. Also limit the use of the systems to what they are specifically designed to do and avoid using them for other personal and business operations.

The larger your company the more data and information you will have and more people will need access to it so keep in mind you may need multiple safeguards to help protect it. Talk to your vendors and make sure they are aware of your security questions and concerns so they can help you set up your point of psale systems up to best serve your needs.

Article Source:

www.ezinearticles.com

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

Conducting an Information Security Self-Assessment

By [Donald Johnston](#)

How can a corporation determine where they are today with their information security program? One can certainly use an international standard as a check list and give it your best guess. However, the best way is to ask your employees; after all they are the ones that live it every day. A set of questions related to the standard and written in meaningful language makes this an easy process. This then lets you go to your senior management with a report backed by a large number of people across your organization.

The steps involved in a self-assessment are:

- choose a standard to meet
- select an assessment scale
- develop a questionnaire
- determine who to interview
- customize the questionnaire
- conduct the interviews
- manipulate the numbers
- create some charts or graphs
- produce a report

- generate a presentation

Sounds simple enough,... let's look at each of these in a bit more detail

1. Choose a Standard to Meet

The three primary standards that I'm aware of are the ISO 27000, NIST SP800, and Information Security Forum's Standard. I have always worked with the ISO 27000 series "Information technology - Security techniques". This set of documents provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS).

2. Select an Assessment Scale

You could select any range you wanted for this, say 0 to 3 or 1 to 10, but it should have some meaning and should never have a center point. It needs meaning so you can explain the intent of the range to all interviewees and get consistent results for your survey. It shouldn't have a center point because people have a tendency to say "we're average" and that's the major rating you'll get. For example if you chose a scale from 1 to 5 you would get a disproportionate number of 3's. I use a 0 to 5 scale based on the Carnegie Mellon University Capability Maturity Model (CMM). The CMM is a 5 level scale so I use 0 to indicate non-existent and to get rid of the center point. The levels then are: nonexistent, initial / ad hoc, repeatable but intuitive, defined process, managed and measurable, and optimized. Tell them before hand that they have

to pick an integer from 0 to 5, nothing like 2.5 is allowed. Once you force someone to decide whether you're above average (3 to 5) or below average (0 to 2) they'll then be willing to make a more qualitative assessment.

3. Develop a Questionnaire

The ISO 27002 document lists a total of more than 150 controls such as:

"8.1.2 Screening - Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks."

This can be worded as a set of questions to check your level of implementation (or maturity level) of this control as follows:

- "Are verification checks on permanent and temporary staff, and contractors completed before they start on site?"
- "Do job promotions, involving access to IT facilities, use proper screening processes?"

The question set I developed included a total of 184 questions. If you want a somewhat smaller set to do an initial review move up to the Objectives level in ISO 29002 and develop a set of 39 questions.

4. Determine who to Interview

You should try for a group of people that work in many roles

and many different departments across your organization. A good sample group would include: security personnel, super users, technology support staff, facilities coordinators, data owners, applications specialists, and general staff. I've always tried for about 15 to 20 people in total based on the size of the organization. This ensures that all of the questions in the set are answered by at least two people (see the next section on customizing the questionnaire). If you have to meet a certain confidence level and confidence interval for the results to meet legal or contractual standards you may have to use a somewhat larger sample size.

5. Customize the Questionnaire

Okay, you may have an extremely skilled employee base but I doubt many of those you're going to interview would know how to comment on all 184 questions that relate to the ISO 27002 standard; nor may they have the time or attention span to sit through the whole set (if you consider about 1 minute per question then 184 questions could push 3 hours of their time). So, subset the questions for each class of individual you are interviewing. The security folks may be the unfortunate ones that get all 184 questions. The general staff may have only about 30 questions to go through. You'd be the best judge as to who can answer the question set you've created.

6. Conduct the Interviews

With 15 to 20 people to interview and with each taking from a half hour to 3 hours of

time you'll want to schedule the interviews over three or more days. Give yourself a gap between interviewees so you can have a bit of a break and in case any of the interviewees are "real talkers". You'll want to get the persons perception of the maturity level (0 to 5) and capture any comments they may have about a question (these come in very handy when generating the report later). Before you jump into asking the questions give them a quick introduction to the standard and rating scale used. For the first few questions offer to help them focus in on a level by having them "think out loud".



7. Manipulate the Numbers

Unless you are a small organization you would likely only question a sample of all employees. You can calculate the mean of the maturity levels given during the interview but you should also determine the standard error; this gives you a measure as to how much the interviewees disagree with each other and where the actual mean of the entire population (i.e. all employees) is likely to fall. The standard error is a measure of the sampling variability or precision of an estimate; an indication of where the actual mean is likely to fall. The nice thing is

spreadsheets can calculate the mean and standard error for you quite readily.

8. Create some Charts or Graphs

One graph I always like to use as a quick overview of the assessment is an histogram of the number of the questions that fell into each maturity level. Since by this time we've actually developed a mean of the maturity for each question I create a 10 bin histogram where each bin is half a maturity level (i.e. 0 to <0.5, 0.5 to <1.0, 1.0 to <1.5, ..., and 4.5 to 5.0). You can quickly look at this graph and decide if you're mostly mature or not. Another useful graph shows the 11 security objectives of the ISO 27002 standard and the perceived maturity level from the interviews. This helps you to decide where you should start your improvement program.

9. Produce a Report

Sure, this part is easy, just put all the above points together into a report for upper management. Start with an executive summary page that shows the top 10 controls (of the 184 in the questionnaire) and the bottom 10 controls... this lets management know where you're really great and where you really need to improve. Expand on that, give some details on the top 10 and how you might be able to capture best practices from these. List the bottom 10 (i.e. lowest maturity level) and do a quick risk assessment and risk statement; after all something could be at a low maturity level because it just isn't important in your environment. Another section I like to include is the 10 controls

that had the largest standard error; this highlights those areas where interviewees disagreed a lot about your maturity level; is this a perception problem or areas that need more work?

10. Generate a Presentation

Unfortunately management doesn't always read through your report, nor should they really. You should create a presentation to use as an overview for them and as a sort of index into your report. If something catches their eye in the presentation they can read the details in the report; keep this in mind when creating the presentation.

If you need additional information or help on this, visit our web site at <http://www.maseconsulting.com/isa>. We have a complete set of documents to help you with your self-assessment and your overall information security program.

Article Source:

[http://EzineArticles.com/?expert=Donald Johnston](http://EzineArticles.com/?expert=Donald_Johnston)

Important News About Bucket Truck Efficiency With a GPS System!

By [Christopher M. Hunter](#)

Acquiring a bucket truck is like acquiring any other piece of heavy equipment: it is a huge investment for a company to make. For years, demand for this vehicle has increased for many industries including electric

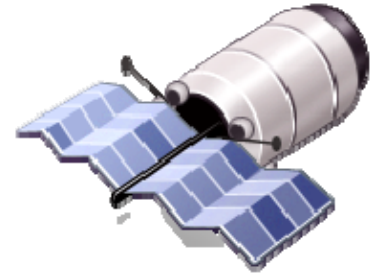
utilities, telecommunications, cable television, exterior building maintenance, forestry, fruit harvesting and firefighting, to name some of the more popular ones. The accessorizing of these vehicles is another important function and need, the most of which tend to specialize in the area of worker safety, which is indeed an important consideration for any company.

On the other hand, technological advancements have also made important contributions to worker safety as well as to a company's ability to operate their fleet of vehicles with greater productivity and efficiency. GPS or "Global Positioning System" is one of the accessories your company can take advantage of for your bucket trucks especially in any rural or remote work locations.

So what is a GPS, how do they work, and how will they help efficiently maintain a fleet of commercial vehicles? Hopefully, we can offer some helpful information in this article.

The GPS (Global Positioning System)

The science knowledge that is comprised in this system actually dates back to pre-World War II. It was based on ground navigation designs used during that war. After the launching of satellites into space, the U.S. Navy first tested this new technology application in 1960 and from that developed the ongoing usage of atomic clocks in satellites that is the basis for the current process.



The early technology was very costly, so usage was limited to the military that could justify its development to help them during the Cold War arms race and its perceived nuclear threat to the United States. In 1978, the original GPS was launched which was officially named by the Pentagon as DNSS (Defense Navigation Satellite System), then later that year changed to NAVSTAR (Navigation System with Timing and Ranging). This gadgetry was strictly for military use during that time. Since this technology works with the deployment of navigational satellites, between the years 1978 to 1985, eleven satellites were launched and positioned in space solely for military GPS use.

Civilian GPS usage was begun in 1983; however, the signal designated for civilian use was intentionally degraded with the highest signal quality being reserved for military usage. In 2000, complete usage was opened to all users as by then the U.S. military had the technology to selectively deny this system's service on a region-by-region basis.

GPS is entirely owned and run by the U.S. government to be used as a resource for the entire nation. The Department of Defense (DOD) manages the

operation of this national asset and there is, of course, a Committee established by presidential directive to offer advice and coordination to all federal and civilian agencies. The DOD is charged to maintain this service and keep it safe from disruptive use.

GPS Systems and Bucket Truck Fleets

Equipping bucket trucks with GPS provides a tremendous advantage to a company that operates a fleet of these vehicles, particularly in any widespread rural area or even remote working locations. These systems can be used to determine routes and driving time to work locations as well as monitor a crew's progress in reaching that site. Thanks to a decrease in cost over recent years, it is just a very wise monetary investment to help ensure the efficiency of the operation of a company's fleet of expensive bucket trucks.

Following are two specific advantages as to why your company should equip your fleet of bucket trucks with GPS devices.

- The GPS helps the driver get to the location site more quickly and will help the vehicle and crews travel a safer route since the device shows the exact job location position. If the vehicle can get the workers to the correct job site in the best time possible, more time can be spent working and less time traveling.

- GPS devices will help your company track your fleet of vehicles while they are gone, particularly at locations that are distant from your home base and probably out of most cell phone range. Through this system, you can track how many hours are spent at the actual job location as well as if the crew has traveled to some other point that is not part of the route. This will help the crew concentrate on their assignment since they will know that they are being monitored.

It can be clearly seen that the efficiency of a GPS system can certainly contribute to the efficient usage of your fleet of bucket trucks and help your company achieve its goals in a more timely fashion. The more efficient your fleet is on the job means the faster the job will be finished and the more rapidly your company can earn money. Don't give it a second thought: equipped your bucket trucks with GPS devices today!

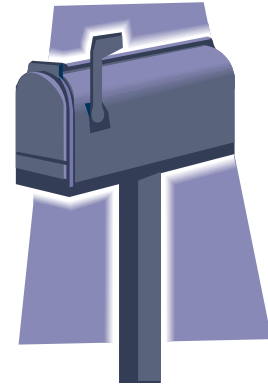
Christopher M. Hunter is an expert in commercial specialty trucks. To find out more about [Bucket Trucks for Sale in Canada](#), go to the main website at: <http://www.nueco.com/>.

Article Source:

Ezine Arucles

Your Mailbox - Is It A Security Risk?

By [J Godwin](#)



Most people only think about their home and property when considering home security. Just as important is the residential mailbox. Every day, there is a lot of personal information that enters your mailbox. Identity theft should be just as big of a concern as a home burglary. Most people don't even think about making their mailboxes theft-proof which leads to the rise in identity theft across the nation. Most mailboxes are easy targets, giving thieves immediate access to your private information.

Every day we get personal information delivered to us by mail. We get credit card offers or bills that contain private information. Without thinking, most of us head out to our mailbox, gather the mail, and then go back about our business. You need to think about your unsecured mailbox as an engraved invitation to a thief. All it takes is for a crook to get to

your mailbox before you and your personal information is stripped from you, putting your identity in great jeopardy.

To safeguard yourself against identity theft you should always include your mailbox in your home protection plans. If you have a traditional mailbox, you should consider replacing it with a safe and secure mailbox. Those made of solid steel are the best choice. The safest boxes have a slot for the letter carrier to put mail into and an entrance door that can only be accessed by a key. Sturdy, steel mailboxes that are key locked are your best defense against identity theft through mail thefts.

Secure mailboxes can be found at any hardware or department store or on the internet. Good safe mailboxes are truly reasonably priced and to prevent the theft of your personal, private information, it's a small price to pay. If you cannot replace your current unsecured mailbox for some reason, at least place a padlock on the mail door.

On your next trip to the mailbox, you need to ask yourself, is my mailbox really secure? If the answer is no, then you need to act now before your identity is hijacked and your world is turned upside down.

Providing you with the best information on self defense, home and business security. Visit

<http://www.moonlitesecurityproducts.com/>

for the latest in safety gear and home protection.

Article Source:

http://EzineArticles.com/?expert=J_Godwin

Amalgamated Security provides a GPS Tracking service with the most detailed maps of Trinidad

Security Screens Vs Grilles and Bars

By [Brendan Sydes](#)

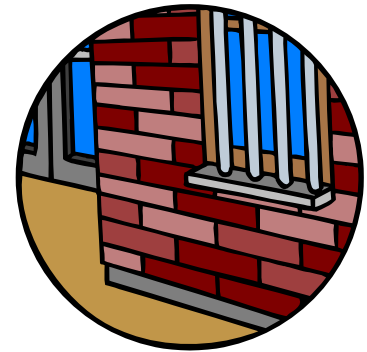
So you want to improve your home security but don't want the hassle or expense of installing an alarm? Do you feel that security screens or other types of barriers would do the trick? Then you need to get up to speed on what your options are.

It can be overwhelming when considering your security options for your home. After all, you want to have the peace of mind that your loved ones and your hard earned possessions are always safe and sound. The most common forms of home security are security doors and screens, grilles and bars. Choosing which one is best for your needs shouldn't be a nightmare and can be worked out quite easily if you way up the pros and cons.

Security Screens - are they the better option?

Mostly made from stainless steel or aluminium, this material can either be woven into a mesh, or have holes made into the sheet to

give the illusion of mesh. Although these screens can sometimes look like fragile fly screens, an intruder is bound to get a shock if trying to kick it in, as they are a lot stronger than they appear. The good thing about security screens is that they aren't visually imposing and blend in quite nicely with the rest of the house. You also don't get that 'closed in' feeling with this type of security option. Mostly designed for doors and windows, there are also options to have them fitted with escape mechanisms to allow easy opening from the inside, in case of an emergency. Nowadays, security screens must meet the Australian Standards and usually come with a ten-year warranty to ensure continued safety for you and your loved ones.



Security Grilles and Bars - not quite the prison bars they used to be.

Affixed to your doors or windows, grilles and bars are designed to provide improved

Amalgamated Security has offices in Trinidad and Tobago, Barbados, St Lucia and Grenada.

security levels to your home - either on their own or in addition to security doors and screens. Grilles and bars are instantly a visual deterrent for a potential intruder, looking impossible to get past. Although providing impenetrable security to your home, grilles and bars can be a little harsh on the eye. Rest assured that you now have options. You can now get grilles and bars in an array of designs and colours to suit your personal style, while still being highly functional. It's important that they are made from aluminium or steel, and that they are designed to be protected from the elements and harsh weather that isn't uncommon in Australia. Don't forget to look into options that allow easy opening from the inside so you can easily leave your home in case of an emergency.

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

Ultimately the choice is yours. Both the security screen option and the grilles and bars option will provide improved security to your home. You can never be 'too safe', so do your homework, work out your budget and ensure whichever product you choose meets the Australian Standards and is installed with this standard in mind so your home is as secure as possible.

By the way, do you want to learn more about home security? If so, I suggest you check [security doors](#) and [security screens](#).

Article Source:
http://EzineArticles.com/?expert=Brendan_Sydes