BraveSecurity®
YOUR TRUSTED PARTNER

SECURITY INSIDER SECRETS

Find out how what you need to know, get the best value for money and ensure your security system works for YOU!!

Table of Contents

Security Systems in a Business Environment – what to consider and what to look out for 1

Top tips on selecting an installer 6

Security Systems - Cloud or no Cloud? 7

Camera resolution - Is more always better? 15

Important considerations when evaluating an access control system? 18

NVR or VMS for my CCTV - What's the difference? 22

What should I think about when considering an alarm system? 25

Security Systems in a Business Environment – what to consider and what to look out for

Businesses have a responsibility to ensure the safety and security of all employees and visitors to their building. This can be a difficult task in a business environment where there are multiple needs and priorities.

Risks abound in providing a safe and secure environment to ensure that your employees and visitors feel safe and secure. Ensuring a good outcome is also vital in ensuring that your investment is protected, therefore protecting your reputation and business as Management Professionals.

In this 4 part series we take a quick look at the main issues surrounding Compliance and how you can ensure you get the best out of your system whilst remaining on the right side of the law. We will then take a dive into Data management and its implications, challenges and benefits. Following on we examine post incident investigation and how to ensure your system is able to handle the many investigative tasks you throw at it. Finally, we will then end with some tips on how to ensure your installer is up to the job and capable of delivering.

Legislation - understanding your obligations

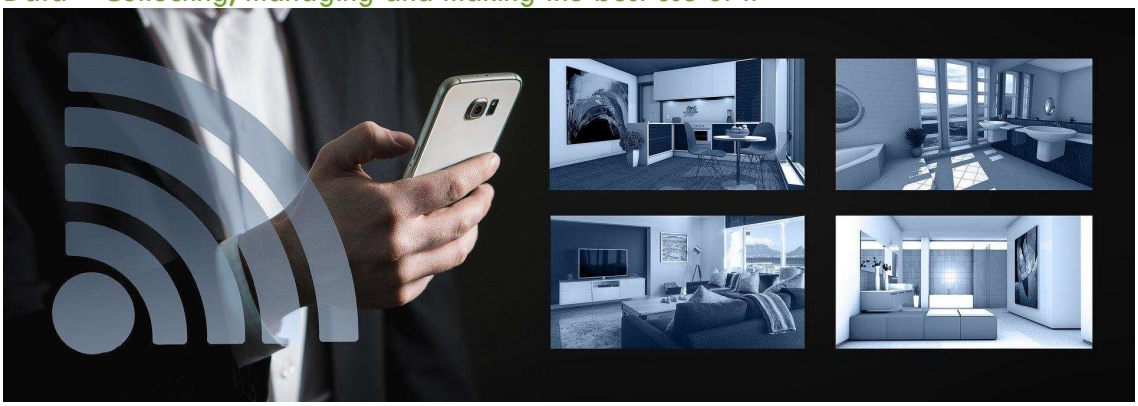
One important aspect of managing security is understanding and complying with the law. Unfortunately, there are no specific laws for use of CCTV on a business property and so this is generally covered by existing laws, for example *The Surveillance Devices Act 1999 (Vic)* for any sites in Victoria. The general theme is that you can use cameras as long as they do not infringe on peoples' privacy, or if you have express/implied consent. The trick is to understand what makes consent. Is it specific written consent? Can it be written into an employment agreement? Does a person entering into an area with clearly posted signage imply consent? In light of this it is generally safest to install cameras in common areas where people do not reasonably expect privacy. This might include car park entrances, reception areas, building entrances and foyers areas. Any BBQ and/or outdoor areas may be well covered under the rules as well.

It's not just CCTV that is subject to the law – Access Control can also present challenges to managing the compliance of a site. For example, access control is often installed on a fire exit potentially creating a hazard by restricting exit in the event of a fire. This can occur at any exit point from the building, as well as exit points from each floor in a multi-storey setting into a fire stair exit path. This means that any doors or thoroughfares within the building marked as an exit path must be planned to ensure people can safely get out of the building in the event of an emergency.

A less considered point is entry. What happens in an emergency if the access control system restricts entry to the building for emergency services like fire, rescue and/or law enforcement? When selecting an installer, it is very important to ensure you ask the right questions. This helps to confirm their understanding of the regulations and risks associated with interfacing with fire systems and/or lift control systems.

For these reasons, it is absolutely critical that any Security works done on a strata site are completed by an installer that is fully licensed and registered with the relevant state authority. You should also ensure that your installer is a member of ASIAL (Australian Security Industry Association Limited)

Data – Collecting, managing and making the best use of it



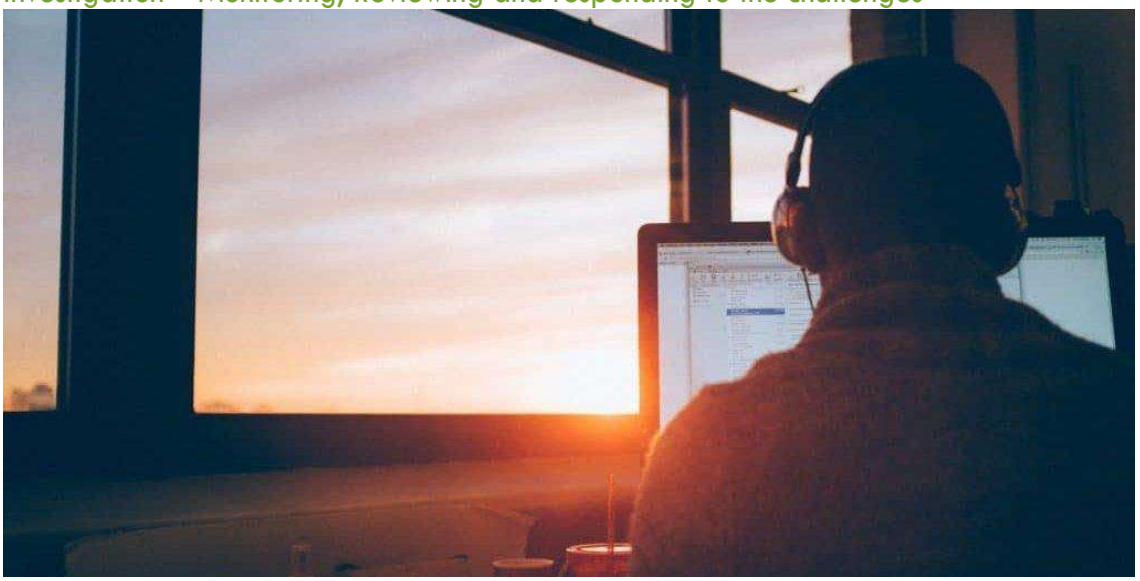
Another key factor in managing security is data management. It is essential to have up-to-date information and contact details for everyone which can be used to track who is in the building and when, where they are allowed to be, and if they are authorised to be onsite. This allows you to have situational awareness in real time; but also ensures that you minimise the possibility of unauthorised access. It is very common for access credentials (cards, key fobs, remotes and Bluetooth credentials - among many others) to simply be entered into the system as a “user number” with no identifiable link to a person. This presents multiple challenges that may start from simple auditing process inefficiencies, i.e.. Who has access to what areas? What type of credential do they have? Do they have multiple types? Do they have access to multiple sites? At the other end of the scale, a poorly managed database can lead to OH&S issues and or liabilities to the owner. For example old/lost credentials being used to gain access to the property, people having access to areas that they should not be authorised to enter. From a liability perspective, it is extremely important to have accurate records for OH&S purposes. In the event of an emergency such as a fire or other major event, poorly maintained data can lead to significant time delays. This can include communication with witnesses and/or ascertaining who is physically onsite at any given time. Over and above the obvious safety risks, the legal ramifications for insufficient data management can be catastrophic.

Access to CCTV data such as footage is also vital to ensure live and recorded video is accessible for monitoring, OH&S applications and incident investigation. User access to the CCTV system should be tightly controlled so that only those with a need to view footage can do so. Not only should access to the system be managed effectively, there may be certain

cameras on the site that should only be available to specific people. This should be considered when selecting your system, to ensure that adequate control measures are in place and that your installer is aware of best practice when it comes to mitigating the risks involved.

A professional and proficient installer will always have a clear data collection and management plan as part of their standard practices. When adding, upgrading or installing a new security system, make sure the installer can clearly explain each step in their data management plan before making your choice. It is worth noting that for a data management plan to be effective, the installer must plan ahead of the install and have a method of data collection that does not require unreasonable work from residents or onsite staff and covers all required information for the various systems to be installed.

Investigation – Monitoring, Reviewing and responding to the challenges



An effective security system can deter people from exhibiting undesirable behaviour on your site simply by being present and visible. For example people are less likely to behave in an unacceptable manner when they are aware of CCTV recording them. It is also well documented that people will be less likely to attempt unauthorised entry to a property when they are aware of an alarm system and/or access control system onsite. The reality is however, often just having the system is not enough. Incidents occur every day, and while we can do our best to minimize them, it is almost inevitable that at some point the security system will be tested as an investigative tool. It is therefore critical that Investigation and response procedures are implemented when managing security in a multi-tenant building. In the event of an incident, it is important to have a plan in place for how to deal with it, as well as the tools needed to ensure you can carry out your plan efficiently and effectively. This information should be regularly updated in consultation with your security provider, and shared with anyone who needs it. Your plan may include working with the police or other emergency services such as fire, rescue or medical. Investigations can be a major challenge for owners corporations. If there is a security incident, it is essential to conduct a thorough investigation to identify the cause and respond effectively.

Effective footage search and review is absolutely indispensable when it comes to CCTV. Valuable hours can be lost when trying to find footage of an event if your system is not set up to efficiently search and provide video. Many strata properties opt for entry level or low end CCTV Systems to save money initially; but end up paying significantly more with large amounts in the end. This comes via hourly costs to onsite staff who need to look through sometimes days' worth of footage to find who stole that bike, fees from security providers to find the footage of yesterday's break in or assault or simply higher insurance costs because it is simply too expensive to investigate. Delays in responding also provide time and opportunity for perpetrators to maximise their chances of avoiding repercussions and reduce likelihood of recovering stolen goods and/or obtaining recourse. Ensuring that you invest in a CCTV system that is set up correctly right from the beginning will ensure that you maximise return on investment. It will also increase your ability to respond to an incident as quickly and efficiently as possible. For more information, see our blog on NVRs vs VMS here.

It is also important to set up your access control and alarm systems to ensure that records of all alarms and access events are recorded, stored and managed properly. For example, reading the event "door 1 accessed by user 32" does not mean much and is not particularly useful in an investigation. However careful data planning and management means that that same event is read as "Foyer Entry Door accessed by John Smith". Adding to the complexity of this task, what happens when John moves out? This is a data change that needs to be managed effectively. This is where working with a provider that has strong knowledge of not only the systems and the data involved; but also how it is used specifically in the Strata world is absolutely indispensable.

Ensuring that you invest in a CCTV system that is setup correctly right from the beginning will ensure that you maximise return on investment; but more importantly, it will optimise your ability to respond to an incident as quickly and efficiently as possible.

So we know how to get the best out of our security system; but without the right partner you planning won't amount to much. Jump to part 4 below for our top tips on spotting and selecting the best integration partner to ensure you get the right system from the beginning.

What to look for when choosing a provider

Now that you have seen just some of the many considerations to be aware of when planning and using your security system, how do you know who to choose as your provider? Have a look at our list of things to look out for below:

Top tips on selecting an installer

Understanding of your needs

Any service provider should spend most of their time with you asking questions, not teaching!!

Many service providers fall into the trap of telling you what you need before finding out what you want fixed. Without doubt one of the biggest causes of systems that do not perform is a lack of specific understanding by the installer. It is tempting to think of a security system as just a collection of cameras, doors and alarms that don't do much. They only record peoples' movement, control access and alert someone in the event of a break-in right? However, it is vitally important that your installer understands YOUR issues, otherwise you will spend good money on a system that does not address your needs.

Make absolutely sure your security provider understands your problem and objectives - are they asking the right questions?

Robust planning and deployment processes

Does your proposed installer have that "she'll be right" attitude? Run……..get away fast……they may be cheap; but they will cost you a fortune. If your installer cannot supply you with a scope of works, plans, a rollout plan and project milestones at a MINIMUM, they have no idea how they are going to install the system. Commonly you will hear the "I've been doing this for xx years, we don't need to see the site" line, well the reality is that they have never done it on YOUR site.

If your installer is not prepared to put in the time to pre-plan, then you are a number not a customer.

They back themselves and their work

Look for guarantees, clear deliverables and strong communication in the initial process. A Service Level Agreement (SLA) signifies that the installer will take account of their work and will work with you to ensure the best outcome. SLAs should be customised to your business needs, so look for an installer that will work with you to find out what service level items are most important to you. At the end of the day if a provider will not stand behind their work then they are not confident in getting it right. The service you receive from your installer should not stop when the install is done. They should have a well-developed support process that provides clear guidance on what to expect going forward and what level of service you are entitled to.

Your installer should offer consistent and well documented maintenance and service packages to give you peace of mind.

Partner Support

Be wary of offerings involving the "latest in European design" or brands that you can't find multiple suppliers for locally. Opting for an "exclusive" brand can leave you exposed to an informal lock-in with your installer. If no-one else supports the product being proposed, you are putting all your eggs in 1 basket and will have nowhere else to go should your installer

not perform. Your installer should have the backing of highly regarded vendors and suppliers that have a presence in your region. Installers that directly import products from overseas often have no real support, or cannot get it until support operators become available in different time zones.

Ask your installer who they work with and are they locally supported to ensure a much smoother experience.

Knowledge

Security is a very specific technology and requires very specific knowledge and skills to effectively deploy a security system. Your installer needs to know how to effectively apply these skills to your specific requirements or you will end up with a system that simply does not do what you want it to do. Does your installer know what product best suits your application? Ask them why they are proposing a particular solution, and if you don't understand the answer…..ask until you do. Remember you will have this security system for many years, so it needs to work for you. Always remember that your concerns and priorities will be different to someone else's, so make sure your installer spends the time to understand your site and offers a solution that is tailored to your needs.
Of particular importance is how they will enable you to effectively manage your data going forward. You cannot effectively manage poor data, therefore it is vital that your installer can communicate a clear, structured and efficient plan during the preparation and/or install phase to collect the necessary data. Ideally installers will offer a service to manage the data for you on an ongoing basis. This is something that can save you a fortune in total cost of ownership over the years.

Ensure you only work with a knowledgeable installer to avoid costly mistakes.

Innovative approach

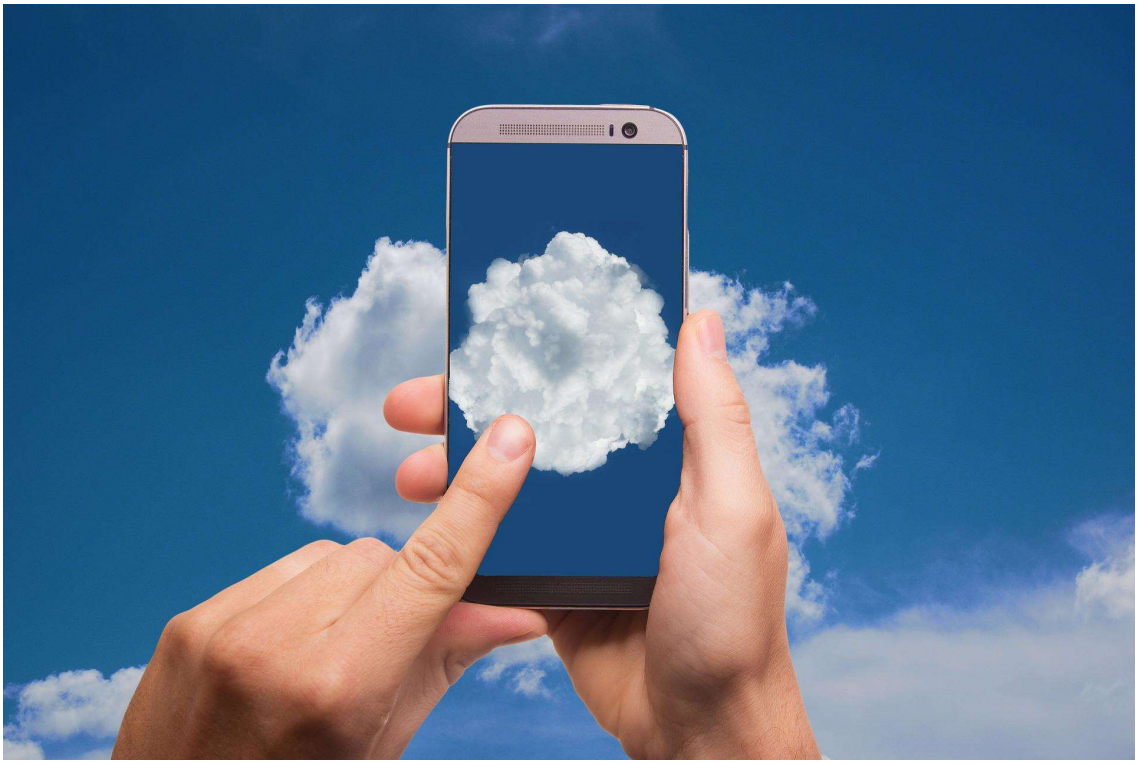
Try to select an installer that is across the latest in security technology. For example many of the latest products offer cloud services and internet based management. This allows you to consider a product that not only gives you access from anywhere in the world; but can also mean a far less intrusive install process as much of the initial setup can be done offsite. The result is less management of the process by you, and less disruption to your business as the installer spends less time on site with noisy power tools.

Look for installers that are constantly finding ways to enhance your experience of the system.

Security is a critical part of any Strata environment, and it's important to make sure you select the right provider and adhere to all applicable legislation. By understanding your obligations, and collecting data in a meaningful way, you can set up an effective security system that will keep your sites and residents safe from harm. Make sure to review your options carefully and ask the right questions when selecting an installer – covering all of the points we've raised in this post should help you make an informed decision.

Security Systems - Cloud or no Cloud?

Are you still debating whether or not to switch to a cloud-based security system? You're not alone – a lot of people are still on the fence about this relatively new technology. But is it really worth the switch? In this blog post, we'll take a look at the pros and cons of cloud-based security systems, and help you decide which option is right for you.



It's hard to believe that just a few short years ago, cloud technology was something of a novelty. These days, it's becoming increasingly normal for security systems to make use of cloud-based technologies. There are a number of reasons for this. First, cloud-based systems are more scalable and flexible than traditional security systems. This means that they can be easily adapted to the changing needs of businesses. Second, cloud-based systems are often more cost-effective than their traditional counterparts. This is because they make use of shared resources and don't require businesses to invest in their own infrastructure. Finally, cloud-based security systems are often more innovative than their traditional counterparts. This is because they offer businesses the opportunity to take advantage of the latest developments in artificial intelligence and machine learning. As a result, it's no surprise that cloud-based security systems are becoming increasingly popular among businesses of all sizes.

In this 4 part article we'll be looking at:

- What is cloud-based security and how does it compare to traditional security systems?
- Pros and cons of using a cloud-based security system?
- How secure are cloud-based security systems, and are they safe from cyber-attacks?
- Which type of security system is best for your application - cloud or no cloud?

What is cloud-based security and how does it compare to traditional security systems

In a world where more and more businesses are moving their operations online, the question of security is becoming increasingly important. While selection of the best system for your specific requirements is a key consideration, many businesses are now looking for systems that offer both security and accessibility. So how do cloud based systems differ from traditional "hardware based" systems. Put simply, a traditional system is installed onsite at a fixed up-front cost. A cloud system consists of site “devices” connected to a web based network and is “rented” for a monthly/yearly cost.

The difference between cloud based systems and hardware based systems comes down to the way they are accessed and set up.

Traditional "Hardware based" systems

A traditional system consists of a set of core hardware products that work together to make up a system. For example a CCTV system typically consists of CCTV cameras, a recording device (either an appliance or a dedicated Server Computer) and some form of network to set it up on. Many traditional systems can be connected to the internet via configurations on the recording device and the network, or a newer technology called "P2P" which essentially sets up the internet connection for you. Traditional alarm, intercom and access systems are often a mix of non-connected devices that are physically wired to a "controller". This controller sometimes acts as a gateway to the internet, allowing access via remote devices and computers - in a sense, adding a connected controller to a traditional system makes it the lowest level of cloud system.

“Cloud based” systems

Cloud based systems offer many (if not more) of the features that traditional systems offer, with a different architecture. These range from traditional systems with an internet connected controller right through to fully connected IP systems that connect directly to the internet. Referring to a security system as a cloud based system means that not only is it accessible via the internet, but that some, many or all of the features offered by the system are delivered via the internet. For example, a traditional CCTV system might allow access to recorded footage via a mobile phone app. The app connects to your recording device and retrieves footage stored on hard drives physically installed in the traditional recording device. A fully cloud connected system may not require an app allowing you to simply logon to a website to view cameras and footage.
Some cloud based systems work 100% on the cloud, meaning that all features and functions are available only via an internet connection (more detail in the pros and cons section).

So with the basic differences between the technologies understood, let's look at the advantages and disadvantages of the cloud based system.

Pros and cons of using a cloud-based security system

Flexibility

One of the biggest advantages of cloud-based security is its flexibility. CCTV, alarms, intercoms, and access control systems can often all be easily integrated into a single system, allowing you to tailor your security setup to your specific needs. For example, many cloud based CCTV systems can talk to Access Control allowing cameras to be focussed on a particular door every time a person of interest uses their access card there. We can also use cameras to detect number plates and open boom gates in parking scenarios, allowing for automated billing and access based on registered cars. Features and functions can be added and removed as needed, often allowing for significant advantages when deploying systems over time. Often, cloud based systems provide for trial periods to test out basic functionality, and allow addition of extra features - many times at just the click of a button. Because cloud systems often have no "controller", there is no system bottleneck. This means that a cloud based system can be much larger than a traditional system, and can be spread over multiple remote sites with relative ease.

So the disadvantages - there really is no disadvantage to any of the above when it comes to flexibility. The cloud system delivers significant flexibility over and above that of a traditional system

Accessibility

One of the greatest challenges facing security management today is the balance between security and accessibility. Generally, these two aspects of the system have been polar opposites of a sliding scale, more secure means less accessible and vice versa. Today's systems have made great strides in this area; but there is still a compromise when it comes to cloud availability.

Due to the fully connected nature of cloud based systems there is an inherent ability to access your system at any time and from anywhere in the world. This makes it easy to keep an eye on your business even when you're away.
For example, today's CCTV systems allow a user to access video footage instantly from anywhere you have an internet connection. Combined with a feature called the "smart search" this can greatly speed up the process of finding footage of an incident and making an informed decision on how to respond. New users can often be added remotely, giving a system admin the ability to work remotely as required whilst minimising the interruption to their workflow.
Many higher-end installers will also offer “law enforcement access”, which means remote access can be granted to law enforcement temporarily to allow them to review and save footage. Again minimising the work required for footage review.

Another advantage of this extended accessibility is the ability to share data across multiple sites and/or stakeholders. For instance, businesses with multiple sites to protect no longer need to install separate systems when their security is cloud connected. They can simply

connect all devices to the internet and then manage them centrally via a web portal, allowing access to building areas (doors, lifts, boom gates etc) as needed across all sites.

Accessibility can also have advantages when it comes to decisions on alarm responses. For instance, with traditional systems an alarm signal being sent to a control room was somewhat of a gamble. Was there a real intruder onsite, did a bird fly into the warehouse, was there a warm breeze or a reflection from the sun setting of movement detectors? Do you attend the site yourself and risk a physical confrontation?, or do you dispatch a security patrol? - incurring large costs every time this happens. Now we can perform "video verification", which means we can pull up video of the premises to visually confirm the alarm. This can save thousands of dollars a year in costs and, more importantly, help to keep people safe by giving a more accurate assessment of the risk level onsite.

Along with accessibility though comes a level of risk. The internet is not a private space, it is a public space and therefore carries a lot of the risks associated with putting sensitive data on a public network. Connected systems can be vulnerable to attack from hackers, disgruntled ex-employees, 3rd party attackers and many more. Does this mean that cloud systems should be avoided? Not at all.....as with all risks, we weigh up the advantages against the risks and make a decision from there.
A good installer will always have the skills to secure your network to minimise the ability for a 3rd party to gain unauthorised access. In particular, many devices when connected to the internet use a protocol called "P2P". This essentially involves the device calling a server on the internet, reporting its details in and then establishing a secured (encrypted) connection. The device will then refuse to talk to any other devices that are not similarly registered with the same service, allowing for internet connectivity; but with a private connection. Many of these cloud services use military grade encryption which makes it very difficult to gain access.

An often overlooked disadvantage to some cloud services is the need for an internet connection. Many cloud based systems will use a hybrid combination of cloud based functionality and local functions. This means that some tasks happen on the internet, and some happen on the device. Typically, critical functions are best performed locally. For example, a fire/evacuation system that relied on the internet to open doors or turn on sprinkler systems would not be a very safe product. Similarly, a CCTV system that relied on the internet to store footage could represent a major security risk in that if the internet was lost, there would be no footage in the event of a break-in or other incident.

Cost Effectiveness

Cloud-based security systems can be significantly more cost effective than their traditional counterparts. This is because of a few reasons:

They often require less hardware – Cloud systems typically require less physical hardware in the background as they are able to offer features and services via the internet. A good example is storage. Traditional CCTV uses either a small recorder onsite (NVR) or a PC with multiple hard drives attached. This means expensive, bulky, power hungry hardware that must be paid for in advance and can break down (introducing extra cost) at times. Many

cloud based systems record footage to the cloud or to an SD card on the camera, therefore reducing the need for hardware to manage the process.
Cloud systems often require significantly less install and configuration, hence they can reduce initial outlay even when paying upfront.

Features can be added and removed as desired – One of the most significant advantages of cloud based systems is the ability to add and remove from the system without any physical changes. Many cloud based systems allow the user to choose from a suite of "features" that can be added to the system as needed. This gives the freedom to decide if a feature is worth paying for or not. This also means that new features or functions can be added as they are introduced to the product. Allowing the user to upgrade their system to allow more features without physical changes in many cases. Often, cloud based systems can incorporate retail analytics, information systems and other useful services that allow a return on the system itself. Drastically increasing the cost effectiveness and even providing return on investment

Services can be customised to your business – Most higher-end installers are able to overlay valuable and useful services that can be delivered remotely with cloud based systems. Maintenance agreements can be inclusive of monitoring, maintenance, footage retrieval, analytics such as face recognition, number plate recognition, smart clothing based searches etc for a much smaller monthly fee, saving thousands of dollars in upfront costs. Many of these services are bespoke functions that can be deployed after deep collaboration between the installer and the business owner/user.

The difference in system ownership is the main consideration here as cloud systems are often subscription based. This means the system is effectively being rented over a period of time. Although not strictly a "con", it is important to understand this difference and the way it affects overall cost.

How secure are cloud-based security systems, and are they safe from cyber attacks

This is somewhat of a "how long is a piece of string" type of question. The short answer is that cloud based systems are as secure as the network environment they are on. It is important to remember that most traditional systems have some form of internet connection today, so the risk profile difference between the systems is not as large as you may initially think.

Most of the same considerations exist surrounding security of Data, management of access, retention practices, and legal compliance among many others. The main contributor towards the security of a cloud based service is a secure connection. As mentioned above, a well secured system will involve a dedicated connection between the device onsite and a secure server. This connection or (pipe) will act like a barrier; both concealing and protecting visibility of data you send across the internet. This is done by a process known as encryption.

Although many cloud security manufacturers will build strong cyber-security features into their products, many rely on installers, IT departments and end users to secure the network themselves. For this reason it is important that your installer is well versed in securing networks from 3rd party attackers. Quality installers should now have specialist IT security

professionals as part of their offering. They should be capable of applying cyber-security best practice principles when deploying your system. For this reason it is imperative that an installer be able to explain clearly how they will secure your system.

Which type of security system is best for your application - cloud or no cloud

The answer to this question depends on what you want out of your system vs how you want to manage the costs.

As previously mentioned, a cloud based system offers unique features that are often interchangeable and customisable. For example if you are trying to identify specific persons of interest and want a warning when they are on-site you have 2 options. Either pay upfront for a camera that is capable of performing facial recognition internally with the required hardware, or add the functionality to your cloud service as part of your subscription. Often cloud based services can add functionality to existing cameras, eliminating the need for an expensive new camera. Perhaps you are looking for license plate recognition for a parking/boom gate application. Local "LPR" cameras can be purchased for this application, which are usually significantly more expensive than standard cameras. Alternatively, some cloud offerings can use existing cameras (dependent on the camera specifications). The license image is sent to a cloud server and processed online, with the results sent back to the software for viewing, or to grant access to a boom gate/door etc onsite. Looking at it from this perspective, the choice comes down to whether you see your system as an investment to be owned or a business tool to simply have access to as needed.

One new development in the area of cloud security is the emerging analytics "Appstore". Increasingly the various features, functions such as analytics (movement detection, face recognition, retail heat mapping etc) are moving towards an "app ecosystem" approach. This means that analytics can be purchased off the shelf and applied to existing compatible cameras. This app approach allows for outright purchase of analytics or subscription access, depending on how you like to approach the investment of a new security system.

Finally, a feature that is almost specifically unique to cloud based services is the ability for many of these products to be deployed on an existing network in a "demo capacity". Allowing you to try the system before making a decision to ensure the best fit for your business. Traditional systems typically make this service a lot harder for both installer and customer due to the significant time and labour investment incurred by the installer to set the system up. Most installers will want a fee for the demo and/or a significant purchase commitment for a demo. Traditionally this has made this service something that has been available only to large enterprise customers that have the funds for testing and development built in to procurement. Now even smaller customers have the option to engage with their supplier to arrange demo periods with far less risk to the installer. 1 – 2 points of protection can now be added to a site to test functionality, features, useability and security on the network – this is a significant advantage to cloud based systems, and one that should be very high on your list of selection criterion for your new system and security provider.

Finally, one last point to note is the intrusiveness of install. Traditional systems require teams of installers onsite to physically install devices, networking, computers, servers, storage and a host of other components. Typically cloud systems require much less “time on site” with a lot of configuration possible remotely due to a lot of the backend systems being owned and managed by a third party. This can lead to a shorter and less intrusive install period.

Wrapping it all up

So as you can see from the above, cloud based systems offer a significant amount of flexibility, access and functionality. They offer flexible payment, scalability and opportunities to try before you buy in many cases. Traditional systems provide a more secure environment out of the box; but much of this is mitigated as soon as you connect them to the internet. Traditional systems offer local operation that generally does not need the internet to function, while cloud systems offer a range of internet reliant features combined with local functions.

Hopefully this has given you some checkpoints to mark off next time you are considering the question of Cloud vs Traditional security systems on your site.

Camera resolution - Is more always better?

One of the most common topics of discussion within the security industry revolves around camera resolution. With the advent of modern cameras and IP technology, the resolution of CCTV cameras has grown exponentially to the point where 12 Megapixels is no longer unheard of. With so many different resolutions available, it is tempting to just select the highest resolution every time - after all a 4K tv is always better than a 1080p tv right?

Not necessarily.....today we will have a look at how camera resolution works in a security setting and give some tips on how to ensure you get not just the best camera; but the RIGHT camera.

Let's get very slightly technical here, just enough to get an understanding of how pixels on a camera work. Inside every camera is a little light collecting circuit called a CCD. The CCDs job is to collect light and pass it through to the camera for processing into the image you see on your screen. The CCD is covered in little sensors that collect the light - the higher the megapixel, the more sensors on the CCD, the higher the resolution image you will get. So this all seems to point to higher resolution being the better option; not so fast.

CCDs come in a range of sizes; but ultimately on CCTV cameras they are standardised. Which means that whether your CCD has 2 million pixels or 12 million pixels.....the space to cram them into is the same. The obvious approach is to make the little sensors smaller so they can all fit, great...done. So now we have 12 million sensors in the same space as 2 million, we of course need to make them smaller to fit. Now we have a problem....light sensors collect light based on their physical size, so a larger sensor will collect more light than a smaller sensor. It's like a bucket, the bigger the bucket the more water it can collect. This means that in low light situations, a higher resolution camera will tend to suffer from light issues that can lead to blurry images. Ironically, the resultant of this can lead to less clarity in your image.

So how do I know which resolution to use?

Fortunately, security installers have been working with this technology for many years and have a pretty good grasp on where to apply it. A good provider will be able to advise you on the best camera fit for each application. It is good to have a basic understanding though, so with that said let's have a look at some applications.

Car Parks and higher megapixel

Higher megapixel cameras are particularly good at minimising the need for multiple cameras. For instance, to cover a 50m x 50m carpark, you would have once needed multiple 2 megapixel cameras. An 8 megapixel camera (4K) with a wide angle lens can theoretically do the work of 4 x 2 megapixel cameras (depending on the layout of the car park), potentially saving you the work and expense of installing 3 cameras. However the trade-off is less low light performance, so unless the car park is reasonably well lit, you may find yourself looking at a dark or blurry screen.

Top tip - Think about the size of your space and the ambient light levels

Corridors and lower megapixel

Lower megapixel cameras may not give you the resolution; but they are much better in low light situations. A great example of where a lower megapixel camera is actually a better bet may be in an internal corridor. Remember the point of CCTV is to record and recognise an intruder, not make them look like a Hollywood star in 4K!! As a general rule of thumb, if you can see what you want to see, then any more pixels are just wasted. As a corridor is by nature quite narrow, there is no point having a high resolution image as most detail will be pretty clear at such close range. The real advantage comes into play when the lights go down. That low megapixel camera will give you far superior low light footage with less motion blur and/or graininess and a better framerate. This means your footage will actually be clearer and sharper with lower megapixels....how's that for irony!

Top tip - Consider how close the camera will be to the target

Storage is EXPENSIVE

Put simply, the more resolution, the more data and therefore the more storage needed in your recorder. Believe it or not, often in larger CCTV installations the storage required for the footage is actually more expensive than the cameras. That's because more cameras and higher resolution = more hard drives to store the footage. This in turn means that the recorder needed to manage all this needs to be more powerful to handle all the work of encoding and decoding that video onto a hard drive. It gets worse though.....this ALSO means that the networking infrastructure needed to handle all of this data on its way to the recorder needs to be taken into account. A good provider will be able to take all this into account and optimise the system using framerates, resolution and picture quality setting among many other tools.

Top tip - Think about how many days footage you want to keep

Tips

- Beware of the security provider that proposes the same camera for every part of your building - they are **NOT** planning based on **YOUR** requirements
- NVRs almost **NEVER** live up to their specifications - a "4K" NVR usually means **1-2 cameras** at 4K maximum is all it can handle
- Your security provider **MUST** have strong networking knowledge - ask questions to ensure they do

Hopefully the above info will help to make the decision a little easier. Follow the tips to ensure you get the right product installed and maintained by a professional security provider.

13 000 THEFT (1300 084 338)
info@bravesecurity.com.au
www.bravesecurity.com.au

Important considerations when evaluating an access control system?

Are you looking to upgrade an existing or install a new access control system? In this blog we have a look at 3 aspects of access control that can maximise your return on investment and ensure you have an effective system for years to come.

Access control can be tricky, which is why with a little bit of planning and consideration, you can maximise the effectiveness of your new system right out of the box. Today we are going to look at 3 considerations that can have a vast impact on the quality of your new system. We'll tell you what they are and give you some important advice on how to ensure you get it right, let's get into it!!

In this post we'll be looking at:

- High and low level security
- Types of credentials
- The database

High level and low level security

If we go back a few years, many readers may remember the concept of the registered key. A registered key was essentially a standard physical key; but it was registered to a property or property owner. This meant that to duplicate the key, a key cutter would need authority to do so. This usually involved a letter of authority or some type of valid document that authorised a copy of the key. This was then added to the "register" for existing keys. This practice is what we refer to as "high level security". "Low level security" is essentially the type of key you might see on the average residential building (house, unit, storage units etc). These are standard issued keys that generally come pre-cut from the manufacturer when you buy a padlock, front door lock and/or internal door handles. Not only can anyone take these to a key cutter and get a copy made with little to no regulation, often the manufacturer uses standard key templates. This means that if you took your front door key and tried for long enough, you would eventually find a door that your key works with. So with that said, it is pretty clear which one is preferable from a security standpoint; but what about access control systems where there is no physical key?

Access control systems replace the typical key with what we call a "credential". This may be in the form of a remote, card, tag for keyring or, more recently, a bluetooth/NFC "mobile credential" (more about these credential types later). Each of these credentials works in a similar way to a key in the sense that you carry it to use to unlock a door. Where they differ is in the technology. A credential is an electronic key that transmits a bit of information via a reader to the security system that tells it whether the holder has access to the door. This data comes in a few formats, with the most widely used format called "Wiegand". The problem is that there are only finite combinations of data to identify the user. This means that the same problem applies (albeit to a much less degree) regarding the ability to find a door that will open given enough time. So how do we solve this issue?

We solve it in the same way we solved the physical key issue.....we register the keys. Via a process referred to as "encryption", another layer of data with sometimes billions of possible combinations is encoded on the credential and also in the reader. This means that the user's details must match to open the door; but the reader will actually ignore the credential if the encrypted data on top does not also match. As an extra layer of protection, the encryption is registered to your security provider and their supplier to ensure that no-one other than your authorised supplier can create, duplicate or add credentials without your express authority. This also means that a good provider will manage the credentials on your behalf, reducing your need to administrate users and simplifying the ordering process.

As you can see from a security perspective, high level security will deliver much better levels of control and will greatly minimise the risk of misuse.

Types of credentials

A very important consideration is what type of credential you want to use. Below is a table which shows the main types of credentials and some of the pros and cons.

Comparing the different credential types

Type	Pros	Cons
Card	•Can be printed on (photos, instructions etc) •Relatively compact (size of credit card) •Can be printed on (photos, instructions etc) •Can be worn around the neck on a lanyard for easy access	•Can be bent or broken •Has a very short read range •Printing will wear off in time •Can be lost/stolen
Fob	•Very compact •Tend to be much stronger construction •Can be a bit cheaper •Can be kept on a keyring	•Stronger but can still be broken •Shortest read range •Cannot be printed on •Can be lost/stolen
Remote	•Compact size (ok for keyring) •Usually very strong construction •Allows operating doors from large distance (garage doors etc) •Allows for multiple functions with 2-4 buttons and can also work as a fob	•More expensive •Breakable •Cannot be printed on •Can be lost/stolen
NFC/Bluetooth	•Exists only on a mobile phone •Has all the protections common to mobiles •Generally has the longest read range •Can be deployed and managed rapidly and more cheaply	•Usually requires an app •NFC can have compatability issues •Sometimes not transferrable •Requires mobile phone

As you can see from the above table, there are quite a few to choose from, all offering different features to suit different applications. The key here is to involve your security provider deeply in the decision making process to ensure that they are advising on the credential that suits your needs.

The database

Possibly the most important aspect of any access control system and, in fact, any security system be it CCTV, Alarms, Access or intercoms. See out 4 part series for more information on what to look for when it comes to data management HERE.

Your access control system will require a database to perform its functions. This database needs to be accurate and will require significant work to set up and maintain. Many system owners will manage this database themselves; but this is not recommended as managing the data requires a deep understanding of how the security system operates. In the case of an access control database, the main considerations are:

Doors - What are they called? Where are they located? What devices are present on the door (typically locks, readers, open/closed detectors, exit buttons, emergency release buttons etc)

Users - What users have access to what doors? When do they have access?

Devices - What doors are they connected to? Do they function as an alarm device as well?

So what is the best way to manage the database? It all depends on how much management you want to perform. A modern, technology connected provider will offer a database

management service or plan which should cover initial install (data collection and entry) as well as ongoing maintenance. It is absolutely vital that the initial install include a full database setup covering all users, their personal contact information, department (or unit if a residential/strata building) as well as a host of other data. This data then needs to be managed on an ongoing basis to keep it up to date and accurate. If you lose track of who has what credential and what doors that credential has access to for instance, you can quickly find yourself in an administration nightmare. When people leave, you need to be able to track their access and credentials to ensure they are removed, or redeployed (depending on the credential type).

Some modern providers offer cloud based services and data management portals that allow you to access your data via a secure internet connection. An even higher end service is a full management function in which your provider can perform real time changes and updates that will be reflected on your system immediately. This is a service that is well worth looking into and can save you significant amounts of time, energy and confusion. It can also save significant amounts of money in liability if something happens onsite as well as reduce callout and labour fees as your provider can remotely make changes on your behalf. Lastly, this type of service allows credentials to be issued and deployed rapidly (often same day for new credentials, or even sooner with pre-purchased credentials).

So there you have it, the main 3 considerations to take into account when looking at a new access control system.
For further information on how to select the best provider for your install, see our top tips HERE.

NVR or VMS for my CCTV - What's the difference?

We are living in an increasingly hi-tech world. Every day new security products are being created and marketed to us, the pace of these new products can be overwhelming. Today's new innovation is next year's old technology….so how do we decide which product to use?

When it comes to video surveillance, one of the most common questions we are asked as a security installer is what is the difference between an NVR and a VMS, and which one should I use. As professionals in the security industry, we start with one question – what problem are you trying to solve? Let's start with a quick comparison between the two product types:

NVR (Network Video Recorder)

An NVR is an appliance, it is a device with built in software that takes camera feeds and records them to inbuilt storage. They are often cheaper and easier to deploy and have a wide variety of features and functions such as smartphone apps, windows/mac apps for management, and network capabilities. NVRs generally come in different flavours relating to

the number of cameras you can attach – 4, 8, 16 channel models are the standard these days.

VMS (Video Management Software)

A VMS is a program that allows a computer to record video in much the same way as an NVR. A VMS provides all the functions and features of an NVR; but also offers a much greater array of benefits, flexibility and expandability. The difference is in the functions, longevity and ease of use that they offer the user.

So how do we decide?

Start with the problem……are people vandalising the site? Do you have OH&S considerations? Do you need to have good visual awareness of the site at all times? An NVR will provide good awareness onsite, giving you the ability to display cameras on a screen providing very effective, live visual awareness. The NVR will also let you review footage when looking for who spray painted your front door, or when your tenant slipped over in the foyer and what led to the incident. A VMS will also offer these benefits; but with a few advantages. Finding NVR footage takes time….and lots of it. Using an NVR to review footage can result in significant time investment including:

- Reviewing footage – requiring someone to sit in front of a screen and search through at times hours of footage
- Interviewing witnesses to get approximate times if times are not known
- Obtaining footage from the recorder is a much more time consuming and labour intensive task

In contrast, a VMS allows most or all of the above steps to be skipped due to 1 major feature….the search. With a VMS we can simply ask the VMS to show us a 3-4 second piece of footage showing everyone who has entered a certain part of the camera view over a specified period of time. The VMS will then organise the snippets of video in a way that makes it easy to just browse until we find our person of interest. We can then investigate the video directly from there and either export for law enforcement or for our own investigative purposes.

Apart from usability and management efficiency, there are also business considerations that must be taken into account such as initial outlay, expandability and longevity.

An NVR will cost less initially due to the mass produced nature of these products. They require minimal setup and configuration and can be deployed rather quickly, saving further costs on the initial install. However, once installed there is a very limited amount of expandability and flexibility available. The amount of cameras, and the quality of the video obtained from the cameras is set in stone from the moment of purchase, making the NVR a true appliance. This introduces a much higher level of risk and depth into the decision making process. If you need more cameras down the track, or require more out of your existing cameras…you may need to upgrade to a new NVR (adding cost) or add another NVR (adding cost and complexity to the management of your CCTV system). New features and functions are generally packaged into newer “models” of NVR, meaning that as new

innovations become available, you may not get access to them without the cost of a new NVR.

On the other side of the coin, a VMS will usually require a higher initial cost outlay due to the fact that it uses higher end technology and is generally a customised solution. Once installed however the flexibility and expandability is significantly increased and the ongoing costs associated with VMS ownership are significantly lower. Cameras can be added with minimal if any extra costs over and above the cameras themselves. Quality and video clarity can be changed, increased and or customised as site requirements change. New features and functions are generally available free of charge as the product is developed, allowing the user to take advantage of new innovations as they become available. This gives the VMS a distinct advantage when looking at the operational lifetime of your new system and the total cost of ownership.

There are of course a vast array of other considerations when selecting the best system for your needs; but the above should give you a good starting point when making your initial decisions. To really make sure you get the right solution, it is recommended to get a professional security installer to help you decide, that way you can be sure you will get a high quality system that suits your needs and serves you well into the future.

What should I think about when considering an alarm system?

In today's world, securing your business is more important than ever. With the National Retail Association estimating the cost to Australian businesses at around $9b per year the value of having an effective security system cannot be overstated. The question is which system do I choose and how should I manage it going forward.

When it comes to security systems, and this can include CCTV, Access Control, Intercoms and various other products, there is usually a trade-off between security and accessibility.

- How secure is the system?
- How accessible is the system?

Many traditional systems will place a call to a "control room" to alert them when an alarm is triggered. This allows a call to be placed to you from the control room in the event of an incident; which then allows you to decide on a course of action. This really is the minimum service level required as it allows you to have 24hr monitoring on your system, creating a more professional and safe way to respond to issues. Another advantage of monitoring is that insurance policies generally provide for a discount if you have a monitored "back to base" alarm system. Historically, this was pretty much where the service ended with no real

consideration given to the usability or accessibility of the system - a result of the fact that a security system was there just to turn on when you leave, and turn off when you arrive. The advantage of this approach was also the difficulty someone would have in getting into your system, as there was generally no connection to the outside world (internet/4G etc). In today's connected world however, people generally expect more from their installed systems.

There are now a host of extra features that an alarm system can offer outside of these traditional functions. For example, many alarms can now turn your lights/heating/cooling on when you arrive - or off when you leave. We can open/close garage doors or unlock electronic door locks, with many systems being able to use "geolocations", which means all these things can happen automatically depending on how far from the premises you are. Most systems connect to your network to allow turning the system on and off remotely via a mobile app. Many apps also allow simple programming such as adding users and/or changing codes, allowing for temporary access to be granted remotely for visitors, contractors etc. Self-monitoring is now a viable reality that can actually save you money. For instance, go back a few years and when a control room alerted you to an alarm on your system you needed to take a bit of a gamble. Should you get a patrol car response (costing money), do you get law enforcement involved or do you make the call to investigate yourself, potentially putting your or someone else in harm's way. Nowadays, when the control room calls, you can jump onto your CCTV app and have a look to see if someone is in the building, or has the AC/Heating, bugs on detector lens etc set off the alarm.....this is called video verification. Apart from the convenience, this also allows the business owner to minimise risk to themselves and others by reducing the likelihood of disturbing an intruder onsite.

From a convenience perspective, these are all useful features; but the increased accessibility extends not just to users but would be criminals. Whereas once upon a time someone would need to physically interact with your system to get access, it is now possible to gain remote access from hundreds, even thousands of kilometres away. This means that any systems installed at your premises should be provided by an experienced installer with knowledge of how to mitigate the risks involved. Some security providers can offer networking and network security packages to minimise the risk, other products are attached to a secure network by the manufacturer with state of the art security processes and protocols applied out of the box. Either way, ensure that you ask about the risks and ensure your installer clearly explains how they work with them.

There are many different types of systems ranging from hardwired (all devices are physically connected via cable) through to wireless (detection devices are connected via a wireless signal to the alarm system), or hybrid (a mixture of wired and wireless devices and components). Which one you choose will generally be the result of the structure of the building and the surrounding environment as well as the convenience vs cost associated with setting up. Wireless devices are much more prone to interference by radio waves, Wi-Fi etc than wired devices; but are generally less time consuming to install allowing you to get your system up and running faster. Wireless devices can at times be cheaper to install as they do not need to have cables run to them; but this depends on the building. On the other

hand, wired devices are arguably more reliable, less prone to interference and come in a wider range of options; but can be time consuming to install and prone to issues down the track if cable gets damaged.

There are many other considerations; but these are the main ones. Your security provider should be able to guide you through most of the process, but make sure you ask about the points above to ensure you get the best value and performance for your investment.

Key benefits and features of a modern alarm system

- Turn your alarm system on or off from your mobile device (internet connection required)
- Get notifications immediately in the event of an alarm
- Take control of your response plan
- Integrate your alarm system with auto garage doors, lights and many other home appliances
- Integrate with CCTV from the one app (available on select systems)
- Reduce your insurance premiums with "back to base" monitoring (check with your insurance company or refer to your pds)
- Choose from wireless, wired or hybrid systems

Key tips for monitoring your security system:

It is important to have an action plan in place for security events and we can assist you to create a process to ensure that issues are dealt with quickly; but most importantly….safely.

Call the police

Ideally, you should always contact the police if you suspect you may have an intruder in your premises. Should you witness an intruder leaving the building, do not attempt to intervene, you can always supply CCTV footage to police later if available. It is better to lose some of your assets than to risk personal harm. Chances are they will know your intruder by name already!!

Use extreme caution if dealing with an unverified alarm

It is important not to panic when you receive a notification. If you do not use CCTV, be aware of the situation before acting. As part of your action plan, make sure your staff members know never to enter the premises alone if the situation is unknown. If you decide to enter the building (not recommended) it is better to call someone else to accompany you.

Use a CCTV system to allow for verification of events

Although alarm systems are very reliable these days, it is still possible to see false alarms caused by air conditioning, heating, bugs/spiders crawling on the detectors etc. A connected CCTV system will allow you to remotely view the cameras on the property to get a visual confirmation as to whether you have an intruder or not.