EYEWITNESS SURVEILLANCE

SECURITY SYSTEMS 101

An Industry Guide to
Commercial Security Systems

CONTENTS

FOREWORD

THE GREAT, WIDE WORLD OF SECURITY

You've got a problem on your hands.

A huge, ugly problem that's bleeding money from your margins every month.

Your business is losing revenue to theft and damage.

THERE'S ONLY ONE WAY TO STOP THIS DRAIN ON YOUR RESOURCES: A modern security system. One that takes a proactive approach that deters theft before it even happens—maybe even stops it mid-progress.

But what does a "modern security system" really mean? Are you talking about security guards, or a burglar alarm, or video cameras—or a combination of all three? Ultimately, you need to figure out what these security solutions can—and can't—do for your specific business security needs.

That's where this guide comes in. In the next 30 pages, we're going to cover the basics of six different security services, including: **Security Guards, Guard Dogs, CCTV, Interactive Video Monitoring, Keyless Access Control, and Intrusion Systems**.

We'll dive into the history of each of these security services, and go over the nuts-and-bolts of how each system actually protects your property. We'll also offer the pros and cons of each service, depending on the situation. Every business is different, and a great security solution for someone else might not work especially well for you.

This guide will arm you to make the very best choices when it comes to selecting a comprehensive security system that will give you the biggest bang for your buck.

01

SECURITY GUARDS

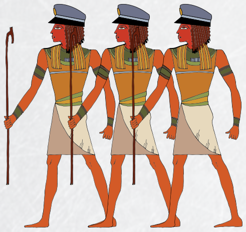
WHERE THEY BEGAN

People have been selling physical protective services in some form since the dawn of civilization—though it was very rarely recorded in official documents recovered by archaeologists and historians. (Ancient peoples had more interesting things to record for posterity, like mammoth hunts.)

However, there are a few early records of people serving as "security guards"—that is, private warriors hired specifically for protection and not otherwise serving formally within a country's military.

1279 BC

ANCIENT EGYPT - *Egyptian Pharaoh Ramses II hired local Shardana as personal bodyguards, to supplement his own personal and national troops.*[1]



24 AD

ANCIENT ROME - *Closer to true police officers than the modern security guard, the Roman regiment of Vigilies Urbani ("Watchmen of the City") was assigned to arrest burglars, maintain order, and track down runaway slaves within the city limits of Rome. Guarding was more of an ancillary duty—they were primarily responsible for putting out fires. The group was also known as Spartoli ("little bucket fellows"), in honor of the tarred wooden buckets full of water they hauled to put out fires.*[2]

905 AD

ANCIENT JAPAN - *Japanese samurai began as humble freelance warriors to the elite upper classes of Japanese nobility, protecting important personages and fighting on behalf of their patrons. Eventually, they seized power as war leaders of powerful clans, but their name reflects their origins. Both the Chinese and Japanese characters that comprise "samurai"/"saburai" translate to "one who waits nearby" as a servant.*[3]

TODAY, security guard firms operate on the same principles they have for thousands of years: train likely candidates and hire them out to clients to guard assets and people until the end of their contract.

THE LOW DOWN

Of all the security options available, this is one of the most straightforward. You find a local security guard firm, and agree to pay them every month in exchange for an agreed-upon number of guards to patrol your property (usually during the night).

Should a criminal be spotted, your guards will either have the authority to confront and physically remove trespassers, or keep watch while contacting the police.

PROS	CONS
✓ A physical, visual deterrent from theft	✗ Not as cost efficient as modern security systems
✓ Can offer fast, on-site resolution	✗ Prone to boredom-related failure
✓ Peace-of-mind assistance for clients/customers	✗ Human element opens possibility of attack
	✗ Guards lack evidence of their encounters

ADVANTAGES

They offer a physical, "human" visual deterrent from theft.

The number-one reason why folks go for a security guard over more "high tech" (and possibly more effective) security options is the comfort of a physical presence on-site.

Any security system will involve advertising its presence on-site to alert criminals that a potential target will be a hard nut to crack. But, the presence of an alert, attentive, and reasonably fit security guard can serve the same purpose.

Should crime occur, a security guard offers on-site resolution.

If a security guard catches sight of a trespasser while on-duty, he or she can approach to resolve the issue.

For common trespassers like teenager hooligans or homeless folks, security guards can offer a stern—yet compassionate—deterrent. For those with more nefarious intentions, the approach of a security guard can be their cue to run.

Security guards can offer visual security and assistance for potential clients.

Security guards provide a unique public relations opportunity for your business as uniformed representatives (or direct employees). Given the right training, security guards can be another weapon in your customer service arsenal. They can be yet another smiling, helpful face to boost the experience of visitors and prospective customers alike.

DISADVANTAGES

Other modern security systems offer the same advantages—without the large retainer, paycheck, or potential liability.

There's very little security guards can do that modern live surveillance systems can't replicate at a fraction of the cost.

Video cameras placed in high-visibility, public areas can provide the same visual deterrent that a security guard does—assuming some proactive additional components like live monitoring—without the same salary requirements that a human presence necessitates.

Also, a physical security presence can mean personal injuries, both to the accused trespasser and to the security guard him- or herself. While most jurisdictions agree that security guards can use a "reasonable amount of force" to control the situation and resolve physical conflict, what would be considered "reasonable" is open to interpretation.

It opens the guard—and the company—to liability for negligence or even assault, on top of whatever workman's compensation the guard may need for injuries sustained during work.

On top of potential assault and battery, employers must also consider the risk for wrongful detention—if a guard holds back someone without cause—and damage to property, either their own or someone else's.[4]

These considerations and possibilities require expensive insurance to mitigate that financial risk and liability in the event of a worst-case-scenario. (Remember—you hire a security firm anticipating worst-case-scenarios.)

Security guards are prone to boredom-related failure.

Security guard protection is inherently passive. You have a few (at best) security guards simply waiting for crime to happen. However, that crime may not happen for hours, days, weeks—even years.

That sort of inactive boredom makes falling asleep incredibly easy to do, no matter the facility under protection. A few years ago, security guards at a United States nuclear power plant were discovered sleeping on the job.[5] You'd assume that a government-run nuclear power plant would have the best of the best guards on staff to protect the plant.

So, that story of a security guard falling asleep mid-shift due to inactive boredom might seem like a stereotypical joke. However, it's a real, widespread problem within the security guard industry that directly impacts the security and safety of client companies and investments.

> [Boredom] is a real, widespread problem within the security guard industry.

Security guards are "only human," making them targets for attack.

People like patterns, and security guards are no different. Untrained guards will commit to the same routines day in, day out—and that creates a huge security risk for the company.

Smart thieves will watch security guards from afar, learning those routines and leveraging them for criminal advantage.

In a small group, a few thieves might learn the guard's routine and steal when they know the guard is patrolling a different area of the facility.

In a larger group—or facing a guard who looks like he or she may offer little resistance—thieves may overwhelm a security guard. The news is rife with stories of guards becoming injured on duty.

Desperate people will do desperate things—including attacking security guards who stand between them and their targets. In these situations, security guards offer not a deterrent, but a liability to the company who employs them (and the building in which they're hurt).

> Security guards may not be able to accurately recount what happened during intense situations, missing critical details that can help authorities track down criminals.

Security guards lack evidence of their encounters.

Should the worst come to pass and an altercation occur, it can be exceptionally difficult to uncover what happened, when, and to whom. In an attempt to save their own hides, criminals may lie to the authorities about what happened—and the security guard will only have their word to gainsay the criminal's account.

Even in a best-case scenario in which everyone is trying to give accurate accounts of a given scenario, stress hormones like adrenaline can interfere with memory retention. Security guards may not be able to accurately recount what happened during intense situations, missing critical details that can help authorities track down criminals.

SECURITY IN THE NEWS

click a link to see more >

Police investigate mall attack

Guard shot at resort in Galveston, TX

Security officer attacked at Metro Station

GBCI guard's career ended due to attack

Security guards can't see the entire site at once.

This last point against using security guards as a primary security solution is a bit obvious, but stands to be repeated. Guards can only be in one place, doing one thing at a time. If crime occurs on multiple parts of the property—or a guard is distracted by something ultimately unimportant while a break-in occurs—then a guard would be unable to stop or delay a crime in progress long enough to summon police officers.

"Eyes in the sky"—or propped on light poles at strategic areas of the property—can cover virtually every inch of a secured area, and continue monitoring no matter what other activity occurs in another part of the property.

> Guards can only be in one place, doing one thing at a time.

THE BIG PICTURE

Security guards have basically existed since the start of human civilization, and for good reason. Properly trained guards can provide an intimidating physical deterrent that more technology-driven solutions can lack. However, if system reliability and recorded evidence are important parts of your security strategy, avoid relying on human guards as your primary security solution.

[1] The Struggle of the Nations: Egypt, Syria and Assyria by Gaston Maspero
[2] The Classic Journal Vol 27, No. 4 "Conflagrations in Ancient Rome" by H. V. Canter
[3] The Lone Samurai: The Life of Miyamoto Musashi by William Scott Wilson
[4] http://southernstatesinsurance.com/3-reasons-your-security-company-insurance-should-include-professional-liability/
[5] https://www.youtube.com/watch?v=x2o0Wh8dVZY

02

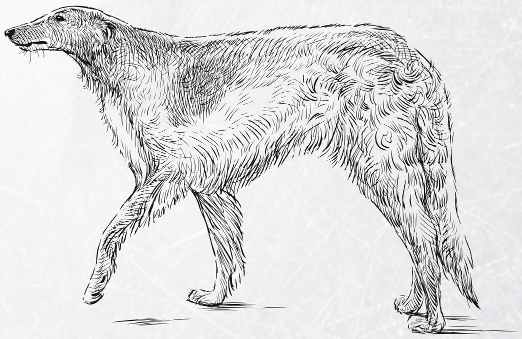
GUARD DOGS

WHERE THEY BEGAN

Man’s best friend was also one of his best protectors. Historian Wolfram von Soden, for example, says that ancient Mesopotamians kept only two breeds of dog: greyhounds for hunting, and extremely large dogs that were “more than a match for the generally smaller wolves and, for that reason, were especially suitable as herd dogs.”[10]

Canines’ instinctively protective nature for their pack were venerated as mystical by these early civilizations. In the ruins of Kalhu (located in modern day Iraq), scholars unearthed clay statuettes of dogs, buried beneath crumbled thresholds to protect the home’s occupants.

At Ninevah, other dog statues were found engraved with inscriptions describing the figurines’ imbued power of protection.[11]



TODAY, guard dogs continue to intimidate and harass would-be thieves with their human security partners.

THE LOW DOWN

See, when you hire guard dogs—proper guard dogs bred and trained to be dangerous to intruders alone, not just a random "guard dog" picked up at the pound—you need to hire their trainers, too. (Assuming you'd rather not take on the enormous expense of purchasing and training the dogs yourself, but we'll talk about that later.)

They'll patrol your property together, just like an ordinary security guard pair. But this duo comes with the secret weapon of a trained snout and sharp teeth to take out any criminal on command.

We don't encourage your rescuing a dog and expecting it to immediately become a suitable guard dog. That's setting you up for disappointment—and possible lawsuits.

If you manage to find a dog with effective protective instincts, then you must ensure that it's trained to turn those guarding instincts off. After all, it'll be difficult for an untrained aggressive dog to separate intruder from customer or employee—and then you're liable for damage done by an aggressive dog on your property.[12]

Therefore, to minimize risk, we recommend partnering with a proper guard dog trainer or an agency that supplies guard dogs—if you decide to get a guard dog for your property.

PROS	CONS
✓ A physical, teeth-filled visual deterrent	✗ Expensive and time consuming
✓ Durable and able to navigate tough terrain	✗ Animals can be unpredictable
	✗ Short window of service, lifespan

ADVANTAGES

They offer a physical—and teeth-filled—deterrent from theft.

The primary reason to hire guard dogs is to supply the same physical-presence deterrent that human security guards do.

However, they're equipped with much better senses than your average guard. That makes them better at sniffing out intruders, hearing out-of-place sounds, and intimidating the pants off a would-be criminal. (Seriously—those teeth are not for show!)

They are more durable over a more rugged area of terrain.

Depending on the type of environment your property covers and the chosen breed, guard dogs may be more suited than human guards to ranging over a wide area of land on patrol. Their paws and claws give them traction in rough areas, while their coats insulate them from the elements. (No whining that it's raining here!)

DISADVANTAGES

They're incredibly expensive in time and money, upfront and over the long run.

To ensure that the guard dogs are a menace only to criminals and not the public at large, they require extensive, exhaustive training and impeccable breeding lines.

You'll pay for that quality through the nose. Quality guard dogs can cost $50,000 or more when bought outright.[13] Training a hopeful pup into a guard dog can run anywhere from $15,000 to $35,000.[14]

That doesn't include continued training, medical expenses, and random purchases bought throughout the dog's 10+ year lifespan.

Plus, they're living creatures. They'll require someone's time, love, and attention to feel close to their family, further cementing their bonds. If you're not prepared to incorporate new furry family members into your home, then purchasing guard dogs isn't a great idea for your business.

> Dogs and their handlers can still cost thousands more than other security options

If that time and money cost is too much to stomach, you can rent—but that'll cost you, too. Dogs and their handlers can still cost thousands more than other security options every year.

Guard dogs can be incredibly expensive:

$50k+	$15k+
TRAINED, ADULT DOG	TRAINING YOUR OWN

They're animals, no matter how well-trained they might be.

Dogs are, well, dogs. They can be highly trained and trusted to do amazing things, but at the end of the day, they're still driven by instinct. Trainers and business owners alike benefit from those instincts when training for guard duty, but they can still, uh, bite you. (Excuse the pun—we couldn't help it.)

Take your property, for example. You may try to leave guard dogs unattended, but if the dogs are improperly trained—or simply distracted—they could wander off the property altogether, not performing the job for which it was trained or hired.

And what happens if your guard dog bites an innocent bystander through instinctual aggression or terror? If it's your dog, you'll most likely be liable for damages—and possibly have to put the dog down, if you live in a "one-bite" state.[15] If you're renting the dog's services, but the bite happens on your property… well, you're probably liable then, too.

Guard dogs are only useful for a limited number of years.

Say you choose to purchase a guard dog outright for your property. From a strictly financial sense, it's a depreciating asset. Guard dogs don't get better with age. And, eventually, they'll pass away, taking your entire investment with them.

Typically, service dogs retire when they're no longer capable of serving, which could mean years of guard duty before they're done. But, considering most dogs aren't ready for proper "work" until age two—and most retire at 10 years of age—you'll probably get a max of eight years of actual guarding from your dog.[16]

THE BIG PICTURE

Man's best friend also strives to be his best crime deterrent. However, guard dogs are terribly expensive—in terms of training and potential liability—for the potential security they provide, making them one of the least valued and recommended options for ongoing commercial security.

[10] Einführung in Die Altorientalistik. Anglais by Wolfram von Soden
[11] "Nimrud: Materialities of Assyrian Knowledge Production" by the Open Richly Annotated Cuneiform Corpus
[12] http://www.nolo.com/legal-encyclopedia/dog-bite-statutes.html
[13] http://www.simanovich.com/protection-dog-pricing/
[14] http://www.protectiondogsplus.com/our-training-services/pricing/
[15] https://dogbitelaw.com/legal-rights-of-dog-bite-victims-in-usa/one-bite-states-and-mixed-dog-bite-statute-states
[16] http://www.canineassistants.org/faq.html

03

CLOSED CIRCUIT TELEVISION (CCTV)

WHERE IT BEGAN

Commercial video monitoring as we know it wasn't possible until the 20th century. Actually, it wasn't until the 1970s—when VCR technology allowed video reels to be recorded and erased for repeated use—that commercial businesses began to use closed-circuit television (CCTV) systems with any regularity.[17]

Its popularity boomed in the 1990s, when advances in recording technology let several cameras record on the same channel, at the same time. The innovation saved money and time for folks trying to watch the video feeds, which encouraged adoption.[18]

TODAY, CCTV systems are used in some capacity on most business properties—from convenience stores and retail shops, to financial institutions like banks and credit unions.

THE LOW DOWN

Today's CCTV systems no longer require the VCR tapes of the past. Unless set on a timer, they'll constant record in the direction they're pointed. The video is either stored within the camera memory, or transmitted via the Internet to an online storage file of some kind. (This type of storage is what people call "on the cloud.")

Sometimes CCTV cameras are set up for live viewing only. That is, they don't put the memory within storage, and someone must watch the cameras' live feed constantly for incidents to happen. Think of that set up as something like a traditional baby monitor. The speakers don't store the audio, but rather constantly broadcast in case the infant cries in distress.

CCTV systems can come in all-in-one DIY packages for business owners to install themselves. Or, businesses may opt to have their cameras selected and installed by professionals.

PROS	CONS
✓ Always on, always recording	✗ Can't actively stop a crime
✓ DIY kits available for many applications	✗ DIY kits aren't perfect for every location
	✗ Prone to failure or even hacking
	✗ Subject to privacy laws

ADVANTAGES

CCTV systems record what happens at your business, all the time.

There's nothing more valuable to a criminal police investigation than video footage of the crime—unless it's a confession, of course.

Video surveillance of any kind offers impartial, recorded evidence useful for determining exactly what happened, when. There's no way to distract them, no possibility of sleeping on the job.

CCTV DIY kits now exist for business owners to install themselves.

While we think there are significant disadvantages to do-it-yourself'ing your security plan, its upfront cost reduction and immediacy can't be overlooked.

Upfront, self-serve CCTV cameras are less expensive than their professionally installed alternatives. They take less time to set up, too, without having to wait for contractors to add your project to their schedule.

DISADVANTAGES

CCTV cameras do nothing to actually stop or deter crime.

At best, CCTV cameras are passive witnesses to crime as it occurs. Unmonitored CCTV cameras have no way of processing what's actually happening in the footage. They raise no alarms, and they can't contact the authorities if crime's taking place.

You'll get to watch an incident unfold retrospectively, unable to stop it in real time.

Several cities have experimented with security cameras as a crime deterrent in public and commercial areas, and have found that there was no reduction in crime after installation. (See "Chicago Case Study: CCTV vs Live Surveillance" on pg. 25)

Kit CCTV systems are "one size fits all" — and can't accommodate every business's unique security needs.

Manufacturers of do-it-yourself CCTV security systems try to accommodate the broadest number of customer needs. They make a large set of assumptions to create something that will help the largest number of people with the least amount of tweaking.

In doing so, they limit how well a given system will work, based a business property's unique security needs.

These kit CCTV systems won't account for you business's lighting needs, for instance. The cameras will all assume a certain level of light to enable them to record—what happens if you need to record in a particularly dark area?

> At best, CCTV cameras are passive witnesses to crime as it occurs.

That's not even thinking about your property's ability to supply power to the cameras, your Internet capabilities, your landscaping and architecture. All of these things require thought and attention when designing a video camera surveillance system that will actually record what it's supposed to.

CCTV systems are prone to failure due to incorrect installation, camera selection, and external hacking.

Effective video camera placement is exceptionally difficult for the layperson to implement, not to mention the selection of appropriate hardware.

For example, you may opt for a "better" camera that can record up to 400 feet away. But, that camera leaves your property vulnerable at closer ranges, failing to record the first 150 feet or so. Those long-range cameras should be paired with shorter range cameras to ensure full coverage.

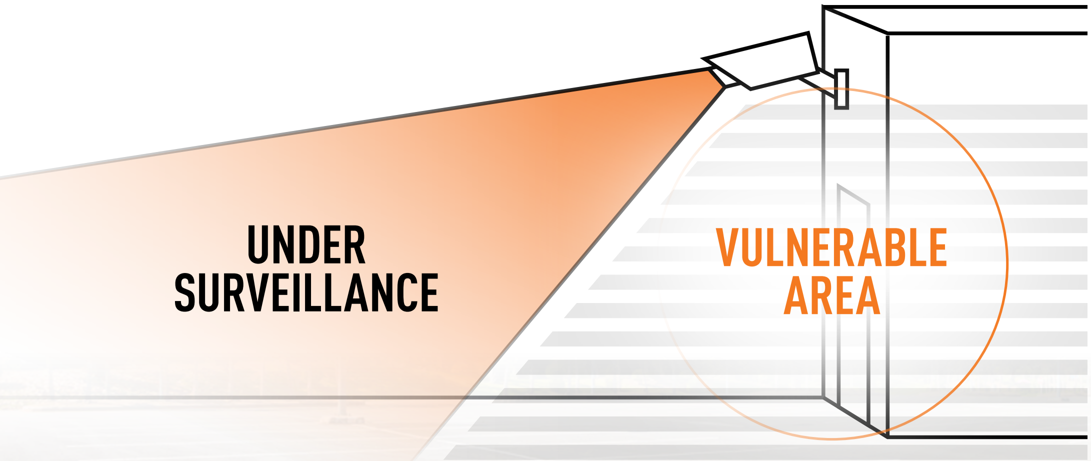
And when should you opt for a crystal-clear image quality over a less-expensive but slightly less clear image? What about infrared—should those be installed everywhere, or just in certain spots?

Then, there's the installation itself. Have you correctly connected the camera to the CCTV network? Will it shake in a windstorm or other environmental situation? Is there sufficient power available to make the cameras work? These questions all must be addressed if a video surveillance system will work as advertised, and not just be a drain on your time and resources.

Finally, CCTV systems that aren't installed properly or constantly monitored lay exposed to computer hackers looking to exploit vulnerabilities within the camera's software.

In March 2017, a devastatingly simple security loophole was discovered within the firmware of the most popular security camera models, including Dahua and Hikvision. Unscrupulous hackers could access the user authentication screen and "pass the hash" to force the camera's system to admit the hacker—thereby granting access to all the security cameras on the user's system.[19]

Ensuring that Internet-capable cameras are insulated from hackers requires a sophisticated installation process that uses absolutely no "factory preset" options and constant updates. Even after the 2017 camera hijacking, most CCTV cameras remain vulnerable to this and similar attacks.



Long view cameras leave your property vulnerable at closer ranges, failing to record the first 150 feet or so.

DIY'd CCTV might run into privacy laws and regulations.

Should you choose to run a CCTV recording system on your property, you may run afoul of privacy and consent laws in your state.

Even though it's your own personal property, who can record whom—and whether the recorder needs to obtain the recordee's consent—can quickly land you in hot legal water. It won't matter if the person being recorded is doing something wrong, if you illegally recorded them without permission.

THE BIG PICTURE

If all you want out of your security system is a way to review exactly what happened post-incident, then a CCTV video camera setup is all you need. If you want to actually stop theft from happening—instead of letting the police chase them down and maybe recover your property—then you've got to step up your security game.

[17] CCTV Surveillance: Video Practices and Technology by Herman Kruegle
[18] "The History of Video Surveillance – from VCRs to Eyes in the Sky" by Lucy P. Roberts
[19] https://krebsonsecurity.com/2017/03/dahua-hikvision-iot-devices-under-siege/

04

INTERACTIVE VIDEO MONITORING

WHERE IT BEGAN

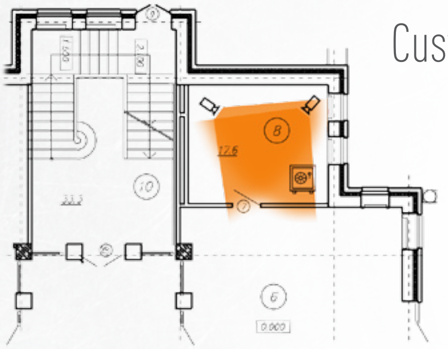
Interactive video monitoring is the next generation of the traditional CCTV camera surveillance systems. Some CCTV systems manage live surveillance through security guards constantly watching its screens. However, interactive video monitoring means that the monitoring of the systems happens offsite at a professional security provider's command center.

Frankly, interactive video monitoring systems are lightyears beyond where commercial CCTV started over three decades ago. Allowing for live interaction and mid-crime arrests, this modern security system allows for proactive security measures that grant you—and your employees—peace of mind and active criminal deterrence.

THE LOW DOWN

Eyewitness Surveillance installs thousands of cameras and speakers every year for live remote video monitoring, so we think we know the process pretty well. Here’s what a business owner can expect from a reputable provider of interactive video monitoring security solutions—like us!

A professional security provider reviews the property in person with the business owners. This way, the service provider can assess known weak points, and evaluate resources already on-site like electrical sources and Internet bandwidth.



Custom Camera Placement Strategy

From there, the security company develops a custom camera placement strategy to maximize coverage with the fewest number of cameras. If extra lighting or specialized power sources are needed to sustain the cameras, these recommendations are made and approved by the owners before installation. Eyewitness also installs speakers that sync with specific camera—an important part of our crime deterrence strategy.

Once the appropriate hardware is in place, analytics software “filters” the footage that’s recorded and transmitted to the remote surveillance facility. While all video footage is recorded in its entirety, these filters allow the cameras to ignore events that aren’t important—like the headlights of a car off the property—while simultaneously alerting security staff to possible intruders on property.

Modern live video surveillance systems require highly trained security personnel to understand the various alarms and alerts that funnel into the remote surveillance facility. These security professionals sort through the chaff of hundreds of “false alarms” a night to ensure that when a true intruder appears on your company’s property, they can respond immediately.

When cameras alert on suspicious activity, a monitoring security professional consults the company’s unique site map to verify that individuals should not be in a specific area. Security personnel then make a live announcement through speakers on the property to alert the intruders that the property is being monitored and videotaped. Often, that announcement is enough to scare away criminals who didn’t count on someone being awake and aware of their presence on the property.

Alert intruders they are being watched with on-site audio

If a trespasser decides not to heed the live warning—or the situation requires immediate intervention—the remote surveillance facility calls the local police dispatch and alerts them to the confirmed criminal activity occurring in real time.

Staff continue warning the suspects while marking the footage for later retrieval and even run license plate numbers when available. The security professionals then guide the police to the appropriate location, apprising dispatch to changes in the situation as appropriate.

PROS	CONS
✓ Includes advantages of every system	✗ Greater up-front cost compared to other systems
✓ Can stop theft while it's happening	✗ Properly installed systems take time to put in place
✓ Saves money by increasing operational efficiency	✗ Does not offer the same on-site visual deterrents as guards
✓ Professionals can install cameras exactly where they need to be	✗ Poorly executed systems can't identify false alarms
✓ Faster police response	
✓ Removes cost and liability risk of traditional guards	

ADVANTAGES

As an evolution of CCTV security systems, interactive video monitoring incorporates all the advantages of a traditional recording system.

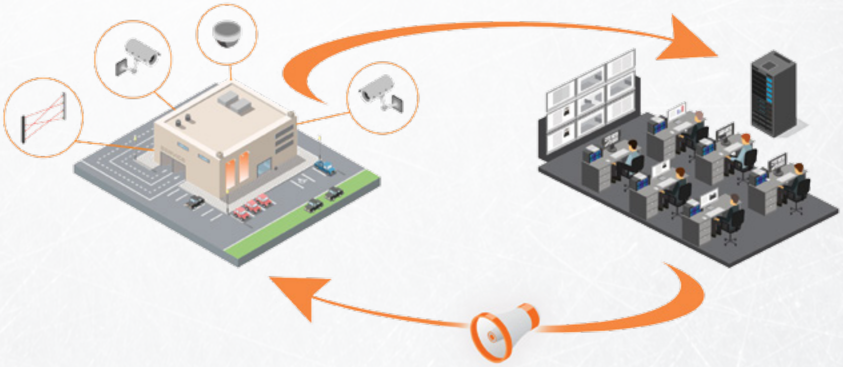
The advantages of installing a CCTV system—the clear footage of criminal activity to help police solve crimes, its comparatively inexpensive cost compared to hiring traditional security guards—are still present in a interactive video monitoring system.

Plus, Eyewitness Surveillance clients enjoy 30-days of video storage available for retrieval should they or the police need clips of a particular incident. While our video monitoring software (VMS) allows clients to inspect footage whenever they want, we'll also retrieve it for them at no additional cost.

Interactive video monitoring removes the cost and liability risk of traditional security guards.

Interactive video monitoring like Eyewitness's doesn't need a person on-site to be effective. The live interaction via speakers and the police's arrival at the scene of the crime remove the need for physical security.

Plus, there's no risk of a physical or fatal altercation, since the security professional monitoring the site is safe in a remote surveillance facility!



Live video surveillance actually stops theft from occurring in the first place, saving users money in reduced loss and damages.

What's better than having clear evidence of a crime? Stopping crime from happening at all! Live video surveillance can do that.

We'll go into more detail when talking about a case study in Chicago that used both passive CCTV video cameras and live video surveillance in two similar parks. (See "Chicago Case Study: CCTV vs Live Surveillance" on pg 25).

For now, we'll spoil the ending of the case study: Live video surveillance won hands down when it came to reducing theft. Thanks to the savings in police hours and reduced theft, the live video surveillance paid for itself and the (comparatively ineffective) CCTV systems.

The trend carries through at the national level, from what we've observed at our client locations. About 70% of would-be thieves flee when they hear our security professionals warning them through the synced speakers.

Effective live video surveillance saves users additional money when used for increased operational efficiencies.

We see clients take advantage of their surveillance system in other ways, too. For example, we help automotive dealerships use their constantly monitoring cameras to avoid daytime losses like workman's compensation and false customer claims.

One dealership client told us that he installed the cameras, just thinking they'd help him stop inventory loss. Instead, the cameras revealed that one employee pocketed $10,000 cash from a customer that otherwise would've been impossible to know about.

Ultimately, he and three other employees were fired for misconduct and theft, thanks to the evidence of the well-installed surveillance cameras.

Speaking of which…

Professional security companies know exactly which cameras are required, where—and can install them correctly.

Effectiveness, value, and efficiency are crucial to every commercial security systems. While professional installation and monitoring may require more of an initial investment than your average CCTV system, they'll pay back their costs in time saved and expertise earned.

Professional security providers understand which cameras and other security systems commercial properties need, having done installations on comparable sites. They can offer recommendations and custom options unavailable elsewhere—and they usually have access to higher caliber technology than the average self-starter.

Plus, it's the security provider's responsibility to ensure everything is in working order. You won't need to do any maintenance or supervision to keep your security system up-and-running.

Video surveillance leads to faster police response times—and ensures they'll dispatch at all.

According to Community-Oriented Policing Services (COPS), the United States' national rate of false alarms is 94-98%. These false alarms cost taxpayers $1.8 billion annually in wasted police time and resources.

To reduce the police resources wasted on false alarms, municipalities are instituting new regulations that impose fines on business owners responsible for repeated false alarm. Some go so far as to forbid dispatch to release police officers to a crime scene unless the alarm has been verified as an actual crime.

Live video surveillance requires professional security staff to visually affirm a crime in progress before dispatching police to a client site. This avoids any false alarm penalty for the business owner.

Plus, security staff stay on the phone with police dispatch, updating them as the situation unfolds and guiding police to the specific area where crime is taking place. (Otherwise, police can and do wander aimlessly around a large business property, giving criminals enough time to make their escape.)

DISADVANTAGES

Interactive video monitoring systems (usually) require a greater upfront cost than CCTV.

Professional grade, comprehensive security systems like live remove video surveillance will cost more than your out-of-the-box CCTV security—at first. (It'll still be less expensive than 24/7 security guards or guard dogs would be.)

Ultimately, the system will pay for itself in prevented crime and operational efficiency boosts, but it does require a company to invest in its security system.

Interactive video monitoring systems—properly installed—will take longer to start than other security options.

Anything done well takes time—and the same is true for any professionally installed security system. Impatient businesses might try to install cameras themselves or hire security guards for immediate "protection," rather than wait for professionals to finish the job.

However, as opposed to trying to hack it with a DIY kit, a well-installed security system shouldn't require constant adjustments and security-breaking malfunctions.

Most interactive video monitoring systems will not have on-site deterrence capability.

Professional security guards and guard dogs are frightfully intimidating to on-site thieves and vandals. Most camera systems can't make burglars stop mid-theft, as physical security might be able to.

Eyewitness gets around this problem with its synced speaker system and live security professional warnings, with no liability concerns that a security guard represents during physical altercations. However, it's a limitation worth considering when evaluating various live remote monitoring solutions.

Clumsy live video surveillance security plans will not differentiate between lawful presences and active intrusions.

Effective interactive video monitoring relies on cooperation between the security provider and the client business, to determine who is allowed on which parts of the property, when.

Surveillance must begin with a comprehensive schedule of vendors, employees, and operating hours matched with an up-to-date site map. If the client company plans any changes to that set operating procedure—a late night at work, or their cleaners change their usual schedule—they must communicate those adjustments with their security partners.

That way, security professionals can report true intruders to the police, rather than an employee working after-hours.

THE BIG PICTURE

There's a reason Eyewitness Surveillance offers live video monitoring services, not guard services. Live remote monitoring gives clients the advantage of recorded video plus proactive security measures to stop theft before it happens. It does require a greater investment from businesses upfront, however, so it's not for those who aren't dedicated to reducing theft.

[17] CCTV Surveillance: Video Practices and Technology by Herman Kruegle
[18] "The History of Video Surveillance – from VCRs to Eyes in the Sky" by Lucy P. Roberts
[19] https://krebsonsecurity.com/2017/03/dahua-hikvision-iot-devices-under-siege/

CHICAGO CASE STUDY:

CCTV VS LIVE SURVEILLANCE

BACK IN AUGUST 2003, Chicago police placed security cameras in two neighboring parks—**Humboldt Park** and **West Garfield Park**—to see if they would reduce crime in the area. They installed the cameras in highly visible places (complete with flashing blue lights!) to make sure that everyone knew the cameras were in place.

WEST GARFIELD PARK - CCTV cameras in the park failed to reduce crime rates at all, even though residents knew the cameras were turned on and recording. When researchers tried to figure out why the cameras didn't deter crime, they discovered that residents didn't believe the cameras were actively being watched by police—and so crime continued unabated.

HUMBOLDT PARK - Unlike neighboring West Garfield Park, where crime rates remained virtually unchanged, Humboldt Park's violent crime rate reduced by 20%. Monthly counts of drug-related offenses and robberies fell by almost a third.

When the researchers dug into possible reasons for the reduction, it turns out that residents of Humboldt Park thought their cameras were being monitored by police. That belief resulted in reduced crime where the cameras really were "watching" potential criminals' every movement.

Not only did crime reduce significantly in Humboldt Park, but the cameras also drastically reduced police costs. Researchers found that Chicago saved $4.30 for every dollar it had spent on installing cameras, just from the number of crimes the Humboldt Park cameras had prevented. (This number even includes the expense of the ineffective CCTV cameras in West Garfield Park!)

Ultimately, the report concluded that "the cameras—when actively monitored—were effective at cutting down crime. And the savings and benefits of fewer crimes outweighed the cost of the surveillance system."

20%
REDUCTION
IN CRIME

$4.30
SAVED FOR EVERY
$1.00
SPENT

05

KEYLESS ACCESS CONTROL

WHERE IT BEGAN

When you consider the history of keyless security measures, you should really begin with the history of physical keys and locks. (After all, you can't go keyless unless you start with a key.)

When we think of a lock-and-key system, the type most of us think of first—the pin tumbler lock—is actually based on an ancient Assyrian design.

A lock contains a large bolt running through the keyhole to secure the lock in place. Special pins of various lengths rest inside drilled holes in the bolt, preventing its movement.[22] When the owner inserts the matching key, the key lifts the pins from the bolt. Finally released, the bolt can draw back and allow the lock to open. Today's pin tumbler locks now use a flat, serrated key that probably looks a lot like the house key you had growing up.[23]

But those keys are ancient history—literally. As computers began to grease the wheels of everyday commerce and society in the 1960s, a need for equally convenient access grew that didn't rely on the pin tumbler method.

The first automatic teller machine (ATM)—built in 1967—used a personal identification number (PIN) that matched a submitted check to check for authenticity, becoming one of the first public examples of "keyless" access control. Five years later in 1972, another bank issued the first magnetic strip banking card, also with a matching PIN for enhanced security.[24]

These PINs became the backbone for modern keypad security system authentication. But keycodes can be clumsy, and lack additional security measures.

So, many organizations have traded manufactured metal keys for the more economical card or fob. These devices overwhelmingly operate on RFID technology, or Radio Frequency Identification. Originally developed during World War II to identify friend airplanes, modern day keyless entry cards project tiny radio-frequency magnetic fields into the surrounding area.[25]

THE LOW DOWN

Modern keyless access control systems use that RFID technology in cards, fobs, and a variety of other sensors to send a radio signal to the lock mechanism inside a door or secured container. A base reader is always “listening” for these frequencies. If it picks up a frequency it knows, the reader initiates a set protocol—anything from opening a door, to triggering a request for secondary authentication (like a user-specific PIN).

Keyless access control systems can be programmed to do many things to better secure your building, including automatically lock all doors from outside intruders in the event of a lockdown situation.

However, fire codes prohibit any doors from keeping people inside from leaving the building. So, intruders can’t get in, but staff and customers inside the building can still leave it in the event of an emergency.

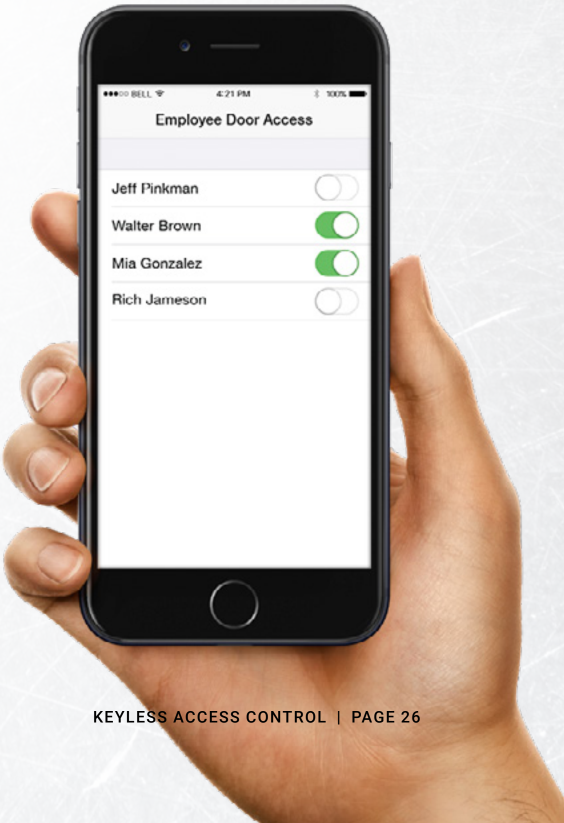
PROS	CONS
✓ Safer than traditional lock-and-key method	✗ Requires specialized installation and ongoing service expenses
✓ Can save thousands in key replacements	✗ Unauthorized entry alerts are not considered a “verified” alarm to police
✓ Simplifies security audits and user permissions	✗ Can be neutralized by bad employee habits like “piggyback”

ADVANTAGES

Keyless access control keeps your buildings safer than traditional lock-and-key installations.

Easily, one of the biggest advantages to a keyless entry system is its increased security capabilities compared to regular key and tumbler-locks available on most buildings.

If employees lose their cards or fobs, they can be deactivated with a few clicks on a computer. Anyone picking up a misplaced card or fob will find themselves unable to use it to trespass. And, would-be thieves can’t drop off a “key” at the local hardware store to make an illegal copy.



Employee Door Access

Jeff Pinkman ○
Walter Brown ●
Mia Gonzalez ●
Rich Jameson ○

Keyless access control saves businesses thousands in key replacement costs.

Companies with large numbers of employees and high turnover rates know the struggle of tracking every (known) copy of various building keys. Once a key is missing for 72 hours, the company must pay to replace the lock and its corresponding keys, redistributing the keys to appropriate parties.

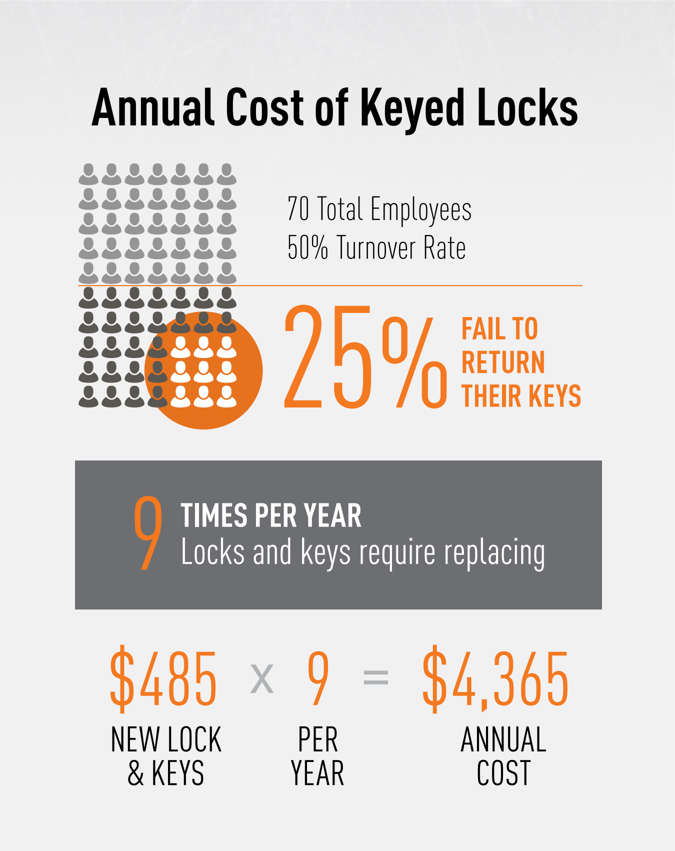
Otherwise, the building remains compromised, waiting for that missing key to reappear in the hands of someone who means the business harm.

Let's say that a company has 70 employees at any given time. The company has a turnover rate of 50%, meaning that 35 employees leave (for whatever reason) and new folks are hired to replace them. Perhaps 25% of those employees will fail to return a key to the business on their departure, either accidentally or maliciously.

Now, that's about 9 times a year that locks and keys will need to be replaced to maintain the building's security. A commercial door lock costs about $135 every time a professional locksmith must replace it, and new keys must be made for every employee (70) who requires access at maybe $5 apiece.

In all, our business will spend around $4,300 annually just to replace locks and keys every time someone either loses or "forgets" to return a key. Over five years, that's more than $20,000 in key and lock maintenance costs. (If an employee fails to return more than one key at a time, these costs easily double and triple.)

With a keyless access control system, replacing the lock and key isn't necessary. Just reprogram a new fob or card and deactivate the old one whenever it goes missing.



Annual Cost of Keyed Locks

70 Total Employees
50% Turnover Rate

25% FAIL TO RETURN THEIR KEYS

9 TIMES PER YEAR
Locks and keys require replacing

$485 x 9 = $4,365

NEW LOCK & KEYS | PER YEAR | ANNUAL COST

Keyless access control makes security audits and individual user permissions simple.

Computerized keyless access control systems automatically know who uses their fob at which door and at what time. It's easy for administrators to audit the records and see if any unauthorized entries were attempted at sensitive areas.

Plus, the keyless management system lets administrators adjust permissions at an individual user level. One card or fob can open as many (or as few) doors as that employee needs to access during the regular course of their day. No more multiple keys for them to use and fumble with!

Access can be "scheduled" at the user level, too. For regular staff, they might only need access to the main building during regular business hours. Their keys can then be denied access when the business is closed—preventing unauthorized entry later.

DISADVANTAGES

Keyless access control systems require specialized installation and ongoing service expenses.

Your average locksmith won't be able to wire together the specialized pieces of hardware that make up an effective access control system. So, you'll need to partner with a professional security provider to install your access control system.

Also unlike regular key-and-lock configurations, you'll need to pay an outside professional company every month for service and upkeep. Compared to the costs of replacing locks and keys every time you lose something, though, the value of a keyless entry system outweighs the cost of the traditional locking mechanisms.

Alerts of unauthorized entry from a keyless access control alone do not constitute a "verified" alarm for police dispatch.

Earlier, we discussed the prevalence of false alarms and how police departments are cutting back their responses to automated security system alerts that aren't somehow "verified" as an actual crime.

While your access control system can (and should!) send you alerts whenever someone tries to enter an area they shouldn't, that alert isn't necessarily "actionable" by the authorities unless it's verified by a second source. In that way, the system and its auditable records of attempted user access are more of a passive security system like CCTV, rather than a proactive one.

However, integrating a video surveillance system to watch doorways where access points are installed is a great way to verify unauthorized access alarms by keyless control systems, if you're interested in using your access system as a quasi-burglar alarm.

"Piggybacking" and other unsafe employee habits may counter the system's ability to secure the building.

Whether it's a regular lock-and-key system or access control, bad employee habits often find ways to counter the latest security innovations.

They might let other people into the building without making them use a card or fob to unlock the door themselves, a process known as "piggybacking." They might prop a door open with a rock, so they don't have to carry their card or fob out during a smoke break. Or, they might loan their card or fob to a coworker who "forgot" theirs at home—thereby labeling all of their entries as someone else's within the system.

These habits are insidious and effectively negate a proper security system. Proper employee training must be enforced if this—or any!—security program is to effectively protect them and the property.

THE BIG PICTURE

Keyless access control systems provide unbeatable protection for companies worried about unauthorized access to sensitive areas. However, they're not a comprehensive security solution, and work best in concert with other, more active security measures.

[22] International Symposium on History of Machines and Mechanisms, edited by Marco Ceccarelli

[23] A Dissertation on Locks and Lockpicking: Showing the Advantages Attending the Use of the Magic Infallible Bank Lock by Linus Yale, Jr. & Co

[24] Strategies of Competition in the Bank Card Business: Innovation Management in a Complex Economic Environment by Jarunee Wonglimpiyarat

[25] "Introduction to the RFID" by the French National AFID Center

06

INTRUSION SYSTEMS

(BURGLAR ALARMS)

WHERE IT BEGAN

Modern electric burglar alarms owe their popularity to the American businessman Edwin Holmes. The original electromagnetic alarm design and patent was made by the obscure Reverend Augustus Russell Pope, but he sold it to Holmes in 1857 for $1,500. In today's currency, that's $40,451.96!

Holmes then tried to sell the alarm to Bostonians, but they weren't having it. So, he decided to move to New York City, telling his son that it was a place where "all the country's burglars made their home."

(By the way, if you're looking for a good read on New York City crime during the 1800s, try *The Gangs of New York: An Informal History of the Underworld*. It's a smashingly well researched and fun history originally written in 1928 by Herbert Asbury.)

Thanks to the gangs of thugs roaming New York's streets, Holmes did indeed have much better luck selling his alarm systems in NYC. He and his son, Edwin Thomas, figured out how to use the newly lain telephone cables to facilitate massive alarm networks that could relay messages back to a central monitoring station—a model which security companies (like Eyewitness Surveillance!) still use to this day.

THE LOW DOWN

Intrusion systems vary wildly, depending on what you install and what your business's specific needs are. However, they all follow three basic steps: Detection, verification, and notification.

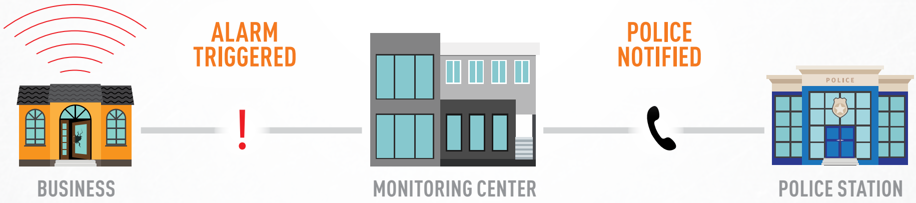
Alarm systems have a variety of sensors and circuits installed within their hardware to monitor the conditions of its installed environment. Usually, the environment doesn't change when the alarm system is "armed"—or active—and so it doesn't alarm. It's only when a sensor detects some sort of shift in the area that it begins the alarm process.

When it detects an intrusion, the sensor notifies a central control panel, which begins the verification process. (Remember those "false alarm" statistics? This is the system's effort to keep those to a minimum.)

So, the alarm system must verify that a sensor's alarm is truly triggering on a crime, and not just a keyholder who forgot to cancel an alarm. Excellent alarm systems will follow a customized, multi-step process to have a human—either a keyholder or the security monitoring center—verify that the sensors' alarms are triggering on crime, not owners.

Once the burglar alarm system verifies that an alarm indicates a crime-in-progress—or multiple attempts to further verify the alarm are unsuccessful—the monitoring center then calls local authorities. Depending on the jurisdiction, the authorities will request verification before sending patrol units to the scene, which the monitoring center should be able to supply on request.

An open alarm ends when the authorities and system keyholders arrive on the scene to address the break-in with minimal loss and property damage. The alarm system's logs also provide additional evidence to the authorities, should charges be pressed against the would-be burglar.



PROS	CONS
✓ An automatic deterrent to thieves	✗ Ongoing expense rather than one up-front cost
✓ Potential insurance cost breaks	✗ DIY systems are still vulnerable
✓ Can monitor more than just access	✗ Can be turned off or ignored
✓ Adds extra support to other systems	✗ May cause false-alarms

ADVANTAGES

Intrusion systems provide an effective and automatic deterrent to would-be thieves.

A research team at the University at North Carolina interviewed 422 incarcerated burglars of both genders in North Carolina, Kentucky, and Ohio prisons to ask about their decision-making processes and methods.

According to the study's results, most burglars said that the presence of security systems affected their decision whether to go ahead with an intended heist. 60% of interviewed burglars said they would seek another target if they realized the property was protected by an intrusion alarm system.

If they heard an alarm activate mid-theft, about half of respondents said they would discontinue the attempt. (Only 13% said they would always continue with the theft, even after an alarm sounded.)

Eyewitness Surveillance's 2017 survey *Where Americans Don't Lock Their Doors* reiterates this finding, discovering that homes without any security or alarm systems are up to 300% more likely to be broken into.

MORE LIKELY TO BE BURGLARIZED
WITH NO SECURITY SYSTEMS

Many insurance companies offer breaks on premiums and deductibles when businesses install security systems—including intrusion systems.

Just like owning a fire extinguisher usually lowers your home owner's insurance, installing and maintaining an active intrusion system can lower your business's insurance premiums and deductibles.

> An active intrusion system can lower your business's insurance premiums

While this advantage isn't specific to intrusion systems, it is one of the more "automatic" security measures you can take to lower your insurance payments.

Intrusion systems can monitor more than just unauthorized access.

Depending on the provider and your state's laws, intrusion systems can include specialized sensors that trigger on fire, carbon monoxide, temperature, flooding, and more.

Really, just about anything you can think to measure or watch, customized and professionally installed intrusion systems can monitor.

Intrusion systems add extra support with other integrated security measures.

Whether you've got a security team on-site or interactive video monitoring, intrusion systems are a great way to ensure that no corner of your property is overlooked. The alarms trigger under a very specific set of environmental conditions. The blaring alarm gives your human security monitors reason to investigate that specific area immediately.

DISADVANTAGES

Intrusion systems are an ongoing expense, rather than a one-time charge.

Whether you install a DIY intrusion kit or bring in a professional security company, intrusion systems require constant maintenance and supervision. A monthly fee is usually charged for professional monitoring services.

Even if you choose to personally monitor your intrusion system, that false alarm rate goes up. You'll pay hundreds in false alarm penalty fees, on top of the intrusion system permitting expense.

(Of course, the only really "free" security option is going for nothing—and we've seen how well that works for companies who choose to play dice with Lady Luck.)

DIY intrusion systems are vulnerable to "Crash and Smash" crime.

A "crash and smash" happens when a burglar *crashes* into a building and *smashes* the alarm's control panel to prevent the alarm signal reaching the system's owners. While some manufacturers have made significant strides in this area, it's still a significant risk to consider if you've got an all-in-one alarm keypad and control panel within easy reach.

Most DIY security systems are intentionally crippled by their users.

While this is true of most technology-based security systems, it's especially prevalent for those who choose to monitor their own intrusion systems.

System owners quickly tire of false alarms triggered by moving shadows or an employee staying late at the shop. So, they'll turn off the alerts and ignore notifications whenever something happens—including those times when a burglar really is breaking into the building.

What is the point of a security system with its alarms turned off?

Unmonitored intrusion systems that alert on every sensor alarm—without secondary verification—rack up false alarm fees and slows police response times.

It's a classic case of "Boy Who Cried Wolf." If your security system continuously "cries wolf" (and the police) every time a shadow moves without taking the time to verify the potential crime, then the police will start ignoring your system's cries for help—and charge you for their inconvenience.

That's why intrusion systems are often a great part of an overall security system that can verify whether a crime is occurring, rather than as a standalone "all in one" security solution.

THE BIG PICTURE

Intrusion detection systems provide both passive security protection, as well as actively deterring criminals. However, its high levels of false alarms—as well as unintentional crippling by well-intentioned users—make an intrusion systems tricky for DIY management solutions. Like access control systems, we'd recommend pairing a solid burglar alarm system with another security measure for additional protection.

[22] International Symposium on History of Machines and Mechanisms, edited by Marco Ceccarelli

[23] A Dissertation on Locks and Lockpicking: Showing the Advantages Attending the Use of the Magic Infallible Bank Lock by Linus Yale, Jr. & Co

[24] Strategies of Competition in the Bank Card Business: Innovation Management in a Complex Economic Environment by Jarunee Wonglimpiyarat

[25] "Introduction to the RFID" by the French National AFID Center

TABLE COMPARISON

ALL SYSTEMS

WE BELIEVE that any security option would be better than not having any security program at all. (Even if you've got to make do with a particularly angsty parrot!)

Still, based on the features of modern security systems, there are some clear winners that will give you the best return on your investment. Here's our official breakdown of security systems, taking into account both startup and ongoing expenses; the effectiveness of the system in deterring, stopping, and reporting on crime; effectiveness of "do it yourself" options; liability risk to the system owner; and whether the security system could be used for things other than strict theft and vandalism prevention.

	SECURITY GUARDS	GUARD DOGS	PASSIVE CCTV	INTERACTIVE VIDEO MONITORING	ACCESS CONTROL	INTRUSION ALARMS
Lowest Upfront Cost	●●●●	●○○○	●●◐○	●●◐○ *	●●○○	●○○○
Lowest Ongoing Expense	●○○○	●○○○	●●●○	●●○○	●●●○	●●●○
Effectiveness at Deterring Crime	●●○○	●●●●	●○○○	●●●◐	●○○○	●●●○
Effectiveness at Stopping Crime	●●○○	●○○○	●●○○	●●●◐	●●●○	●●●○
Effectiveness at Reporting Crime Evidence	●○○○	○○○○	●●●○	●●●●	●●○○	●●○○
OVERALL VALUE (Effectiveness for the Cost)	●●○○	●○○○	●●○○	●●●◐	●●◐○	●●◐○
Time to Implement	●●●●	●●○○	●◐○○	●○○○	●●○○	●●●○
"DIY" Options	◐○○○	●○○○	●●◐○	○○○○	●○○○	●●●○
Low Liability Risk	○○○○	○○○○	●●○○	●●●●	●●●○	●○○○
Flexibility of Use	●○○○	○○○○	●●○○	●●●◐	●●◐○	●●●○
Ease of Use	●●○○	●○○○	●●●○	●●●●	●●●○	●●●○
Integration with Other Systems	●●○○	●○○○	●●◐○	●●●○	●●●○	●●●◐
OVERALL RECOMMENDATION	●●○○	●○○○	●●○○	●●●◐	●●●○	●●●○

* Varies between "zero-down" installation plans and all-down installation costs.

EYEWITNESS SURVEILLANCE

SECURITY SYSTEMS 101

An Industry Guide to Commercial Security Systems

The entire staff here at Eyewitness Surveillance hopes that this guide has helped you better understand the security options on the market, and that you choose to invest in your business's security before a criminal makes you a target.

If you'd like to talk more about what security options would be best for your unique business needs,
CALL US toll-free at **800-518-3911** or
EMAIL info@eyewitnessmail.com for more information.

Because while any security is better than no security, some security companies work harder to protect your employees and your bottom line than others. We'd love the chance to prove that we're one of the "good ones."