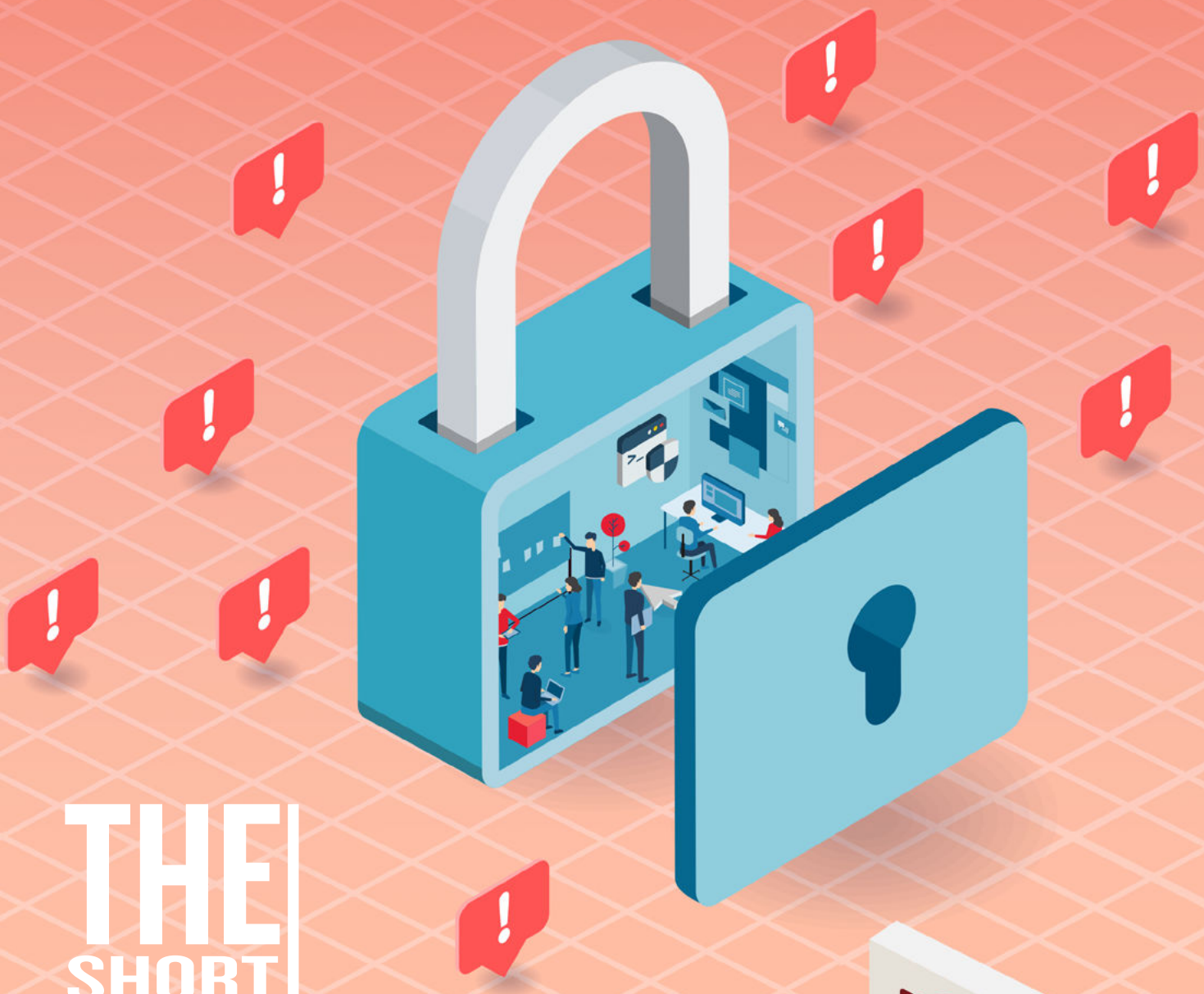
TAYLORED

Advisor



THE SHORT LIST of PHYSICAL SECURITY SOLUTIONS

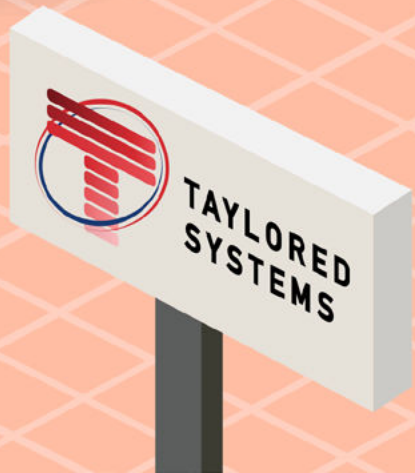


TABLE of CONTENTS

PHYSICAL SECURITY: Increasing threats have business owners concerned

WHETHER YOU'RE TALKING ABOUT TERRORISM, active shooters or run-of-the-mill commercial robbery, there's no denying that we live in dangerous times. Security organizations report that terrorism in North America is on the rise; indeed, the National Consortium for the Study of Terrorism and Responses to Terrorism (START) shows a **29 percent increase in terrorist attacks between 2016 and 2017.**

Perhaps more troubling, START research also indicates a **70 percent increase in terrorist-related deaths**, so last year's attacks were much more deadly than those in years prior. And while it's easy to write off those events as distant political exploits, the truth is that many were what experts refer to as "lone wolf attacks" or "homegrown terrorism."

In these cases, amateur threat actors operating on their own carry out deadly attacks against a wide range of different targets. According to one source, over the last three years, **73 percent of attacks in Europe and North America** have fallen into the homegrown terrorism category.

What makes lone wolf attacks so dangerous is that they are not just more violent but also more difficult to predict. They can come from anywhere, at any time: even from inside your organization. An employee with a grudge and violent tendencies might suddenly snap, leaving a wake of tragedy in his or her path.

Or perhaps the attack comes from an outsider with individual motives, a situation similar to the Pulse Nightclub shooting in Orlando, Florida, which the shooter **allegedly considered a kind of retaliation** for US anti-terror policies abroad.

What these events highlight is just how important physical security controls may be to your business's assets — namely, your most important assets: your employees.

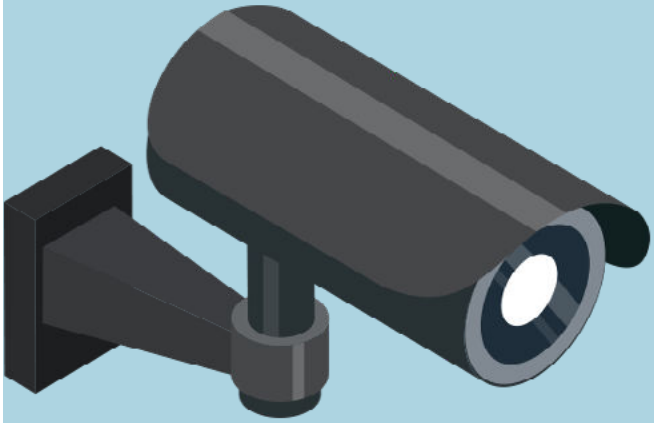
SECURITY IS NOT JUST A SAFETY ISSUE

WHILE THE SAFETY OF YOUR EMPLOYEES obviously ranks highest in your security priorities, physical security protects more than your team members alone. Your assets — including privileged data — are all at stake as well.

Physical theft is **the most common way that data is stolen** today. Where infrastructure security is lax, physical data is at risk. Giving employees blanket access to data rooms and on-site servers — or neglecting to secure spaces from outsiders — leaves digital assets and sensitive data unguarded. Anyone could walk right in with a flash drive and immediately gain access to critical data, including business secrets, customer credit card numbers and private health information.

Even if you have your individual rack secured behind a locked door, a simple control like this may not be enough to prevent physical data breaches. A lock is easy to force open with the right tools, particularly if the thief has the backing of a larger entity, such as in cases of corporate or political espionage.

To truly secure data centers and other physical computing assets, businesses need the reliability of sophisticated electronic controls, which are more difficult to tamper with and simpler to integrate with alarm and surveillance systems. To put it another way: your business is going to need smarter security if you're going to stand tough against today's threats.



THE DAWN OF A NEW ERA IN PHYSICAL SECURITY

CLEARLY, AS PHYSICAL SECURITY THREATS GROW MORE NUMEROUS, varied and complex, physical security controls must become more sophisticated and nuanced as well. Fortunately, that's exactly the promise offered by new security equipment.

New technologies, like automation and the internet of things (IoT), are offering richer security solutions based on real-time environmental data. From motion-detecting surveillance cameras that automatically tilt to record potential targets to mobile management platforms, businesses now have much more control over who has access to physical sites — and how security threats are dealt with.

These evolving security solutions demonstrate a marked transition in the industry, one where simple physical controls are being replaced by complex digital networks. Ultimately, we may be moving toward the unification of IT and physical security controls.

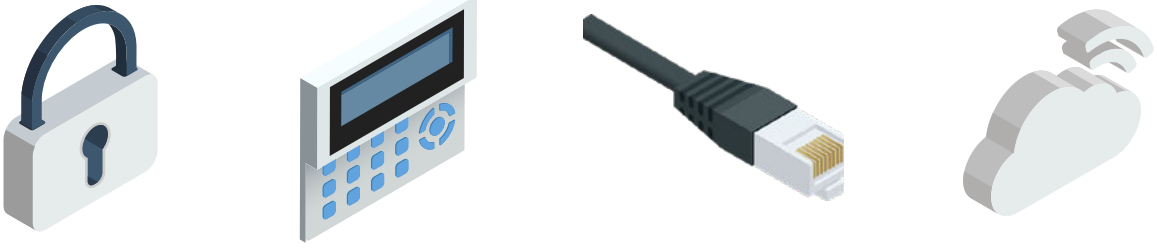
For now, however, the digitalization of security equipment requires a strong supportive IT infrastructure. Before we get there, we need to talk a little bit more about the types of equipment available — and how physical security tools are evolving to meet new organizational needs.

ACCESS CONTROLS: Keeping you safe from the inside out

WHAT'S THE SINGLE MOST IMPORTANT physical security solution? It would be difficult to say for sure, but one thing is certain: Access controls rate pretty high up there. Door controls allow you to protect privileged areas such as a computing room, banking office or laboratory. And, of course, they provide one more stopgap between cybercriminals and your data.

Naturally, modern access control systems are much more advanced than a simple lock and key, or even than conventional magnetic or radio frequency identification (RFID) key cards. Today, businesses can digitally control access points and remotely manage IDs and user permissions for very high-level control. IP- or cloud-based systems allow organizations to customize controls and track entries and exits for more accurate event reporting.

That's not to say that IP controls are a great fit for every business. Still, the more sophisticated features make a compelling argument for upgrading your company's access control system. Below, let's examine the different options in greater detail so you can decide which controls are right for you.



LOCK AND KEY CONTROLS

Since their humble origins in the early 1800s, the lock and key have undergone many advances and iterations. But the basic structure has remained the same for decades: The right key releases spring-loaded pins so that the lock can open.

Understandably, such a simple technology has its limitations. If you have multiple employees entering and exiting the building at different times, they each need a set of keys — which must be relinquished when employees leave or are let go. If a key is lost or stolen, it can be used by anyone until the lock

is rekeyed. Rekeying is in itself an inefficient process. Your office or site manager has to schedule an appointment with a locksmith and wait for him or her to arrive, taking time away from more important work.

Then there's the threat of a break-in. It only takes a quick internet search and a little practice to learn how to bypass a mechanical lock. For less patient criminals, a hammer or a wrench will do the job just as well.

Essentially, if you're still relying on a basic lock-and-key system to protect your premises, you're going on faith alone.

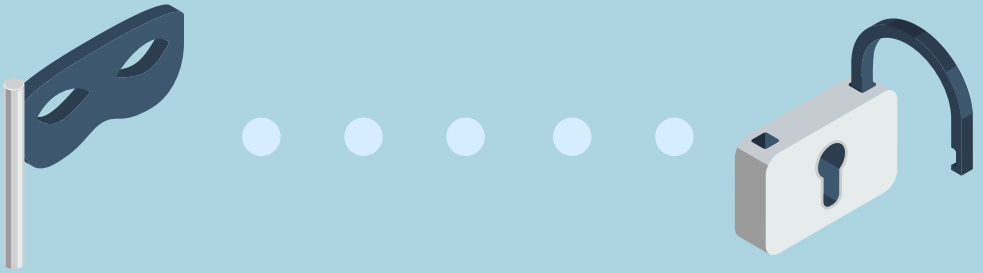
CONVENTIONAL KEY CARDS

In order to circumvent the inconvenience and imperfect security of lock-and-key, many businesses opt for more advanced credentials, namely magnetic or RFID key cards or fobs. These systems allow you to create unique identifiers for each user, and since access points are electronic, each entry and exit can be tracked to detect unusual activity.

Key card systems typically come with a separate device that allows you to create new cards and set user permissions, so there's a great deal more managerial flexibility. Naturally, the benefits vary depending on the type of technology you decide to go with. Let's take a look at some of the differences.

- **SWIPE CARDS**. Similar to a credit card, these systems write data to a magnetic strip on a card. When users swipe their card through the reader, the system checks their credentials and authorizes or refuses access based on their ID and your settings. This makes swipe cards a much more convenient solution for organizations with many employees coming and going at different times of day.

  Most businesses find that swipe card systems fit well within their security budget. However, with those savings come some drawbacks; namely, magnetic access controls are just not as secure as RFID and other systems.



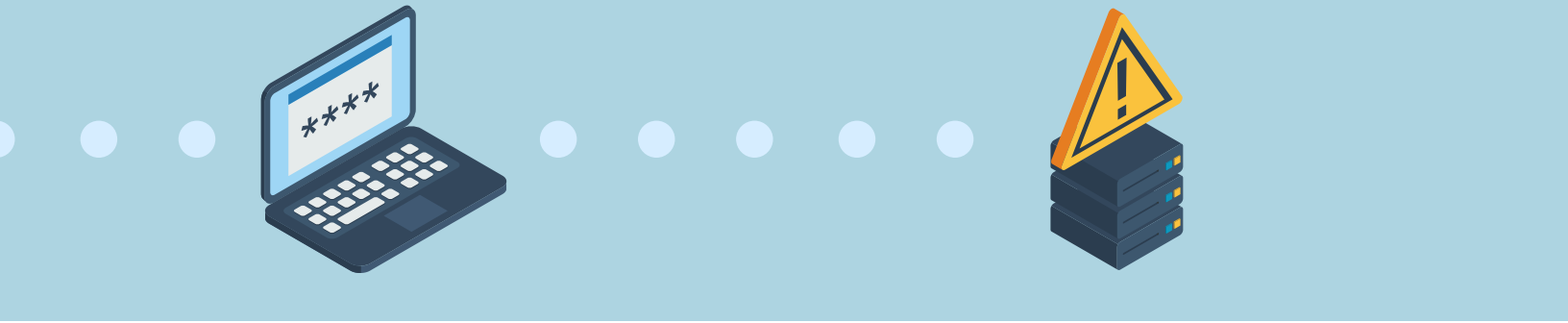
Consider your credit card for instance: A few years ago, your bank probably sent you a new card with an EMV chip. That's because magnetic strips alone lack comprehensive security; all user data is stored directly on the card, which means that personal data and credentials can be easily stolen by someone who knows how. Additionally, magnetic strip cards are easy to duplicate. All in all, you should really only expect low-level security protection from these systems.

RFID. These systems use radio waves to communicate between the reader and the key card. Each key contains a transmitter that sends signals to the access point when it is in range of a reader.

Because of this, these systems offer a great deal of flexibility and convenience. From the employee's perspective, it's simpler, since there's no need to root around for the card in order to swipe it.

On the administrative side, RFID systems allow you to manage cards, users and permissions as well as track employee access.

While these units provide more security above and beyond magnetic strip readers, they are certainly not tamper-proof. Radio signals traveling between card and reader are vulnerable to side-channel attacks, allowing unauthorized persons to break cryptographic algorithms and potentially gain access to privileged areas.



Unfortunately, magnetic strip and RFID systems are not always a very elegant solution, at least as far as infrastructure is concerned. They require independent wiring and a separate power source to operate, with an on-premise controller hardwired to the panel. This often costs employees valuable time in maintenance and upkeep. The more wiring, the greater room there is for something to go wrong, making these systems less reliable and often more costly in the long run.

IP ACCESS CONTROLS

The maintenance issue is precisely why many businesses have opted instead for IP-based access controls. These systems have all the benefits of traditional electronic access controls: Access points are networked and can be managed through vendor software. The flexibility is there, but the wiring structure has been simplified to reduce hardware maintenance. Here's a sampling of some of the benefits.

- **POWER OVER ETHERNET**. IP access controls like the Pure Access system offered by Isonas are powered over ethernet (PoE). There's no separate power source; the controller is wired directly into existing ethernet connections. The effect is a much leaner, more flexible access control system. All you need is Category 6 cabling, and you can set up new access points and install readers.

- **SIMPLIFIED ACCESS MANAGEMENT**. IP-enabled access controls are connected to an on-premise server. You can manage system administration from any device hosted on your network, adding and removing users, setting permissions and accessing reports through Isona's Pure Access Manager software.

CLOUD-BASED ACCESS CONTROLS

Just as the cloud revolutionized computing, cloud-based access controls are changing the game for business security. Here, businesses still reap the benefits of IP-based systems, such as PoE controllers, coupled with the reliability and reduced maintenance of an off-site database.

Cloud controls like Isona's Pure Access Cloud are the height of convenience: Employees can convert their mobile device into a key card, eliminating the need for a physical key card or fob. On the administrative side, site managers can log into a remote platform from any internet-connected device, updating users and permissions or even triggering a complete lockdown in the event of an emergency.

More specifically, here's what you get with a cloud system:

- Reduce server maintenance.
- Scale server CPU and disk space up and down as necessary.
- Power over ethernet means fewer cords and less hardware maintenance.
- Multi-locations can be controlled in the cloud from your corporate headquarters.
- Software is constantly upgraded — unlike an on-premise IP system, where you might need a maintenance contract or more end-user involvement to keep software up-to-date.

IP AND CLOUD-ENABLED ACCESS CONTROLS: AT-A-GLANCE BENEFITS

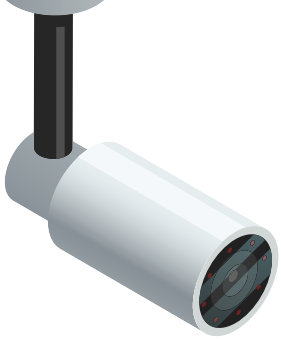
A COMPLETE AUDIT TRAIL.
An IP or cloud-based controller maintains a record of every opening and attempted opening of each door or area.

TIME AND DAY RESTRICTIONS.
s. Customizable permissions allow you to restrict access times for staff members based on their role.

EASY DEACTIVATION.
Lost or stolen keys? Remove access easily by remotely deactivating ID badges or other security credentials.

REMOTE ACCESS CONTROL.
Manage credentials and lock down your business from anywhere at any time.

EVENT NOTIFICATION.
Set your system to send email or text notifications when particular events occur.



SURVEILLANCE: Have eyes on your site at all times

While access controls have improved immensely in the past decade, they're obviously not foolproof. And for those in retail or other businesses open to the general public, a spike in credit card fraud and more sophisticated shoplifting techniques probably has you ready to do whatever you can to protect your place of business. Surveillance fills in the gaps in commercial security.

Surveillance systems allow you to patrol areas like a retail center or parking lot where access controls don't necessarily make sense. Stored footage from surveillance can be used to improve employee efficiency, create better safeguards against theft and prosecute criminals in an investigation. Cameras also keep employees, customers and visitors safer and reduce your **likelihood of being the victim of crime.**

TODAY'S SYSTEMS BEAT OLDER MODELS HANDS DOWN

When we talk about surveillance, we don't mean the grainy, awkward cameras of years past. Today's equipment vastly surpasses older models in terms of camera resolution, image quality, angle and zoom. Businesses can select cameras that work in almost every environment, including outdoor locations and low-light situations.

It's not just cameras that have improved, however. Modern surveillance systems are networked to a server, not written to video tape. There, footage can be stored for months or even years if need be. Surveillance software allows you to view footage remotely and manage your system from anywhere, at anytime. Reporting and analytics give you a sense of your system performance and help you evaluate where improvements can be made.

For a deeper dive into today's surveillance features and specs, check out some of the different options below.

CAMERA RESOLUTION. One of the most impactful advances in camera technology has been the development of higher pixel-count cameras. Older **720 pixel cameras** are being replaced by more sophisticated **1080 pixel HD** and **4K Ultra HD cameras** for sharper, clearer images.

These newer models soar above 720p cameras, providing millions of pixels per image. 4K cameras, in particular, offer immense benefits. It's not just that the images from these cameras are crystal clear — quality doesn't degrade when in zoom — but the wide-angle lens means coverage in a wider area. In short, it reduces the number of cameras needed to secure a single space.

ADJUSTABLE LENSES. While some businesses find that the coverage offered by **fixed lenses** — those with set focal length — meets their needs, it's certainly not your only option when shopping around for cameras.

Varifocal lenses provide an adjustable focal length, which allows you to zoom in and out, narrowing the field of view for a more in-depth image. **Pan, tilt and zoom (PTZ)** cameras feature a zoom lens that performs much the same function as a varifocal lens, except the lens is motorized, moving closer to the target when a triggering event occurs. Additionally, these many PTZ cameras can perform a 360-degree pan or 180-degree tilt. Most are fixed with motion detectors to track movement in the area and instantly adjust for the best image possible.

ENVIRONMENTALLY SENSITIVE CAMERAS. While an **indoor camera** might meet all your surveillance needs, a weather-ready **outdoor camera** includes many of the features you'll find in indoor-only models, with the additional abilities to withstand the elements and adjust to low-level lighting.

Meanwhile, **day-night cameras** automatically adjust the picture depending on the amount of available light. Using a filter, color adjustment or infrared rays, these cameras switch to black-and-white images after dark to continue surveillance even at night.

Thermal cameras, on the other hand, offer a different take on nighttime recording. These cameras detect heat signatures to create thermal images. Because the picture is not dependent on visible light, thermal cameras often produce more reliable imaging at night — and can often "see" through physical obstacles like smoke and fog.

ON-BOARD CAMERAS. On-board cameras increase the security of buses, trucks and company vehicles with integrated features like day/night recording to handle all the rigors of the road.

VIDEO MANAGEMENT SOFTWARE. You can manage cameras and access video remotely, download reports and analytics, and adjust storage space and server configuration with the help of video management software. Many systems have a mobile component that allows you to access features from a separate device, whenever and wherever you want. Software is continuously updated, so you can feel confident that you're getting the most up-to-date video management and features.

TYING IT ALL TOGETHER:

Robust cabling and network solutions support optimal security

The equipment is just one part of the story, though. Surveillance and access control systems need the support of versatile, powerful infrastructure. Moving from an ad hoc network to planned cabling and ethernet lets you harness the power of cutting-edge security solutions while future-proofing your business for networking needs down the line.

More specifically, structured cabling provides the framework for high-resolution cameras and PoE. Cabling allows you to leverage high-level security networking, establishing mesh networks and point-to-point wireless — networking solutions that help you overcome the physical barriers that make traditional surveillance difficult or even impossible.

But it's not just about security systems: with planned cabling, other networks' performance improves too. You can segment your physical security solutions onto separate networks to prevent lag on other devices.

The overall effect is a safer — and more productive — business. Our technicians here at Taylored can produce a streamlined network that will satisfy all your security requirements while preparing you for the challenges that lay ahead. In an unsecure world, our solutions offer a small margin of safety.

THANK YOU!

We hope you found this information useful and will be able to implement changes in your company. If you would like a consultation to assist you, please feel free to reach out!

EMAIL: sales@taylored.com
PHONE: 317-776-4000
WEBSITE: Taylored.com
ADDRESS: 14701 Cumberland Rd, Suite 100, Noblesville, IN 46060

LINKEDIN: https://www.linkedin.com/company/taylored-systems
FACEBOOK: https://www.facebook.com/tayloredsystems/
TWITTER: https://twitter.com/tayloredsystems

ABOUT US

Taylored Systems is a leader in technology.
Our dedicated employees provide clients with innovative voice, data and security solutions.

Our solutions are designed with managed services and supported by superior customer service.

We measure success by the continued satisfaction of our clients – "our partners" in communication.