# Wired vs. Wireless Commercial Security System:

## What to Consider in Making the Right Choice

Produced By

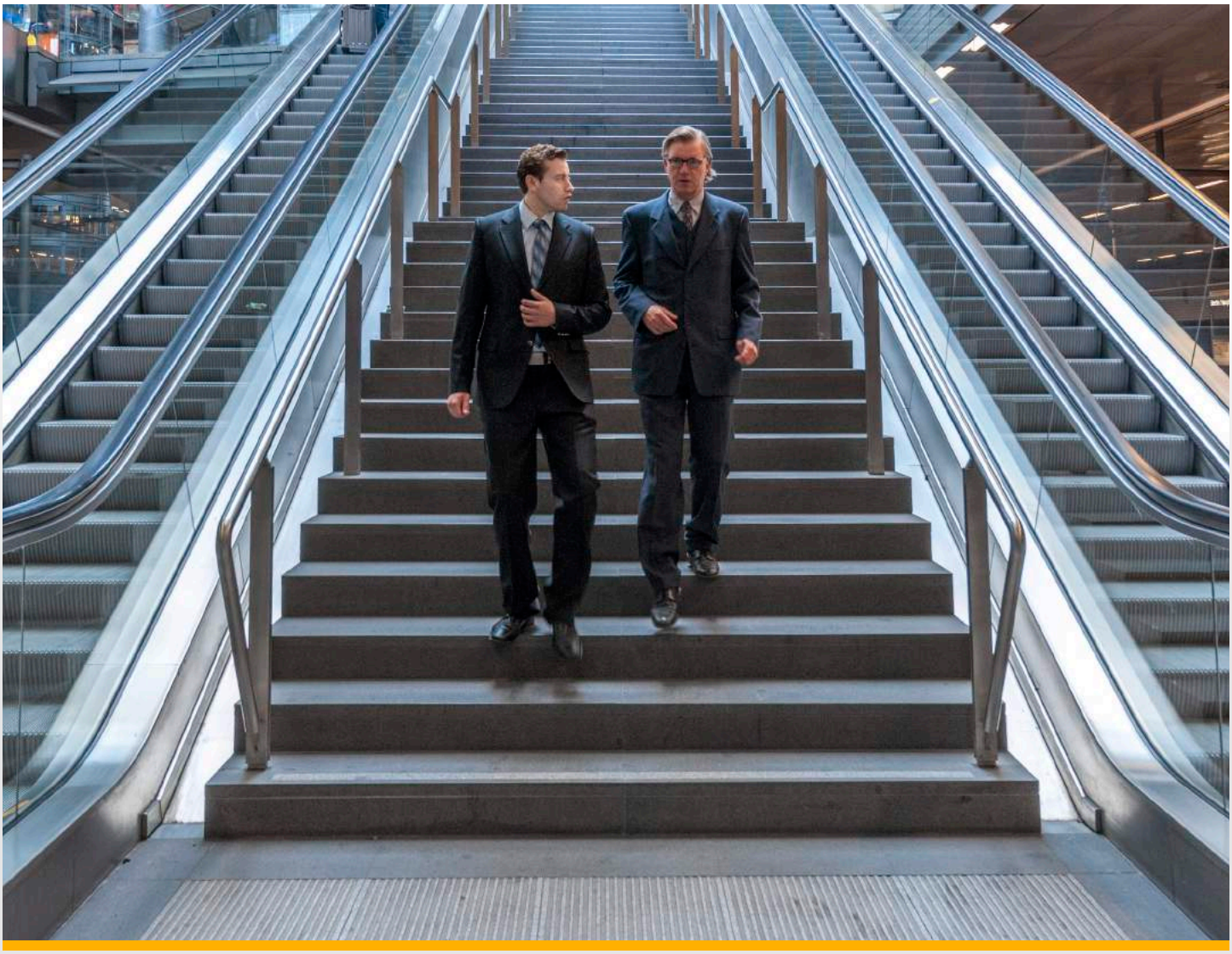
CanadianCIO

Sponsored By

tyco Integrated Security

# Executive Summary

The rapid evolution of commercial intrusion security systems is being driven in part by innovations in wireless networking and sensor technologies as well as a maturing Internet of Things (IoT). Reliability and security remain table stakes when evaluating and selecting a wireless intrusion security system. To make a choice that will bring long-term benefits to your organization, there's a lot that must be considered, including wireless technologies and whether a wired infrastructure might play a role going forward.



# Introduction

Consumers and businesses today expect wireless connectivity across a range of devices and environments, and have gained such confidence in the performance and reliability of wireless options that they now prefer them to a wired one.

The trend toward wireless technologies is impacting the intrusion security systems market as commercial operations discover immediate and ongoing operational benefits. With installers and security firms growing evermore confident in wireless systems, customer adoption is surging and insurance companies that once questioned the integrity of of wireless system are now much less hesitant.

More broadly, connected devices, as part of the Internet of Things (IoT) phenomenon are leading to the development of smarter and cheaper sensors, as well as the evolution to even faster wireless networking technologies. In its recent report, Internet of Things (IoT) Market by Software Solution, research firm MarketsandMarkets is predicting the IoT market will grow from US$157.05 billion in 2016 to US$661.74 billion by 2021, at a compound annual growth rate (CAGR) of 33.3 per cent.

The research report found that increasing penetration of connected devices has unleashed growth potential through predictive maintenance, security, and analytics which is expected to drive the market. In another report, Physical Security Market by System, Services, Vertical, and Region, MarketsandMarkets forecasted that the global physical security market will grow from US $65.41 billion in 2015 to US$105.26 billion by 2020, at a CAGR of 9.98 per cent.

It's clear that wireless technology, driven in part by IoT innovation, is heavily influencing the evolution and deployment of intrusion security systems. However, to truly leverage the benefits, both from a CAPEX and OPEX perspective, there are many things to consider when selecting a wireless intrusion security system, including the role that wired infrastructure may still play.

“ The global physical security market will grow from US$65.41 billion in 2015 to US$105.26 billion by 2020, at a CAGR of 9.98 per cent

# The Commercial Intrusion Security Landscape

The market for physical security equipment and services encompasses a wide array of technologies while serving a broad range of vertical industries, including homes and businesses.

Today's intrusion security systems include access control, video surveillance, intruder alarms, mobile video and body-worn cameras, and remote monitoring services, among others. Drill down into a specific system and you'll find more specific devices and features that make up a security system, including control panels, keyboards, and electronic locks.

> "Intrusion security systems are no longer a siloed endeavor for many larger organizations and facilities

All these pieces that were previously hardwired into a building as part of a larger system are now able to connect wirelessly, although in some industries (depending on the location's physical limitations) a wired connection may still be required.

Business owners and commercial landlords face a number of challenges when selecting and deploying an intrusion security system, and their individual requirements for a robust physical security system vary. Building managers and property operations managers, whether for a residential property such as acondominium tower or apartment complex, are either looking to deploy a physical security system directly or through a systems integrator or a consultant, to improve the value and desirability of their building.

Part of selecting an intrusion security system involves satisfing insurance companies that are only now beginning to trust wireless systems. Insurers often conduct risk and needs analyses at the premises, with the business owner, to determine the most appropriate equipment for securing the particular business based on a variety of parameters, including: the amount of crime in the vicinity; asset value; ease of asset transport; risk to life on the one hand, and equipment security and service levels on the other. These categories are used as guidelines to match systems and component requirements to specific businesses.

Owners of commercial properties are concerned with protecting the physical property, and in some cases they take the lead in installing some aspects of security infrastructure. For example, in small projects such as strip malls and shopping malls, property owners may, to some extent, secure the businesses with cameras and fire detectors. Property owners are often advised to become consultant to the smaller businesses and commercial locations to ensure all other tenants are protected. When making these security infrastructure decisions, commercial landlords and intermediary companies must consider tenants' interests.

Given that many customers need guidance to understand what they need to adopt and the support required for a physical security system, they turn to dealers, distributors, systems integrators, and consultants as trusted resources to evaluate, implement, and operate their security system. Advances in technology, including more robust and secure wireless technology, increase functionality, improve efficiency but also add to complexity. Intrusion security systems are no longer a siloed endeavor.

IT professionals can be key decision-makers in vendor procurement for all things security, including physical security systems, as they integrate into a broader portfolio of IT infrastructure.

Regardless of who in your organization is making the procurement decision, you or the systems integrator or consultant guiding the purchase and deployment need to keep several considerations in mind:

- **Reliable communications and protection from hacking and other security threats:** As previously mentioned, physical security systems are no longer siloed away from other IT systems, particularly from an operations perspective. While wireless technology enables mobility and improved ease of use, any decent security system not only secures the property but has digital safeguards in place just as any other IT system.

- **Future proof:** Physical security systems have become easier to deploy. They must be scalable, to cost-effectively address future requirements or alterations. Wireless technologies have made systems more easily updatable and flexible. Mobile access control and firmware upgrades can mitigate maintenance costs over the lifetime of a system.

- **Plays well with others:** How well a system integrates capabilities with third-party peripherals or devices is critical to accommodating customers' changing needs, budget constraints, or preferences. As mentioned before, this might include broader IT infrastructure and smart environment capabilities, to address growing demands. This also includes support for interactive service and hardware for smart business solutions.

- **Flexibility:** Intrusion security systems must address complex requirements, such as the ability to monitor certain locations where wired would be impossible or highly expensive — historic buildings, construction sites, remote areas, locations that demand temporary installations, buildings with significant interior brick, stone or marble construction.

An effective wireless system must have a long transmission range for reliable communications in large premise or multi-site applications.

- **Keep your premium down:** No matter how modern your physical security system, it still must meet the stringent requirements of your insurance company.

# Taking the Road of the Tried and True

Wired intrusion security systems still have a lot of advantages in the wireless world. For one thing, they are more reliable than a wireless system in that they support long transmission distances without a loss of signal. In addition, they are immune to outside interference. Equipment costs are lower in that wireless systems have elements that are powered by batteries that need to be changed — it is not only the price of these batteries that adds up, it is also the operations cost of doing such maintenance.

A hardwired system is more secure than a wireless one as they are not the targets of signal scanning and replication tools of hackers. A wired system can also be easily connected to an existing telephone or computer system to enable remote monitoring.

Although wired security intrusion systems have a proven track record, they have drawbacks. Depending on the size, age or layout of the building, a hardwired system can be difficult and hence expensive to install. In fact, it may not be feasible at all depending on the location. For example, wiring sensors to a particular point in the building may not be practical. Even if it is feasible to take a fully wired approach, it may not be possible to hide all the wires; this can be an eyesore. In addition, exposed wires are more likely to get damaged.

A hardwired approach system may also be difficult to remove for the purposes of using it at a different location. The installation work alone for a wired system is generally pricier due to the labour costs and time required to install and run all the wires. And if you are only renting the building, your landlord may not permit you to drill holes in the walls, floors, and ceilings to accommodate wires.

These drawbacks, and others, now have people considering wireless over wired. However, the latter is not a panacea for all the challenges in deploying a modern intrusion security system.

# The Benefits of Joining the Wireless Revolution

The advantages of wireless systems over wired begin at the deployment stage. Because there aren't long lengths of wires to be laid and pulled through walls, installation is quicker and easier, which translates into lower labour costs. Installation can be done at the time of occupancy as no pre-wiring of the building is required.

Of course, the lack of wires also allows for modular deployments and makes wireless systems ideal for older buildings, for properties with structural impediments, or for retrofitting existing systems. And again, wires can be an eyesore if run in exposed areas. With wireless systems, there are no exposed wires, only compact and sleek devices that can be discretely placed throughout a location and can better reach inaccessible locations.

From an operational perspective, wireless systems offer a lot of benefits that can translate into cost savings. They can be easily and quickly extended, to keep pace with a growing business at the same location, or easily uprooted and augmented for a larger facility — they move when you move.

Wireless systems also lend themselves to secure, remote access so they can be managed from afar, and they can also be integrated with other wireless systems, including smart building automation and IT systems. Remote monitoring can also be supported by connecting it through a phone or computer.

"From an operational perspective, wireless systems offer a lot benefits that can translate into cost savings

# Protocols: A Key Consideration When Going Wireless

If you decide your intrusion security system should be wireless, either completely or partially, there is still a lot to consider, and it is not just selecting the vendor of the equipment or the integrator who will deploy and manage it for you.

When deploying a wireless security system for a commercial location, it is important that you look at the protocol on which the system operates as this greatly affects the performance, reliability, and scalability of the system. There are several wireless protocols commonly used in intrusion security systems. Some are open protocols while others are proprietary.

# Open Protocols

**Bluetooth Low Energy (BLE):**

Branded as "Bluetooth Smart," BLE is a wireless personal area network technology that has a broad array of use cases. Developed and marketed by the Bluetooth Special Interest Group, it has been aimed at applications in healthcare, fitness, beacons, home entertainment, and security. One of the key benefits of BLE is that it operates at a greatly reduced rate of power consumption without sacrificing communication range.

**Digital Enhanced Cordless Telecommunications (DECT) / DECT Ultra Low Energy (ULE):**

Originating in Europe, where it has become the universal standard, ULE is primarily used for cordless telephone systems. DECT ULE is specifically designed for home security and automation. Its communication range is among the longest of the short-range wireless communication technologies, supporting more than 50 metres in buildings and up to 300 metres in the open air, and repeaters can be used to extend the range.

**Thread:**

Relatively new, Thread is an IPv6-based networking protocol designed to enable IoT smart home automation devices to communicate on a local wireless mesh network. IP-addressable, Thread supports up to 250 devices in one local network mesh, and uses 6LoWPAN, which in turn uses the IEEE 802.15.4 wireless protocol with mesh communication, as well as AES encryption.

**Z-Wave:**

Another mesh networking technology that enables devices to communicate with each other, Z-Wave also minimizes power consumption. Used for security as well as access control, lighting and HVAC systems, its potential range is more than 100 metres.

**ZigBee:**

Similarly, ZigBee is a set of mesh network communication specifications for WLANs covering a large area, and is also designed for low-power-consumption applications, including wireless control and monitoring. Because it is scalable for up to thousands of devices, ZigBee supports large installations and the easy expansion of existing systems with a transmission range of more than 50 meters. There are currently two major ZigBee specifications: ZigBee PRO, or device-to-device communications, and ZigBee IP, targeted to applications such as smart metering.

# Proprietary Protocols

**PowerG:** Introduced in 2011, PowerG Technology is a tree topology-based proprietary protocol, optimized specifically for the monitoring and control of battery-operated devices for security and safety applications. With ranges of more than 2,000 metres, PowerG has numerous built-in technologies and features to support reliable, secure and efficient communication, including frequency hopping for dependable and secure message transmission. Because it is proprietary, PowerG is less likely to be hacked than open technologies, and is well-protected against malicious and accidental interference.
While PowerG was designed specifically to deliver the reliability required by intrusion security systems and is the most suitable protocol for wireless commercial security systems, open wireless protocols are better for building automation systems than PowerG, since they are built for low power consumption and high scalability. The ideal choice is a hybrid system that combines the benefits of an open protocol with the robustness of a proprietary one.

# Hardwired vs. Wireless Security Systems: Must it Be One or the Other?

Given that we live in a wireless world, where the average person is cutting their landline in favour of using only a smartphone, and where most computers connect to the local area network and Internet via WiFi, the pressure to make everything wireless is omnipresent. There are some drawbacks to wireless systems, however. Compared to a wired intrusion security system, the equipment for a wireless system tends be more expensive up front. And because many wireless devices run on batteries, there are higher maintenance costs because they need to be replaced every three to five years to remain operational.

The larger the building, the higher the labour costs to get those batteries replaced. In addition, these wireless devices can be subject to external radio interference.

In the case of an intrusion security system, wireless technologies have hit a tipping point when it comes to demonstrating their security and reliability to a degree that satisfies insurance companies, solving many of the cost, deployment, and cosmetic challenges that come with a hardwired approach. However, there remain areas where a partly wired system might make sense — when interference may hinder a wireless system, for example.

In addition, some commercial property owners may not want to go completely wireless; rather, they may want to augment their existing wired infrastructure and expand their footprint with wireless, or gradually make a transition to an all-wireless intrusion system to get the most out of their existing wired investment.

There is a lot of value in taking a hybrid approach as it maximizes the strengths of each and minimizes the weaknesses.

# Case Study: An Education in Wireless Security Systems

The Travis Unified School District in California includes five elementary schools, a middle school, a comprehensive high school, an alternative high school, and a community day school. It is an active district as people are added to or deleted from the employment roster while others move among the various schools and need to access one or more alarmed doors.

Accommodating the frequent changes was time-consuming as those responsible for monitoring and maintaining the alarm system had to modify each school's alarm system. Just adding a single person, such as a newly hired custodian, could take up to an hour, while a long list of changes could be a one- to two-week process from submission through verification.

> "Being able to make updates, identify usage errors, and review the system for maintenance-related issues were some of the immediate benefits of PowerSeries

Another challenge to both personnel time and the school's budget was the maintenance required on the individual door sensors. Insufficient battery life required batteries to be changed out every two or three years on the alarmed doors.

The school district was also under a mandate to eliminate phone landlines as its alarm system backbone.

For Travis Unified School District, It supported the school district's need to make changes from a single location, and to monitor alarm activity as it happens. The goal was to simplify the management of its intrusion system by giving district employees the opportunity to add new employees into the system, and to remotely monitor activities and incidents.

Being able to make updates, identify usage errors and review the system for maintenance-related issues were some of the immediate benefits of PowerSeries Neo. David L. Florez, the district's risk manager, said the customization of PowerSeries Neo also allows Florez to share responsibilities with others in the district so it isn't a one-person-only job.

Unlike the old process of in putting data for each door, now adding someone requires only typing in a name and code and then selecting the appropriate doors from a list, according to Phil Speck, Operations Manager for Alarmtech. "The new PowerSeries Neo system reduces the time involved from just a couple of minutes, compared with an hour or more previously," he said. The system enables Speck to set his own parameters for actions such as auto-arm or setting specific timeframes based on scheduling needs.

Another opportunity presented by the upgrade to PowerSeries Neo was the ability to use outdoor wireless beam detectors without having to trench and run wires. There is an area near the transportation building and maintenance yard that was the target of vandalism that the district now protects with motion sensors. PowerG technology allows it to cover the 300-by-300 maintenance yard without the use of repeaters, said Speck. The school district also leveraged the range of the PowerSeries Neo to help monitor its transportation building and maintenance yard.

"We decided to put up a perimeter and have two motion sensors on the back side of the transportation building, to provide greater coverage of this area," said Florez. "PowerSeries Neo integrates seamlessly with this system so we could leverage its wireless capabilities and the range it has to offer."

# Case Study: Keeping TABS on a Big Warehouse

TABS Security Service's John Amerman has a long history in the security system installation business, and has a great deal of experience installing Honeywell Vista panels. But when tasked to upgrade a Coca Cola bottling warehouse, he saw an opportunity to upgrade the bulk of the facility from a wired security system to a wireless one; this presented an opportunity to use a different technology.

Prior to the Coca-Cola warehouse installation, Amerman was unaware of PowerSeries Neo from Tyco Security Products and its wireless range capabilities thanks to the PowerG technology. But having been fully trained on the PowerSeries Neo, he found much to like about it and decided it was the better option for the Coca-Cola facility.

The 300,000-square foot warehouse with 40-foot ceiling was wired in the late nineties with a Honeywell system that was in dire need of replacing, and given the dimensions of the building, completely rewiring the building would have been an onerous task. Having received comprehensive training on Tyco's PowerSeries Neo, Amerman decided it was well worth the time and effort to switch to it rather than stick with Honeywell.

The Tyco deployment in the Coca-Cola facility involves 36,000 overhead sensors, two strobes, and a horn. For the most part, the entire system is wireless, except for eight motion sensors on doors in the warehouse's offices area; those offices have eight-foot ceilings. The range of the PowerSeries Neo easily met the distances found in the sprawling facility.

The wireless deployment drastically reduced the labour hours required in comparison to a wired installation, according to Amerman. Having a completely wire-free keypad meant saving three days and only needing two people to check more than 70 nodes.

With the deployment of Tyco's PowerSeries Neo having been operational for nearly three months, Amerman said there have been no issues with ongoing management.

TABS, based in Tampa, Florida, can easily address any issues at the Orlando-based warehouse by looking at it online, which saves TABS money. Amerman noted that 90 per cent of the service calls were customer errors in the first few months as they adjusted to the new system.

> "The wireless deployment drastically reduced the labour hours required in comparison to a wired installation

TABS manages and monitors everything at the Coca-Cola facility remotely and can guide a customer who is onsite through the resolution of most issues, which is why the PowerSeries Neo is so much less costly to manage.

"That's why we like it on the operations side," Amerman said. "The cost has gone down tremendously. It's worked out for us."

# Have the Best of Both Worlds

Until recently, the choice for most business owners was between hardwired and wireless security, with wired being the default whenever an insurance company imposed such requirements. That led to many business and property owners having to compromise on performance, convenience, and/or scalability. Fortunately, business owners can now benefit from hybrid systems that combine wired and wireless elements within the same security network.

A hybrid wired/wireless intrusion security system provides all the benefits of a wireless system while eliminating the inherent weaknesses of wired systems, at the same time meeting insurance company requirements. By covering all the key requirements, hybrid security systems present an ideal solution for many commercial premises.

For more information about creating a hybrid wired/wireless network that combines the best of both worlds, contact your local Tyco Security Product Representative and ask about the PowerMaster Neo solution for commercial security installations.

# About Tyco Security Products

Tyco Security Products and its leading brands conduct business in more than 177 countries around the world, in multiple languages and employ more than 2,800 employees globally, including research and development, marketing, manufacturing, sales, service and logistics teams in the Americas, Europe, the Middle East, Africa, and Asia Pacific. Our products, built by developers from all product disciplines, consistently allow customers to see more, do more, and save more across multiple industries and segments including healthcare, government, transportation, finance, retail, commercial and residential. Worldwide, Tyco Security Products helps protect 42% of Fortune 500 companies, transportation systems on five continents, 37% of the world's top 100 retailers, more than two million commercial enterprises, thousands of students in more than 900 educational facilities, and more than five million private residences. Learn more about Tyco Security Products at **www.tycosecurityproducts.com.**