White Paper

New Security Technologies
Does your provider have your best interests in mind?

Prepared by: Cypress Private Security

January 2016

“Observe and Report” Is Not Enough

As our awareness of potential threats increases, so does the demand for smarter security. In an era where the fear of mass violence has overshadowed the more benign concerns of the previous decades, a security program whose mission is merely to “observe and report” now strikes many as woefully insufficient. **The demand is now for security that can deliver greater detection and prevention capabilities and faster incident response time.**

Concurrently (and seemingly paradoxically), those in need of security services are also demanding that those services be provided at a lower cost, as the belts tightened during the economic downturn have yet to be fully relaxed. The question, then, is this: **How can security firms provide smarter, more capable services at a lower cost?**

Unsurprisingly, the answer is to look to recent technological advancements in the design of a security program that is both more efficient and more effective. However, the decision of which technology to use, and how that technology should be implemented, must be approached carefully and thoughtfully. **Catchy buzzwords and exciting gimmicks may be used to make a security program appear more advanced than it actually is.** This white paper aims to take an objective look at recent technological developments in the security industry to examine their true efficacy and overall benefit to the client.

What “Integrated Security” Really Means

Anyone who has looked into contract security in the past year is likely to have come across the term “integrated security.” Most of the world’s largest security firms have touted their integrated services as the foremost advancement in security offerings, supposedly placing them on the cutting edge of the industry. But what does the term really mean?

At its core, integrated security is simply the offering of human security officers, intelligent data collection, and remote monitoring services, all by the same company. While traditionally clients have had to go to one company for in-person guarding and another for remote monitoring, the two services are now more commonly being offered together. The idea is surprisingly intuitive, to the point where it almost doesn’t sound like a new idea at all.

To be sure, “integrated security” falls under the category of buzzword, and the service is often trumped up to appear as more of an advancement than it really is. However, offering both human guards and remote monitoring together does allow for possible benefits. These benefits may include:

- **Flexibility:** An area can alternate between posted officers during busy periods and digital monitoring during slow periods.
- **Mobility**: This flexibility allows officers to spend more time patrolling various areas rather than staying fixed to one position.
- **Efficiency:** The combination of flexibility and mobility has the potential to allow a more targeted deployment of officers so that fewer man-hours are wasted.

- **Cost:** The more efficient use of man-hours means that the cost, for both the security provider and the client, is reduced.

It is important to note that simply providing both manned guarding and remote monitoring isn't enough for a security firm to truly deliver on the benefits of integrated security. Rather, **the advantages of these two elements exist in the way in which they are made to work together**. One must ensure that the digital monitoring systems are able to immediately alert officers of any occurrences, just as it is vital that officers are trained in how to respond swiftly to the automated alert. If this coordination between monitoring system and officer isn't there, then the point is moot. Two security services may be provided, but **they have not been truly integrated**.

Is Integrated Security Truly Beneficial to the Client?

Thus, one realizes that **true integration doesn't depend on having one company provide both services.** There is no reason why a company that specializes in manned guarding can't coordinate its services with a company that specializes in remote monitoring or one that provides the software and/or hardware that collects and filters the data. It may be simpler on the part of the security provider, but is this beneficial to the client?

Consider the fact that the offering of integrated security is most often **an investment on the part of the provider**, typically through the acquisition of a pre-existing remote monitoring company and the development or purchase of proprietary technology solutions. Providers who have made this investment **have a strong motive to cover the costs of their acquisition, regardless of efficacy**. A security firm who has purchased a monitoring company has dedicated itself to sticking with the technology and methods employed by that company, whereas a security firm who leaves itself open to cooperating with outside monitoring companies is free to employ the best technology and methods available at any given date and for any given client. Just as the Cloud replaces on-site servers, and just as DVD replaced VHS and VHS beat out Betamax, **those who commit themselves to a single technology solution that has been disrupted will of course offer lower prices, but those who are able to adapt are the ones who succeed.**

Furthermore, it is well known that one of the major reasons why so many large security firms are emphasizing integrated security is that it allows them to operate with greater profit margins. Much of these savings come from the higher margins it can charge for its technology over margins available for providing personnel. While there is of course nothing wrong with the security provider earning higher margins if it is able to reduce overall costs, it must be remembered that the primary benefits of integrated security come from the actual *integration* of digital systems with human guarding, and the ratio between these elements must be calibrated to meet the specific needs of each client. However, **a greater emphasis on digital systems means better margins for the security provider**, and so the provider may be tempted to push a ratio on the client that is suboptimal performance-wise for the sake of the provider's own financial benefit.

Without a doubt, remote and automated monitoring systems are extremely useful in maintaining awareness of what is taking place at a given site at all times. **But the point of security isn't just to observe; it is also to help.** This is especially true at sites that are open to the public, where the human element of security is crucial in assisting with those who are lost, sick, or otherwise in need of face-to-face assistance. The ability to coordinate in-person officers with monitoring systems allows each element to function more effectively, but if one element is sacrificed for the convenience or affordability of the other, then **the overall security of a site has, in fact, diminished.**

Cameras That Can See

Whether or not they are part of an integrated service, security camera systems are more advanced—and more affordable—than ever before.

While security cameras once could only record footage, now they can **see**. At least, they can recognize distinct characteristics of what they record. **Facial recognition** is now common, as well as the ability to **identify license plates.** In addition, some camera systems can be taught to recognize **specific colors and shapes**, such as vehicles or other objects of note.

What does this mean for the practice of security? For starters, it makes the task of sifting through hours upon hours of security footage much easier and significantly less time-consuming. As one large industry participant noted in its white paper, "The Business Argument for Integrating Security Systems," the software can be taught to recognize a white pickup truck. In the event of an incident involving a white pickup truck, the footage can be automatically searched for that specific color and shape, rather than having to waste time watching hours of irrelevant feed in order to seek out a single crucial moment.[1]

The analytic capability of the modern security camera is striking. The feeds from these cameras can be used to generate reports, such as lists of all license plates to enter or exit a site at a certain date and time. The use of motion sensor technology can alert operators to when a certain camera's feed needs to be attended to, or if a certain location needs immediate in-person response, instantaneously. Building on that, cameras like the SightLogix SightSensor can differentiate between the motion of an intruder and the normal occurrences that cause false alarms, such as moving shadows or the wind in the trees. The cameras can be programmed to look for objects of a certain size, in a certain location, and at a specific time of day. They can identify loitering, wrong-way traffic, and forgotten or abandoned objects. **The modern camera is aware of its surroundings**, which allows for incredible detection and prevention capabilities. These analytics give us the ability to respond to situations in real-time as they arise, allowing for **a more effective use of security personnel.**

This appears to be a key example of how services marketed as "integrated security" can benefit the client. However, this kind of true integration, in which human officers are able to respond immediately to automated alerts, will be available from **any truly modern and intelligent security provider**, regardless of whether they ascribe to such trendy labels or own a proprietary monitoring system.

[1] J. Nicole McDargh, CPP, GISP, "The Business Argument for Integrating Security Systems," Securitas Security Services USA, Inc., 2015, retrieved December 2, 2015, from http://www.securitas.com/globalassets/us/files/knowledge-center/whitepapers/integrated-technology-whitepaper_2015.pdf

Secure Access without the Bottleneck

As technology advances, we find more and more alternatives to relying on our own two eyes in verifying the legitimacy of what we see. While it has been around in one form or another for a while now, RFID, or **Radio-Frequency Identification**, is a security technology that has become a growing part of many aspects of twenty-first century life. If you use an automated toll payment system such as FasTrak, you likely have an RFID tag affixed to the windshield of your car, and if you've adopted a pet in the last couple of years, there may be one implanted under its skin. Passports, merchandise, and even people can all be verified and tracked with ease using RFID technology.

RFID tags are small devices (sometimes as small as a grain of rice) used to quickly verify the identity of whatever the tag is affixed to. The use of radio signals allows the interrogating device to collect the tag's information instantaneously, even if the tag is at a distance or obscured by other materials—hence the ability to function when implanted in an animal. This makes them **ideal for keeping track of moving systems.** For example, if a shipping center has many trucks continuously carrying cargo in and out of the site, those trucks may be fitted with RFID tags. Each truck can be scanned as it enters and exits the site, and any truck that fails to scan properly will be instantly identified for close examination. In the event that a truck is stolen, its tag can be used to identify it as such.

This technology also allows for a more **fluid facilitation of access control.** By placing tags in identification badges, the bearer may be identified easily, having only to hold the badge within a certain distance of the reader. This allows for the maintenance of secure entry to a site without causing unnecessary delays.

RFID tags are practical for broad use because of their **size, simplicity, and affordability.** The simplest versions of these tags don't even have an onboard power source; they draw their power directly from the signal of the interrogating device. The cost of these passive tags is typically less than a dollar per unit, and some particularly rudimentary tags go for just pennies. Active tags, those that have their own batteries and somewhat more sophisticated technology, are still reasonable, starting in the range of $25 per unit.[2]

Digital Incident Reporting Is Now a *Minimum*

The key to effective security is efficient communication. Information must be gathered, recorded, analyzed and communicated in a fast and reliable way, and the handwritten reports of officers aren't enough. To meet this need, **incident reporting software** can facilitate the gathering and transmission of information with consistency and speed. While less flashy and even practically invisible to anyone outside of a given security team, this software has become **essential to running an effective modern security program.**

This software is designed to generate whatever form is necessary so that reports can be made quickly and in the proper format. Once the report has been made, it can be automatically transmitted through the proper routes so that no cross- or miscommunication prevents the information from successfully reaching the

[2] "How much does an RFID tag cost today?" RFID Journal, retrieved December 2, 2015, from https://www.rfidjournal.com/faq/show?85

people who need it. Qualitative and quantitative filters can be used to sort the reports by relevant subject, providing the basis for meaningful analytics.

These analytics are incredibly powerful. Graphs and charts breaking down the distribution of what types of incidents occurred can be generated, allowing one to **identify what issues most need to be addressed** (e.g. a pie chart depicting that, of incidents reported, 20% were vehicle break-ins, 30% trespassing, 10% accidents and injuries, etc.). Images and narratives of significant events can be gathered to provide for a **comprehensive understanding** of what transpired in a given period. Line graphs can demonstrate whether or not a certain category of occurrence has increased or decreased over time, **aiding one's understanding of how effective certain security measures may be.** The analytics provide for in-depth breakdowns of what's happened, where and how often it happens, and how that is changing over time. Essentially, **they turn an incident report from rote paperwork into powerful information**—powerful in the sense that it gives us the power to act on what we know.

This ability to analyze generated data is extremely useful. When faced with a large amount of incident reports, it can be a struggle to make heads or tails of what needs to be done in response. Are more officers required? Have cameras been installed at the most important locations? Is the vehicle patrol following the route that it should? **What's being missed?** Incident reporting software allows one to bridge the gap between information and action.

Some incident reporting software allows for collaboration between multiple people on a single report, something that can otherwise lead to confusion. It is also possible to analyze a given report to identify a specific cause, which allows for **a more targeted response that can actually prevent future occurrences.**

It may not sound impressive. That's because **the best technology's primary goal isn't to make an impression but to be useful.** This is what gets the job done, and this is what makes for more effective security.

A Look at the Impending Future

That isn't to say that the impressive can't be useful. While many developments in security technology consist primarily of improvements upon or smarter implementations of existing technology, some of the most cutting edge advances are totally new. Take, for example, the **Knightscope K5**, the "autonomous data machine" beginning to patrol a few select sites in Silicon Valley.

The Knightscope K5 almost seems like *Star Wars* come to life, reminding many who see it of R2D2. According to Knightscope's website, this five-foot-tall, three-hundred-pound robot **uses technology similar to that found in self-driving cars** in order to **autonomously patrol a given site.** Its various sensors—including infrared, light detection and ranging (LIDAR) devices, low-light video cameras, directional microphones, an inertial measurement, a wheel odometry unit, and GPS—allow it to navigate and gather data on its surroundings.

Gathering data is the key point. **The K5 is not meant to do the job of human security officers but to provide them with information.** It combines the information it gathers with preexisting data from business, government, and social sources to determine when it has detected a threat. In the event that a threat is detected, the K5 automatically transmits a notification of the threat and the level of alert to authorities and to the community.

Knightscope, while still developing, could be extremely useful in augmenting security services. One of the most difficult aspects of a security officer's job is maintaining vigilance while carrying out monotonous duties, an issue that doesn't come into play for the K5. It is also designed to operate 24/7, autonomously recharging on a regular basis so that there are **no extended periods of downtime.** Interestingly, the K5 is not for sale but for "hire"—its services currently go for $6.75 per hour, though that rate is charged for all 24 hours a day of operation.

When technology like this arises, it often prompts the question, "Can this replace the human security officer?" The answer, for now, is no—nor would we want it to. Though the Knightscope K5 is shielded and equipped with an alarm to protect itself against tampering or vandalism, it does not carry any kind of weapon or deterrent. More importantly, though it can be used to call for help, the K5 itself cannot directly help a person in need. **The purpose of the K5 is to provide data to people**—security officers, law enforcement, and the local community—and **if people are taken out of the equation, then the K5 will have no way of fulfilling this purpose.**

Conclusion

Obviously we have only covered a handful of recent technological developments here; the realty is that **there are countless new developments being made** in what technology is available to security providers and how these developments are implemented in the design of security services. As the rate of technological enhancements has accelerated, we have all seen a **growing unpredictability** in terms of which developments will become truly integral to modern life and which ones will turn out to be novelties quickly falling by the wayside.

For a security company—or any company, for that matter—to succeed in modern times, **it must be nimble in its use of technology,** willing to stay on the lookout for bold steps forward, but also willing to move on from those that turned out to be missteps. Only time will tell which technologies are best suited for the security industry, and **a firm that invests too deeply in a given technology may cling to it long after its usefulness has faded.** A manned guarding security firm that has made a major investment in buying out a remote camera monitoring company will have a harder time adapting when the Knightscopes of the world take center stage.

And this is the most important thing to consider: **new technology is much more likely to replace other technology than it is to replace people.** The Knightscope K5 will likely never be able to effectively replace human security officers. However, something similar could conceivably replace digital recording devices one day.

The reason we utilize technology is so that we can **do more with less:** cover more ground, gather more information, and help more people while wasting less time, spending less money, and making fewer mistakes. **Efficiency should never be viewed as simply a cost-cutting measure**, as this leads one to cut corners rather than make true improvements. Efficiency is about achieving the most quality with the least cost. If technology is implemented as a substitute for, rather than an augmentation of, human officers, the quality of security will suffer. **That isn't efficiency, and it isn't progress.**

When making security decisions for your company or organization, it's important to consider what technology each security provider employs. Don't be content with letting anyone tell you what's best for you. It's crucial that a security provider has the flexibility to quickly adopt improvements, rather than clinging to an outdated technology in the hopes of amortizing sunk costs. **Make sure that your security provider uses technology to enhance its services, rather than to cheapen them.**

About Cypress Private Security

Founded in 1996, Cypress Private Security prides itself on being the most customer-focused contract security company on the West Coast. With a custom-tailored approach for each client, Cypress provides unmatched security solutions to meet the specific needs of various organizations. For additional information, contact Kes Narbutas, CPP, Chief Executive Officer, Cypress Private Security, at (415) 240-4500 or knarbutas@cypress-security.com.