The Autonomous Remote Services Industry

A Manifesto summary for a classic Fourth Industrial Revolution Corporation

By Steve Reinharz
Artificial Intelligence Technology Solutions, Inc., Founder & President

CONTENTS

INTRODUCTION

ALEXA. SIRI. GOOGLE. In just a decade, they've gone from clever novelties performing "tricks" at parties to becoming our indispensable daily helpers. The speed and degree to which we've traded in skepticism and paranoia to fully embrace the use of virtual assistants, smart IoT devices, and machines and software driven by always-connected, predictive artificial intelligence is truly astonishing. Sure – we're all aware of privacy issues, data breaches and other risks that exist, but when technology can make our lives so much more efficient and convenient, for not a lot of money, the jury has spoken. We'll take the technology, thank you. It's estimated that in 2019, more than 1/3 of the US population used a personal voice assistant at least monthly[1], and researchers predict 8 billion devices will be in use worldwide by 2023[2] – as many devices as there are people.

> ―――
> When technology can make our lives so much more efficient and convenient, for not a lot of money, the jury has spoken. We'll take the technology, thank you!
> ―――

This same confluence of forces is beginning to make its mark on the Physical Security and Guarding Industries. Pre-COVID, corporate CSOs and CTOs were already under pressure to make their own security organizations more efficient, convenient, and cost-effective. They've benefited from smarter, more flexible dedicated systems that are incorporating enhanced AI, analytics and aspects of the IoT.

Now, more than ever, these new technologies are all the more relevant. Moving forward, intense cost pressures and changing workplace realities, driven by extreme economic challenges, will create converts from among mainstream technology users and buyers. In addition to guarding the safety and security of people and property, physical security responsibilities will include added emphasis on protecting workers' and visitors' health. These may include activities such as screening for temperatures, contact tracing, verifying workplace sanitation procedures, monitoring for social distancing and enforcing the use of masks. It will also require the creation

---

[1] US Voice Assistant Users 2019; Who, What, When, Where and Why. eMarketer Report Executive Summary
[2] ZDnet.com; Eight Billion Voice Assistants Will Be in Use by 2023, Charlie Osborne

of security and safety related continuity plans to accommodate for prolonged worker absences due to illness or quarantine requirements, and figuring out how to best incorporate remote workers as part of a security operations force. For those responsible for security, these new challenges further magnify their long-standing frustration with traditional, labor-intensive security services, where mandated wage increases, sub-par performance by guard workers, and a desire to better leverage available technology has made the status quo unsustainable.

A different approach is clearly needed. "Autonomous Remote Services," or ARS, is the next generation of holistic solutions that can – as the name suggests – *autonomously* and *remotely* support the full spectrum of technologies needed to provide robust security, facility, concierge and health screening services. Through the use of interactive, cross-functional robotic devices, powered by intelligent, self-learning software, ARS will enable guard companies to restructure their contracts with customers, integrators to expand and repackage their breadth of offerings, and end-users to benefit from superior security services at a lower cost.

> Autonomous Remote Services – as the name suggests – *autonomously* and *remotely* support the full spectrum of technologies needed to provide robust security, facility, concierge and health screening services.

What follows is a vision for the widespread adoption of ARS, a discussion of its anticipated impact on the $50 billion security industry and a framework to help guard companies and security integrators begin constructive conversations with customers about this exciting new paradigm.

AN INDUSTRY IN FLUX

THE TITLE OF *Security Magazine*'s recent state-of-the-industry report says it all: *2018 Guarding Report: Changing Times for the Guarding Industry*. Based upon conversations with high-ranking executives representing guard service providers, technology manufacturers and companies that employ guard services, the magazine identifies several common themes.

First off, customers are demanding a new level of Guard Services. Basic patrolling is no longer enough; they want services that leverage today's updated technologies and officers who know how to use them. An example of that mindset is voiced by Nancy Bentley, Senior Director, Security Services and BCP for Northwestern Mutual, who says, "We really are looking at hiring security officers that have much more of a technically savvy mindset." She seeks officers who can take advantage of the evolving security technology being used to secure Northwestern Mutual's facilities.[3]

A second theme, echoed throughout the report, is how crucial training is for developing higher caliber, tech-savvy officers. Tom Conley, President and CEO of the Conley Group and a security and risk management expert, says that in today's security environment, traditional, minimum wage level guards "bring no value to an organization … They're putting a uniform on, but they don't have training or capabilities. The guard industry needs to transition to the security profession."[4] As a customer, Daniel Ryan, Vice President of Security for Brookfield Properties Retail Group, says that his organization wants all security officers guarding its properties to be trained and capable.[3]

Thirdly, the magazine addresses the growing use of robots as a cost-effective and viable alternative to human guards for certain situations and tasks. This theme is echoed in other articles throughout security trade press. A post on *SecurityInformed.com* entitled *Robot Revolution, Uncovering the Real Value of Security Robots*, explains that "more mundane jobs typically associated with remote locations [can be] reassigned to robots, thereby saving human

---

[3] Security Magazine, December 2018, 2018 Guarding Report, Changing Times for the Guarding Industry, Ed Finkel
[4] Security Magazine, December 2018, 2018 Guarding Report, Changing Times for the Guarding Industry, Ed Finkel

ability to be used in more important tasks, such as within a security operations center, where sensors [on the robots] can be evaluated and possible threats can be more effectively thwarted. [Also], there are a number of dangerous jobs out there that require humans to be present, but many security-related roles can see significant risk to workers reduced by implementing robotic guards in their place."[5]

A fourth issue that has come to light since the outbreak of the current pandemic is the need for more flexible options in how, and from where, security systems are monitored. The physical design of the traditional SOC, with its monitoring stations packed closely together, makes it incompatible with social distancing guidelines. Just as physical attendance requirements are being rethought for other types of office workers, the same holds true for security staff. Workers can better focus on their jobs when they feel safe and are not distracted by concerns that their health might be compromised by the air they breathe or the surfaces they touch. A recent article in *SDM Magazine* addresses these points, while also spotlighting the flexibility that cloud-based monitoring solutions bring to bear in facilitating remoting monitoring capabilities[6].

> _____
>
> Customers are demanding a new level of Guard Services. Basic patrolling is no longer enough; they want services that leverage today's updated technologies and officers who know how to use them.
>
> _____

TOO NARROW A VISION

THE STATE-OF-THE-INDUSTRY REPORT makes clear that major changes are afoot in the guarding industry. We, in the nascent Autonomous Remote Services industry, couldn't agree more. However, here's where we part ways.

The future business models proposed, thus far, fall short. They are trapped within the confines of existing paradigms – basically trying to "work better with what we've got." This is typical of the security industry, which is often at the forefront of advocating for technological change and

---

[5] Security Informed, Robot Revolution: Uncovering the Real Value of Security Robots, Steve Reinharz
[6] SDM, March 2020, Companies Adapt During Crippling Coronavirus Pandemic, Courtney Wolfe

yet, when it's time to put its money where its mouth is, lags behind many other industries in actually adapting it.

To summarize, these models rely on:

1. **More extensive use of complex facility-wide third-party systems** in the delivery of guard-related services
2. **Exhaustive and expensive training of guards** so they can manage those systems
3. **Customized, deeper integrations** between those systems to provide better monitoring intelligence to guards
4. **The use of robotic guards** to handle the most mundane tasks, like patrolling, or those that would expose human guards to inherently dangerous physical conditions, such as toxic environments

In short, these visions advocate for adaptation rather than transformation.

At the same time, one adaptation that we have recently seen in response to the COVID pandemic is a cornerstone of Autonomous Remote Services, our own model for the future.

The flexibility to monitor and manage systems remotely, made possible through cloud platforms, is not only key to maintaining continuity of security operations in an emergency, but can also provide cost savings and efficiencies under normal conditions.

THE ARS TRANSFORMATION

AUTONOMOUS REMOTE SERVICES represents a wholesale business transformation of the security guard industry. It's a pure, Fourth Industrial Revolution application of how we should be thinking about the best ways to deliver security, facility, concierge and health screening services – by engineering solutions from the ground up. Forget about how humans have traditionally managed those operations! ARS is the culmination of technology and engineering to seamlessly

combine communications, artificial intelligence, hardware, software and people-power. As a result, it is uniquely capable of delivering the most efficient and cost-effective security services, impossible to match through the use of legacy solutions.

ARS empowers security decision makers with the ability to save costs while blanketing their facilities with unprecedented levels of security and safety. Furthermore, these can include COVID-related health screening and monitoring functions, all performed while minimizing virus exposure and transmission to employees and security guards.

The diagram below represents the novel approach ARS brings to the convergence of security technology and services. Rather than attempt to bring third-party technology systems under the auspices of facility or IT services (as in the 2010 decade), ARS embodies its own proprietary technologies and services within a single, fully functional silo, delivering powerful, effective and streamlined results. Facility-wide security technology systems may still exists, in tandem, but are not part of the ARS ecosystem.

ARS' combination of dedicated, proprietary hardware, powered by robust cloud-based software, revolutionizes the legacy security integration business. Disruptive contracting projects will be challenged, as ARS' connectivity via 4G LTE, and soon 5G, requires no network infrastructure. This is a typical example of how the Fourth Industrial Revolution immediately replaces what was done in the Third Industrial Revolution.

Multi-functional capabilities, pre-integrated within the platform, are delivered via a range of ARS hardware devices that are site and task appropriate. ARS technology, along with a much smaller but more capable human guard force, can perform any number of complex service-related tasks. The underlying technology is easy to manage, purpose-designed, and empowers human security officers to engage in their security service roles in more interesting, more responsible ways – without undergoing extensive training. ARS can do all this because its technology is NOT intended to replicate the capabilities of a facility's more mundane, site-wide systems that are used for forensic surveillance, interior door access, and other non-service functions.

> ———
> ARS embodies its own proprietary technologies and services within a single, fully functional silo, delivering powerful, effective and streamlined results.
> ———

WHAT DOES ARS LOOK LIKE?

THAT DEPENDS on what you need it to do, but ARS-based solutions can substitute for many guard post-related services including typical intrusion detection and response functions, intelligent automated gate entry and the handling of a host of automated orders. The results are equally, if not more, effective. What's different is the dynamic balance between the humans and technology involved, and how each are deployed.

The physical hardware of an ARS system – which serves as a conduit for delivering software-driven services – can take any form factor. Free-standing towers can serve as intelligent multi-function kiosks. Gate stanchion units focus on ease of use for vehicles. Wall units may be conveniently located near doorways. Mobile units – either autonomous ground vehicles and airborne drones – can offer roving, flexible coverage. These are just examples. Hardware configurations will continue evolve to meet customer needs.

All devices operate on a shared ARS cloud software platform that brings together an array of integrated sensors and features including 2-way video, audio and data communications. The proprietary platform is a like a Swiss Amy Knife of security technologies – simple, easy to use tools that are packaged together and, when combined, can help to deliver any security, facility, concierge or health screening service – albeit in novel ways. (We'll provide some concrete examples in a bit.) When managed by capable security personnel, ARS is a force multiplier that enables far fewer humans to deliver superior services on a much larger scale, including across multiple sites simultaneously and from flexible monitoring locations.
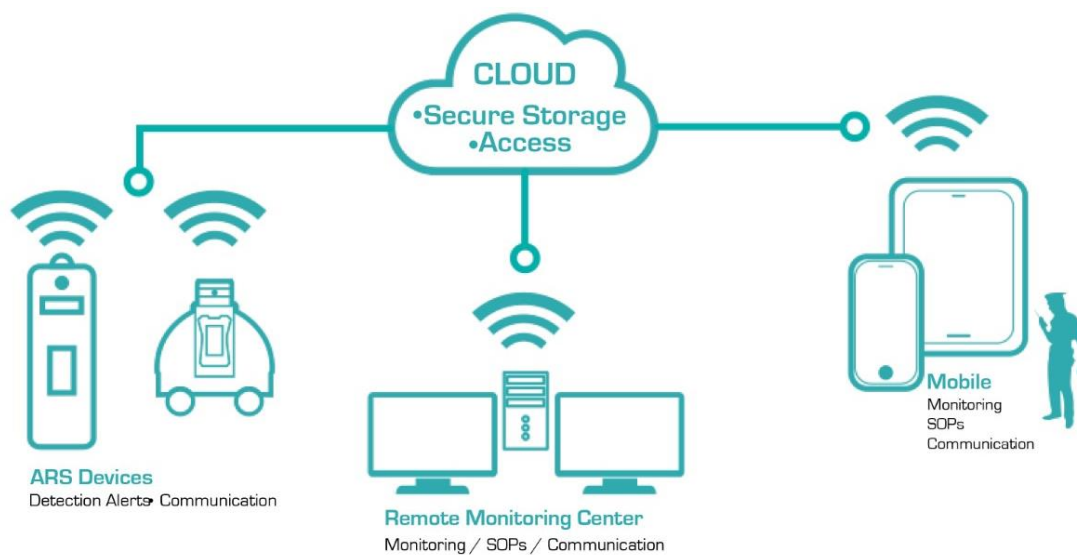
Essential to its identity as a fully functional, turn-key service solution, ARS is fundamentally designed to operate independently from its property host' networks, although facility-provided communications be still be used. Unlike traditional in-house security technologies, all ARS communication is optimized for transmission over cellular. This is a significant technology achievement given the limits of 4G LTE and the massive demands of video. The cloud-based ARS platform has been designed to deliver highly responsive, low-latency transmission exclusively through mobile connectivity. In terms of installation and configuration, there's minimal work involved. Devices can be up and running almost instantaneously, with no involvement or concerns from in-house IT staff. Plus, as software is upgraded or new features introduced, the cloud platform keeps all systems current without the need for onsite maintenance.

INDUSTRY IMPACT

UNTIL NOW, guard companies have been in the business of managing people. Whether part time or full time, people are expensive. *Guard Force Trends: Multipliers and the Market*[7], published in the April 2019 issue of *Security Management*, provides wealth of insights.

Before an officer earns a single dollar for his employer, there are out-of-pocket costs to advertise, interview, screen, hire, onboard and, of course, train him. Then there's high turnover, which has been reported to range from 100% to 400%[8] for guard positions. Although the replacement cost per employee is lower for hourly workers like security guards than for salaried employees, the exceedingly high turnover rate, combined with the expense of recruitment and extensive training, adds up – potentially equaling the cost of a full additional salary.[9] New public policies, like ACA mandated healthcare and paid sick leave, are additional expenses. Even more burdensome are the penalties incurred when guarding companies fail to provide adequate meals and rest breaks. Now comes COVID-19. The expense of paid – or unpaid - time-off for employees who are either sick or quarantined for lengthy periods is boosted by the need to pay overtime to healthy employees assigned to cover for their out-of-commission colleagues. And, as we've already addressed, a new breed of security officer will justify a higher salary and more extensive, non-billable training in order to support the changing nature of his job. This, in itself, is a foundational requirement of the Fourth Industrial Revolution: changing the nature and earnings of employees as they move from low-skilled jobs that can be automated, to technology-skilled positions that create, manage and monitor those new, automated systems that have replaced them.

---

[7] Security Management, April 2019, Guard Force Trends: Multipliers and the Market, Joseph Ranucci
[8] Security Magazine, September 2004, Turn Away Turnover
[9] Peoplekeep.com, Employee Retention – The Real Cost of Losing an Employee|2019, Christina Merhar

It's no wonder that, as of 2018, the US Census Bureau was predicting that the guard industry would experience slowing growth in the coming years, with year-over-year revenue growth below 1.5%.[10] This prediction is obscured today as guarding companies show revenue growth, mainly through acquisition. But fundamental challenges persist: As hourly labor rates increase, these hikes can't just be passed on to the customer. This is more true now than ever, as our society struggles to adapt to economic conditions not seen since the Great Depression. Budgets are being slashed, leaving security practitioners with no choice but to use new technologies that can do more with less.

It's this approach – leveraging novel technologies to do more with less – that defines the ARS movement and its attendant business model, offering a win-win to customers and guard companies alike. While industry revenues will decline, profitability can be maintained or even increase as ARS spawns new markets for security services as well as channels for delivering them.

THE TIPPING POINT

IF YOU SEARCH the web, you'll find statistics that indicate just a few players dominate the guarding industry. These companies are huge! But if you're in the industry, you know how those numbers can be misconstrued. In fact, there are new entrants to the market on a regular basis, many founded by former executives from those big companies who want to break away and run their own business. The market is brimming with successful local and regional entities.

These smaller companies, many of them newly minted, are being run by executives who must innovate to survive and compete. ARS makes it easier for them to do so, by reducing the barrier to entry with exponentially less risk and upfront investment. While employing far fewer

---

[10] US Census Bureau, Statista 2018

employees, they are able to offer a "security-in-a-box" solution that is quick and simple to install, leverages technological capabilities beyond what on-site humans can do, allows for a combination of autonomous and remote management, and does all of this at a surprisingly affordable price. Clients save money while providers make more money. ARS not only allows them to compete successfully with larger guard companies for new contracts, but opens doors to customers in new markets who, in the past, assumed that paying for such services was beyond their budget.

The "big boys" are taking notice too. It obviously takes longer for large multi-nationals to pivot, but ARS is slowly making headway as the major players test the capabilities of ARS within their own facilities and introduce it to select customers. Once momentum grows, we will quickly reach a tipping point at which ARS becomes the new normal.

LEAD OR BE LEAD?

LARGE OR SMALL, it is the guard companies who accept the premise that *business transformation is in progress*, and choose to transform *now*, who are destined to become tomorrow's leaders. The ARS market delivers long-lasting benefits and competitive advantages over those who fail to adapt. Compared to traditional guard services, early ARS evangelists will be able to provision additional high-value services that:

- **Increase profitability**. These companies will be able to support more customers with less infrastructure, growing revenue without scaling up. They will also be better positioned to protect their own workforce from exposure to health risks, which ultimately keeps wages, insurance and overtime in check.

- **Deliver superior service and additional services.** Less mistakes will be made due to human oversight or boredom, as ARS solutions automate the more tedious tasks.

- **Reduce the barrier-to-entry** for cash-strapped clients who must balance the need for security with other pressing business expenses – a challenge magnified by the COVID economy.

- **Distinguish their organizations as forward-thinking**, staking out ownership of the ARS category and its uniquely relevant security solutions, thereby differentiating themselves from the competition.

- **Bring greater job satisfaction** to their workforce. More interesting guard jobs, managing ARS systems, will translate to happier employees and lower turnover.

With so many reasons to embrace ARS, the next logical question for guard companies is how to sell it. How do you communicate to your customers the value that ARS delivers, in language and a framework they will appreciate?

SELLING ARS

FOR SALESPEOPLE accustomed to selling guard services in the traditional sense, moving to an ARS model may, at first, seem a bit intimidating. Certainly the sales process and sales cycle changes when selling ARS. In legacy times the primary buyer is the security practitioner and finance; in the Fourth Industrial Revolution era, the buying group increases to include risk, facilities, IT and ultimately the senior executive management. Similar to how security guards' skills will be upgraded, security company sales staff skills will need to be upgraded.

> In the Fourth Industrial Revolution era, the buying group increases to include risk, facilities, IT and ultimately the senior executive management.

The list of benefits to the customer will help sell itself, while dampening any potential objections that might arise from various stakeholders. Advantages to customers include:

- **ARS offers superior security** by bringing autonomous responsivity and remote connectivity to incidents in real time with minimal investment or complexity.

- **ARS poses no burden on in-house IT staff.** The technology is self-contained, requires no network connectivity and minimal infrastructure support.

- **Pricing is simplified,** with services and maintenance of all systems, including software updates, quoted as a single a price. Plus, the investment is futureproof, as cloud software is kept ever current and new capabilities are introduced to the platform and supporting hardware.

- **ARS delivers a superior employee and visitor experience** as they interface with systems. In many instances, interactions with the technology are more efficient, safer, accurate and less intrusive than dealing with a human.

- **ARS offers lower out-of-pocket costs and increased ROI** over time. Once you quote an ARS system, this point will become obvious to the customer.

Although technology driven, ARS is still a service, sold and delivered through trusted security partners. While consulting with customers, present some of ARS' functionality that simply doesn't exist in legacy solutions' bag of tricks. Become a subject matter expert so you can offer true value and help guide your clients to fully utilize the ARS solution while completely solving existing challenges. Understand the workflow that's required, both in "normal" and "not normal" scenarios. Then, strategize how ARS can make it happen. Here are few examples:

VISITOR MANAGEMENT | The Traditional Way

Managing visitor access to a building is one of the most common assignments for a security guard. Visitors arrive through a main entrance and provide identification. If they are pre-registered as a guest, they are may be issued a badge. If not, then they are – in some cases – checked against a blacklist, asked to provide some basic information, have their ID checked, and then often issued a badge. The host is contacted, arrives at the door, and escorts the visitor inside.

This is the way we're all used to dealing with visitor management, but it's hardly an ideal solution. From a security perspective, human guards do not usually have the time or resources to carefully vet each visitor against bolo lists. Most folks are getting a badge, whether or not they should. From a process perspective, it's inefficient. The guard must take time to contact each host to alert them when a guest arrives. The host may need to be paged and tracked down. If the guest is unexpected, the call may take some time as the visitor explains, through the guard, why the host should come meet them. And, if the visitor is pre-registered, he or she still has the hassle of checking in and providing ID – which can take a while if they're waiting behind an "unexpected guest." Finally, from a personnel perspective, it's wasteful. If a building has more than one entry point for visitors, or multiple buildings, separate guards must work at each location.

VISITOR MANAGEMENT | The ARS Way

ARS offers an enhanced version of visitor management that provides a higher level of security, greater convenience for visitors and staff, and requires less people-power and significantly less cost. A single reviewing officer can be responsible for a large number of buildings or entry points. Here's how it works.

Arriving visitors approach an unmanned kiosk equipped with technology connected to the ARS cloud platform. It may feature a video and/or still camera, two-way audio capabilities, a touch screen, maybe a fingerprint reader (or other biometric device), a QR scanner, and possibly other hardware. Much depends on how the customer wishes to identify visitors. Remember – ARS is flexible. The kiosk is also connected a nearby badge printer.

At the kiosk, visitors identify themselves. If they are pre-registered, they may already have already received a QR code on their phone which they can present to the kiosk's camera or scanner. If they are not pre-registered, they will be guided through an automated registration process at the kiosk. This might involve presenting a license or photo ID to the kiosk's camera, completing a short form on the touch screen, having their photo taken or fingerprint scanned, and waiting a few seconds while their identity is checked against a list of prohibited guests. ARS

communicates with the badge printer, issuing badges for approved and pre-registered guests. ARS unlocks the main door, providing entry to an interior waiting area. Hosts are automatically contacted, via text message, and informed that their guest has arrived. If, at any point during this process, a problem arises, a live guard can intervene, via video, chat and assist the visitor. Working from a remote location, the guard can be responsible not only for this site, but many others simultaneously.

As you can see, the process of managing visitor access translates perfectly to ARS. The majority of the workflow is handled **autonomously**, any unexpected or non-standard issues can be addressed **remotely**, and all of this is provided as a turn-key **service** by a kiosk that requires little more than being rolled into place. The customer wins, and saves, when used at just one location, but the savings are exponential when deployed across a campus or multi-site operation with multiple points of visitor entry.

SOC MONITORING | The Traditional Way

Facility-wide surveillance, access control, intercom and paging, incident tracking and other technology systems have typically been managed through a centralized Security Operations Center (SOC). The prevailing designs for these centers are outdated, unnecessarily expensive and complex, often delivering capabilities that are more relevant for forensic analysis and reporting than live monitoring. Costs for a modest "starter" SOC can run upwards of $250,000 when considerations are made for space, power backups, PC hardware, network infrastructure, redundancy and receiving system hardened platforms.

The expenses don't end there. Learning to operate a traditional SOC requires lengthy and-ongoing education. This may be a reasonable investment when training in-house security professionals, but it doesn't make much sense for hired guards. And yet, as guard services are being asked to better leverage technology systems, hired guard workers are often being extensively trained to use a facility's SOC systems. This is overkill – a poor use of human

resources that's unlikely to deliver optimal results and often requires skills beyond the guard workers' abilities.

SOC MONITORING | The ARS Way

With ARS, management of a facility's SOC is left to the company's in-house staff. In fact, sometimes the need for a traditional SOC (along with its expense) may be eliminated completely. ARS provides guard companies with the ability to create a virtual SOC that makes equally effective, technology-aided security services possible by aggregating an array of propriety systems designed specifically for the tasks at hand.

Turnkey ARS hardware is installed at all locations that require live monitoring. These may include lobbies, perimeter doorways, elevator bays, warehouse space, loading docks, parking garages…anywhere a guard's route might take him. The physical design of the hardware

depends on its intended placement. A system may combine any number of devices, including towers, wall and overhead units, and even roving autonomous vehicles. Each is equipped with the array of cameras, sensors and communication devices appropriate for its respective location and intended use.

The feed from these units can be monitored, remotely, by officers trained on the ARS platform with much greater fluidity and ease than if using a complex traditional SOC. Depending on the system, an ARS-based virtual SOC provides operators with the same functionality as a traditional SOC, including:

- Live video on demand
- Easy call up of incident history, along with associated video and snap shots
- Alerts based on human or vehicle detection, with ability to immediately evaluate and interdict
- Two-way audio and voice or just audio, initiated from either side

- Paging, in the direction of the detected or identified event

- Digital messaging for emergencies or common facility communications

- An event archive for at least the last 12 months, stored in the cloud

- Advanced Visitor Management Remote Support

- Advanced Employee Access Remote Support

- A variety of methods to remotely unlock doors

- Advanced entry documentation

Multiple sites can be monitored at once by a single guard. In fact, the built-in autonomous nature of an ARS solution allows vSOCs to significantly improve efficiency – more systems can be monitored with less personnel. They can be securely monitored from anywhere, protecting both the worker's health and the customers' privacy. And, should a situation be identified that requires intervention, there are both remote and on-site options for response. In some cases, issues can be quickly resolved through audio or video conferencing with a remote guard. Or, on-site assistance can be quickly and automatically summoned, with video and data from the ARS platform shared with the responding officer.

In short, an ARS virtual SOC provides a powerful and cost-effective way for security guard companies to provide SOC monitoring services – either as an enhancement to a company's in-house capabilities or as a full replacement. It allows them to train their officers on a single platform – the ARS platform – which is relatively easy to use and will be deployed consistently across all customer sites. It gives them control over the technology in use, flexibility in assigning officers to different customers and juggling staffing issues, and far superior visibility and control over the spaces they're responsible for guarding. And all of this costs way, way less than attempting to leverage a conventional SOC solution.

HEALTH MONITORING | The Traditional Way

The need to monitor the health of employees or visitors as they enter a workplace or public space is new to our culture, but is probably here to stay. We've seen temperature checks deployed in a limited scope in the past; think of old news footage of airport agents scanning the foreheads of international travelers during SARS and Bird-Flu outbreaks. This time it's different. Until COVID-19 is licked, it's highly likely that we'll be submitting to temperature checks before we do everything from entering our workplace to attending a class; eating in a restaurant to shopping in a mall. These processes may not be in place yet, but they will be. In many cases, the job of checking temperatures will fall to security guards, who will also be expected to bar entrance to anyone deemed sick and to report them to the appropriate authorities. These same guards might also be expected to enforce the use of masks, or social distancing.

Traditionally, these guards would be human. Humans who could themselves be asymptomatic carriers of the coronavirus. Or could be infected by the people they are testing. They might fail to gather information on a subject who tests positive, making follow-up difficult. Or, they could be temporarily absent from their post during a break, causing a lapse in security.

HEALTH MONITORING | The ARS Way

ARS allows guard firms to deploy technology, rather than humans, to assist with front-line health screening and policy enforcement. A screening kiosk, located at all entry points of a facility, can screen all employees and visitors who present themselves requesting entry. In fact, screening procedures can be integrated with the visitor management functions to create a seamless protocol.

Here's how it works: An ARS kiosk, equipped with thermal sensors, takes the temperature of any individual who stands before it. Visitor or employee information is gathered before any scans occur, ensuring that those with a fever, and therefore denied entry, can be

identified and their information stored and shared with authorities. The kiosk can also scan for use of a facial mask and deny entry to anyone not wearing one. Should questions or a problem arise, a human guard, monitoring the kiosk remotely, can view the subject and communicate with them via two way audio, as needed.

The use of ARS eliminates exposure of a human guard to the parade of employees and visitors that require scanning each day. The scanning procedure requires no physical contact between kiosk and subjects; furthermore, the kiosk can be disinfected frequently by a simple wipe-down with an anti-bacterial agent. A single human guard can remotely monitor multiple kiosks simultaneously. The process is faster, always in place, and provides full integrity of information and accountability stored in digital form, laying the groundwork for an easier process of contact tracing when necessary. And, of course, ARS is much more affordable than its alternative. Beyond the initial purchase or lease of a kiosk, the monthly operating and monitoring fee is a smidgen of what an on-site human guard would cost. This makes it a prime example of how it will open new markets for the guard industry.

> ———
> ARS-enabled health-screening kiosks may soon be recognized as offering one of the greatest returns-on-investment for establishments trying to lure back a paranoid public.
> ———

Prior to COVID-19, many small to mid-sized companies considered the use of guard services to be a security "luxury," but are now recognizing that health screening services will be a non-negotiable expense. Employees will not come to a workplace they deem unsafe. Similarly, customers, clients, patients, shoppers and visitors will only patronize locations where they feel sufficient precautions are being made to protect their health. In-house employees will not want to be tasked with the job of "screener", and companies will be looking to guard-services for help. ARS-enabled health-screening kiosks are an affordable, turn-key solution that can be deployed immediately and, in fact, may soon be recognized as offering one of the greatest returns-on-investment for establishments trying to lure back a paranoid public.

ARE YOU READY?

FOR EVERY BUSINESS SECTOR, including security services, the Fourth Industrial Revolution, with its convergence of IoT, artificial intelligence with machine learning, robotics, high-speed data streaming and a slew of other technologies, is causing mass disruption. Those who are unwilling to aggressively think outside the box, to educate themselves about new technologies and resources, and devise better ways to serve their customers in these changing and demanding times … these organizations and their offerings will soon be white elephants.

Other industries have moved faster than security to embrace the current zeitgeist, successfully exploiting the next generation of game-changing innovations to pivot toward an ARS business model. Robotic devices already deliver food, take care of the elderly, perform cleaning services, serve as cashiers and provide customer help and support. Early adapters, who have embraced their use, have sought a competitive advantage with the expectation that ARS will deliver superior customer experience, more consistent and reliable performance and lower operating costs. The same fate awaits the security space.

> Those who are unwilling to aggressively think outside the box, to educate themselves about new technologies and resources, and devise better ways to serve their customers … these organizations and their offerings will soon be white elephants.

As the new decade dawned, the security and guarding industries were on the cusp of an ARS transformation. Security executives were aware of what new technologies could offer, and where current paradigms were falling short. Those shortcomings are all-the-more vivid in the context of our COVID economy, in which all elements of the status quo are under scrutiny – not just in how we address traditional security concerns, but in a much broader sense. Priorities have shifted, security responsibilities expanded and budgets reduced. These forces are accelerating the pace with which change *must* occur.

As has been the case in other industries, ARS transformation within the security space will rely on first movers, empowered by progressive organizations and senior management, who are

willing to throw convention to the wind; leaders who recognize that the surest road forward is not a smooth continuation of the path they've been on. It requires "jumping the curb."

Now, all of our steering wheels have been jolted. Never, in our lifetimes, have we seen the entire world change course, in so many ways, so quickly. As we seek solutions on a multitude of dimensions in light of unprecedented challenges, few are as obviously "right" as automated robotic services. The air-tight alignment between the security services we need and the results ARS can deliver will make it the security "new normal" within a world full of "new normals." To maintain legacy models for delivering security services makes as much sense as pretending that nothing has changed in how we work, how we shop, how we travel, how we learn, how we live. ARS improves accessibility to advanced solutions through reasonable pricing, high return on investment and ease-of-use. It enables guard companies to restructure their contracts with customers, integrators to expand and repackage their breadth of offerings, and provides end-users with superior security services at a lower cost.

> ―――
> The air-tight alignment between the security services we need and the results ARS can deliver will make it the security "new normal" within a world full of "new normals."
> ―――

Benefits only increase going forward. The next wave of innovation in this space will be driven by visual identification advances, allowing for evaluation of even more complex situations and more complex responses. This makes ARS not only a wise investment now, but positions its users to access new and exciting solutions on the horizon.

The brilliant Brian Solis, whose research on Digital Darwinism and its impact on business disruption and transformation, coined the mantra:

Arrogance + Ignorance = Irrelevance[11]

For the state of today's security guarding industry, that equation says it all.

―――――――――――――――

[11] LinkedIn, Brain Solis, Global Innovation Evangelist@ Salesforce, posted May 12, 2020