SIA Insights TECHNOLOGY

Volume 9, Issue 1
Summer 2021

Welcome

Dear Reader,

After placing it on a one-issue, pandemic-related hiatus, we are pleased to resume publishing *SIA Technology Insights*.

This edition is very much a reflection of the time. The lingering effects of the pandemic and its impact on security operations – from touchless access control to temperature screening – form key parts of several of the articles, including the lead story, simply headlined, "The Year that Changed Security."

Of course, the past year changed not just security, but nearly everything else, as well. To varying degrees in the United States, we have returned to pre-Covid life, but certain changes will be lasting. So it is with security technology, with some of the adaptations and innovations born of necessity having been found to be beneficial even without the imminent threat of a virus.

And, if you need a break from the topic that has been dominating much of our lives, you can find non-coronavirus articles here as well, including a provocative piece that closes the issue about security technology evolving from detection to intervention and prevention.

If you have any comments, questions or article proposals, please contact our editor, Ron Hawkins, at rhawkins@securityindustry.org. And if you are currently reading a hard copy of *SIA Technology Insights*, remember that you can view and share all articles – past and present – by visiting www.securityindustry.org/techinsights.

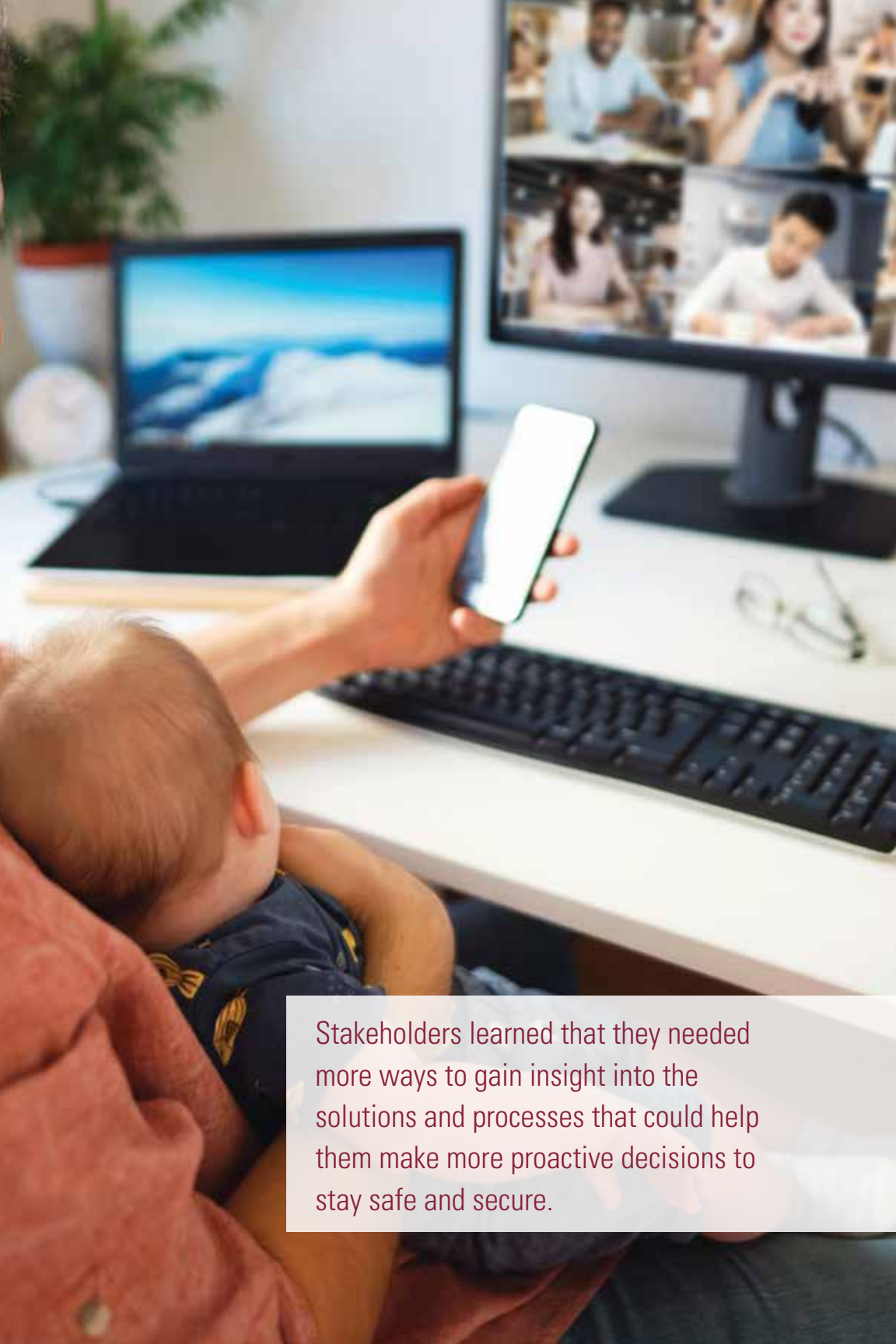
Thank you for reading.

Sincerely,

Pierre Trapanese
Chairman, Board of Directors
Security Industry Association

Don Erickson
CEO
Security Industry Association

Table of Contents



Stakeholders learned that they needed more ways to gain insight into the solutions and processes that could help them make more proactive decisions to stay safe and secure.

The Year that Changed Security

How the pandemic shaped the uses of technology in 2020 and going forward

By Alan Stoddard
Cognyte Software North America

To say that the year 2020 was challenging is a huge understatement. In March of last year, the COVID-19 pandemic disrupted life around the world. Regular business operations and the economy came to a halt. Businesses such as those in retail, stadiums, casinos, hotels and restaurants were particularly hard hit. Unemployment spiraled, as did frustration and discord.

In June, organizations in the U.S. private and public sectors were under mounting pressure to restart their operations as quickly as possible in order to compensate for lost revenue and jumpstart the economy. With social distancing and other measures in place to help reduce the spread of the virus, organizations turned their attention to a critical question: "How do we resume operations while protecting the health and safety of our employees, customers, partners and community?"

In the absence of defined contingency plans, industry standards, or regulatory guidance, businesses sought new ways to address these

challenges and focused on how Internet of Things (IoT) and security devices, mobile applications, and cloud solutions could help them achieve their goals. Stakeholders considered what "after the pandemic" would look like, when employees returned to the workplace under a very different set of circumstances.

This journey required a critical element: the insight to adapt. As organizations restarted operations, they had to consider many factors. Adjusting to rapidly changing situations demanded an approach that addressed the potential threats while instilling confidence that meaningful steps were being taken. They needed a strategy that kept people safe and healthy, and also ensured that operations could run smoothly. As circumstances evolved, adapting to daily changes and implementing workplace health and safety tools were essential to staying in business.

Adjusting to rapidly changing situations demanded an approach that addressed the potential threats while instilling confidence that meaningful steps were being taken.

There was an increase in the deployment of mobile applications to provide remote health checks of employees. Security and IT managers saw a sharp rise in new IoT use cases as businesses implemented new processes. The underlying driver to everything was that access to information was critical, as was the ability to respond quickly to situations (such as outbreaks), and connected, intelligent digital transformation plans would be beneficial.

Overall, stakeholders learned that they needed more ways to gain insight into the solutions and processes that could help them make more proactive decisions to stay safe and secure. Moving into the next wave of IoT, data capture and analysis, here are some of the ways in which organizations are expected to leverage this technology.

Tackle Mission-Critical Challenges

The challenges are different based on industry, physical infrastructure and geographic location, but all have direct effects on operational integrity. Security and IT managers must adjust their strategies for business continuity, digital transformation, and safety and security based on their specific requirements; for example, a residential building has different needs than a corporate facility. To address their challenges, organizations will leverage processes and IoT technologies in unique ways to protect people, property and mission-critical assets.

Focus on the Things That Are Within Control

A focus on protecting what matters most depends on an organization's direction, but it always incorporates employees, processes and property. Maintaining vigilance over current risks while ensuring safety and compliance is critical to ensuring high levels of protection. Minimizing disruptions can be achieved with an IoT-centric, scalable approach that enables businesses to support operations and protect highly dispersed teams.

Implement Processes and Policies That Are Unique

Adaptability is critical – whether in regard to regulations, standards, procedures or new technologies. Technology is essential to ensuring a high level of safety and health, and now it plays a more vital role than ever. For example, mobile applications on IoT devices are being used to provide remote health checks of those entering a building, while collaboration tools enable security leaders to work together seamlessly even when in different locations. These immediate access points to information help leaders to be more proactive with health planning and ensure awareness of new and ongoing issues.

> Minimizing disruptions can be achieved with an IoT-centric, scalable approach that enables businesses to support operations and protect highly dispersed teams.

Remain Pragmatic Above All Else

Luckily, several solutions were brought to market to make reopening

easier. Some focused on managing and monitoring temperatures through video, others on social distancing and utilizing health and safety intelligence platforms that provide complete oversight across a given environment. No matter the function, all of them help leaders realize more vital risk awareness, more resonant threat detection, and more in-depth insight. Used together, they helped enable facilities to get up-and-running quickly through the development of effective return-to-work strategies.

In 2020, we learned that adaptability is critical. In 2021, we know that the ability to embrace change quickly and effectively improves efficiency and operations. Knowledge, contingency plans and technologies are essential parts of proactively preparing for future challenges. As we continue to recover from the effects of the pandemic, maintaining this awareness will enable security and business leaders to be better positioned to implement protective measures and provide much-needed peace of mind. ■

In 2020, we learned that adaptability is critical.

Alan Stoddard (alan.stoddard@cognyte.com) is President of Cognyte Software North America (www.cognyte.com).

When properly managed, the cloud enables organizations to enhance operations and create a proactive and reliable data strategy to mitigate risk and make intelligent decisions.

Moving Video Security to the Cloud

Whether public, private or hybrid, cloud technology can offer functionality and flexibility

By Nigel Waterton
Arcules

The use of the cloud is increasing globally as more organizations look to reap the benefits of this flexible and scalable service-based business model. The growth of cloud-based business functions allows for security-as-a-service (SaaS) options that had previously been unavailable, especially for small to medium-sized businesses. A recent global video surveillance-as-a-service (VSaaS) report by Data Bridge Market Research estimates the market will exceed $11.16 billion by 2026, registering a compound annual growth rate of 21.9 percent from 2019 to 2026.

This increase is primarily due to the SaaS approach, which shifts the burden of data maintenance and infrastructure spending to integrator partners looking to incorporate recurring monthly revenue into their business model. However, there are still some uncertainties about cloud-based security. This article will look at all aspects of cloud-based services for growing businesses, including the benefits of the technology and the options that are available.

Why Consider the Cloud for Video Surveillance?

Cloud-based video surveillance can be a highly valuable option across several vertical markets. But it has not always been seen as such. For most in the security industry, the term "cloud" has evolved from an unknown or vaguely understood technology into a comprehensive service that can provide significant value. The cloud has proven to be a highly functional, flexible and convenient technology that businesses can leverage as part of their strategies to protect and modernize their facilities. When properly managed, the cloud enables organizations to enhance operations and create a proactive and reliable data strategy to mitigate risk and make intelligent decisions. In addition, the cloud provides numerous other benefits, including:

Centralization. One of the most valuable components of the cloud is its ability to allow users to access information from anywhere on a range of connected devices. All pertinent data is aggregated into one platform. In the event of a crisis – whether security or business-related – stakeholders can obtain the most relevant and up-to-date information in minutes.

> While the security of data in the cloud is a highly discussed issue, the fact is that, with proper protocols in place, the cloud can enhance data protection.

Scalability and Flexibility. Video is a valuable tool for any organization. As a business grows and its technological systems become more advanced, using a cloud solution to store and manage video data allows for rapid adjustment and agility, reducing the complexity that might come with expansion. With the cloud, stakeholders can gain more insight into daily operations and ensure that all organizational and security goals are met.

Data Security. While the security of data in the cloud is a highly discussed issue, the fact is that, with proper protocols in place, the cloud can enhance data protection. By utilizing vulnerability testing, password etiquette, software patches, and encryption, stakeholders can protect sensitive data from bad actors. Additionally, public cloud providers have invested significant efforts into ensuring their networks are protected and provide maximum uptime.

> The addition of cloud functionalities can save a business significantly on the cost of server hardware and installation while offering a breadth of additional advantages like scalability.

Automatic Updates. The cloud relieves IT departments of burdens related to system management,

as upgrades and security fixes are automatically installed. Cloud services are therefore exceptionally beneficial for organizations with small – or nonexistent – IT teams.

Cost Effectiveness. The investment in a cloud services model can be much more affordable than a hardware-based model. Deploying a cloud-based solution substantially reduces the upfront capital investment by introducing more of a service-based arrangement.

Evaluating bandwidth is a critical step in determining the right kind of cloud-based service to meet an organization's needs.

Options for Incorporating the Cloud

Traditional, on-premises surveillance solutions require organizations to use proprietary architecture to run the system within their own data center. Therefore, all security operations and monitoring take place in-house. Several types of businesses prefer to control all decision-making and data handling, making an on-premises solution ideal for a customized configuration that is unique to the organization's needs. However, businesses and facilities that are interested in incorporating the cloud into their overall security posture have three options to consider.

Private Cloud

The private cloud offers the usability, scalability and flexibility for which the cloud is known and is a

viable option for those businesses looking to adopt cloud technology on their private network in order to limit access to outside users. The private cloud, however, is not without its limitations. The oversight and management of this storage solution require extensive training and knowledge of best practices for protecting the data being transmitted. In general, private cloud systems have a higher cost of ownership due to the required hardware investments and maintenance costs.

Public Cloud

The public cloud refers to the delivery of hosted services over the internet, making it possible to shift the storage and management responsibility to a service provider. The public cloud is an optimal surveillance solution for SMBs looking to gain scalability and flexibility when it comes to streamlining video and business operations and identifying the most prominent risks facing the organization. If an organization is looking to centralize surveillance and data management, the public cloud is an excellent choice. Cloud solutions also provide automatic updates and a long-term relationship with the integrator for continued support. However, the public cloud may not be the best option for businesses lacking the bandwidth required for streaming footage. The cost of streaming video 24/7 can add up, and if a business demands extensive live viewing, an on-premises solution could make more sense.

Hybrid Cloud

Hybrid cloud models allow for a mix of on-premises, private and public cloud services. Forrester defines a hybrid cloud solution as "one or more

public clouds connected to something in my data center." That thing could be a private cloud or a traditional data center infrastructure. Workloads and data are then able to move freely between the various pieces, creating an advantage for those looking for a balance between the two options mentioned above – and a solution that is tailored to their needs. For example, if demand increases and exceeds the limits of an on-premises solution, the cloud solution can take over.

Additionally, while many locations are a good fit for an on-premises solution, the addition of satellite offices across a city, state or even country can change things. In this case, the addition of cloud functionalities can save a business significantly on the cost of server hardware and installation while offering a breadth of additional advantages like scalability. A hybrid cloud solution might not be the right fit, though, for an organization that requires very high speeds and large amounts of data transfer, which can create integration and capability issues. Hybrid cloud models also still require cloud expertise and management through an IT team, which may not be readily available within an organization.

Implementing a Cloud-Based Service

Despite the adoption of cloud-based services in multiple areas of organizations (think about how one saves files, conducts business, and communicates with coworkers), many of these same businesses have resisted adopting the cloud for

physical security. However, for those organizations ready to take this step, there are several things to keep in mind.

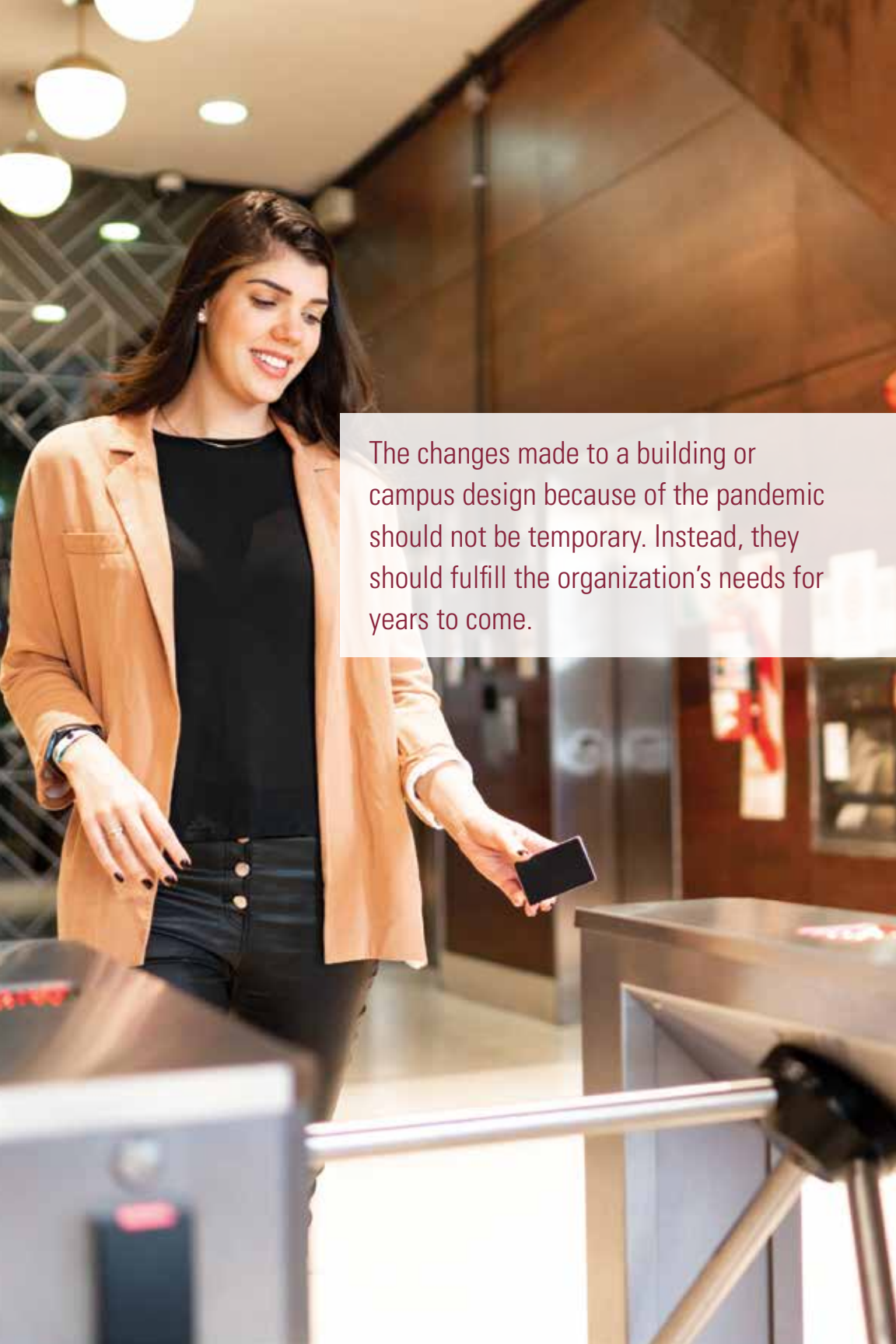
Evaluating the business model is an essential first step. Before pursuing a cloud-based physical security service, leaders should answer several questions: How many locations need to be incorporated? How many cameras per location must be integrated into the system? Are there insights that can be captured that would help a business streamline operations? What level of support is required?

Evaluating bandwidth is a critical step in determining the right kind of cloud-based service to meet an organization's needs. Low bandwidth can cause issues with the amount of data the network can handle at one time, significantly reducing the user's ability to access critical data when it is needed.

It is also essential to determine the level of support needed within an organization. For many, the service-based model can help ensure high levels of system oversight – beyond the regular security updates – to include regular monitoring. To determine this, users must identify who will be responsible for using the system. Again, this will help give partners a better idea of what will be needed in terms of support.

In short, users should find a platform that will mold to their business model. Every organization is different, so it is critical to identify a cloud-based service that can be tailored to its specific needs and to find a partner who can meet its unique service requirements. ■

Nigel Waterton (nigel@arcules.com) is the Chief Revenue Officer of Arcules (www.arcules.com). He is also a member of the SIA Executive Council.



The changes made to a building or campus design because of the pandemic should not be temporary. Instead, they should fulfill the organization's needs for years to come.

Touchless Entry Is Here to Stay

Modifications to building access promote both security and safety

By Greg Schreiber
Boon Edam

The COVID-19 pandemic has had an immense impact on nearly every aspect of our lives, including how people interact and perform their jobs and even how buildings are designed. The goal of all these changes? Reducing human-to-human contact and, thus, slowing or stopping the spread of the virus. As a result, businesses are challenged to find new ways to open their doors again while providing a hands-free entry experience – all without compromising security.

As organizations develop return-to-work plans, there are several common and necessary security requirements, including "future-proof" designs that support social distancing and touchless entry. The changes made to a building or campus design because of the pandemic should not be temporary.

Instead, they should fulfill the organization's needs for years to come.

Why is Controlling Access Important?

A prerequisite to discussing a new lobby design with increased safety

and security in the post-pandemic world is examining *why* it is critical for organizations to control access in the first place. What would happen if an unauthorized person were to infiltrate a building's lobby? The potential risks and liabilities include, but are not limited to:

- Theft
- Loss of productivity
- Violence
- Loss of life
- Civil lawsuits based on a failure to fulfill "duty of care"
- Regulatory fines for non-compliance (HIPAA, NERC, etc.)

While organizations often deploy various physical security solutions (guards, access control systems, cameras) in an attempt to mitigate unauthorized entry, if these technologies are used in conjunction with swinging doors, then infiltration is still possible. "Tailgating" occurs when someone presents a valid credential at a swing door, opens it, and either holds the door open for others or is followed by an unauthorized person who "catches" the door before it closes and gains access. When it comes to mitigating tailgating and unauthorized entry, building designers and security professionals must answer two key questions to

> Security professionals may want to *deter* tailgating at the fence line, or outer perimeter, *detect* tailgating in the lobby, and *prevent* tailgating on an upper-level floor holding restricted data or records.

decide on the appropriate physical security strategy for a facility:

1. Who is in the building at any given moment?
2. How many unauthorized people are acceptable in the facility?

Answering these questions reveals an organization's stance on tailgating. Do they want to deter it? Detect it? Or completely prevent it? And it is acceptable to have more than one strategy – a layered approach – across multiple areas of a building or campus. For instance, security professionals may want to *deter* tailgating at the fence line, or outer perimeter, *detect* tailgating in the lobby, and *prevent* tailgating on an upper-level floor holding restricted data or records.

Sophisticated security revolving doors and turnstiles provide significant benefits over traditional swinging doors in that they effectively mitigate tailgating while also reducing the burden on the people and processes needed to keep a building secure. This allows guards to focus on visitors, rather than on monitoring the lobby.

Changes in Design Post-Pandemic

When planning a lobby for a post-pandemic landscape, there are two key design elements to consider:

1. Assessing the building population and creating separate entry and exit points
2. Supporting and reinforcing distance by design

Every organization funnels different types of people through their building or campus. Some lobbies process only employees while others handle both employees and visitors. Some buildings are open to the public and others might receive deliveries in the lobby. The lobby tends to be a multi-functional space utilized by a large variety of people. And, while traditional security strategies endorse a single, secured entry point for controlling access, today's "new lobby" requires multiple entry and exit points as a means of reducing congested, two-way traffic by spreading people flow across the entire building.

The first step to creating separate entry and exit points is to identify and categorize the building population,

then determine where and how each set of users should enter the building. For instance, can employees be directed to separate employee-only entrances so that the lobby can be used just for visitors and deliveries? Is there an opportunity to funnel employees through different entrances around the building, like office workers through the left side and factory workers through the right? Should packages be received at the back of the building rather than in the main lobby?

Another consideration is designing the flow of people to support and reinforce social distancing. There may be an opportunity to space out work areas, eliminating open office layouts in favor of more private cubicles or small offices. Designers can position furniture to provide multiple ways of moving through a building. And if office layouts cannot be adjusted, organizations may consider increased telecommuting and flexible on-site work schedules. For example, 50 percent of the population works in the office on Monday and Tuesday and the other 50 percent comes in on Wednesday and Thursday.

> The first step to creating separate entry and exit points is to identify and categorize the building population, then determine where and how each set of users should enter the building.

Rethinking Existing Security Technologies

There are a variety of security technologies that have been used in building design for decades – access control systems, cameras, elevator dispatch systems, the list goes on. It is common knowledge that these technologies are not silver bullets;

users cannot just choose one or two, install them, and alleviate security risks. Technologies must be deployed in layers and work in concert with people and processes to effectively control access. This approach still applies when it comes to the new lobby design.

Below are three technologies that have gained popularity in the new lobby for their ability to support social distancing, scan for symptoms, and "virtualize" entrance processing.

Touchless Entry

When it comes to entrances, touchless technologies are nothing new. We have seen automatic sliding and swinging doors installed in buildings across the globe for many years. With the new lobby, touchless entry is no longer optional. It is important that users touch door handles, buttons, etc. as little as possible. And, an essential requirement, the new lobby design must provide an automated entry experience without compromising on security.

When COVID-19 began and the requirement for touchless environments became urgent, many facility managers started researching ways to make all entrances automatic. A popular solution was retrofitting existing manual swing doors with low-energy, electric operators, which are typically used with wide doors for disabled access. While this can be an easy and quick fix, these automatic swing doors do not stop unauthorized entry from tailgating.

Automatic security revolving doors, mantrap portals, and turnstiles allow contactless entry without compromising security. It may not be practical to replace every swing door with an automatic security entrance, but one can consider how to deploy security doors and turnstiles as part of a layered physical security strategy at certain entry points across a building.

It is worth noting that security entrances approve or deny access based on the data they receive from an access control system. While scanning an RFID employee badge or proximity card at a turnstile is a very common way of entering a building, there are other credential or identity verification technologies today that support touchless entry, including facial recognition, iris recognition, hand-wave technology for contactless

fingerprint scanning, and Bluetooth on mobile phones.

Temperature Screening

An existing technology that has received a lot of attention in the new lobby design is thermal imaging. By placing a thermal camera in the lobby and asking employees and guests to pass by it to check for an elevated body temperature, it may be possible to screen for a virus symptom. But, while a fever may be an indicator of a sick person, it also may not be. Researching the symptoms of any virus(es) affecting the local area will help determine if this technology could be an effective means for keeping staff safe.

There are some critical things to keep in mind regarding the use of thermal cameras for body temperature screening:

- **Ineffective for mass scanning.** According to the Food and Drug Administration (FDA), thermal imaging systems are not accurate when used to screen multiple people at the same time.
- **Reduces throughput.** Using thermal cameras can significantly slow down traffic in the lobby.
- **Forces separate entry/exit points.** Because throughput will be reduced in the lobby, there may be a need to funnel different types of users through different entry and exit points to cut down on traffic. Building managers will also need to decide whether to scan for temperatures at every entry point or just in the lobby.
- **Requires a new process.** What happens if a screen shows that somebody has an elevated body temperature? What is the process? Who will carry it out?

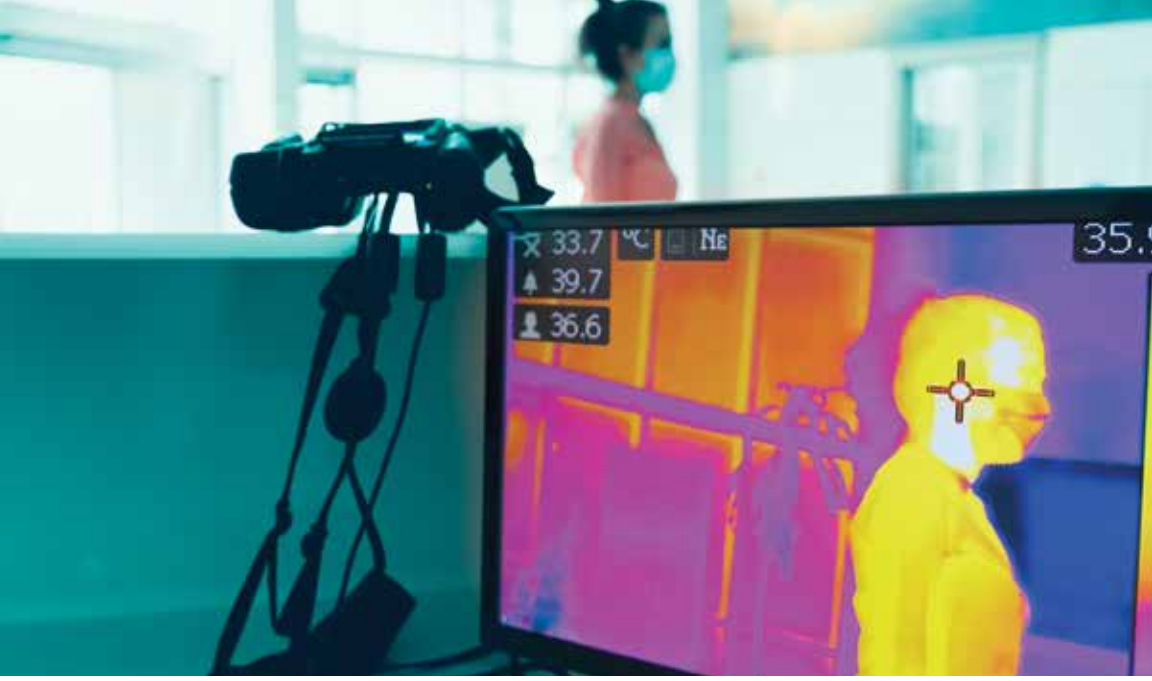
Upfitting Security Entrances

Security entrances are an effective way to deter, detect and prevent unauthorized entry from tailgating. While automatic security doors and turnstiles are effective touchless entry solutions, there are ways to make manual entrances a bit safer for users, as well. Note that all entrances are hardware that can be outfitted with antimicrobial finishes or special films to control germs and kill microbes on contact.

While automatic security doors and turnstiles are effective touchless entry solutions, there are ways to make manual entrances a bit safer for users, as well.

Manual Tripod and Full-Height Turnstiles

Tripod and full-height turnstiles require users to touch and push through the entrance to gain access to a secure area. Sleeves and braces are now available that allow users to enter by pushing with their forearms instead of their hands. Manual turnstiles require 24/7 supervision since they do not have sensors and can be defeated by jumping over the arms or by two



people piggybacking in a full height compartment. These solutions work best when used in conjunction with other security technologies, such as cameras and access control systems, and as the first "deterrence" layer in a physical security plan.

Automatic Optical Turnstiles

Optical turnstiles are automatic solutions that can be outfitted with touchless credential readers for hands-free entry. To support social distancing, some organizations design and install a large array of optical turnstiles to handle building traffic, then restrict use to every other lane. This method enables building and designing for long-term needs by installing a complete turnstile array, while also addressing immediate health and safety concerns.

Automatic Security Revolving Doors and Mantrap Portals

Security revolving doors and mantrap portals can provide the highest level of security by preventing tailgating without the need for manned observation. They, too, are automatic entrances that can be furnished with touchless credential or identity verification devices, allowing users to simply approach and proceed into the entrance while tailgaters are reliably excluded.

Short and Long-Term Planning

When designing or redesigning a lobby, consider what design elements and technologies can be used to reduce interpersonal contact and the potential spread of infection. Features should support both touchless entry and social distancing and should be able to stand the test of time, with the flexibility to offer new solutions should the need arise. Many technologies exist today that can be deployed quickly to make buildings both safe and secure. ■

Greg Schreiber (greg.schreiber@boonedam.com) is Senior Vice President of Sales at Boon Edam (www.boonedam.com).

As unique biometric traits are highly specific and difficult to steal and spoof, integrating biometric technology into the workplace for physical and logical access could be the solution businesses need to realize a new era of workplace security.

The Key to Modern Access Control

Biometric solutions can offer both security and convenience

By Maria Pihlström
Fingerprints

Meeting the security challenges of modern office environments is a complex and long-standing issue for many organizations. Businesses use a range of enterprise technologies to boost productivity, connect employees, and accommodate a more distributed and flexible workforce. However, with greater flexibility come increasing security demands – both in and outside the office.

Employers and employees alike are more conscious about privacy and security than ever before. Meanwhile, traditional security measures are no longer aligned with modern needs.

Today's workplaces require access solutions that combine convenience, simplicity and robust security, placing biometrics firmly in the spotlight.

Beyond Passwords and PINs

Relying on traditional security methods, such as passwords and PINs, is not viable long term, and the demand for more streamlined access continues to escalate. As our daily lives become more connected and digital,

60 percent of consumers feel they have too many passwords to remember, with the average person having as many as 85 passwords across all professional and personal accounts. Unsurprisingly, 40 percent admit to re-using the same password or injecting simple variations, increasing the risk of a breach.

Businesses are keen to look beyond passwords and PINs, especially as 60 percent of hacking incidents involve stolen credentials. Although passwords are currently the most common authentication method, Gartner predicts that, by 2022, 60 percent of large and 90 percent of mid-size enterprises will implement password-less authentication methods in more than half of use cases.

> By choosing solutions with on-device authentication, businesses can deliver to their employees the benefits of biometrics, without the complex administrative burden of a centrally managed and secured biometric database.

So where does the answer lie? As unique biometric traits are highly specific and difficult to steal and spoof, integrating biometric technology into the workplace for physical and logical access could be the solution businesses need to realize a new era of workplace security.

Securing Convenience with Biometrics

In the workplace, biometrics can secure a wide range of devices and access points, from laptops, PCs and peripherals to access pads and key fobs. Biometrics can offer a standalone authentication method or be part of a multi-factor approach, providing an additional layer of security to existing solutions without hindering user convenience. They can also offer personalization benefits. Once authenticated, users can instantly access their stored settings on PCs at office "hot desks," and even on coffee machines.

> By implementing biometric access cards, enterprises can provide a secure and hygienic environment and remove some multi-touch surfaces, like keypads for PIN entry.

Ensuring robust data security is critical. April 2021 saw approximately 1 billion data records exposed through breaches and hacks, while the introduction of data privacy legislation such as Europe's GDPR has placed organizations at serious financial risk if they are lax with their protection and policies. Biometrics have a role to play here, too. By limiting access to authorized users, the risk of hacks through lost or stolen credentials is dramatically reduced.

On-Device Security

While the benefits may be clear, some organizations are wary of

implementing biometrics because of privacy concerns. After all, managing employee biometric data poses several technical and ethical challenges.

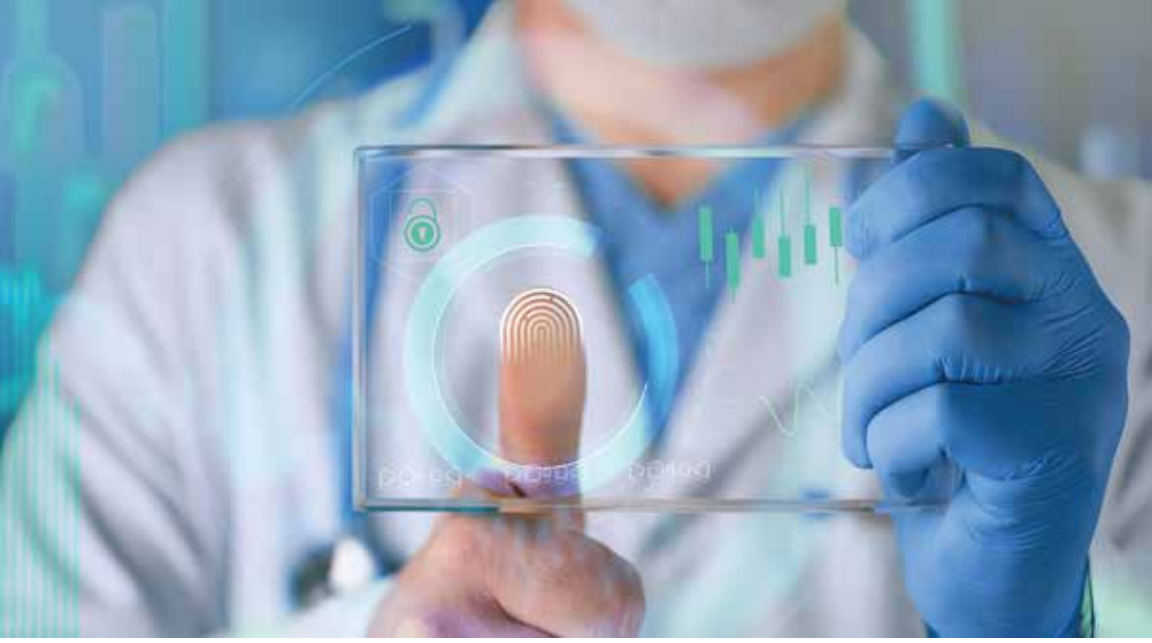
By choosing solutions with on-device authentication – whereby a user's biometric data is encrypted, contained and matched within the device – businesses can deliver to their employees the benefits of biometrics, without the complex administrative burden of a centrally managed and secured biometric database. This type of authentication is available in devices such as smartcards, laptops, smartphones and even USB tokens. Not only does this approach to implementing biometrics reassure businesses, but it also reduces employee concerns regarding the protection of their most personal data.

> Biometric authentication is highly robust, and the latest solutions offer considerably greater security than their authentication predecessors – PINs, passwords and physical keys.

Playing the Strongest Card

Biometric access cards are one way to implement biometric authentication. Each access card is linked to a specific cardholder, who registers their fingerprint on it. When entering a building or office, or logging into any system, the card's biometrics must match the person using the card, ensuring that only authorized employees gain access.

In workplaces where restricted access is in place for different environments, such as labs, hospitals or private offices, biometric cards ensure that only authorized employees can gain access to each area. When



combined with other smartcard functions, such as ID badges, time and attendance logs, and alarm management systems, the value of biometric access cards only increases.

As demand for more hygienic access grows in the wake of the pandemic, users are increasingly drawn to contactless access methods. By implementing biometric access cards, enterprises can provide a secure and hygienic environment and remove some multi-touch surfaces, like keypads for PIN entry.

Put simply, biometric access cards can be thought of as a modern-day key. Compared with traditional access cards or keys, though, biometric cards offer far greater flexibility, simplicity and convenience. Furthermore, as use is limited to the authorized user, there is no security risk should an employee lose control of their card.

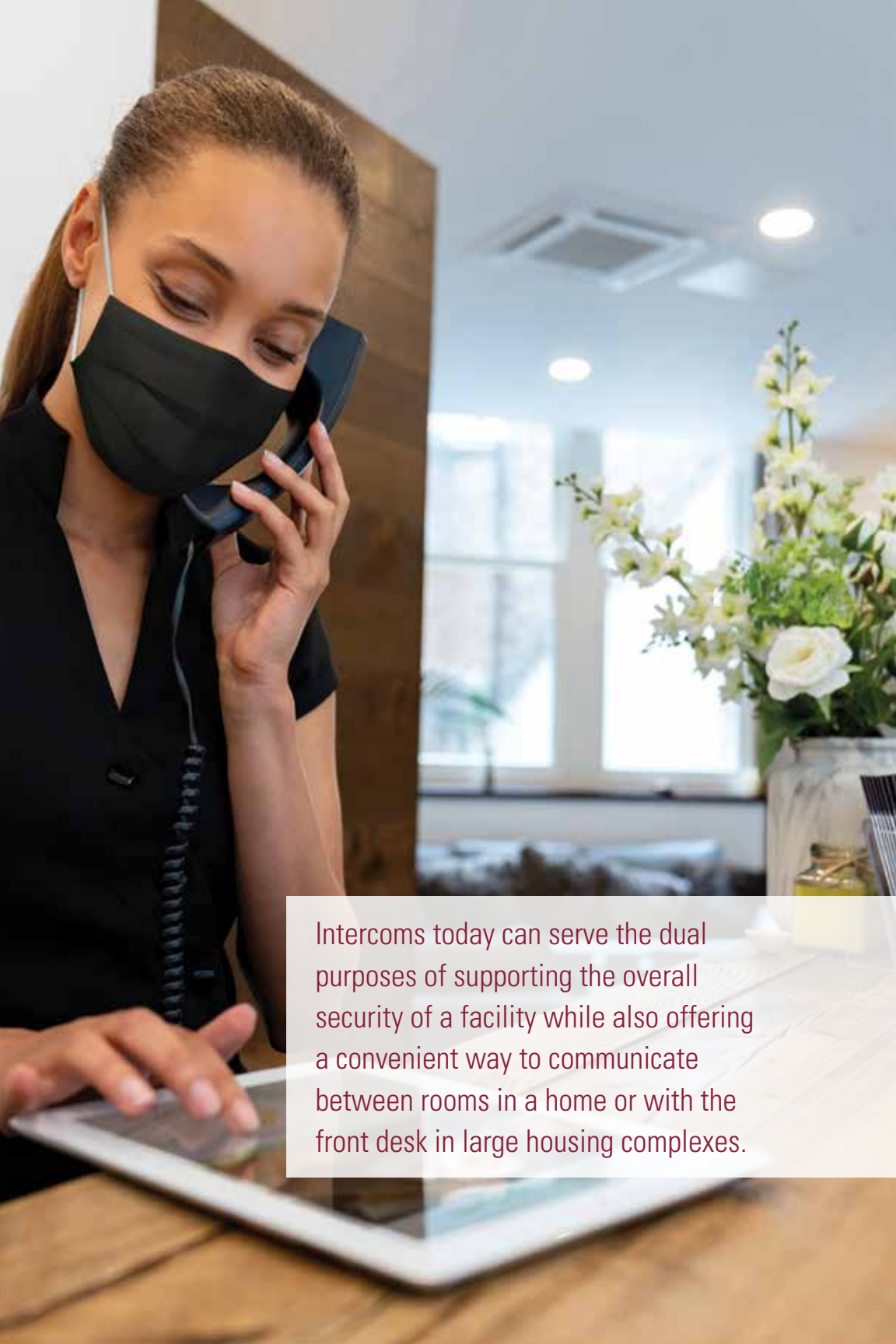
Integrating Biometrics

Biometric authentication is highly robust, and the latest solutions offer considerably greater security than their authentication predecessors – PINs, passwords and physical keys. It represents an opportunity for enterprises to empower their employees with smart, secure and convenient access.

Taking steps to realize the future of workplace security with biometrics is easier than many might think. Biometric sensor technology has gained momentum in smartphones and other commercial products, so it is already familiar to many employees.

Security, both logical and physical, remains a complex challenge for many businesses. As the need for convenient yet secure authentication grows, biometrics will play a vital role in building the future of workplace security. ■

Maria Pihlström (maria.pihlstrom@fingerprints.com) is Senior Global Marketing Manager at Fingerprints (www.fingerprints.com).



Intercoms today can serve the dual purposes of supporting the overall security of a facility while also offering a convenient way to communicate between rooms in a home or with the front desk in large housing complexes.

Video Intercoms in a Post-Pandemic World

Residential security systems have taken on new functions

By Marty Schutt
Aiphone

During the past year and a half, our homes have become much more than living spaces. They are schools, gyms, workspaces and so much more. Investing in a comprehensive security solution is as important as ever, and providers and integrators should be ready to discuss a system that not only enhances security but also offers end users ease of use. Video intercoms can provide this, in addition to the peace of mind that comes with knowing that help is only a call away.

Intercoms have been a communication staple for years, especially in the education, healthcare, workplace and residential spaces. However, we are far beyond the simple button and speaker system, or telephone, of days past. Intercoms today can serve the dual purposes of supporting the overall security of a facility while also offering a convenient way to communicate between rooms in a home or with the front desk in large housing complexes. Here are a few reasons why video intercoms are an essential component of residential facility security.

Enhanced Occupancy Management in Common Areas

Prior to 2020, many security providers might not have seen many requests for occupancy management, but as we enter a post-pandemic world, efforts to maintain social distancing may continue. As such, IP video intercoms can be used to manage occupancy in shared spaces or common areas. Entertainment rooms, conference rooms and other locations can all be equipped with IP video intercoms that require credentials for access. Additionally, some facilities might have an onsite theater for viewing movies, a gym, or a rooftop lounge area. Building managers can use an intercom system to admit tenants into these shared spaces and deny access if maximum occupancy has been reached. Integration with IP cameras means that building managers can access surveillance inside the shared spaces to ensure that occupancy has not been exceeded and, if necessary, that proper distancing measures are being adhered to.

> Flexibility and ease of use are top of mind for residents as they find value in taking their building security into their own hands.

Mobile Credentials Enhance Security and Visitor Management

Flexibility and ease of use are top of mind for residents as they find value

in taking their building security into their own hands. This can be achieved through the use of IP video intercoms integrated with mobile apps. These systems can assist in managing access to condos and private living spaces, as well as common areas. For unit access, tenants want the ability to open doors remotely – a capability that is in very high demand. Not only can they manage access to their individual living space, they can also manage access to lobby doors remotely. It is not enough to just be able to speak to someone requesting access to a building or unit; tenants and building management also want to be able to see the visitor.

Facilities can equip each unit with a video intercom, or they can choose to have tenants use the mobile app to communicate with a concierge or lobby manager. Many residential facilities see a steady influx of visitors and deliveries, especially with so many residents still working from home. With this in mind, a video intercom can add the security measure of allowing tenants to use an app to

A video intercom can add the security measure of allowing tenants to use an app to oversee entry into the building lobby, from a safe distance, while confirming identification.

oversee entry into the building lobby, from a safe distance, while confirming identification.

With mobile app communication, tenants can call down to the front desk and ask to get a vehicle out of valet, or they can request maintenance if they have a water leak or a garbage pick-up. Conversely, building staff can contact tenants to inform them of a package delivery or a visitor.

As we enter a post-pandemic world, we have once again seen a shift in the technology used in our residences, only this time it has been driven by our homes taking on new functions.

Increased Perimeter Security and Remote Monitoring

Many IP intercom systems can be monitored remotely so the provider will know if there are any issues before building management does. Having a provider monitor the health of the system also ensures that any repairs or security concerns can be dealt with swiftly.

Additionally, audit trails of access and other daily activities are kept. This is valuable to building managers since it provides them with easy access to logs from specified dates and times following an incident or security breach. For example, if someone was let into the building after hours, or if there was suspicious activity at the front door, building staff or security can access saved video

footage to see who was there. An IP system can integrate with cameras and a network video recorder, offering a 24/7 security system for the building.

Cost Effectiveness and Flexibility for Tenants and Staff

With mobile access, an IP video intercom system can be deployed in a large, multi-family residential facility, as well as a smaller condo association. Installation in both scenarios offers cost effectiveness, as well as ease of move-in and move-out for building managers. With a mobile app, the tenant's private information can be deleted from the software platform, and if there is a video intercom station inside the residence, the software can be reset for a new tenant. This eliminates the possibility of previous tenants gaining access to an apartment, without incurring the cost of having to replace key cards.

Over the past few years, it has become increasingly common for residents to outfit their homes with connected devices. From voice assistants to smart thermostats and appliances, ease and convenience of use have been in high demand. Now, as we enter a post-pandemic world, we have once again seen a shift in the technology used in our residences, only this time it has been driven by our homes taking on new functions. This has spurred more investments in security systems to keep residents and assets safe. In addition, security solutions are now almost required to serve multiple purposes. Residents and building managers alike should not have to sacrifice safety for convenience. ■

Marty Schutt (marty.schutt@aiphone.com) is Director of Sales for Aiphone (www.aiphone.com).

The RMR that a cloud access control offering provides can modernize a reseller's business, keep margins up, and produce consistent revenue, all while better serving the customer.

What RMR Means for Integrators

As use of the cloud expands, so do opportunities for recurring monthly revenue

By Kim Loy
ACRE

The recurring monthly revenue concept in the security industry was once defined as integrators monitoring and managing monthly contracts with end users. With the increase of cloud-based technology, however, the RMR definition has expanded. Companies no longer just sell systems, they also provide services.

With these advancements in cloud technologies, not only do integrators benefit, but their customers do, as well. RMR enables the integrator to develop a stronger connection with the customer, furthering business relationships and increasing the likelihood of repeat clients. In turn, the customer trusts that the integrator understands their specific needs and will be available to provide the necessary services.

Security Industry RMR 101

For any integrator who provides managed access control, a challenge that often emerges is shifting from the traditional "sell and install" model to that of RMR. This new approach demands revised billing procedures for customer support and requires sales

teams to invoice on a recurring basis.

When evaluating potential manufacturer partners, it is essential for integrators to seek out one who understands the business and provides ample guidance while shifting to the RMR model. The system should be easy and quick to install, with efficient management that offers modern features important to a wide range of customers. A truly beneficial partnership needs to be in place to allow both parties to benefit and interact with each other in order to achieve successful results.

As with any new process, there may be a learning curve associated with developing an RMR business model, which is why it is helpful to work with an established access control or intrusion software provider who can provide answers to any questions that may arise as a business adopts this approach.

> Having a stable base of customers and nurturing those relationships over time benefits the integrator by providing opportunities to sell more products and services.

The Rise of Cloud-Based Services and Solutions

The cloud has radically reshaped our day-to-day lives and is increasingly accepted as a highly favorable solution for storing and accessing data, as well as offering valuable services and applications. Cloud services have become well established across almost all industry sectors, and

changing customer demands have required many businesses to reinvent their offerings to harness the power, flexibility, and functionality they offer. This trend will continue as more intelligent software is developed and integrated with cloud-based systems.

So how, exactly, do cloud solutions and RMR work together? This is where software-as-a-service (SaaS) applications come into the picture. These products are a natural fit for start-ups and small businesses, as they allow organizations to hand over the management of the cloud to an integrator. The customers most likely to be interested in such services are the ones who would typically *not* be interested in deploying and managing on-premises infrastructure and who would prefer a service-based approach from an integrator.

> A cloud-based solution that facilitates automation is always up-to-date and does not require an IT team to ensure that updates are installed.

SaaS Benefits – From Integrator to End User

Cloud-based RMR services provide integrators with a steady flow of revenue each month. In a business that has traditionally been built on a "per project" basis, revenue that can be regularly anticipated makes the budgeting process easier. Additionally, having a stable base of customers and nurturing those relationships over time benefits the integrator by providing opportunities to sell more products and services.

These off-premises solutions are the best option for the customer who does not want to manage their security infrastructure. By choosing a cloud-based system, the end user enjoys several benefits, including reducing the up-front investment in hardware and software by spreading the bulk of the cost out over monthly installments. In addition, a cloud-based solution that facilitates automation is always up-to-date and does not require an IT team to ensure that updates are installed.

RMR Payments and Invoicing Explained

How does the RMR pricing and invoicing structure work for integrators and end users?

For the integrator, the manufacturer charges the installer/dealer directly every month of the device's or application's subscription, including the service fee and a fee per device. Integrators can then charge their customers on a regular basis (monthly, quarterly, yearly, etc.) and set their own prices for each device. In some cases, service providers may offer an annual discount for paying upfront. The main advantage is that each service provider can set their own billing protocols, whether they want to do an automatic payment or bill monthly for the service to the customer.

How can integrators, dealers and installers bill the service to customers?

Many service providers that already offer alarm or central station monitoring have subscription-based tools and applications in place to help

streamline the billing process on a monthly, quarterly or annual basis. One challenge that smaller locksmiths have with transitioning to an RMR model is the investment in these kinds of subscription services. Since the market seems to be trending in the direction of increased RMR opportunities, many smaller integrators are investing in software to grow that side of their business.

> By choosing a cloud-based system, the end user enjoys several benefits, including reducing the up-front investment in hardware and software.

What if customers can only pay in their local currency or cannot pay internationally?

As with any service-based contract with integrators, dealers and installers, services can be paid for in the currency accepted in a given location. Many times, a company's subscription tool/application has a gateway that manages different currencies. Integrators that are already set up to provide service-based solutions typically have these mechanisms in place, especially when offering alarm/central station monitoring.

Delivering Long-Term Value

For dealers, integrators and installers who are interested in offering a cloud-based service that leverages an RMR business model, there can be significant value for both them and their customers. However, it is essential to have a clear picture of what is required to build this kind of model. The future of RMR, as a whole, will depend on many factors, with the most important being the type of systems and solutions involved. As long as cloud-based technologies remain at the forefront of the security industry, more and more integrators will desire the ability to add value to their offerings by way of monthly service agreements.

Cloud-based access control empowers integrators to offer managed services to their customers. Not only does this allow integrators to provide services with RMR, but it also offers ample flexibility for the management of an organization's access control, including the ability to update or remove permissions and view cameras or open doors from a PC, tablet or smartphone.

The RMR that a cloud access control offering provides can modernize a reseller's business, keep margins up, and produce consistent revenue, all while better serving the customer. Beyond that, having a constant source of income can provide an integrator with the financial resources to grow and expand their business. ■

Kim Loy (kimloy@acre-co.com) is the Chief Product Officer of ACRE (www.acre-co.com). She also serves on the Executive Committee of the SIA Board of Directors.

The security industry needs to redefine what security systems do and add the value of intervention in order to provide a new level of service.

Developing the Security Solutions of the Future

To add value and effectiveness, systems will need to focus on intervention and prevention

By Haim Amir
Essence Group

Traditional professional and do-it-yourself (DIY) alarm systems are too limited to address today's challenges of protecting people and property. To meet these challenges, systems must evolve from the detection of security breaches to active intervention and, ultimately, prevention. Although technologies exist that allow systems to provide active intervention, there are a number of obstacles to overcome before they can be fully implemented. Once in place, though, these technologies will make security systems far more valuable for homeowners and businesses.

Traditional Security System Limitations

Historically, residential and small business security has been based on the concept of deterrence through detection. The user has a security system that notifies the police when an intruder enters the home or business. There might also be a siren that alerts neighbors. These systems were primarily developed to protect a homeowner's property.

This model worked when police were able to respond quickly. In addition, intruders were usually breaking in to steal things, not harm people. However, a number of changes have occurred that make the deterrence-through-detection approach less effective.

Changing Environment Challenges the Old Model

Verification Requirements

Traditional security systems historically have high rates of false alarms. At times, as much as 98 percent of all notifications to monitoring centers are caused by factors other than actual intrusions. This resulted in many wasted trips by the police. Although there have been significant efforts made to address this challenge, the damage was done. Many local authorities now require verification before responding to an alarm and some fine providers or owners for false alarms. As a result, many systems now enable verification through audio, video or other methods. Although these improvements add value, today's systems still provide only reactive responses to intrusions, causing costly delays.

Decreased Police Responsiveness

With increasing demands on law enforcement and the history of false alarms, police have become less responsive to residential and small business alarms, particularly if they are unverified. This has lowered the likelihood of intruders being caught and has emboldened them.

Self-Monitored DIY Systems

Some say that the new trend of DIY systems, self-monitored by homeowners, has reduced the

likelihood of apprehension even further. In theory, the homeowner's familiarity with the property, residents and potential guests would make them effective in identifying intruders. However, without 24/7 monitoring, what is the likelihood that an intruder will be caught? Will intruders even see this type of system as a deterrent?

With increasing demands on law enforcement and the history of false alarms, police have become less responsive to residential and small business alarms.

Intruder Behavior

Since the early 2000s, intruders have become more likely to confront and even harm homeowners than they were in the past. One explanation is that harsh penalties for causing injury during a break-in no longer provide the deterrence they once did. Another is that attitudes have changed. Whatever the reason, these changes have made traditional security approaches less effective.

COVID-19

The global pandemic will cause lasting changes in threats and security requirements. Cycles of lockdowns and unrest have altered the nature of security threats. Intervention-based solutions will be even more important as our environment becomes more dynamic and less predictable.

Community Approaches

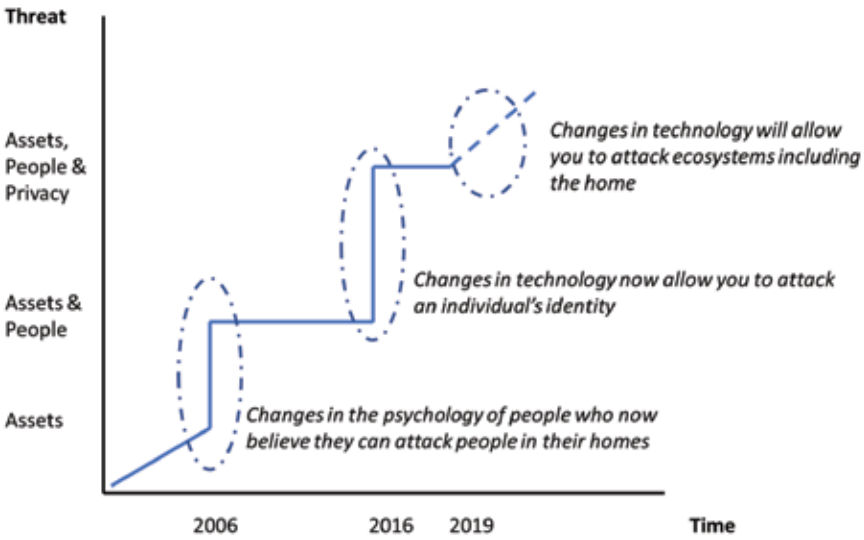
With the deployment of outdoor cameras came the realization that community watch strategies could be supplemented with technology, thereby making distributed security stronger. Police and neighbors can share information so that they can become better informed faster, giving them the ability to respond more effectively. Imagine, now, the ability to anticipate intruders, verifying in advance of events and taking preemptive action.

Evolution of Security Systems

Throughout the history of the security industry, systems have evolved as a result of two factors: new challenges posed by changes in human behavior and the costs of addressing those challenges. We would all like to live risk-free lives but the costs of attaining that are far greater than we can afford. Generally, we assess risks and spend whatever we feel those risks warrant. If we had a system that provided greater protection at a lower cost, we would certainly use it.

In the past, the amount that we were willing to pay for a security system was a function of how much it was worth to us to protect our property from theft and damage. Now, systems must evolve to protect ourselves and our families from harm. This increases their value, along with consumers' willingness to pay more for them.

While we try to develop ways to address new threats to our physical safety, we are also faced with new threats to our identity. Intruders are not just coming at us physically but also virtually, which enables them to steal much more. Cyber-intrusion of our homes though connected devices allows thieves to disable security systems and physically enter the property with no risk of detection. Security systems have to further evolve and encompass the entirety of the



Approach	Goal	Tactics
Deterrence	Make the intruder think twice about breaking in	Basic detection security system tied to a central monitoring center
Intervention	Engage with intruders to deter them from starting or continuing to break in; slow intruders down to enable police response	High-decibel audio, strobe lights, fog emission, smoke screens, laser beams, high-intensity light
Prevention	Make a break-in extremely difficult	Walls, guards, cyber protection

residence's network infrastructure as well as its physical borders.

Intervention: A New Approach

Preventing harm by making it impossible for an intruder to enter the premises is obviously the most effective approach, but, for the average homeowner, it is also very costly and restrictive. For most of us, building high walls around our property, hiring guards, and implementing other means of prevention are out of reach. Even the least intrusive form of prevention, deterrence through detection, is becoming less and less effective. We must find ways to intervene before an intrusion takes place in order to enable stronger deterrence or buy more time for authorities to respond.

As our security needs change, it is useful to think about security in terms of what we must protect. We need to protect our families, our property and our identities. Simply knowing that they are in danger (basic detection) is not sufficient. We need more comprehensive solutions. Faster and more effective responses help, but intervention and prevention will be crucial. Furthermore, approaches may need to be different for different needs. For example, for identity threats, just being aware of a threat (detection) will not help; what is needed is a blocking method (prevention) that saves us from harm. And we need to develop the equivalent for our person and property.

> While we try to develop ways to address new threats to our physical safety, we are also faced with new threats to our identity.

Potential Solutions

In the near future, we will see many instances of intervention technologies being developed and deployed. In its simplest form, it could be a warning. For example, when a camera detects an individual in a location that should be empty, a speaker could notify the individual that they have been seen,

are being video recorded and will be apprehended unless they leave immediately. Going further, the system could turn on all the lights in the area and sound a siren.

In more advanced approaches, methods that affect all of the senses could be deployed to make it very unpleasant to continue a break-in or more difficult to get to the desired target in a home. These approaches could eventually provide preventive capabilities as well.

New capabilities will be needed to protect not just people and property at home, but also on the go. Methods exist to protect people from attack, like pepper spray and whistles, and cars and boats can be secured with alarms. But, as we become more mobile, and as new threats arise, we will need to develop and deploy new intervention technologies.

> By using intelligent scoring, events can be given a severity level that allows the response to be appropriate to the scenario.

Role of Technology in Intervention

Technologies exist today that can enable intervention, with the most significant being artificial intelligence (AI). Here are a few ways that AI could be used:

- Better accuracy can be achieved through facial recognition, anticipating an event through monitoring of a variety of sensors and/or connecting with other systems, both internal and external.
- AI can create a seamless user experience by deducing that a certain event is likely and controlling the sensors that are involved with that event. For example, if a door is opened every day at 3 p.m. when the kids come home, the AI would use its historical knowledge and not trigger an alarm automatically.
- Current systems' decision-making processes are binary (alarm/no alarm). By using intelligent scoring, events can be given a severity level that allows the response to be appropriate to the scenario.
- Inputs can come from external sources, such as weather forecasts, social events in the area, and more. This information can be used to set the system to different thresholds (e.g., a shock sensor during a storm)
- Warnings that notify an intruder before triggering an event, thereby deterring the intruder and/or gaining more time for an event to be verified. For example, if an intruder is trying to enter a house and trips a shock sensor, the system may sound a command to leave.

AI can thus decrease response times by giving law enforcement more confidence that a real event, not a false alarm, is in process. AI can also aid in facilitating deterrence, potentially eliminating the need for police to respond at all. These steps improve security and enhance the value of the security system.

Robotics represent another technological development that enhances detection, verification and intervention. Whether indoors or outdoors, we now have the ability to dispatch a robot or drone when a threat has been detected to gain situational awareness and, potentially, video evidence.

In terms of cybersecurity, we have the ability to not just detect but repel attacks. Imagine a scenario in which a cyber-intruder seeks to steal personal data but has their attempt deflected and their own system attacked and disabled.

Challenges to Intervention-Based Security

There are challenges to full implementation of intervention-based security. These technologies are not fool-proof and false alarms can still occur. This can result in negative consequences. For example, a smoke-like substance meant to disorient an intruder might be mistakenly deployed. In the best case, the premises would simply need to be cleaned, but in the worst case, innocent people could be affected. Also, systems that are not pet-proof could be activated by a dog running into a yard – and waking up the neighborhood by triggering lights and sirens. AI and other technologies can increase the reliability of devices, but it is likely that errors will still occur.

Another challenge, at least in the United States, concerns legal liability. For example, a criminal in a house who gets distracted by an intervention and trips, breaking an arm, might sue the homeowner and alarm company. This might be a remote possibility, but, in a society where lawsuits are common, it is a potential concern.

Finally, there is the expense. These systems will cost more than traditional ones, and the current trend in the industry is toward commoditization of systems. When price dominates, though, it is because of a perceived lack of value. If a user is as well off with an inexpensive, self-monitored DIY system as with a professionally monitored system, then where is the value in spending more? The security industry needs to redefine what security systems do and add the value of intervention in order to provide a new level of service.

Conclusion

There is a major need for traditional security systems to evolve. With so much change having occurred and with growing threats to people, identities and property, we need new types of solutions with better technology and lower cost. Implementation challenges exist, but the industry should be able to overcome those hurdles and help to better secure people, homes and businesses. ■

Haim Amir (haim.amir@essence-grp.com) is the Chief Executive Officer of Essence Group (www.essence-grp.com).

SIA Technology Insights is published twice a year, in the spring and fall, by the Security Industry Association in Silver Spring, Md. All editions are available at no charge at www.securityindustry.org/techinsights. Questions, comments and article proposals may be submitted to the editor, Ron Hawkins, at rhawkins@securityindustry.org.

www.securityindustry.org

Security Industry Association
8405 Colesville Road, Suite 500
Silver Spring, MD 20910
301.804.4700