SIA
TECHNOLOGY
Insights
Fall 2022
Volume 10, Number 2

Precognition in Security

Proactive video monitoring can provide the tools to stop crimes before they occur

Page 2

Access Has Left the Building
Cloud solutions offer advantages over on-prem
Page 6

Data Alchemy
Turning information into insights
Page 16

RMR ASAP
4 Key Video Trends for Alarm Companies
Page 24

SICC™

SECURITY
INDUSTRY
CYBERSECURITY
CERTIFICATION

THE CYBERSECURITY CERTIFICATION FOR SECURITY INDUSTRY PROFESSIONALS

Why Earn the SICC?

The only credential focused specifically on cybersecurity for physical security systems

Validate your understanding of essential topics like:
- Infosec principles
- Networking and network security
- Device security
- Software security
- Social engineering

Accelerate your career and build trust with your colleagues, partners and clients

"We will be making the SICC certification part of our essential staff training to ensure everyone in our organization has the skills and knowledge they need to face changing cybersecurity challenges and build innovative, secure solutions for our customers."

– Courtney Gibson, SICC, chief technology officer and chief information security officer, BioConnect

Learn More About the SICC

www.securityindustry.org/sicc

SIA SECURITY INDUSTRY ASSOCIATION

Co-developed with support from

PSA SECURITY NETWORK®

security specifiers

TECHNOLOGY Insights

Fall 2022

Volume 10, Number 2

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.

Turning Security from Reactive to Proactive

Intelligent video monitoring can be used to prevent, not just investigate, crimes

Justin Wilmas (jwilmas@netwatchgroup.com) is President of Netwatch North America (www.netwatchusa.com).

VIDEO SURVEILLANCE HAS BECOME THE PRIMARY DATA SOURCE for security and insights that help businesses operate. Typically, video is a reactive process used to investigate a crime after damage has been done. But more impactful solutions are now available. Proactive video monitoring (PVM) is one of those offerings. Like certain other advanced technologies, PVM focuses on *preventing* crimes by drawing immediate attention to unauthorized activity and empowering a trained operator to direct a response and, if necessary, notify local authorities.

PVM has effectively turned the concept of video monitoring on its head. The difference is in how it incorporates artificial intelligence (AI) to identify intruders and stop them before any harm occurs.

So, is PVM the same as video verification or voice-downs that use recorded messages? The answer is no. PVM adds another layer – real-time monitoring and customized live voice-downs. While video verification services may have been a practical option in the past, PVM is a more than worthy successor for multiple reasons.

PREVENTION IS KEY

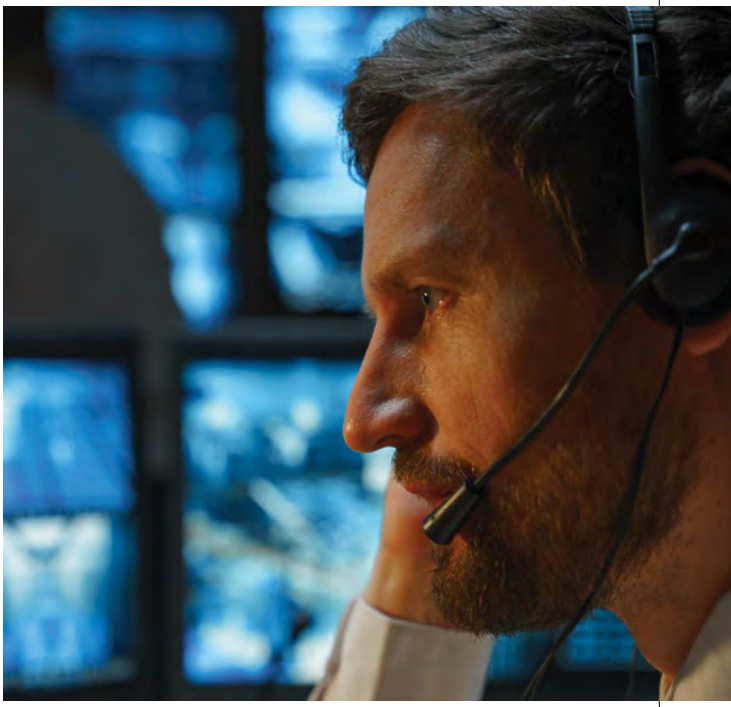
While video verification can address the problem of false alarms, it is still a reactionary approach. A central station operator will check the alarm's video footage and call to confirm if there was an intrusion. The operator will then report the incident to the police if a security incident is identified. In confirming that a crime occurred, it reduces false alarms, but it does not prevent crime.

PVM is different. It deters and stops criminals in their tracks. PVM's AI-based engine "watches" for potential security events. Built-in intelligence automatically detects possible criminal activity and sends a real-time alert to an intervention specialist at a monitoring center. The operator investigates the situation and, if needed, speaks to the intruder, letting them know they have been detected.

> PROACTIVE VIDEO MONITORING IS DIFFERENT. IT DETERS AND STOPS CRIMINALS IN THEIR TRACKS.

LIVE FROM THE CENTRAL STATION

When illicit activity is identified, central station operators can challenge the intruder



> CENTRAL STATION OPERATORS CAN CHALLENGE THE INTRUDER WITH A PERSONALIZED AUDIO WARNING. IN 98 PERCENT OF CASES, THIS, ALONE, IS ENOUGH TO STOP A PERPETRATOR.

The U.S. Department of Labor reports that more than 1 million security guards are working in the United States.

with a personalized audio warning, customized to the customer's requirements. In 98 percent of cases, this, alone, is enough to stop a perpetrator.

Because the operator sees live video footage of the situation, they can point out specifics, such as, "You in the green hooded sweatshirt, you are not authorized to be on this property." If the intruder does not retreat, operators inform the individual that authorities will be contacted.

The ability to identify specifics regarding clothing and movement prevents crime because the perpetrators now know they are being watched in real time. It is these details that make the difference. Video verification and pre-recorded voice downs do not have the same impact.

AUGMENTING FEET ON THE STREET

Guards are essential to ensuring security across a wide variety of environments, and PVM will not entirely replace the human element. It can, however, make a guard force stronger. While video verification can help guards identify valid alarms, it cannot support an informed response or prevent damage. Instead, it leaves an onsite guard waiting for the police to arrive, which could lead to the situation becoming more complicated and dangerous as time progresses.

PVM supports guards by enhancing their ability to identify threats. Hazardous activities, such as chemical spills or violent situations, can now be managed more effectively, significantly

increasing safety and reducing liability.

PVM can also provide additional support during staffing shortages, as well as for less desirable postings, such as those in remote, desolate or dangerous locations or during the overnight shift. PVM relives guards of much monotonous and risky work and enables them to apply their expertise to more strategic duties.

STRONGER REPORTING

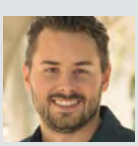
After a security incident, it is essential to generate a detailed report to document the event. PVM produces comprehensive reports that can help security leaders spot trends and emerging risks. It can also analyze activity over time, learning where the most high-risk facilities are based on the frequency of alerts. Video verification does not provide this level of reporting and statistical analysis.

Overall, while video verification can be an effective tool for reducing false alarms, it is unable to offer many other benefits. Proactive Video Monitoring, in contrast, provides dealers with a way to differentiate themselves in the market, increase revenue, stay on top of industry trends, and meet the growing demand for intelligent video services. ◀

> PVM WILL NOT ENTIRELY REPLACE THE HUMAN GUARD ELEMENT, BUT IT CAN MAKE A GUARD FORCE STRONGER.

Getting Ahead in the Cloud

Leaving behind on-premises access control is a step toward the future



Mike Maxsenti (mmaxsenti@getgenea.com) is Director of Key Accounts for Genea (www.getgenea.com).

THE SHIFT HAS BEGUN. OR, MORE ACCURATELY, IS GAINING MOMENTUM. Since 2020 and the pandemic-induced hybrid workplace, IT and security teams have faced mounting pressure to reevaluate their physical access control. Many teams have found that their on-premises systems simply will not cut it anymore.

As a result, enterprises are leading the migration from rigid on-premises systems to more flexible cloud-based options. And the change makes sense. Enterprise teams face the daily challenge of managing multiple facilities (sometimes spanning the globe) and overseeing thousands of users. Cloud technology eases these processes.

But ditching the on-prem dinosaurs raises another question: Which cloud-based system is the right one? IT and security teams have a variety of options, and choosing the right one can be difficult. Teams must not only address current problems but also be cognizant of potential future challenges. The unpredictable climate of security means personnel must ensure their operations remain flexible for the future, something that

on-premises access control cannot do.

ON-PREM ON THE WAY OUT

The problems with on-premises access control systems can be categorized into three buckets. First, they operate using outdated hardware architecture. In the case of an enterprise customer who wants to install access control in more than 1,000 locations worldwide, for example, an on-premises system would require each site to house its own server. Cloud-based access control, however, eliminates the burden of equipment costs associated with all those servers, including the space needs and maintenance requirements.

The second problem plaguing on-premises access control is the antiquated user interface that lacks the simplicity and functionality seen in many cloud-based systems.

Finally, on-premises systems do not natively integrate with other technology solutions. Making the systems work together requires costly custom integrations at each location.

SECURITY, REDUNDANCY AND ENCRYPTION

For much of the 2010s, there was a debate about

> WHEN LOOKING INTO UPGRADING TO THE CLOUD, ENTERPRISE SECURITY TEAMS SHOULD MAKE SURE THAT ALL OF THEIR DATA AND SERVERS WILL BE ENCRYPTED USING 256-BIT ENCRYPTED HTTPS PROTOCOL.

the security of data in the cloud, with questions being raised about potential cybersecurity vulnerabilities. Today, though, the cloud is safer than its on-premises counterparts for various reasons. Chiefly, the cloud creates redundancy, reducing the possibility of losing important access data. Storing access data onsite runs the risk of it being damaged, lost or stolen. When an on-premises server fails or a hacker gains access to vital information, companies can lose months of information. Cloud networks, in contrast, keep data in multiple locations. In an enterprise solution, having redundancy that is accessible from anywhere should be a requirement.

Cloud encryption was another early concern. Encryption has improved tremendously over the past decade, and, when looking

into upgrading to the cloud, enterprise security teams should make sure that all of their data and servers will be encrypted using 256-bit encrypted HTTPS protocol. This protocol prevents anyone or anything, including a supercomputer, from gaining access. It would take years for hackers to decrypt this type of information.

CLOUD HESITANCY

Despite the progress cloud access control has made, some IT and security professionals remain reticent. The Apache Log4j2 vulnerability may have contributed to this. In December 2021, a vulnerability in open source code was exposed. The remote code execution vulnerability theoretically enabled hackers to take full control of devices, including cloud servers. Among those at risk were some of the biggest cloud providers. Hot patches were deployed, however, and companies took

> WHILE ON-PREM PROVIDERS CAN ALSO USE APIs, THEY CANNOT INCORPORATE THEM INTO THE SYSTEM AS QUICKLY AS CLOUD PROVIDERS.

immediate action to secure their servers. It all ended without a catastrophe.

In the end, Log4j2 served as a sobering reminder to all in the tech industry. But there was also a silver lining when considering the response time, one that emphasized the agile and flexible nature of cloud computing and showed that solutions could be quickly deployed and threats excised. Contrast this to the actions needed for on-premises servers affected by the Log4j2 vulnerability. In an enterprise environment with access control running across multiple servers, deploying hot patches would take exponentially more time. Having to coordinate and implement changes across multiple systems could leave enterprises exposed for an extended period.

UNIFYING SECURITY THROUGH INTEGRATION

Like a streaming service's ability to quickly add new titles to its library, cloud access control providers can rapidly deploy new solutions, including application programming interfaces (APIs) that connect software and hardware to access control platforms, allowing them to communicate with each other. In short, these integrations offer a way to streamline security by uniting multiple systems.

While on-prem providers can also use APIs, they cannot incorporate them into the system as quickly as cloud providers. Why is this a problem? Because software companies come and go, and consolidation of property technology will continue. IT and security teams need the capability to pivot.

Security teams can quickly add API integrations to their company's existing hardware, so that the software addresses new challenges more quickly and cheaply than can be

done with on-premises systems.

API integrations come in two types: native and open. Top-tiered access control companies offer native integrations, meaning that, with a single API token, IT and security teams can connect their access control system to other hardware and software tools, including video, visitor and identity management, tenant amenity apps, and more. Everything from elevators to security cameras can be connected with an API token.

REMOTE VISITOR MANAGEMENT

Consider a cloud-based access control system at a U.S.-headquartered company that has a native API integration with a visitor management system. The firm is made aware of an after-hours delivery being made to a satellite office in Belgium.

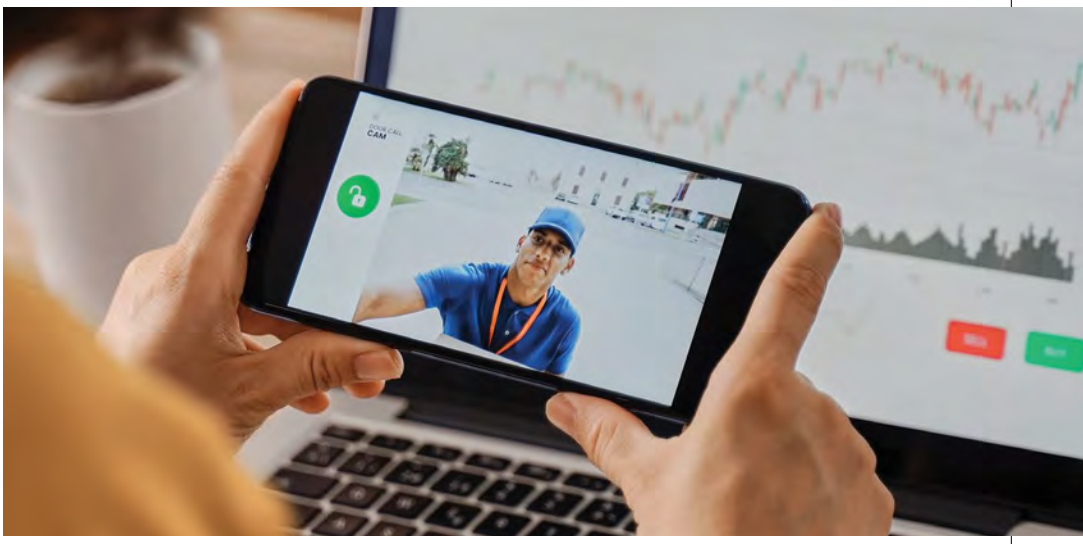
Without having to make the Belgium team stay late, the American team can issue a temporary QR code to the delivery person. Some access control companies even have custom parameters for their guests, so, for example, they might be permitted to enter the building between the hours of 6 p.m. and 8 p.m. Any time outside of those hours, the credential will be inactive.

Visitor management systems are just one of the many APIs that are easily incorporated into cloud-based access control.

VIDEO MANAGEMENT

As with visitor management, cloud-based access control can be integrated with video management systems. These integrations help IT and security teams improve the speed at which they respond to emergencies by connecting security cameras with access control dashboards. Users have the capability of mapping door alarms to security video feeds. When a door event occurs, such as a door being

> WHILE A COMPLETE TRANSITION TO NON-PHYSICAL CREDENTIALS HAS NOT YET HAPPENED, TEAMS IN THE MARKET FOR ACCESS CONTROL SHOULD LOOK FOR A PROVIDER THAT OFFERS BOTH PHYSICAL AND MOBILE OPTIONS.



forced open, video from the security camera can appear within the access control dashboard.

Some cameras even include facial recognition features to identify who is coming and going within a given workspace, enabling video management systems to reduce passback and tailgating problems. If an unauthorized person attempts to gain access by using an employee's credential, the integration will note the discrepancy and alert the security team.

SCALING, ADDING AND REMOVING CREDENTIALS

The scaling of an enterprise brings about many new challenges from a security standpoint. One of these is credentials. As veterans of the industry are aware, the landscape of credentialing has changed. Teams that used to rely on physical credentials (e.g., key cards, smartcards, key fobs) have transitioned to biometrics or mobile. While a complete transition to non-physical forms has not yet happened, teams in the market for access control should look for a provider that offers both physical and mobile options.

There is good reason to consider using mobile credentials. When operating within a cloud infrastructure, mobile eliminates certain restraints. From an end user standpoint, physical credentials are more likely to be lost, cloned or stolen.

> NON-PROPRIETARY HARDWARE ALLOWS ENTERPRISES FLEXIBILITY WHEN CHOOSING SOFTWARE. IF PRICES INCREASE OR THE PROVIDER FAILS TO UPDATE THE SOFTWARE APPROPRIATELY, THEN SECURITY TEAMS CAN SIMPLY FIND ANOTHER SOLUTION.

The access control industry is predicted to expand to $20 billion by 2027, with growth driven by increasing demand for cloud-based systems, according to Fortune Business Insights.

For enterprises, using mobile credentials also means the ability to access multiple offices without having to use multiple badges.

And the advantages extend beyond the user experience. System administrators can remotely assign credentials to any of their team members in any location. For example, if a company's headquarters is in the United States and a new employee is brought on at a location in England, administrators can add credentials without ever leaving the office.

HARDWARE MATTERS: PROPRIETARY VS. NON-PROPRIETARY

Hardware is an aspect that tends to get overshadowed by the sleek user interfaces and sexy mobile experience of the latest generation of access control. For enterprises, though, hardware is especially important. Selecting a platform that has all the bells and whistles on the frontend but is weak on the backend can lead to disaster as enterprises scale.

With hardware, there are, basically, two options: proprietary and non-proprietary. Many proprietary options exist, but IT and security teams run a significant risk with this option. Selecting proprietary hardware ties enterprise security to a single provider. If that provider goes out of business, then all of the hardware will have to be ripped out and replaced.

Obviously, this is a worst-case scenario, but there are also other risks that come with proprietary hardware. Proprietary providers could choose to sharply increase the annual price of software, for example, or they might fail to keep everything updated and secure, either of which would leave customers with few good options.

In contrast, non-proprietary hardware allows enterprises

flexibility when choosing software. If prices increase or the provider fails to update the software appropriately, then security teams can simply find another solution.

FUTURE-PROOF SECURITY

Enterprise teams must try to find future-proof security solutions in an ever-changing environment. As businesses grow and locations and employees are added, it is natural for new security vulnerabilities to arise. The challenge is finding a solution that grows with the business itself. Cloud-based access control provides clear advantages in scalability, flexibility and security compared to on-premises systems. Native API integrations are one part of the equation when it comes to selecting a provider, but aspects like 24/7 customer support and features updates are valuable, as well. As security technology continues to improve processes for enterprises, the power of cloud-based access control could be transformational. ◀

Knowing Is More than Half the Battle

Protective intelligence technology can turn data into insights and action

Thomas Kopecky (tkopecky@ontic.co) is Co-Founder and Chief Strategy Officer for Ontic (www.ontic.co).

PHYSICAL SECURITY TEAMS ARE IN A STATE OF TELEMETRY OVERLOAD. From CCTV cameras to access control systems to the vast number of public records databases used to investigate threat actors and persons of concern, teams have more data and more information at their fingertips than ever before. The visibility of information has become a commodity. Intelligence, however, is at a premium.

The challenge for security teams is sifting through the mountains of information to connect the dots, even as more dots are added every day. In the aftermath of a mass shooting or a workplace violence incident, we often learn that the perpetrator signaled their intent to do something *well before* they actually committed the act. This means that timely, effective analysis has the potential to prevent assaults.

To minimize the risk that a significant danger is missed, companies are adding new threat

> ALTHOUGH INDICATORS MAY BE PRESENT AND DETECTABLE, THE ENORMOUS VOLUME OF DATA MAKES IT EXTREMELY DIFFICULT TO MANAGE AND MAKE SENSE OF.

intelligence monitoring and alerting solutions for both physical security and cybersecurity programs at an unprecedented pace. These solutions affect not only corporate security but other important teams such as human resources, legal, compliance and IT.

Most companies do not have a comprehensive strategy for analyzing and reporting security information across business units, so it is no surprise that managing this data has been one of the single greatest challenges for security, compliance and risk professionals.

Many of the solutions that have been adopted are not well connected. At best, analysts and security teams still need to toggle between various screens in search of the information they need. At worst, analysts are not even aware that certain solutions already exist within their companies, and often they miss out on critically important information

that is located right on the same floor.

Emerging technology that integrates threat data to streamline the management process is vital to an organization's security strategy, allowing executives and analysts to detect, deter, disrupt and defend against hazards that present a clear and present danger to life safety, infrastructure, networks and brands.

SCALING THREAT IDENTIFICATION

Telemetry overload occurs with all sorts of data points, but some of the most difficult signals to track are threats arising from social media and open source intelligence. Although indicators may be present and detectable, the enormous volume of data makes it extremely difficult to manage and make sense of.

The viral nature of social media means that negative information about a company can quickly become amplified. CEOs are often pressured to speak out on hot button issues, which can inflame opposing sides. What can companies do when caught in a social media firestorm? How might they prepare for threats against executives or protests at company locations?

Most companies with executive protection teams have strategies to track people who make violent threats. It is not uncommon for companies

According to some estimates, the global threat intelligence market is expected to grow at an annual rate of nearly 18 percent to reach $26 billion by 2028.

to rely on time-consuming manual processes and implement a "heads down" approach to investigating and analyzing threats. We often find, however, that those strategies do not scale for the speed and volume in which data is generated.

Context is key, and nothing can replace the human element. But more than ever, security teams need to leverage technology that can streamline and expedite the collection and monitoring of information. This involves not only listening for keywords that indicate threat actor activity, whether overt or veiled, but also gaining greater visibility into the geo-location data of a threat. This is important to know if, for example, an executive is publicly scheduled to visit a particular location, and it is enormously beneficial if the security team needs to plan for protests at offices or plants.

TRACKING, MEASUREMENT AND REPORTING

Purpose-built protective intelligence technology facilitates communication and collaboration throughout the enterprise. Security can and should work across the organization to get a

comprehensive picture of the risk landscape. Some of the tools that risk management, cybersecurity and even human resources teams have may integrate with physical security platforms. Many of these tools are extremely useful when monitoring for threats and prescribing an investigative process once a threat is detected.

Technology can help teams resolve issues in minutes, rather than hours. It is critical that organizations find systems that help teams do more with less. It is equally important to generate metrics that measure activities, develop baselines, and document improvements over time. Physical security teams might benefit from replicating metrics used by their colleagues in cybersecurity – like the mean time from risk detection to remediation. It is also possible to work with colleagues across departments to identify ways security can be improved to generate cost savings.

> AUTOMATION CAN SAVE TIME, AND DOCUMENTING THESE SUCCESSES CAN HELP SECURITY BE VIEWED AS BUSINESS-CRITICAL, RATHER THAN AS A COST CENTER.

An in-depth intelligence monitoring program

> TECHNOLOGY HAS STREAMLINED THE WORK PROCESSES OF ALMOST EVERY INDUSTRY, BUT PHYSICAL SECURITY HAS BEEN AMONG THOSE THAT HAVE BEEN MORE RESISTANT TO CHANGE.

should be able to do more than just collect information. It should also document trends and escalations in activity, as well as alert to incident types or clusters of incidents by geography. Automation can save time, and documenting these successes can help security be viewed as business-critical, rather than as a cost center.

WORKING WITH THE LATEST, MOST ACCURATE DATA

Anyone with significant experience in physical security has relied on time-consuming manual processes, such as hunting down disjointed information from numerous sources, writing and sharing printed investigative reports, or even taking the time to catalog all the information required to piece together a BOLO report. Given the volume of information, a 100 percent manual approach is no longer feasible and cannot guarantee that security professionals are working

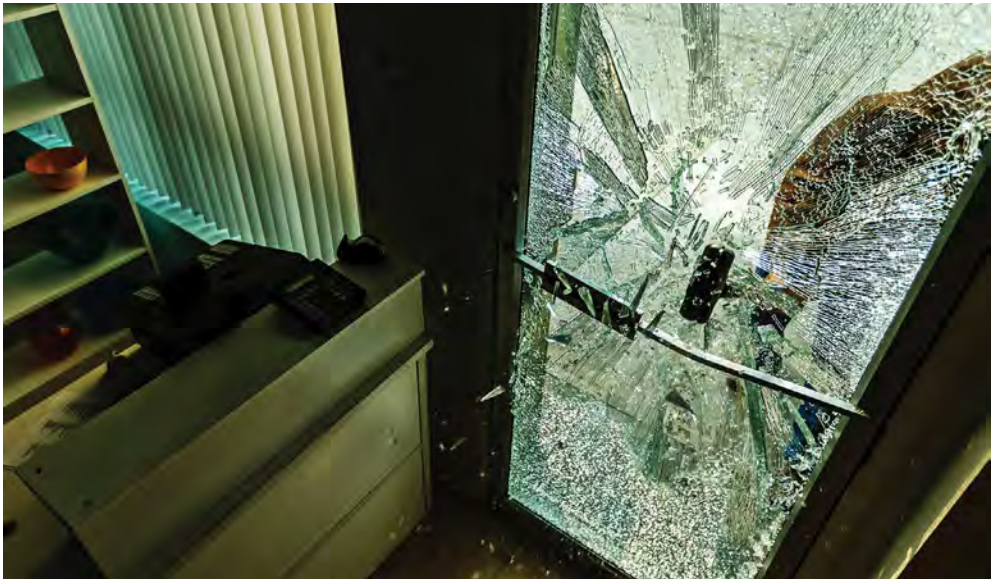
with the latest, most accurate data.

Protective intelligence technology streamlines processes and synchronizes the work of field teams and global security operations centers. Now, every team member has access to the critical data they need to make informed decisions. Collaboration tools often exist within these platforms, so the trail of activity and communication is visible to everyone. Working with the latest, most accurate data can be the difference between success and failure, and in the security realm, failure can have major consequences.

THE FORCE MULTIPLIER

Technology has streamlined the work processes of almost every industry, but physical security has been among those that have been more resistant to change.

For security teams, the ability to ingest and analyze data at a scale that matches the threat environment is mission-critical. They must be able to assess risk and manage threats faster, more accurately and more proactively. By eliminating manual processes, security teams are able to better protect employees and assets and can spend more time doing the high-value, proactive work for which they are trained. ◀



4 Video Surveillance Trends Alarm Companies Need to Know

Emerging technologies can strengthen partnerships, build RMR

DURING THE PAST TWO YEARS, ORGANIZATIONS AROUND THE GLOBE HAVE INCREASED their reliance on video surveillance. The explanation as to why is both simple and intricate all at once: Video has become the source of advanced security and operational insights that enables leaders to adapt to the contemporary business environment. And as the importance of video data has grown, intelligence has also been added to the fold.

Woodie Andrawos (wandrawos@nmccentral.com) is President of National Monitoring Center (www.nmccentral.com).

MARKET ADOPTION

When the coronavirus pandemic struck in 2020, many offices were left vacant. This meant that there were fewer individuals onsite to deter criminals from breaking in and stealing valuable equipment or, possibly worse, private data and trade secrets. This is where security monitoring

services demonstrated their value.

Security monitoring centers were critical partners to enterprises all over the world during this time. Operators served as the eyes and ears of the businesses, diligently monitoring for alarms and unauthorized entries.

While alarm monitoring continues to be the backbone of the security industry, there are other technologies that have been introduced that enhance this service. Technology and innovation continue to advance at record speed, affecting every part of the security market. Keeping an eye on technology trends is critical to the future of an alarm business.

There are opportunities ahead to expand alarm company offerings, enhance relationships with central station partners, and prepare for new areas of growth as video surveillance evolves in the coming years.

BUILDING REVENUE WITH VIDEO

Recurring monthly revenue (RMR) has been transformed. As demand has propelled video-as-a-service offerings, many integrators and dealers have embraced a video-based RMR business model. While the concept remains the same, options are now available that can boost RMR more than ever before, such as proactive video monitoring. (*See below.*) Not only does this service deliver high-value RMR, it also helps alarm companies to develop stronger connections with their customers, leading to more trusting relationships that deliver opportunities

> KEEPING AN EYE ON TECHNOLOGY TRENDS IS CRITICAL TO THE FUTURE OF AN ALARM BUSINESS.

> WHEREAS CONVENTIONAL VIDEO SURVEILLANCE CAN ONLY SUPPORT SOLVING CRIMES AFTER THEY HAVE OCCURRED, PROACTIVE VIDEO MONITORING IS ABOUT *STOPPING* CRIMES.

for continued partnerships and growth.

INTELLIGENCE ABOUNDS

The connected world is shaped by demands for productivity and optimized experiences. However, connections and data mining cannot occur without transformative technologies. Emerging technologies – the AI-enabled devices and platforms being designed today – have dramatically changed how we protect our people, property and assets. Comprehensive systems must sustain openness and efficiently integrate with other devices and services to provide quick scalability and long-term return on investment. As more AI-based solutions are deployed, the opportunity to incorporate them into a video monitoring platform is highly valuable.

THINKING PROACTIVELY

The security industry has long been a reactive market. Traditionally, security leaders fund services and technologies that support the investigation of a crime

after the fact. But times have changed. Modern solutions intelligently evaluate a problem and deliver the details required to stop an event before it becomes a complex and costly situation. Proactive video monitoring (PVM) is one of these solutions. Whereas conventional video surveillance can only support solving crimes after they have occurred, PVM is about *stopping* crimes. PVM directs immediate attention to unauthorized activity, allowing the video monitoring provider to intercede and inform local authorities before harm is done.

TO SECURITY AND BEYOND

Expectations regarding the use of video are growing. More businesses are looking to implement solutions that sustain intelligent processes across their infrastructure. They are evaluating and testing AI-supported strategies that supervise traffic flow, recognize trespassers in high-risk locations, and reduce fraud. The value of intelligent solutions is exceptional: They can aid businesses in identifying the video data that matters most to the company and produce considerably more promising results than traditional approaches.

Rapid technological advancement is happening across the industry, but at least one thing has remained unchanged:

> INTELLIGENT SOLUTIONS CAN AID BUSINESSES IN IDENTIFYING THE VIDEO DATA THAT MATTERS MOST TO THE COMPANY AND PRODUCE CONSIDERABLY MORE PROMISING RESULTS THAN TRADITIONAL APPROACHES.

Security and safety are the highest priority. This fact will continue to drive video surveillance partnerships, integration and innovation onward, while promoting the development of new solutions. ◀

Data, Data Everywhere

The right tools can make security information actionable – even predictive

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

THE FUTURE OF THE SECURITY INDUSTRY IS RIGHT IN FRONT OF US, and it is being driven by data from sensors, smart devices, mobile phones, and other intelligent technologies. This connected environment leads to new opportunities to make informed, real-time security decisions. However, harvesting relevant information is only half of the equation. Security leaders need to make the data actionable to experience its true value.

Security practitioners have always used data to identify new risks, emerging trends, and program enhancements. But locating the correct information at the right time within vast databases is equivalent to finding a needle in a haystack. To extract value from captured information quickly and efficiently, security leaders are turning to technologies that can help automate data mining to identify what matters most. Deploying and using these platforms, including situational awareness solutions, unified software, and artificial intelligence-based devices, can be complex. If not deployed correctly, missed opportunities may result.

Modern security leaders rely on large amounts of data from connected devices, such as video surveillance cameras and access control sensors. Many are not experts at information analysis, however, so they often turn to specialists to work on identifying what is needed to gain operational benefits. This can be an expensive approach.

The intelligent security operations center is designed to address this challenge head-on. By bringing multiple security systems and devices into a single interface and exposing it to an analytic layer, security practitioners can see what is happening at any given time and, more importantly, how it impacts the security program. Unifying information into a centralized hub allows security leaders to embrace a predictive security model and more efficient program management.

> UNIFYING INFORMATION INTO A CENTRALIZED HUB ALLOWS SECURITY LEADERS TO EMBRACE A PREDICTIVE SECURITY MODEL AND MORE EFFICIENT PROGRAM MANAGEMENT.

By aggregating data capture, stakeholders are empowered to spot opportunities and risks

> STAKEHOLDERS NEED WAYS TO TRANSFORM RAW DATA INTO VALUABLE INSIGHTS THAT EMPOWER THEM TO MAKE INFORMED, INTELLIGENT DECISIONS.

by cultivating intelligence and managing and responding to situations more efficiently. With a single view across what were once disparate systems and technologies, security leaders experience new levels of situational awareness, lowered operational costs, and increased efficiency. A centralized approach also allows security information to be shared with other parties, including first responders, private businesses and local agencies. The ability to quickly connect and share findings during a security incident can be a decisive factor when rapid response is paramount.

Having the correct data at the right time helps protect what matters most: people, assets and infrastructure. By gaining additional insights into the data that are most important to a business, security leaders have the opportunity to rise above the noise – orchestrating the pieces that make up their security program for better command and control.

These centralized security solutions are being adopted by organizations across the globe because they are an ideal way to build an effective program and support increased collaboration internally and externally. Security teams are empowered to analyze data points to address future risks and achieve greater situational awareness across the enterprise.

This approach is important because intelligent systems and sensors are the backbone of any modern security program. Data obtained from smart security solutions help ensure safety and security. To achieve these goals, however, stakeholders need ways to transform raw data into valuable insights that empower them to make informed, intelligent decisions.

From video surveillance to health and safety monitoring systems to emergency response, security teams can streamline operations to help achieve higher levels of situational awareness, while gaining more visibility of their efforts.

Open, scalable, adaptable solutions support a converged infrastructure and a more secure program.

We live in a world where security leaders need to move faster than the time it takes to understand data. But they can stay one step ahead if they combine the security department's inherent investigative and risk management capabilities with advancements and technologies that empower growth. ◀

WE LIVE IN A WORLD WHERE SECURITY LEADERS NEED TO MOVE FASTER THAN THE TIME IT TAKES TO UNDERSTAND DATA.

Cloud Solutions Rise Above On-Premises

Flexibility and scalability lead to increased migrations

OVER THE PAST THREE YEARS, ONE OF THE HOTTEST TRENDS within the security market has been the growing demand for cloud-based video services. While many environments still have on-premises solutions, an increasing number of businesses see advantages in moving to the cloud.

The cloud delivers new efficiencies while reducing the complexity of video management, but, for many years, businesses were slow to embrace the technology. Common concerns have included bandwidth, data security, and scalability. Management of video streaming and capture in the cloud is improving, and the benefits of moving video management to the cloud now outweigh the drawbacks. From single-site locations with a few cameras up to multi-site operations with

Jeremy Scott (jeremy.s@arcules.com) is Senior Director of Sales for Arcules (www.arcules.com).

thousands of devices, video cloud services are easy to use, cost effective, and proven to provide significant value. They have become essential components of a proactive and reliable video security strategy.

VIDEO IS NOW CLOUD-READY

Many organizations have adopted a "cloud-first" strategy, with serious questions being raised if a workload is not capable of being run and managed in the cloud.

The challenges of managing hardware, especially at the edge, remain significant, so businesses with tens, hundreds, or even thousands of edge locations are solving the problem by moving to a cloud-heavy, edge-light strategy. Video was historically an outlier for several reasons, and it was not uncommon to have locally sourced break-fix companies providing services. Now, though, including video surveillance in the cloud-heavy, edge-light strategy offers benefits to both CIOs and CSOs, and cloud video services offer a mechanism to support this strategy.

ON-PREMISES EQUALS INFLEXIBILITY

Data is being stored and delivered in vastly different ways than 20 years ago. Leading technology companies provide data storage and management on a subscription basis that allows customers to turn services and capacity on and off depending on current requirements.

THE CHALLENGES OF MANAGING HARDWARE, ESPECIALLY AT THE EDGE, REMAIN SIGNIFICANT, SO BUSINESSES WITH TENS, HUNDREDS, OR EVEN THOUSANDS OF EDGE LOCATIONS ARE SOLVING THE PROBLEM BY MOVING TO A CLOUD-HEAVY, EDGE-LIGHT STRATEGY.

It is becoming harder to justify the estimation and guesswork associated with forecasting a three or five-year purchasing cycle for on-premises video infrastructure. This led, in part, to the rise of hyper-converged infrastructure for on-premises

> HYBRID CLOUD MODELS OFFER THE BEST OF BOTH WORLDS, ALLOWING FOR A MIX OF ON-PREMISES VIDEO TECHNOLOGY AND CLOUD SERVICES.

workloads, including video surveillance, but this is little more than a Band-Aid.

Being able to migrate a video surveillance workload to the cloud and further depopulate the corporate data center will provide a massive advantage for companies that are investing heavily in their cloud strategy.

MIGRATE YOUR WAY

It has become clear that cloud-based services are the future for both small to medium-sized businesses and enterprise organizations. As more and more companies see what the technology can do, there is a growing desire to transition video surveillance and data storage to the cloud, but this process requires a strategic approach.

Organizations must consider their current technology needs, goals for security and business operations, and the future of the business itself, all of which are dynamic and require flexibility for a smooth transition. Hybrid cloud provides businesses with that transitional opportunity.

Hybrid cloud models offer the best of both

worlds, allowing for a mix of on-premises video technology and cloud services. From an integrator perspective, this means obtaining recurring monthly revenue (RMR) and developing a long-term relationship with the customer. From an end user perspective, this means increased functionality without sacrificing the feature-rich and powerful video surveillance that is critical to modern organizations.

SECURE VIDEO DATA

With cyberattacks such as SolarWinds and Colonial Pipeline seemingly always in the news, the cybersecurity challenge can appear overwhelming.

Cloud service providers must be deeply and relentlessly focused on ensuring the security of systems and services. Working with proven cloud providers provides a secure infrastructure base, but it is also important to examine other areas.

Compliance with System and Organization Controls 2 Type 2 ensures that information security practices, policies, procedures and operations meet appropriate thresholds for security and confidentiality. SOC 2 is an auditing procedure that ensures service providers securely

In 2021, cybercrime cost organizations more than $6 trillion worldwide, a recent report found, with more than 50 percent of security incidents being caused by people within the organization.

manage customer data. Developed by the American Institute of Certified Public Accountants, SOC 2 defines criteria for managing customer data based on trust principles that every provider should incorporate in security and compliance initiatives.

Cloud service providers must ensure the utmost security of video data, and organizations should seek a partner that continually searches for new ways to provide data protection. The threat environment demands a commitment to reassess security protocols today, tomorrow and in the years ahead.

DESIGNED TO SCALE

One of the essential features of cloud architecture is that it is built to scale, so it can be modified as businesses evolve and grow. As processing, storage and camera requirements change, the cloud's scalability enables organizations to increase or decrease usage without

worrying about outdated software or hardware.

While cloud flexibility typically refers to its scalability, the term can also apply to its ability to provide organizations with options regarding system access. On-premises solutions are more rigid because they can typically only be controlled through a specific physical location. In contrast, cloud-based systems facilitate remote access from any device and location and have granular user permissions to control management roles. This level of flexibility promotes enhanced security efforts and faster response times to potential threats.

Cloud-ready video combined with robust solutions that simplify the adoption of a cloud infrastructure puts a business in an advantageous technological position. As a result, the C-suite is taking a keen interest in the enduring value of cloud migration. ◀

> CLOUD SERVICE PROVIDERS MUST ENSURE THE UTMOST SECURITY OF VIDEO DATA, AND ORGANIZATIONS SHOULD SEEK A PARTNER THAT CONTINUALLY SEARCHES FOR NEW WAYS TO PROVIDE DATA PROTECTION.

AI in Security and Psychology

Emerging technology tools must account for human factors

Jill Frack (jfrack@istonline.com) is Senior Project Manager for Integrated Security Technologies (www.istonline.com).

Artificial intelligence (AI) is now a part of our daily lives, and how we respond to such technological changes is based largely on psychology and personal experiences, both good and bad. As we examine the impact of AI, it is important to understand how an individual's psychology can shape their views.

The Covid-19 pandemic has created a new set of issues concerning technology, data privacy and AI. Many organizations have software for reporting and analyzing data and, after a security incident occurs, it is important to conduct this analysis and use AI to try to prevent it from happening again. This article will explore examples of utilizing security measures in operations, inventory, personnel and safety.

REMOTE WORK IMPACTS

With various new technologies available, organizations can now hire the best people, no matter where they live, rather than having to limit the applicant pool to a certain radius from the office. Technology has allowed organizations to extend their customer reach around the globe, as well. As security industry professionals, we have a responsibility to our customers to ensure that their technology functions correctly. We all know that technology is great when it works and frustrating when it doesn't, which leads us to the question of whether technology is an asset or a liability for an organization. The technology that an organization uses to protect employees, customers and assets can impact the organizational culture and the level of job satisfaction.

> THE TECHNOLOGY THAT AN ORGANIZATION USES TO PROTECT EMPLOYEES, CUSTOMERS AND ASSETS CAN IMPACT THE ORGANIZATIONAL CULTURE AND THE LEVEL OF JOB SATISFACTION.

During the pandemic, people were forced to adjust their work locations and utilize technology that they previously might not

> WHEN UTILIZING DATA FROM A SECURITY SYSTEM, IT IS IMPORTANT TO ASSESS THE USER EXPERIENCE AND FEEDBACK BEFORE CREATING AI MODELS FOR FUTURE SITUATIONS.

have used to perform their jobs. As workers return to the office, some people are thankful, while others are upset. A person's level of job satisfaction can be linked to how well the technology that has been implemented allows the individual to perform his or her job. When utilizing data from a security system, it is important to assess the user experience and feedback before creating AI models for future situations.

EMPLOYEE SURVEYS

Employee surveys can be useful to organizations if the data is properly collected and analyzed. When deploying AI, it is important to use the correct statistical analysis tools to ensure that the results are actually related to what is being measured. Many places conduct an annual employee survey and announce that the

ratings are higher or lower than the year before. It is important, however, to analyze the data properly to see if there is another factor that might have influenced the results. For example, if you have employees who are on a fixed schedule and you notice that a manager is editing timecard start or stop times, it is important to assess why this is occurring.

Some organizations require employees to clock in once they arrive at the first job site, while others require workers to log their hours immediately upon leaving for the day. In both situations, the process could ultimately affect a person's performance level based on their psychological evaluation of the condition. Additionally,

> AI IS A VALUABLE TOOL BUT IT STILL NEEDS HUMAN INTERVENTION.

bad traffic or a near-accident while driving to work could potentially lower their productivity for the day. There are many such ways in which psychology can influence the data that is being analyzed.

PRACTICAL APPLICATIONS

Within access control, integrations can be done for operations management related to employee time recording based on GPS units in vehicles. This can serve as a time-tracking system to help alleviate the problem of hours not being recorded as required. Additionally, from a safety management perspective, AI can identify driving trends for each vehicle and/or driver.

Depending on the department or setting, data can be collected through various methods and utilized to help the organization's decision-making concerning financial and strategic goals. Another possible use of AI is for inventory

management, so that, for example, alerts are automatically triggered or orders placed when the stock of items reaches certain levels. Within the security industry, high-value items need to be tracked to ensure that they make it to the correct job site without being stolen or misplaced. Tracking devices enable a company to know the exact location of an item. Some people are even starting to attach these devices to their suitcases when they fly.

In a retail or service setting such as a bank or hospital, AI can help with personnel management by analyzing video surveillance and access control to determine the peak level of activity for employees and customers. Automatically generated

> AUTOMATICALLY GENERATED DATA CAN LEAD TO INSIGHTS REGARDING POTENTIAL PROCESS IMPROVEMENTS TO ENSURE THAT SECURITY AND OTHER DEPARTMENTS ARE FUNCTIONING OPTIMALLY.

data can lead to insights regarding potential process improvements to ensure that security and other departments are functioning optimally.

CONCLUSION

AI is a valuable tool but it still needs human intervention, whether on the frontend, setting up the algorithms, on the backend, providing recommendations for organizations to implement, or both. Individual psychology affects how all technology is analyzed and utilized. When assessing security, organizations must connect the dots between the data to understand the full picture of what is taking place. ◀

Ready to improve how you manage security projects?

Improve Your Security Project Management Skills with SIA Training and Certification Programs.

SPM
SECURITYPROJECTMANAGEMENT

More than just knowing the technology, successful project management involves budgeting, client management, timeline execution and more.

Learn more at securityindustry.org/spm

CSPM
CERTIFIED SECURITY PROJECT MANAGER

This highly-respected credential can move your career forward and propel your business. The CSPM credential informs clients that you can successfully manage complex, technical security projects.

Learn more at securityindustry.org/cspm

Security Industry Association
securityindustry.org

SIA

VERIFIED OSDP™ VERIFIED

When you need interoperable, high-security access control solutions, ask for products that bear the OSDP Verified mark.

OSDP Verified means these products have been tested by the Security Industry Association as conforming to one or more profiles of the OSDP standard. For you, that means peace of mind knowing these solutions can communicate securely and seamlessly.

To learn more about OSDP and find a guide to OSDP Verified products,

visit securityindustry.org/OSDP

Security Industry Association
securityindustry.org

SIA