GDPR IS A CHANGE AGENT
GDPR is a driver to change old, inefficient business data protection and availability practices. p03

THE ROLE OF THE INTELLIGENT SOC
The intelligent security operations center increases situational awareness and aids response efforts. p04

AN EYE ON MARIJUANA DISPENSARIES
Intelligent video is critical for security and provides a competitive advantage for retail sales. p05

NON-PROFIT ADOPTS INTRUSION DETECTION
A Johannesburg, South Africa, non-profit adopts a solution to enhance security in the city. p10

A SUPPLEMENT OF SECURITY MANAGEMENT

ALL EARS
As humans rapidly adopt voice technology, these listening devices are waiting to respond. p06
B.I.G. ENTERPRISES ‘WEDGE 2.0’ GUARDS ACCESS POINTS THROUGHOUT TEXAS CAMPUS

PREFAB GUARD BOOTH BEATS OUT ITS BUILT-ON-SITE BOOTH COUNTERPART IN TERMS OF PRICE—ONE OF FIRST IN INDUSTRY MADE TO MEET THE LEED PROGRAM FOR ENVIRONMENTAL RESPONSIBILITY

By B.I.G. Enterprises, Inc.

WIDELY KNOWN for their ability to take custom designs and turn them into affordable prefab units, B.I.G. Enterprises, Inc. (www.bigbooth.com) has unveiled its innovative ‘Wedge,’ 2.0. This updated model was selected by a global technology design and manufacturing company to provide protection for all access control points at the company’s extensive campus in Texas.

The original design for the facility was created by an architect who soon discovered that the design on paper would be way over budget to build on-site. But turning to B.I.G. and its reputation for creating reasonably priced pre-fab units, the same architect was able to realize an architecturally superior and under-budget prefab booth fully factory built and delivered ready for installation.

Though intricate in design, ‘The Wedge 2.0’ booth achieved a 25% cost savings through B.I.G.’s pre-fab construction.

For durability and longevity, the unit is all galvanized steel construction with galvanized steel floor and floor frame, and galvanized steel roof and ceiling. The roof is what stands out and is how the name “The Wedge” was created: A unique wedge overhang design with clean lines and architectural detail.

Other key features to these booths are the butt joint glass corners, large full-height sliding glass door with concealed hanger track and rollers, factory prep including flashing and lath on the outside walls for on-site application of the smooth-coat concrete detail at the lower front and rear walls.

FULL COMPLIANCE IN ALL STATES

B.I.G. manufactures this unit, and all units to be in full compliance to all State codes including energy code. Additionally, B.I.G. takes great pride on incorporating materials and components to make the unit meet the Leadership in Energy and Environmental Design (LEED) program.

LEED is one of the most popular green building certification programs used worldwide. Developed by the non-profit U.S. Green Building Council (USGBC) it includes a set of rating systems for the design, construction, operation, and maintenance of green buildings, homes, and neighborhoods that aims to help building owners and operators be environmentally responsible and use resources efficiently.

For product info #101 securitymgmt.hotims.com
PRIVACY HAS BECOME a worldwide concern as citizens worry about the safety of personal information stored in databases owned and controlled by private and public organizations.

Recent database hacks that compromised personal information about millions of people have only heightened that anxiety. Names, addresses, phone numbers, birthdates, passwords, and other sensitive information are sold on the Internet. Many people have lost faith in the way their data is collected and protected.

The European Union addressed these concerns with May 2018’s General Data Protection Regulation (GDPR) enforcement deadline. While GDPR is EU-centric, its impacts are global. All organizations must follow the regulations for controlling or processing personal data about any EU citizen.

GDPR places substantial constraints on what were largely uncontrolled data-collection practices. EU consumers can now protect their privacy and control how their data is collected and used by opting in, not out, of a company’s policies. An organization’s failure to comply can result in penalties of up to €20 million or 4 percent of a company’s annual global revenue, whichever is greater.

GDPR’s basic concepts are simple enough; citizens have a right to know the information being collected about them, understand how it is used, and be provided with a simple way to delete their data at any time.

GDPR defines personal data as any information related to an identifiable person. That might include a person’s name, home and email addresses, passwords, birthdate, driver’s license number, gender, race, political affiliations, and other categories, such as security-related data and video.

While the security industry was not the prime target of the regulations, GDPR limits how organizations use and collect video surveillance and access control data. The rules consider video to be the personal data of those seen in live or recorded images. Access control databases contain personal information about employees, as well as that of contractors and visitors who share information about themselves in exchange for a temporary pass.

GDPR requires cybersecurity controls ensuring that access to security-related data is available only to those authorized to view it. Typically, passwords have protected databases. But even the strongest password can be shared with anyone.

A data processor may add workstation card readers or keypads to create a second layer of authentication. Again, cards and personal identification numbers are no guarantee the person accessing files is authorized to do so.

**Biometrics.** GDPR requires active consent and represents a choice made by the consumer. Biometric identification can play an integral role in providing an active real-time choice for granting the sharing of data.

Biometrics measure physical characteristics, such as iris patterns, fingerprints, or facial features—something only the owner can possess. Two-factor authentication is possible by combining biometric and access card readers or keypads at computers storing personal data. Passwords become virtually obsolete. Database information remains private, accessible only to authorized viewers.

Biometric technologies are now commonplace. They are embedded into most smartphones. Biometrics are used for access control, time and attendance, border crossings, national ID cards, voter registration, and more. Biometric readers can also authenticate consumers registering for websites or making purchases on the Internet.

GDPR is a driver to change old, inefficient business data protection, privacy, and availability practices.

MOHAMMED MURAD IS VICE PRESIDENT, GLOBAL DEVELOPMENT, AT IRIS ID.
THOUGHT LEADERSHIP: OPERATION CENTERS

THE CRITICAL ROLE OF THE INTELLIGENT SOC

THE INTELLIGENT SECURITY OPERATIONS CENTER INCREASES SITUATIONAL AWARENESS.

By Alan Stoddard

AS THREAT VECTORS continue to increase in complexity and severity, the volume of data needed to be analyzed grows at an exponential rate. Tasked with implementing comprehensive risk identification, mitigation, and response plans to secure the enterprise, security practitioners must sort through data to identify actionable intelligence—while resources to manage, analyze, and react to it become more constrained. How to effectively and efficiently manage and examine all the data available has become a mission-critical task for today’s security leaders.

Deploying a physical security information management (PSIM) solution has traditionally been the response to this challenge. It can consolidate data from disparate sources and streamline the flow of information to key stakeholders.

Dealing with today’s challenges means CSOs need to create integrated security environments that employ technology tools, automating and integrating a coordinated response.

THE INTELLIGENT SOC
The Intelligent Security Operations Center (ISOC) not only collects and manages data from disparate security subsystems and presents it to the operator, it also makes data available to the analytics layer. Organizations can employ situation-specific tools to look across various subsystems to identify actionable intelligence. This frees up time for operators and delivers enhanced threat identification. Furthermore, the ISOC automates threat response—coordinating between operators and responders to provide an integrated threat management system.

By incorporating technologies that unify data collection, correlation, analysis, and response, security departments can correlate information and funnel that data to the right analytic engines, sharing it with the correct stakeholders. When all security domains—IT, physical, and cyber—collaborate, the business increases overall operational efficiency.

TRANSFORMING DATA INTO INTELLIGENCE
As the digital world evolves, CSOs seek to find new ways to capture data, correlate it, and then leverage it to make the most informed decisions. By collecting intelligence from digital sensors and systems such as video surveillance cameras, building systems, weather sensors, and more, operators can identify potential risks and efficiently respond to situations.

A centralized software platform also allows information to be shared with external agencies, employees, and first responders. With an enterprise-wide view, organizations experience improved response times, lowered operational costs, and increased employee safety.

Automation and intelligent solutions, such as artificial intelligence, help organizations make sense of vast amounts of data. These integrated applications can automatically pinpoint potential breaches and significant events and send alerts to the appropriate personnel.

When traditional command centers rely mostly on call and radio updates, visibility can be limited. But centralized software solutions enable operators to oversee a situation and engage with and direct the response force.

LOOKING AHEAD
In today’s global business environment, opportunities, requirements, and regulations can vary widely, change quickly, and evolve over time.

Transforming the traditional SOC into a unified ISOC that combines cyber, traditional security, digital devices, and situational awareness technologies will mitigate advanced threats—either forensically or in real time. All of this contributes to a predictive risk model that prevents attacks before more significant damage is caused.

ALAN STODDARD IS VICE PRESIDENT AND GENERAL MANAGER, SITUATIONAL INTELLIGENCE SOLUTIONS, AT VERINT.
OPENING A NEW RETAIL STORE is an exciting prospect for any business owner—especially in the emerging cannabis market where customers are eager to purchase safe, legal product, while enjoying an in-store shopping experience.

Video surveillance is one technology that’s a must-have for retail dispensaries. Not only is it mandated in many jurisdictions, including all U.S. states where recreational cannabis can be legally sold, it’s also critical to ensuring the security of employees, customers, and merchandise. An intelligent video solution should also deliver loss prevention and operational tools to provide the dispensary with a competitive advantage.

CUSTOMER SERVICE
Using an intelligent video solution to assess and improve customer service in a retail dispensary is one of the most effective applications for many operators.

By combining surveillance video with analytics like people counting, queue length monitoring, or dwell time, operators can generate reports with charts and graphs to see how long customers waited in line, determine which marketing or educational displays generated the most attention, and identify when people are leaving the store without making a purchase.

Owners can set up automated reports that include snapshot images from different areas of their store—or multiple stores—so they can check for empty shelves, proper signage, and opening and closing times.

This information helps owners quickly identify areas for improvement in their retail dispensaries. It enables them to set up software alerts triggered by unusual transactions—such as voids over a set amount or suspect employee discounts—and investigate incidents faster by tying receipt data to recorded video.

Owners can use their video system to run searches on a wide variety of data, including employee number, transaction date and time, and more, across multiple locations simultaneously.

INVENTORY TRACKING
In stores where RFID tags are used to track cannabis products and merchandise, tying that data to intelligent video can deliver several benefits.

An integrated solution enables retail owners to search on any data contained in the RFID tag’s electronic product code, such as the type of item or product serial number.

This search capability is invaluable when merchandise goes missing. Not only can owners use the video solution to pinpoint the last known location of the item, they can also retrieve the recorded video to see how—and where—the item went missing. Perhaps the merchandise went out the back door or through the storefront in a shoplifter’s pocket.

The powerful combination of RFID tracking and recorded video makes it easier to solve the mystery of disappearing items. It provides strong evidence that can be used to recoup losses or be shared with law enforcement if a crime is committed.

Intelligent video provides retail dispensary owners with a unique view of their business, especially when used in combination with other types of data. It can help with compliance, inventory tracking, loss prevention, customer service, and more.

For owners already investing in video surveillance systems for security, moving to a more advanced solution that can provide practical business insights is worth considering as part of a smart return on investment strategy.

JEFF CORRAL IS RESPONSIBLE FOR STRATEGIC PARTNERSHIPS AND INTEGRATIONS AT MARCH NETWORKS, A WORLD LEADER IN THE DELIVERY OF VIDEO SURVEILLANCE AND VIDEO-BASED BUSINESS INTELLIGENCE SOLUTIONS FOR THE CANNABIS INDUSTRY.
“HEY, SECURITY...”

HUMANS ARE ADOPTING VOICE TECHNOLOGY AT A RAPID RATE. SOON, SECURITY TECHNOLOGY WILL FOLLOW SUIT.

By Megan Gates

For most of us, they’ve always gone together. The computer monitor, the keyboard, and the mouse. All three have been necessary components to complete tasks quickly and accurately. But in the future, two of these devices are likely to be used far less as people adopt voice technology at an almost unprecedented rate.
In a recent survey, Pricewaterhouse-Coopers (PwC) found that 90 percent of people were familiar with voice-enabled products and devices. And of that 90 percent, 72 percent had a voice assistant—particularly younger consumers, and households with children or income of more than $100,000.

Voice assistants are digital assistants that rely on natural language processing, voice recognition, and speech synthesis to function. For instance, Apple’s Siri is a voice assistant that users interact with on their iPhone by saying “Hey, Siri,”

and asking her to perform a function for them—like setting an alarm.

“Though the youngest consumers we surveyed (18- to 24-year-olds) are adopting voice technology at a faster rate than their older counterparts, they are statistically more likely to use their voice assistants less,” according to PwC’s Consumer Intelligence Series. “Twenty-five- to forty-nine-year-olds are using them more often and are statistically more likely to be considered ‘heavy’ users.”

These devices using voice technology range from smartphones to tablets to television remotes to wearables, like smart watches. Those surveyed by PwC said voice assistants make it easier to perform normal day-to-day activities—conducting Internet searches or texting friends. But consumers still prefer to manually perform tasks they see as more complex—purchasing products online or talking to a customer service representative.

PwC found, however, that voice assistants help people feel organized (50 percent), informed (45 percent), happy (37 percent), smart (35 percent), confident (31 percent), and free (30 percent). And this is with only a general knowledge of what voice devices and assistants are capable of.

“...there’s no denying that voice is the future,” PwC explained. “The technology will continue to drive and shift consumer behavior, and companies need to prepare and adjust accordingly. Search, advertising, content, and commerce are being impacted industrywide as consumers transform the way they interact with brands as the result of voice technology.”

Because of this, it’s critical for technology developers to keep the power of voice—and voice search—in mind, wrote Alex Robbio, a Forbes Council contributor and president of Belatrix Software.

“It means shifting from thinking in terms of the customer or user using the software via swiping on their phone or clicking on a mouse to how to go about delivering a seamless experience via voice,” Robbio explained. “It means delivering experiences in a world where immediacy is key. People want to ask a question and receive immediate and insightful information.”

And consumers bring this expectation with them into their workspaces, demanding more efficient use of the technology that’s available to them. The security industry began to see this with the rise of search options based on video analytics.

For example, Avigilon released Appearance Search in June 2016. It used analytics to sort through hours of footage to locate people or vehicles of interest. End users could click using a mouse on a person in a frame of video and ask the system to pull all other instances where that person was recorded. The product was designed to improve incident response time and enhance investigations.

“What excites me is that we’re now introducing a true search engine for video,” said Dr. Mahesh Saptharishi, then-Chief Technology Officer (currently CTO for Motorola, which acquired Avigilon in 2018), on the product’s release. “Appearance Search is the first step to provide true video content-based search.”

Now, with the rapid development of voice technology and voice assistants, technology will move towards allowing end users to make verbal search requests of systems—ideally speeding up the search process and eliminating human error.

One company testing this in a pilot program is CodeLynx out of Charleston, South Carolina. After Microsoft released its HoloLens product, a virtual reality headset that provides an augmented reality experience, CodeLynx began developing its Augmented Reality for Integrated Electronic Security (ARIES) platform.
ARIES creates a wearable heads-up display on the HoloLens that brings video feeds, access control, intrusion, and alert information to users. It also provides security operations centers with a real-time body-worn display of what field units are seeing and interacting with.

ARIES is also overlaid with natural language processing, so end users can verbally ask it to provide specific information instead of typing a request in via a keyboard or selecting click through options using a mouse.

“In the security space, someone can walk up to a door and say, ‘Show me the last three people to walk through this door,’” says Drew Weston, CPP, director of sales and marketing for CodeLynx and a member of the ASIS International Security and Applied Sciences ad hoc Council. ARIES then conducts a query and will pull the respective footage to show who walked through that door.

ARIES integrates with AMAG Symmetry and Avigilon for now, and Weston says that its largest adoption is in a pilot program with an unnamed end user. CodeLynx has also seen interest for using ARIES to monitor special events and access control at facilities.

Right now, the platform only accepts verbal commands in English, but Weston says CodeLynx may add additional languages to its capabilities in the future after the HoloLens 3 is released later this year.

And his thoughts on the future of technology mirror PwC and Robbio’s sentiments that the keyboard and mouse will fall by the wayside.

“I have a three-year-old and a five-year-old; they won’t understand the idea of using a keyboard and a mouse to interact with a computer in the future,” Weston says. “The idea that you had to sit down and use this arrangement of keys to talk to a computer won’t compute.”

MEGAN GATES IS EDITOR-IN-CHIEF OF SECURITY TECHNOLOGY. CONTACT HER AT MEGAN.GATES@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @MGNGATES.
JOHANNESBURG, South Africa, is a city plagued by burglaries, home invasions, car hijackings, and theft. Police resources are stretched, and private security guards—once the norm at gated communities and affluent neighborhoods—are less affordable as wages have increased in line with a fair pay policy.

Challenges. Community Active Protection (CAP) was founded as a non-profit organization in 2006 in response to the high levels of crime in Johannesburg. CAP has taken a proactive approach to crime prevention, recruiting highly capable teams to patrol streets and motivating citizens to report suspicious activity to CAP’s Command Center, a state-of-the-art control room that fields all calls and dispatches CAP Tactical Units. The CAP initiative has proven extremely effective, reducing crime in monitored areas by a reported 80 to 90 percent.

NON-PROFIT ADOPTS INTRUSION DETECTION SOLUTION

By Roni Kresner
“THIS IS THE BEST ANALYTICS PRODUCT WE’VE SEEN. ALMOST ALL OF THE ALERTS WE RECEIVE ARE ACCURATE.”

Additionally, in response to customer demand for reactive armed guards, CAP created an off-site monitoring service in 2016 called CAP Smart Guard, which is deployed primarily at and around gated residences, as well as private homes, using privately owned cameras connected to the CAP network.

Solution. CAP was seeking an intrusion detection solution for the Smart Guard service to increase the level of protection and response offered to its customers. It turned to Agent Video Intelligence’s (Agent Vi) innoVi Remote Guarding software as a service (SaaS) to receive accurate and automatic detections of security breaches at the remote sites that CAP monitors.

Cameras at the remote sites are connect- ed to the service via innoVi Edge, a compact appliance preloaded with Agent Vi’s video analytics software, where initial video analysis is performed. InnoVi Edge connects any ONVIF/RTSP IP camera to innoVi Core (a server hosted in the Agent Vi data center) for high-level processing and data analysis.

CAP defines events of interest, including intruders entering private property, movement in sterile zones, and cars stopped in unauthorized areas. When an event is detected, innoVi generates an alert that is sent to CAP’s Command Center and displayed in its Milestone XProtect video management software, along with an event clip that provides video verification of the security breach. The alerts and clips are viewed by the CAP Command Center operators in the XProtect Smart Client. At the same time, an image may be sent by CAP’s control room operators to the client’s mobile device. Operators quickly review the clip and decide on the best course of action.

CAP is also employing Agent Vi’s Deep Learning-driven Anomaly Detection capability. Agent Vi’s Deep Learning infrastructure trains on millions of real-life images taken from surveillance video built over 15 years of Agent Vi’s data collection. Based on this, the algorithm knows to classify different target types (for example, person, car, or object). Once connected to a CAP camera, the Anomaly Detection algorithm learns the specific scene and familiarizes itself with normal patterns and expected behavior. The Anomaly Detection capability can then identify and alert the Command Center to events that are out of the ordinary.

Results. CAP executives say the organization is highly satisfied with innoVi’s technology, performance, and business model. “We’re finding that innoVi’s performance at the property line is significantly better than other systems we’ve used,” says CAP Chief Operating Officer Sean Jammy. “And that’s in complex environments like streets, gates, and the like.”

Having tested several other solutions, Jammy says the Agent Vi solution stood out against products that returned a high level of false alerts. “This is the best analytics product we’ve seen. Almost all of the alerts we receive are accurate,” he notes.

Agent Vi’s innoVi is camera-agnostic, able to connect through innoVi Edge to any ONVIF/RTSP IP camera, with no need to replace existing cameras, leading to a savings in time and money.

CAP says the solution has helped stop crime before it happens. “Our biggest success so far with innoVi is that not one of our monitored sites has experienced an incident of crime at the property line,” Jammy notes. “This is thanks to multiple interventions by the CAP team, following innoVi detections and alerts.”

Another indicator of success for CAP is a high level of customer satisfaction. “We’re giving our clients a service that is more effective, significantly less expensive than a dedicated 24-hour guard, and doesn’t escalate in cost,” Jammy says. “Plus, a human guard doesn’t include a perimeter detection solution.”

These continual learning and enhancement processes are key to achieving the best results, Jammy adds. “Our success will be measured in providing an effective, sustainable solution over a long period.”

Roni Kresner is Marketing Manager of Agent Video Intelligence (Agent Vi), June 2019 Security Technology 11
Don’t risk the failure to communicate a fire alarm

Upgrade any FACP to meet today’s fire code & save thousands of dollars annually vs. the two landlines each StarLink LTE Communicator replaces

• Don’t leave fire alarm control panels in jeopardy of failing to communicate when weather, events or Telephone Companies cut off leased hardlines without notice

• You don’t need a few Fire Alarm System, just a new way to communicate via modern fast LTE Cellular networks - StarLink Fire is the category leader

• Economically and quickly installs with any new or existing FACP brand, 12V or 24V, without requiring additional power supply or conduit

• Improve alarm response times when seconds matter most, with StarLink Fire® cellular LTE reporting to any Monitoring Station & save $1000’s of budget dollars per year as each replaces 2 POTs lines/FACP

• Fire-code-compliant & proven to work, even where others won’t, on today’s most cyber-secure & long life LTE® CAT1 network, using StarLink Signal Boost™ & twin dual diversity antennae for max. signal acquisition & null avoidance (receives signals simultaneously on both)

• NFPA 72 & UL 864 Code Compliant

Actual Net Savings at
Houston Independent
School District
with StarLink

$840,000
StarLink
Savings

$507,000
StarLink
Savings

$165,000
StarLink
Savings

Year 3

Year 5

$165,000
StarLink
Savings

Year 1

- “We saved over $13,000 the first month, even factoring equipment costs replacing 600 POTs lines campus wide.”
   Byron Thurmond, Former Security Manager for HISD

For product info #103 securitymgmt.hotims.com

StarLink, StarLink Fire®, Signal Boost are trademarks of Napco.