SECURITY TECHNOLOGY

ROBOTS SUPPORT RETURN-TO-WORK INITIATIVES

Robots are an ideal way to add automated solutions to a security program to stop the spread of COVID-19. **p03**

SMART SURVEILLANCE AIDS EMPLOYEE HEALTH

Security professionals are searching for additional ways to leverage their existing infrastructure to improve operations and protect employees. **p04**

MANAGING THE SOC IN A TIME OF CRISIS

Security managers can leverage automation to help employees—and themselves—combat burnout and organizational vulnerability. **p06**

A SUPPLEMENT OF SECURITY MANAGEMENT

SEPTEMBER 2020



Putting Your Data to Work to Protect Your Organization

As employees begin to return to work sites, organizations must protect their employees and visitors from COVID-19. AMAG Technology's **Symmetry Business Intelligence** analyzes facility occupancy by monitoring the time of day when high traffic flow occurs, minimizing exposure. Understanding facility usage helps organizations determine cleaning schedules to help reduce the risk of infection. As a contact tracing solution, it helps identify who was in contact with an infected person and when the interaction occurred. Using physical security data via a risk score, organizations can provide a safer working environment.

See how Symmetry Business Intelligence can help your organization.



amag.com/businessintelligence





ROBOTS SUPPORT RETURN-TO-WORK INITIATIVES

ROBOTS ARE AN IDEAL WAY TO ADD AUTOMATED SOLUTIONS TO A SECURITY PROGRAM TO STOP THE SPREAD OF COVID-19.

By Travis Devle

THE COVID-19 PANDEMIC seems like an inflection point for the safety and security industry, and I can't help but think back to past crises and the changes they precipitated—namely the 9/11 terror attacks.

Seemingly, out of nowhere, America was vulnerable. The security industry was at the forefront and had to keep up with sweeping U.S. federal changes, including the Aviation and Transportation Security Act, the Patriot Act, the Enhanced Border Security and Visa Entry Reform Act, and the International Code Council's post-9/11 building codes. Task forces sprang into action—groups such as state-led counterterrorism bureaus, federally mandated security consultants, and Joint Terrorism Task Forces. The security apparatus in America crossed its Rubicon and irrevocably committed to making the nation a harder target against domestic and international threats.

The security sector today faces a similar inflection point with COVID-19. Once again, urgency is forcing innovation. Security manufacturers are springing to market with incredible new ideas, disruptive technology, and equipment, similar to reactions in the post-9/11 world. Technology is rapidly propelling business transformation.

This time, however, businesses are looking to the U.S. Centers for Disease Control and Prevention (CDC) for guidance on how to safely return to the office. Guidelines to mitigate the spread of COVID-19 are focused on stay-at-home initiatives, promoting social distancing, wearing appropriate personal protective equipment (PPE), and screening for elevated temperatures.

Upsettingly, however, these safety guidelines have begun taking on partisan division in today's polarizing political climate. It was heartbreaking to hear about the murder of Family Dollar security officer Calvin Munerlyn in May 2020; Munerlyn was shot and killed while on duty for enforcing Michigan's state-mandated face mask policy. Violent reactions to CDC guidelines are all too common.

The key to safely moving forward is striking the right balance between technology and humanity, and robots are uniquely positioned to respond. Robots are nonpartisan and unbiased, and



Photo illustration by iStock

they can accomplish all CDC-recommended critical tasks while reducing human exposure and breaking the chain of infection.

Robots can not only monitor people's behaviors through machine learning algorithms, but they can also respond and correct issues as they happen. Utilizing two-way video and voice communications, robots can gently change people's behavior in the workspace while limiting human exposure to COVID-19.

Elevated temperature is a primary symptom of COVID-19. Traditional methods for businesses to conduct temperature checks are difficult to scale, unreliable, and put those administering the tests at risk. Robots can be used to conduct reliable skin temperature scans through non-invasive measurement of skin temperature via tear duct scans. Using thermal imaging calibration from blackbody radiation (small devices capable of emitting a known constant temperature) paired with a thermal camera, robots can alert employers of anyone with a temperature exceeding 100.4 degrees Fahrenheit. Remote operators can then direct that person for secondary screening, without putting people in harm's way.

Robots can screen for elevated temperature, verify PPE compliance, and enforce social distancing guidelines while avoiding additional exposure for security officers and other building occupants. Robots provide perfect recall, unlimited attention, and no bias. They are a solution to a difficult situation, and an ideal way to add automated solutions to an existing security program.

TRAVIS DEYLE IS CO-FOUNDER AND CEO OF COBALT ROBOTICS.



SMART SURVEILLANCE AIDS EMPLOYEE HEALTH AND BUILDING OPTIMIZATION

SECURITY PROFESSIONALS ARE SEARCHING FOR ADDITIONAL WAYS TO LEVERAGE THEIR EXISTING INFRASTRUCTURE.

By Fabio Marti

THE BEGINNING OF 2020 saw facilities of all sizes adjusting to new health and safety guidelines as the full extent of the impact of COVID-19 pandemic was realized. The Internet of Things (IoT) was a driving force behind smart buildings with its ability to optimize building operations and goals, such as reducing energy consumption and space utilization.

Facility operators are now pivoting to focus on helping to transition employees back to work and reopening their businesses. As such, security professionals are searching for additional ways to leverage existing infrastructure beyond traditional capabilities.

Developments in technology have ushered in a new breed of smart security cameras that analyze data-rich video to trigger appropriate actions through the use of smart apps on the device. By effectively making smart cameras into multipurpose IoT sensors, these devices can be equipped with applications to address COVID-19 related needs and repurposed to improve building optimization and operations after the pandemic.

OCCUPANCY MANAGEMENT

In a commercial building, such as a high-rise office building that thousands of people may enter and exit every day, there are now regulations to enforce social distancing and cap occupancy. Video-based people counting and crowd management applications



are effective tools to manage occupancy and encourage social distancing. These applications can streamline processes and cut costs by eliminating the need for manual tracking of occupants.

When maximum occupancy is reached, proper personnel receive an alert to take action. This process can be fully automated, with screens that function much like a traffic light at building entrances—notifying individuals when they may or may not enter.

During a health crisis, visitor management at large medical institutions is particularly important and offers many opportunities for smart surveillance systems. Visitors, when arriving at hospital, often have difficulty finding their way to their intended room or department. Computer vision solutions are integral, offering the ability to lead a person from the entrance to their destination—without added in-person assistance from staff.

FLEXIBLE TECHNOLOGY

New, flexible solutions provide the ability to pivot to other uses to provide long-term benefits. If a zone counter application is used for tracking occupancy limits today, tomorrow the same application can be used to notify facility managers when an individual crosses into an unauthorized zone or accesses the facility after hours.

Further aiding in adherence to health guidelines, object detection applications can serve dual purposes for both the detection of suspicious and unattended objects, as well as ensuring proper facial protection is being used.

Tapping into this new flexibility, managers can source more value from smart cameras throughout their lifecycle and get a higher return on their hardware investment.

Smart video analytics can help manage buildings more efficiently. The key to creating long-term, sustainable infrastructure is to invest in the right technology—one that provides the flexibility to adapt to both evolving health and safety guidelines, and latest advancements in smart buildings. ■

FABIO MARTI IS HEAD OF MARKETING FOR SECURITY & SAFETY THINGS.

Why Your Security Company Needs Easily Accessible Software

By TEAM Software

Drastic economic shifts can happen with little or no warning. When they do occur, your security business needs to be able to stabilize operations. One thing to help keep your business operations stable, efficient, and streamlined is a technology solution. When implemented and leveraged correctly, a holistic software solution tailored to your business's industry can ensure your company weathers the impact of an economic change.

As recent global emergencies have shown, having access to your company's data, workforce management solutions, and messaging capabilities are crucial to maintaining uninterrupted operating procedures.

GLOBAL ACCESS

The first step in a having a software solution that can be an asset during times of instability is making sure your software solution can be accessed from anywhere, at any time.

Guards, front- and back-end staff, and even C-suite executives need access to the right tools at any given moment. It's crucial to optimize workforce management through a holistic software solution so employees working remotely have global access to files, data, and other day-to-day



software as a service (SaaS) tool can foster connectivity, productivity, and workforce efficiency by being accessible via the Web rather than localized installations.

VENDOR-PROVIDED INFRASTRUCTURE

One of the benefits of implementing a SaaS solution is your service provider

Having access to your company's data, workforce management solutions, and messaging capabilities are crucial to maintaining uninterrupted operating procedures.

information needed to keep your business running smoothly.

This is possible with cloud-based, mobile software. Even during stable working conditions, an industry-specific cloud-based

should shoulder much of the day-to-day infrastructure of your software solution, whether that be maintenance and patches, released product upgrades, or automated data back-ups.

Assuming your guards have access to a mobile device, a holistic software solution with mobile technology capabilities grants your back office the ability to be in constant communication with them.

The right tools for your security company can provide real-time visibility over your distributed workforce and proof of service for your customers, while granting your employees access to workforce management tools from anywhere at any time.

When used properly, a holistic software solution ensures you have access to everything you need to handle what you're facing at any given moment. For additional information on navigating your business through a time of crisis, download the *Using Technology to Help Your Security or Cleaning Business During a Crisis* eBook from TEAM Software.

teamsoftware.com/securitymanagement



MANAGING THE SOC IN THE TIME OF CRISIS

SECURITY MANAGERS CAN LEVERAGE AUTOMATION
TO COMBAT BURNOUT AND ORGANIZATIONAL VULNERABILITY.

By Cody Cornell

EARLIER THIS YEAR, the World Health Organization (WHO) recognized burnout as a syndrome resulting from "chronic workplace stress that has not been successfully managed."

Security analysts are known for being at a high risk for burnout, which can lead to mistakes and increased vulnerability for the organization. As a former security operations center (SOC) analyst, I remember all too vividly the long shifts, the constant influx of alerts, the minimal room for error, and never seeming to have enough resources to do the job.

In the time since my days on the front lines of security, these issues have only been exacerbated by more alerts being generated by the myriad of threat detection and prevention tools that teams must leverage, an evolving and growing surface area to protect increasingly sophisticated bad actors, and a massive cybersecurity skills shortage. If all of that isn't stressful enough,



Photo illustration by iStock

today's security analyst is often working from home and trying to manage personal stress in an unprecedented situation.

In the wake of a global pandemic and civil unrest across the United States—and the world—we are all consuming a lot of information. Some of it is work-related, but a lot of it is not and bad actors are taking advantage.

For example, we have seen a huge increase in the number of phishing emails exploiting our trust relationships with organizations like the U.S. Centers for Disease Control and Prevention (CDC), the WHO, and state and local governments.

But it's not just the constant phishing attempts that are challenging, it's the fact that adversaries know we are distracted. We are watching what's happening around the world, trying to homeschool our kids, and helping our parents—or significant others—all while many businesses are in the fights of their lives. With so much going on both personally and professionally, the risk for burnout is higher than ever.

WHAT DO YOU DO?

The number one way to begin conquering burnout within your own team is to increase its efficiency and overall effectiveness. If I were managing a SOC right now, before assessing new solutions or vendors I would ask these three questions:

- **1.** How do you set people up for success and reduce opportunities for mistakes?
- **2.** How do you ensure work is being done in a consistent and repeatable way?
- **3.** How do you make sure the work that has to get done is actually getting done?

In short, focus on what you have to do and make sure the processes you must execute are effective, efficient, and have guardrails for an inevitably distracted team.

HOW DO YOU ACCOMPLISH THIS?

Start small. Define your incident response processes with documented standard operating procedures. Identify simple workflows or manual tasks that can be automated now. Set target metrics and key performance indicators, and generate real-time reports to track progress so you can pivot when necessary.

Automation is a crucial tool that can help increase the overall efficacy of your SOC. When it is combined with strong processes and documented procedures, your team is set up for success—minimizing stress and maximizing productivity.

CODY CORNELL IS CO-FOUNDER AND CEO OF SWIMLANE.

Reinventing Perimeter Security with Magos Radars

Theft, vandalism, and poaching are a great threat to fish farms around the world. many of which are finding themselves completely defenseless. Typically, farms are located in open waters, making them susceptible to attack. In most cases, the stolen fish constitute a fraction of the financial damage while the main blow comes from damage to nets or infrastructure which ruins whole crops.

By Magos Systems

A substantial number of Atlantic salmon were stolen from net pens at Cooke Aquaculture's floating farm near Anacortes, Washington, in 2017—resulting in millions of dollars in damage. Traditional security solutions often include video analytics, patrol guards, and drones, all of which entail high costs. Not to mention they only provide a partial solution, especially when more than a single farm is involved.

THE CHALLENGE

Dozens of cameras deployed at each farm failed to deliver a holistic solution. Aside from high installation and maintenance costs, the cameras produced a high rate of false alarms due to environmental movement and wind. Moreover, fog, frequent storms, and humid conditions contributed to the poor operating results, evidenced by missing detections. The problem intensified at night when detecting targets became even harder under low visibility conditions. Finally, extreme humidity and salt conditions coupled with a large number of deployed sensors resulted in low MTBF per site and high maintenance costs.

THE SOLUTION

To prevent future damages to the property, Magos radars have the ability to detect a target within a distance of up to one kilometer and with horizontal coverage of over 90 degrees. Detecting intruders while they are still far from the farm allows for improved response times. The large coverage compared to camer-



as significantly reduces the number of sensors used. A single radar was placed at each fish farm, accounting for approximately 20 cameras, covering all critical areas. By defining interest areas, the radars can alert only when the target is detected within a defined area, minimizing costly nuisance alarms. Magos radars can be easily installed on floating poles with minimal infrastructures required, operating in all weather conditions including rain, fog, and storms with high and proven MTBF. The open sea areas are ideal for radar technology operational taking advantage of the inherent large coverage angle.

Magos solutions provide very good perimeter protection results for critical areas with overall reduced operating costs. Radars protect a wide perimeter and operate in any weather conditions.

Magos radars were installed in fish farms in Latin America. They provide real-time tracking of targets detected in multiple areas. Upon an intrusion detection, the Mass software cues the PTZ cameras to the radar, providing visual verification of alerts. In several sites, the radars were also coupled with remotely operated speakers and lighting. This allowed fully automated threat control, while threat handling was centralized and handled remotely-further reducing the security operation costs. Upon threat detection camera and lights were automatically cued to the target and the speakers automatically played a warning. Only intruders who ignored the warning were handed over for "manual" handling by the remote operator.

One end user described the value of deploying the Magos radar as follows: "We have been searching for a solution to protect our fish farms for a long time," said Mario. "Cameras were expensive and difficult to monitor far from the seashore, causing a high rate of false positives in which patrol teams were sent on boats to investigate each alert. The Magos radar solution generated a substantial cost-savings for us in the short run, allowing us to monitor several areas at once and significantly reducing the number of false alarms."

AUTOMATED ALERTS ON THE RISE

AS THE WORLD RETURNS TO WORK,
ORGANIZATIONS LOOK TO AUTOMATED SOLUTIONS
TO MAKE BUSINESS MORE EFFICIENT AND SAFER.

By Megan Gates



efore the COVID-19 pandemic, investments were being made to advance autonomous technologies to make business processes and life in general—more efficient and environmentally friendly.

With the rise of the coronavirus, however, came even more interest in using and developing these technologies to limit human interaction and the spread of disease. A recent survey by Honeywell conducted 21 April to 7 May found that more than half of U.S. companies are increasingly open to investing in automation to survive changing market conditions brought on by COVID-19.



"The global pandemic caused a sudden and seismic shift in the global supply chain, driving distribution centers to embrace remote operations and social distancing work processes," said Chris Feuell, chief marketing officer at Honeywell Intelligrated, in a press release. "Recent consumer studies have shown increased online purchases by 28 percent globally and buy online/pickup in store is expected to increase by more than 60 percent in 2020."

Automated and connected solutions are also becoming more common in the workplace, where social distancing policies remain in effect while the world races to produce a COVID-19 vaccine.

"The use of robotic technology, guided work solutions, and computer-controlled equipment is seen as very important by companies for future competitiveness," according to Honeywell. "Warehouse execution software (48 percent), order picking technology (46 percent), and robotic solutions (44 percent)—currently three of the most widely implemented solutions—are most expected to receive further investment soon."

And this interest is not likely to wane, despite organizational moves to cut costs to address revenue shortfalls and potential economic downturns, according to a survey by PricewaterhouseCoopers (PwC).

"From March 2019 to the present (June 2020), 32 percent of U.S. finance leaders say their tech-related spend was driven by growth, including ecommerce and new products and services—and 32 percent expect the same for the next 12 months," PwC found. "One in five say their tech investments will enable or accelerate cost reduction efforts, like automation. They also plan to invest slightly more in technology related to health and safety. These investments in safety measures like automated contact tracing and workplace sensors can help employees feel safer than manual efforts as they return to the physical workplace."

Some security companies are already addressing this need, releasing new solutions or enhancing existing ones to allow for increased automation, eased contact tracing, and enhanced ability to carry out best practices to promote a healthy workplace.

Allied Universal, for example, rolled out a new version of its HELIAUS product, an artificial intelligence (AI) workforce management platform designed to improve safety and reduce risk by enhancing on-site guarding services.

The upgrade to HELIAUS added visitor screening applications, such as screening questions based on U.S. Centers for Disease Control and Prevention (CDC) guidelines, like asking visitors if they have experienced any symptoms of COVID-19 in the past week.

HELIAUS also now implements customerspecific visitor screening protocols, such as instructing a security officer to take a visitor's temperature or asking the visitor to use hand sanitization stations when entering the facility.

"The HELIAUS visitor screening application includes new suggestions for workflows that help with visitor screening, social distancing management, workplace signage, and maintaining a safe and clean workplace," said Mark Mullison, chief information officer at Allied Universal, in a statement. "All of the information collected in the course of visitor screening or custom workflows is captured electronically and fed into the platform's AI engine, which makes recommendations for improving the site's condition."

Allied Universal has also upped its offerings for advanced screening solutions, such as thermal camera screening solutions, noncontact screening options, and robotic screenings. All the data collected through these solutions can be fed into HELIAUS to provide recommendations to security officers on site.

In an interview with Security Technology, Mullison explains that the new options for HELIAUS came out of internal conversations about what is needed to "get back to business" in a safe way. Allied Universal identified four main building blocks for returning to the workplace: signage and reinforcing social distancing, maintaining clean workplaces, managing employee traffic, and screening visitors.

Using those blocks, Allied Universal looked at its HELIAUS product and added features that would help implement protocols based on CDC guidelines to enable those building blocks, Mullison says.

"Let's say we had implemented workflows in the lobby around elevator bays checking for the number of people and making sure they were maintaining social distancing," he adds. "HELIAUS would remind the security professional to do that at an appointed time. HELIAUS would record the results of that, and if there happens to be a problem it would suggest more activities for the security professional."

Like Allied Universal, Honeywell had similar internal conversations about the challenges of bringing people back to work safely-especially as the company has divisions in the Asia Pacific (APAC) region, including China where the COVID-19 pandemic began.

"As things started to get better and trend down in APAC, we started to see similar challenges of getting employees back into the office safely. And in late February, early March, we realized it's going to be a global trend-not just China," says Marcus Logan, global offering leader for enterprise leading solutions at Honeywell.

The company began thinking about what customers-and its own employees-would need to safely return to work while continuing social distancing. That led to the creation of Honeywell's Healthy Buildings solutions, which are designed to provide building owners with greater control over health, safety, and security factors in the workplace.

"The COVID-19 pandemic is changing the culture of how buildings are managed by making apparent the need to ensure health and well-being in all aspects of our lives," said Vimal Kapur, president and CEO of Honeywell Building Technologies, in a statement. "Returning to work after a pandemic will not be returning to business as usual. Occupants will want credible information and increased visibility into how building technology is protecting their health and what has been done to ensure that the buildings they enter are safe. Healthy buildings go beyond just energy efficiency to ensure

the health, comfort, confidence, and productivity of the people who use them."

The Healthy Buildings solutions are divided into two packages. The Air Quality package provides insights on containment risk, alerts to change HEPA filters, and cleaning and occupant behavior, among other analysis. It also takes the data collected, presents it on a unified dashboard, and provides a #HealthyBuildings Score to alert owners and operators of noncompliance with a health or security policy.

The other package is Safety & Security, which uses hardware and software to provide monitoring, detection, and response capabilities to manage people flow, temperature screenings, personal protection equipment use, contact tracing, and more.

The ability to implement contact tracing into the solution relies on integrating with the organization's access control system, Logan explains.

"So if you scan into an area, and then two days later get tested and show positive for COVID—we can leverage that existing data to go back and run reports to see who else was in those areas," Logan says.

Outside of office buildings, Logan says Honeywell has seen interest in the solution from college campuses and assisted living facilities—which often need to monitor the environment while providing a high standard for duty of care.

"We're seeing interest in areas where compliance is key, where they need something to show they're not putting employees or residents at risk and proactively monitoring the health of the building," Logan says, adding that this is particularly the case for campus housing and "assisted living where you have vulnerable populations in close proximity with the potential for higher rates of communicable diseases. Those end users...are looking for solutions to help them manage their risk."■

MEGAN GATES IS EDITOR-IN-CHIEF OF SECURITY TECHNOLOGY, CONNECT WITH HER AT MEGAN.GATES@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @MGNGATES.



MAILSECUR: THE NEW STANDARD IN MAIL SECURITY

Every year thousands of companies receive threats through the mail. While usually kept quiet, these have resulted in costly (and sometimes embarrassing) evacuations, injury, and even death.

MailSecur is the new standard in mail security. With its unique millimeter wave technology it can detect more and smaller threats than an X-ray mail scanner, is safe to use, and can be up and running in just 30 minutes.

And **MailSecur** has been designated by the US DHS as a Qualified Anti-Terrorism Technology, which provides you with important liability protections.



When your mail is stamped with the MailSecur stamp, your people know that you're looking out for them. And disgruntled employees know that it's not even worth sending a mail-borne threat because it will be detected.



Sign up to see a free, live demo of MailSecur and understand how well you can protect your people at raysecur.com/sm-signup



www.raysecur.com

617-855-9938

info@raysecur.com



Easier Wireless Access Locking, Your Style, Your Way

- Class-leading wireless access locks for every application Lowest-maintenance, longest battery life, keyless access, multi-credentials, matching models inside & out
- Cost-saving, easily networked No Panels, No PIMs Choose Networx® Ethernet, WiFi &/or POE Gateways & Extenders, each controlling over 60 locks
- Wireless keyless access solutions for all doors, from mortise, to narrow stile, to exit devices. Cylindricals simply retrofit standard locksets in about an hour.
- Global or Local Management & Lockdown Networked to save staff labor from door-to-door operations & provide emergency solutions, via lock, keyfob or server, including Enterprise Integration in realtime, with top platforms, Continental, Lenel*, Software House*
- ArchiTech Networx: Same proven Trilogy* electronics, but designer minimalist look, customizable with hundreds of architectural finishes & Grade 1 Lock styles and various colors/shapes of multi-tech ID reader + Smart Mobile iLock* App
- New! Security Manager App option, makes any smart phone a Virtual Enterprise Workstation; control doors, users, threat levels, etc. (w/CA4K)



MORE AFFORDABLE

Lowest labor & equipment costs without sacrificing top conventional access features



CENTRALLY MANAGED

Auto-Schedule program updates, queries, or free access by time, by door & more



GLOBAL LOCKDOWN or unlock in seconds from

the server or any lock



EASY INSTALL

Replaces any door lock, on any door type, neatly, quickly



ASY NETWORK

No wires to run to doors. Uses customers' existing network or Ethernet & multi-lock (63 locks/gateway) gateways & opt'l repeaters



USERS

Supports thousands of PIN, ID or iLock App users. Easily local/remotely



From the Makers of #1 Trilogy Locks
1.800.ALA.LOCK • www.alarmlock.com