# ELEVATE

ISSUE 4

SPRING 2026

**UNLEASHING INTELLIGENT SITE MANAGEMENT**

How to breed security into your business strategy

**PUBLISHER** LiveView Technologies

**EDITORIAL DIRECTOR** Noelle Baldwin

**ART DIRECTOR** Olivia Juárez Knudsen

**CONTRIBUTING DESIGNERS** Brad Hoen, Marlo Monteagudo, Andrea Portillo

**WRITERS** Noelle Baldwin, Brady Edwards, Steve Lindsey, Dr. Mark Logan, Michael Riordan, Chad Stevens, Dr. Michael Whittington

**COVER ART** Kaveh Taherian

**EDITORIAL BOARD** Derek Boggs, Jared Davis, Robin Dich, Michael Lamb, Jared Richardson, Logan Tanner

**LEGAL ADVISER** John Thomas

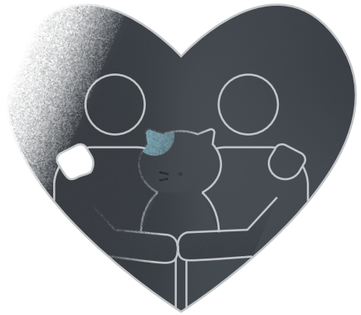
# ELEVATE

ISSUE 4 — SPRING 2026

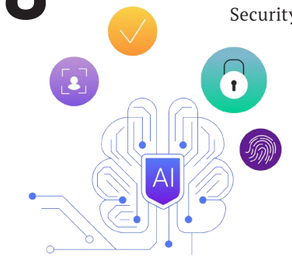


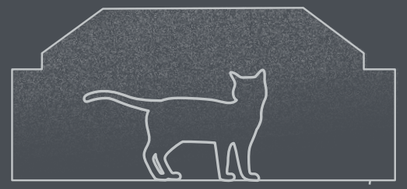












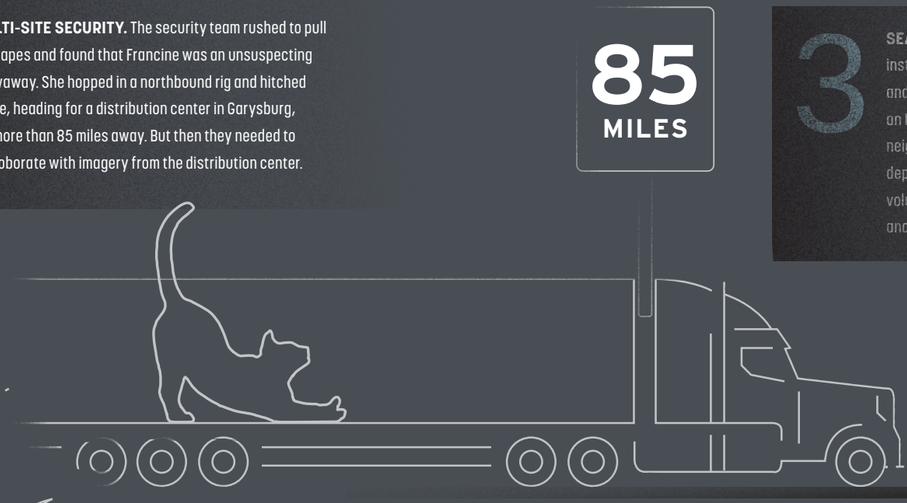
**1** **SHAKING DOWN LEADS.** The investigation hit a fever pitch as the team began pounding the digital pavement. It wasn't just a missing cat—it was a high-stakes search for a "VIP" (very important pet). To establish a timeline, the crew combed through hours of surveillance footage to pinpoint the exact moment the subject went missing, searching for forensic evidence.

# CAT TRACK FEVER

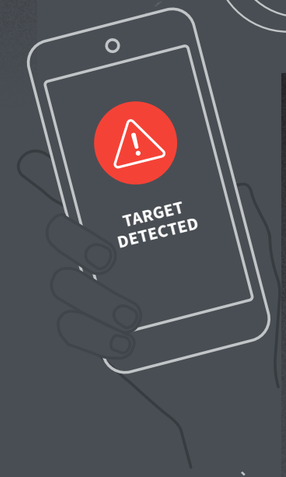

**BY**
Noelle Baldwin


**FOR TEN YEARS,** Francine the cat ran a tight ship at a home improvement store in Richmond, VA. She was a fixture in the garden center, but in mid-September she vanished without a trace. That's when her co-workers turned to LVT to help track their beloved cat.

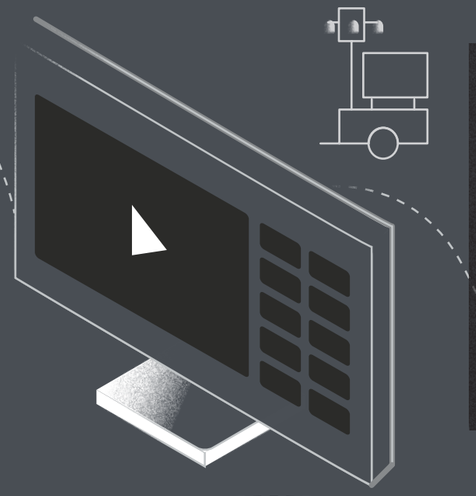
**2** **MULTI-SITE SECURITY.** The security team rushed to pull the tapes and found that Francine was an unsuspecting stowaway. She hopped in a northbound rig and hitched a ride, heading for a distribution center in Garysburg, NC more than 85 miles away. But then they needed to corroborate with imagery from the distribution center.




**3** **SEARCH AND RESCUE.** The community mobilized instantly—placing posters throughout North Carolina and Virginia, offering a $2,000 reward, and building an Instagram following of 35,000 to track leads. From neighbors scouring the woods to the hardware store deploying thermal drones, a massive network of volunteers and professionals joined forces to search and rescue Francine.

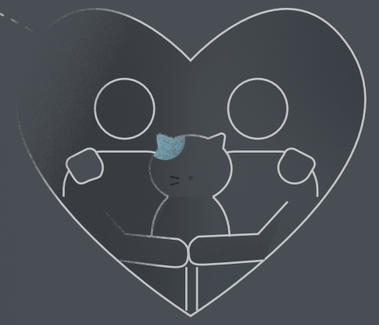




**5** **THE STAKEOUT.** After hours of cat-and-mouse around the unit, Francine set off alerts and was spotted on the camera feeds. Finally, she gave in and entered the trap. Store managers immediately made the drive to Garysburg to bring her home.



**4** **ASSET ACQUIRED.** On October 4, the security team got the first lead: a positive ID on a surveillance camera at the distribution center. Francine was in the area, so they set up a stakeout to humanely trap her, including repositioning and re-tasking the mobile security unit that was already on-site. The unit's analytics were even configured to detect her presence and send periodic alerts.

**6** **LAYERED ASSET PROTECTION.** Case closed. This wasn't just a lucky break; it was a textbook example of layered protection. It demonstrated how integrating mobile surveillance, AI, and remote access creates a scalable security solution that protects assets regardless of location. By linking two separate jurisdictions, it proved that no target is too small to track. Whether you're guarding high-value inventory or a high-value calico, multiple site security powered with AI increases safety, security, and business intelligence.



SHARE

See this article online at **lvt.com/elevate/cat-track**

# A SIMPLE FRAMEWORK FOR COMPLEX SECURITY

BY BRADY EDWARDS AND CHAD STEVENS

Good security programs have many aspects that create a solid program. However, you're never done—sometimes puzzle pieces once in place are suddenly gone or no longer fit.

Security leaders responsible for physical security and risk management face significant challenges in standardizing assessment processes. These include building processes from scratch, insufficient resources, conflicting priorities, attrition, numerous sites, intricate landscapes, and budget limitations. This article presents a framework designed to help security leaders address these difficulties and establish a consistent process for evaluating physical security and risk throughout their organizations.

You're never done—sometimes puzzle pieces once in place are suddenly gone or no longer fit.

## ASSESSING RISK ACROSS YOUR ENTERPRISE
### (THE WHY AND WHAT)

When establishing the foundational framework for your enterprise-wide risk assessment process, a comprehensive and strategic approach is paramount. This initial phase requires careful consideration of several critical factors that will ultimately define the scope, efficiency, and effectiveness of your entire risk management program.



## 1. DEFINING THE SCOPE OF YOUR ASSESSMENT PROCESS

The first and most crucial step is to clearly define the scope of your assessment. This involves answering fundamental questions that will guide all subsequent activities:

- **How many sites will be assessed?** This assessment should encompass all physical locations. A complete inventory of all assets and operational locations is essential to ensure no critical areas are overlooked.
- **What will be assessed at each site?** This requires a detailed understanding of the assets, processes, technologies, and personnel present at each location. For example, a breakdown of what needs to be scrutinized at each site will help tailor your assessment methodology.
- **How will each site be assessed?** Defining the methodology for assessment, including approval and reassessment processes, allows for long-term alignment on security posture at assessed sites.
- **What is your timeline for completion?** Establishing realistic and achievable deadlines is vital for project management and resource allocation. Consider the complexity of your enterprise, the number of sites, and the depth of the assessment when setting your timeline. By establishing these guidelines upfront, your organization will be significantly better prepared for the assessment process.

## 2. ENSURING CONSISTENCY AND EFFICIENCY IN YOUR PROCESS

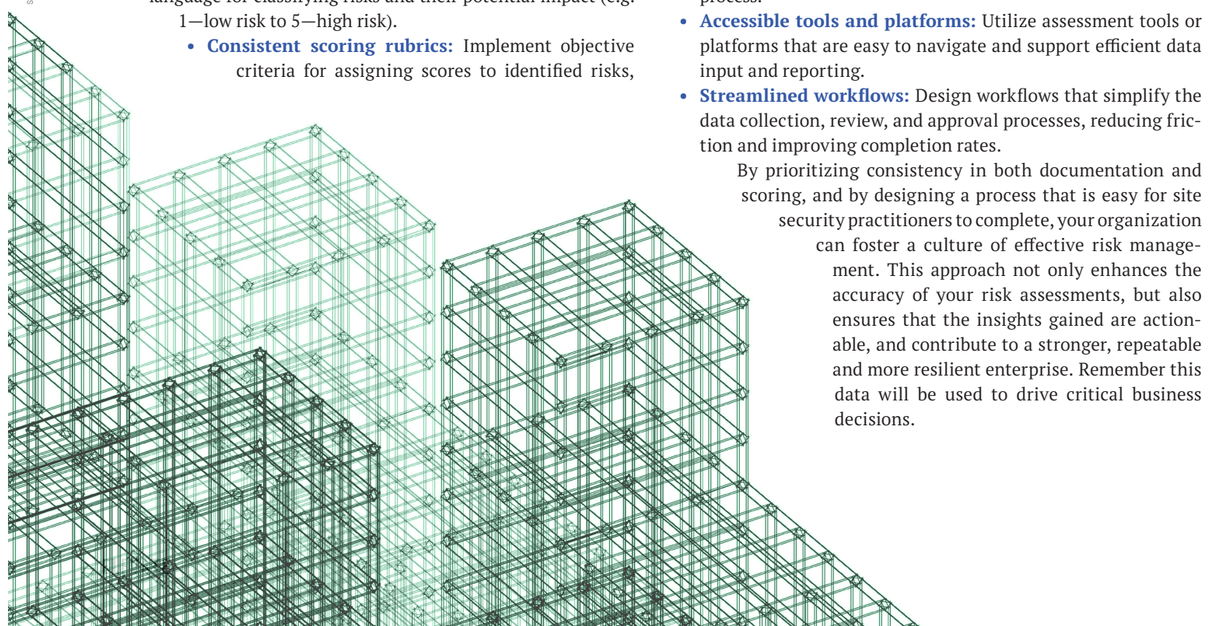
Once the scope is defined, the next critical element is to design a process that prioritizes consistency, ease of execution, and reliable data collection. To achieve comparable and actionable results across all assessed sites, it is imperative to establish standardized documentation templates and a consistent scoring methodology. This means:

- **Standardized questionnaires and checklists:** Develop clear, unambiguous questions that can be applied uniformly across all locations.
- **Defined risk categories and impact levels:** Establish a common language for classifying risks and their potential impact (e.g. 1—low risk to 5—high risk).
- **Consistent scoring rubrics:** Implement objective criteria for assigning scores to identified risks, ensuring that the same risk found in different locations receives a comparable evaluation. This eliminates subjectivity and improves the reliability of your risk profile.

The effectiveness of your assessment process heavily relies on the ability of local site security practitioners to easily understand and complete the required tasks. The process should be designed to be intuitive, user-friendly, and minimize the administrative burden. This includes:

- **Clear instructions and training:** Provide comprehensive guidance and training to all personnel involved in the assessment process.
- **Accessible tools and platforms:** Utilize assessment tools or platforms that are easy to navigate and support efficient data input and reporting.
- **Streamlined workflows:** Design workflows that simplify the data collection, review, and approval processes, reducing friction and improving completion rates.

By prioritizing consistency in both documentation and scoring, and by designing a process that is easy for site security practitioners to complete, your organization can foster a culture of effective risk management. This approach not only enhances the accuracy of your risk assessments, but also ensures that the insights gained are actionable, and contribute to a stronger, repeatable and more resilient enterprise. Remember this data will be used to drive critical business decisions.



S'VIATOSLAVA/DIBBE STOCK

## 3. OPERATIONAL AND PROCEDURAL REVIEW (THE HUMAN FACTOR)

The site security procedures implemented at your site for both internal and contracted security resources significantly influence your risk management strategy. Therefore, it is crucial to routinely test these procedures and analyze data concerning the performance of your security personnel.

- **Training:** Evaluate the adequacy and regularity of training programs for all security personnel. This includes initial training for new hires and ongoing professional development to ensure they possess the necessary skills and knowledge to perform their duties effectively.
- **Alarm response testing:** Assess the procedures and effectiveness of responses to alarm activations. This includes reviewing alarm response protocols, actual response times, and the ability of security personnel to appropriately handle different types of alarm events.
- **Patrol procedures:** Review established patrol routes, frequency, and reporting mechanisms. This ensures that patrols are systematic, cover critical areas, and that any observed anomalies are properly documented and addressed.
- **Post orders:** Examine the clarity, completeness, and adherence to specific instructions for security personnel assigned to fixed posts. This includes understanding their responsibilities, authorized actions, and reporting requirements.
- **Site operations procedures:** Assess how security personnel integrate with and support broader site operational procedures to ensure a cohesive and secure environment.
- **Contracted guard force performance and turnover:** For sites utilizing a contracted security guard force, this includes evaluating the vendor's performance against service level agreements, the quality of their personnel, and the impact of personnel turnover on overall security effectiveness.

## 4. EMERGENCY PREPAREDNESS AND CRISIS MANAGEMENT

Ensuring the safety and security of all occupants requires a comprehensive review and evaluation of the site's readiness to respond to various critical incidents.

- **Fire plans:** Review fire prevention measures, emergency evacuation routes, assembly points, and the roles and responsibilities of personnel during a fire incident.
- **Medical plans:** Assess first-aid provisions, access to medical assistance, and procedures for handling medical emergencies on-site.
- **Evacuation plans:** Review procedures for orderly and safe evacuation of all personnel from the site in case of an emergency, including designated routes, assembly points, and accountability protocols.
- **Site lockdown plans:** Evaluate procedures for securing the site and protecting occupants in response to an immediate threat, including communication protocols and designated safe areas.
- **Drills completed and future cadence:** Examine the history and frequency of emergency drills for each type of emergency (fire, medical, evacuation, lockdown) and the planned schedule for future drills to ensure continuous improvement and readiness.

## 5. EMPLOYEE AWARENESS

It's important to assess employees' general security knowledge concerning the critical security policies and procedures mandated at your site.

- **Interviews to gauge security culture of site:** Conduct interviews with a representative sample of employees to understand their perceptions of security, their knowledge of security policies, and their willingness to report suspicious activities.
- **Badge and visitor policy:** Assess employee understanding and adherence to policies regarding identification badges, visitor registration, and access control.
- **Reporting suspicious activities:** Evaluate employee awareness of how and when to report suspicious behavior or incidents, and their confidence in the reporting process.
- **General security policy knowledge:** Assess employees' overall understanding of the site's security policies and procedures, including data protection, physical security, and information security.



## 6. POLICY ALIGNMENT

The written directives at your site are critical to the effective operations of your site and your risk management strategy.

- **Policies align with operations:** Verify that security policies are integrated with daily operational procedures and do not hinder efficiency or productivity.
- **Meet compliance and regulatory requirements:** Confirm that all security policies and practices adhere to relevant industry standards, local, national, and international laws, and any specific regulatory mandates applicable to the site's operations.

## 7. HAZARD IDENTIFICATION

Hazards represent potential sources of harm that can manifest in various forms, the common denominator being the risk they present to your organization if left unaddressed.

- **Human/Intentional:** These include actions such as theft, vandalism, terrorism, cyber attacks, and insider threats.
- **Accidental/Technical:** This encompasses events like equipment failure, power outages, fires, and human error.
- **Natural:** This refers to severe weather events and natural disasters, including hurricanes, floods, wildfires, and earthquakes.

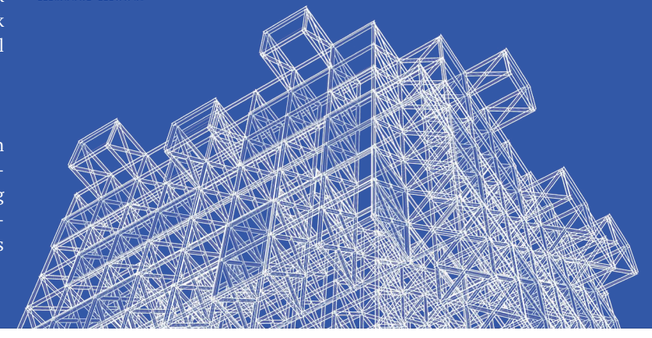


### DETERMINING RISK

Risk assessment begins by scoring vulnerabilities—weaknesses a threat can exploit—based on system gaps, guard performance, and countermeasure health. Each should be evaluated against location, business value, and incident history. Next, an impact assessment determines the financial, reputational, or safety consequences of a successful exploit, while a likelihood assessment calculates the probability of occurrence. These are combined to assign a final risk level (risk level = likelihood x impact). The process ends with risk prioritization, ensuring mitigation focuses on the most critical items first.

### DOCUMENTATION AND FOLLOW UP

Findings are translated into a pragmatic action plan with prioritized recommendations. To ensure success, an implementation plan assigns ownership, deadlines, and budgets. Ongoing reporting keeps stakeholders informed for oversight and decision-making. The challenges of vast sites and limited resources demand a repeatable process. This framework transforms chaotic risk assessment into a strategic, data-driven system. By defining scope, ensuring consistent scoring, and evaluating policy alignment, organizations move from reactive security to proactive mitigation. Ultimately, a resilient enterprise treats security as a continuous cycle of assessment and remediation, ensuring resources are strategically allocated to protect the assets that matter most.



**BRADY EDWARDS**
*AVP of Business and Market Development, LVT*
Brady drives security innovation at LVT as a security leader with 20+ years of experience in law enforcement and physical security. Previously, he led physical security operations at Northrop Grumman, managing enterprise-wide security programs. A U.S. Coast Guard veteran, he holds an MBA and is a board-certified Physical Security Professional (PSP).

**CHAD STEVENS**
*AVP of Business and Market Development, LVT*
Chad joined LVT in 2025 after a variety of security roles at ExxonMobil, including leadership roles designing risk management process, technical security design, and development of security policies and procedures. He holds a bachelor's degree from Penn State University, an MBA from Tulane University, and a master's degree from MIT.

Pass it on. Scan to share the online version: **lvt.com/elevate/risk-framework**

SHARE

# Organized Crime has Entered the Chat

## *How Decentralized Global Networks and Cyber Tools are Reshaping the Criminal Underworld*

**By Dr. Mark Logan and Dr. Michael Whittington**

**Illustrations by Marlo Monteagudo**

Technology isn't just helping the good guys. Around the world, criminals are using it to commit sophisticated crimes quicker and on a bigger scale than ever before.

Before advancements in technology, organized crime had to rely on a centralized presence, a strong man or group, and a physical structure. The groups would collect funds and regulate punishments in the flesh.

But now we live in a digitized world that removes the need for the physical structure and centralized organization. Now a group of criminals can have members on different sides of the globe, never see their victim, and still commit money-making crimes.

The case of one of these victims, an 18-year-old college-bound student, shows the devastating impact of this new age of organized crime. Brian, whose name has been changed to protect him and his family, fell victim to sextortion all because he started a text exchange with an unknown number. Sophia, the name the unknown number gave, convinced Brian to send nude photos and threatened to make them public unless he paid her an ever increasing amount of money. Brian ended up taking his own life, never realizing that "Sophia" was actually three men—one located in Los Angeles and two located in West Africa.

Similar to the group that attacked Brian, organized crime rings have members working together across the globe, often never even meeting their victims. While the actual crimes they commit may have been around for centuries, the methods have changed. And so have the methods of mitigation and investigation. Technology makes it easier for groups to commit crimes, employ freelancers or contract workers, and more, but it also makes it harder for law enforcement and prosecutors under current gang and organized crime statutes.

### DEFINING THE NEW CRIMINAL LANDSCAPE

There are three types of cyber-oriented criminals.

Cyber-dependent: These groups commit crimes only in cyberspace using a computer. They focus on viruses, spyware, Trojans, ransomware, and other illegal intrusions to exploit security vulnerabilities.

Cyber-enabled: These criminals use computers to aid traditional crimes. This includes fraud, identity theft, extortion, child exploitation, and cyber laundering. These criminals also use AI tools to imitate voice, movement, and appearance to appear trustworthy.

Cyber-assisted: These groups support their preexisting criminal activities with technology. They commit crimes like unlawful trafficking of illicit goods and services, medicines, controlled substances, and people.

## THE CRIME THAT REFLECTS DIGITAL CULMINATION

One crime that has spanned the digital and physical world is human trafficking. Similar to other organized crimes, human trafficking has changed with digitization. It used to be that victims were trafficked in person through a single person or pimp. But now human traffickers work in groups and are attacking people in their homes through social media and online chat forums.

Groups target victims, often young women, in digital neighborhoods from all walks of life, not just from socio and economically depressed areas. They look for those who are alone and begin digitally grooming them. Traffickers then use AI to make their lifestyle appear lavish and can even send rideshares to take their victims to the meet location. Once the girl is in the group's "system" everything is done digitally. She is moved from location to location through rideshares, all bookings are managed online by faceless individuals, and all payments are now handled through cash apps, online payments, and crypto. In all likelihood, the girl will never meet the person who is the actual trafficker.

Technology has also changed the demographic of who is targeted. Men and boys are being lured into human trafficking based on the promises of economic freedom. Victims are targeted through social media platforms in their home countries and promised wealth and opportunity. But instead, they are smuggled into the U.S., stripped of their passports, trapped in squalor, and forced into manual labor with no chance to escape. Most of these victims will be herded into a van in the mornings, dropped off to sell products or perform manual labor, and then picked up at the end of the day with no idea who drives the vans.

## DIGITAL INFILTRATION OF THE SUPPLY CHAIN

Crime is opportunistic and the supply chain has become a profitable target of digital-savvy thieves. Even though it deals with physical products, the supply chain and logistics rely heavily on digital support systems. Shipment data and inventories all live on digital platforms and criminals use this data to commit cargo theft. This isn't prying open a trailer with a crowbar, or cutting a lock, now criminals use more sophisticated methods that blend digital with the physical world.

Cyber cargo theft uses deceptive strategies like computer-aided viruses and phishing emails to access a company's system or online load boards which are online marketplaces where shippers and carriers find and book loads. Then once they're in, the criminals manipulate the data to create shipping paperwork. The problem is only growing as companies are using AI to do an initial screen of cargo and drivers, giving hackers another opening to gather information or replace it with their information. Once that's complete, they'll show up with what looks like real paperwork and simply drive off with the shipment, no questions asked.

## HOW TECHNOLOGY IS CHANGING POLICE INVESTIGATIONS

Technology is a force multiplier for criminal behavior and for law enforcement. Until recently there were few tools that law enforcement could use to investigate organized crime. Those that were available were labor intensive and time consuming. For example, wire or phone taps or searching through bank records. Often just to get access to these methods required planting an inside man who could pass intelligence to other officers.

Other methods involved roving on-call teams, strategic surveillance cameras, or even having an officer hiding in a tree calling out directions to their team parked a couple blocks away.

There was a time when investigators could use criminals' Facebook or Instagram to gather internal communications from the group before criminals realized that they needed to cover their digital tracks. Platforms like Signal, WeChat, and WhatsApp are now the favorite hangouts for organized crime groups because it is encrypted and harder for law enforcement to access.

There are other resources that law enforcement can use to their advantage when they are used lawfully, including doorbell cameras, cellphones, and more. There is a proliferation of camera systems that collect evidence of how organized groups are collecting, who they're associating with, and more.

The truth is law enforcement needs more force multipliers. About 46% of law enforcement agencies in the U.S. have fewer than 10 officers. Approximately 68% of law enforcement budgets go towards salaries while only 2.4% is spent on technology and communications.

As security systems continue to become more sophisticated, they'll help law enforcement even more by not only recording evidence, but by using AI to help prevent crimes through identifying patterns and automating alerts and responses. This will transition police from being reactionary to being proactive.

Technological advancements also decrease human bottlenecks and increase reliability. People take time to analyze and act and they are fallible. They may not see everything. Humans are only as good as their presence and their ability to pay attention at the time of the event. But computers remove the fault inherent with being human and will allow officers to be where they need to be when they need to be there.

## THE PATH FORWARD

Do police officers have the technology to eradicate organized crime, either physical or digital? The easy answer is no. But there are multiple realities that they have to deal with. First, law enforcement's top priority is to stop immediate actions of violence in their communities. As long as this is the largest function of any police force, it will always be difficult to get the resources necessary to fight organized crime.

But what if there was a technology in cameras that could identify the same car showing up at the same time every morning? Or could use facial match (which still ensures privacy and is more reliable than facial recognition) and see the same criminal hitting multiple locations? The video could pull descriptors, information, and other documentation to assist security teams and law enforcement. Partners in the community will soon have this technology sitting in their parking lots.

That's why there needs to be a public-private partnership between law enforcement, businesses, and their communities. When they work together, with the addition of better technology, there is an increased vigilance against organized crime and an increase in public safety.

**Dr. Mark Logan**

Dr. Mark Logan is a Professor and Lead Faculty for the Graduate Criminal Justice Programs at Columbia Southern University (CSU). A 37-year law enforcement professional, he retired as an Assistant Director for the U.S. Department of Justice, ATF. Dr. Logan holds a Ph.D. in Public Safety, has completed executive programs at Harvard, UVA, and the FBI Executive Institute, and brings international law enforcement experience to his instruction on constitutional law, terrorism, and critical incident management.

**Dr. Michael Whittington**

Michael "Myke" Whittington, Ph.D., is a servant and adjunct faculty member at Columbia Southern University, teaching criminal justice and homeland security. He holds a Ph.D. from Liberty University, researching police wellness. A graduate of the FBI National Academy and California POST Command College, his extensive experience includes serving as a Supervising Criminal Investigator and a police detective. He is a state-renowned gang expert, is bilingual in Spanish, and specializes in technology-based investigations to disrupt organized crime.

SHARE

Spread the word. Scan to get the digital article and send it to someone.
**lvt.com/elevate/digital-underworld**

# UNLEASHING INTELLIGENT SITE MANAGEMENT

## HOW TO BREED SECURITY INTO YOUR BUSINESS STRATEGY

BY NOELLE BALDWIN AND MICHAEL RIORDAN • ILLUSTRATIONS BY KAVEH TAHERIAN

Every security manager has that one site that is the constant problem. It's the site where your metaphorical guard dog is always barking—the one that demands 100% of your attention because of high incident rates or constant complaints. Because that site is the squeaky wheel, you know every inch of it. You know its strengths and weaknesses, and you know exactly where its "teeth" are in terms of cameras and guards.

But what about your low to medium crime sites? How much do you know about them? Is the dog asleep there? Since most of the industry is reactive, your energy is focused heavily on the problem sites where the dog barks the loudest, leaving you effectively blind to the majority of your operations. This is the productivity ceiling. There are infinite recordings but limited human attention. You simply cannot hire enough people to know what is happening everywhere at once. That is the nature of the industry. But what if that changed?

> *THERE ARE INFINITE RECORDINGS BUT LIMITED HUMAN ATTENTION. YOU SIMPLY CANNOT HIRE ENOUGH PEOPLE TO KNOW WHAT IS HAPPENING EVERYWHERE AT ONCE.*

### A PROGRAMMATIC APPROACH

The traditional approach to increase situational awareness was to add more—more guards and cameras. Even the advent of mobile security units, which take security on the move, still don't push security enough to provide full site coverage. Guards, CCTV cameras, and mobile security units are viewed as temporary solutions instead of as a program. They put the attention where the fire is until it is contained.

A more programmatic approach, also known as intelligent site management (ISM), with video coverage across your portfolio of sites, lays the foundation for the future. ISM collapses the current physical-digital divide and makes security the strategic function that owns the data that brings other business functions (operations, safety, marketing, etc.) to the table to effectively run your physical operations. It transforms your security infrastructure from a passive recording system into a network of active operational sensors. ISM is about bringing not just security online, but the rest of the physical world so you can make better decisions based on real data.

### IT HAS HAPPENED BEFORE

The convergence of security and operations has already happened in the world of cybersecurity. Just look at DevSecOps. Each step of development (Dev), security (Sec), and operations (Ops) used to be separate tasks. But they eventually converged into a single silo so software engineers could develop and ship stronger code faster. Now it's physical security's turn. Instead of having individual systems for security and operations, they are starting to merge into one.

Soon cameras won't just be recording evidence of crimes or incidents. As ISM is fully implemented, cameras could help you verify deliveries, manage access to restricted areas (and grant access with biometric and AI verifications), alert you to anomalies, instigate building repairs, create reports about foot traffic, and other orchestrated responses. As cross functional silos collapse, security and business operations will merge similar to how DevSecOps did. And the results will be faster, smarter, and more secure businesses.

## WHAT WILL BE DIFFERENT?

A main difference for this convergence is the type of data. Video is high quality and unimpeachable data. It shows you what is happening at your site. It offers rich context about events and tremendous insights that can be mined by computer vision and other powerful AI tools, allowing you to direct any human efforts to the needed areas. You will be better at your job with better capabilities to do it faster and more completely.

Video transforms everything from security to facility management. It could potentially create more personalized site management at different locations, swifter responses to emergencies and maintenance issues, and of course better crime prevention and response. Video footage will be the trigger point for AI to orchestrate responses across functions.

Thanks to generative AI and large vision models, video is structured data that pushes us into the era of understanding. Your camera will now read the site and offer rich context. For example, without ISM context, a camera that sees a person at 3 AM triggers an alarm, but with ISM context, the system references the schedule, identifies the employee (i.e. that is John who is scheduled to work this morning), and logs the arrival instead of dispatching a guard. By trading this context, it eliminates false alarms and makes the existing software smarter. The cameras aren't just a sensor on the edge. Instead they are the missing link between your business logic and physical reality.

*THE CAMERAS AREN'T JUST A SENSOR ON THE EDGE. INSTEAD THEY ARE THE MISSING LINK BETWEEN YOUR BUSINESS LOGIC AND PHYSICAL REALITY.*

Those companies who fall behind will have a competitive disadvantage without the visibility ISM will give them. They will be less agile and won't have the insights and data available to them that those with ISM programs will have.

## WILL IT MAKE YOU OBSOLETE?

Site management is a future vision. Similar to any other tech, it will be driven by people. Yes, it will change your work, but it will remove the mundane and monotonous. ISM will be able to distinguish between false alarms and threats, or it will help you sift through old footage for specific incidents. The goal is not replacement but a partnership where technology handles routine tasks, allowing people to focus on strategic oversight and problem-solving.

Site management is creating an opportunity for those to drive the future of physical site management, rather than be a passenger. It is setting up the opportunity to drive value across all departments (operations, marketing, security etc.).

## PREPARING FOR THE FUTURE

ISM is in its infancy. We're just starting to scratch the surface of what it will be capable of doing. But now is the time to prepare for it.

The first step is to create security as a program, one that gives you full site coverage and establishes your physical platform. Camera coverage will be the vehicle for AI and orchestrated responses. The beauty of a full site coverage program is that it solves the immediate safety, security, and situational awareness problem you have at your sites today and sets you up for the future. It also increases real-time deterrence capabilities that, in turn, increases safety and security. The camera infrastructure you deploy at your sites, across fixed-site cameras and MSUs, will be the vehicle you have to deploy AI and make decisions confidently.

With full site camera coverage, you will be prepared to implement the next phase, as long as your infrastructure is built with the processing power to handle the demands of the future. It will keep you at the forefront of the security AI race and put you ahead in the sprint to realizing ISM.

*CAMERA COVERAGE WILL BE THE VEHICLE FOR AI AND ORCHESTRATED RESPONSES.*

## THE RACE IS ON

The transition to intelligent site management is not a question of if, but when. Physical operations will fundamentally shift and go fully digital. The way to prepare is to create a security program that is built on full site video coverage that will help you increase situational awareness now and get the tools in place for future iterations. The coming shift will ensure businesses work faster, smarter, and more securely.

Those who move beyond the "one dog per gate mentality" and invest now will be positioned to deploy the next generation of AI tools, transforming their security from a reactive cost center into a strategic data center that drives efficiency and growth across the entire enterprise.


*NOELLE BALDWIN*

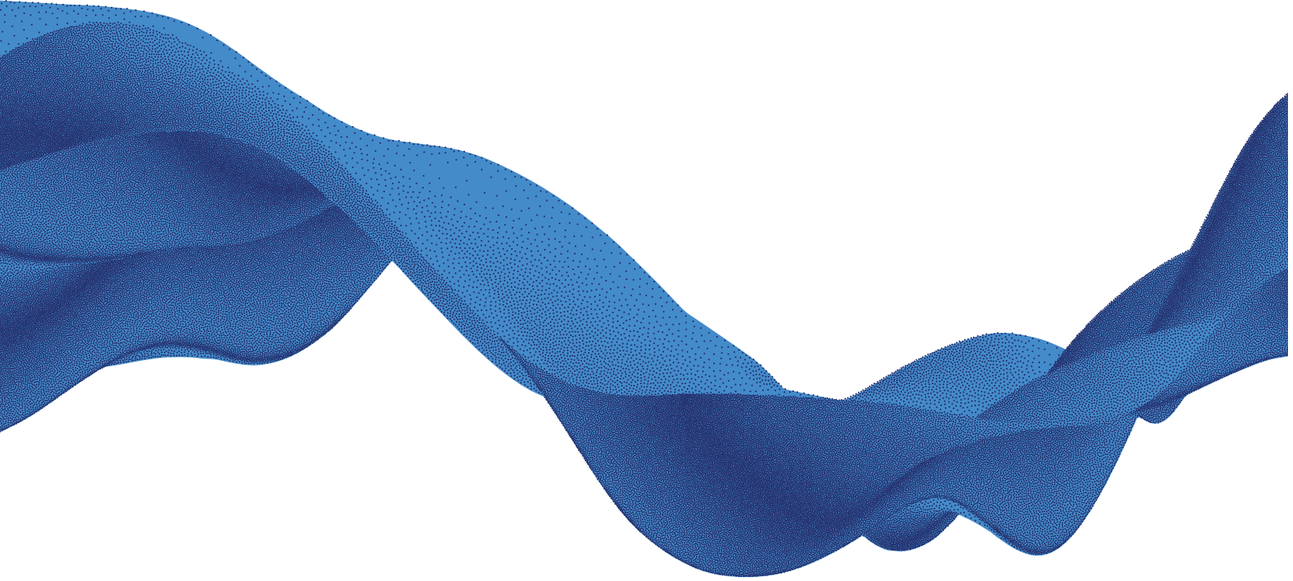
is the Editor of Elevate and LVT. She joined LVT in 2021 as the Content Marketing Manager. Noelle holds an MBA with a marketing emphasis from Utah Valley University and a bachelor's degree in English from Weber State University. Prior to joining LVT, she worked as a reporter and writer for Deseret News, Deseret Digital Media, and 4Life Research.

*MICHAEL RIORDAN*

is the Head of Product Marketing at LVT, leading the team and strategy for the mobile surveillance category creator. He has significant B2B product marketing experience, previously driving GTM for cloud-native companies like Sumo Logic and Fastly, and spending six years formalizing the product marketing function at Axon. He holds a BA in English from Dartmouth College.


SHARE

If you enjoyed this article, be sure to share it online: **lvt.com/elevate/ism-unleashed**



# Riding the AI Wave

## *Catching the wave and positioning teams for the AI shift*

BY
Noelle Baldwin

The AI wave is sweeping across all industries, including physical security. It is here whether we like it or not. Now is the time for physical security leaders to place themselves and their teams in the middle of the wave instead of being swept away by it. That is the message that long-time asset protection and loss prevention leader, Mike Lamb, is sharing with the retail industry.

The traditional physical security strategies for asset protection (AP) and loss prevention (LP) are shifting. Not only are retailers and other businesses dealing with more complicated threats, but they are also dealing with more of them—organized retail crimes (ORC), internal theft, and cargo theft. It is eroding profits and threatening customer and employee safety, forcing security leaders to confront the truth that their traditional security measures will no longer make the cut. It is no longer feasible to have a high headcount that is paid just to monitor and analyze security footage.

This reactive posture—where teams only review video after a loss has occurred—is being rendered obsolete by the speed and sophistication of crime. The answer is not just more cameras, more guards, or even more security solutions. The answer is more intelligence. "AP and LP leaders need to be courageous and think about tomorrow. AI is coming to security whether we like it or not so now is the time to plan down the road and around the curve," said Lamb.

"AI," said Lamb, "is already starting to transform security from a reactive cost center into a proactive, data-driven business intelligence tool." But AI isn't about replacing people with computers. It's about elevating what humans can do. "An ORC case could easily take 40 hours to gather evidence, file paperwork, and process but now it can be done better in four hours because AI can help. Anytime you can improve efficiency, why wouldn't you do it?"

### *A Proactive Force Multiplier*

AI's strength is that it is a force multiplier. It has the potential to shift security strategies from reactive to proactive, allowing security professionals to get ahead of threats instead of just waiting for a loss or incident and investigating it after the fact. AI helps increase the deterrence factor for security, making their property harder.

Traditional cameras are great at only one thing—recording. They don't help identify suspects, narrow down time stamps, or detect other anomalies. They are just an eye in the sky. They can provide evidence or corroborate eyewitnesses but that's it. But when paired with AI, traditional cameras are so much more.

IMAGE COMPOSITES BY BRAD INDEN, WITH IMAGES BY LOGIN/ADOBE STOCK



"AI can become a safety tool," said Lamb. "Soon things like facial recognition, behavior analysis, and license plate recognition will be integrated into a store's security systems and will prompt actions in real-time from the systems themselves or the personnel." Another advantage of AI is it can automate routine tasks. It can correlate data and link events to free up personnel from tedious tasks like searching through video.

### *Cost of Doing Nothing*

If security leaders stand by and watch the AI wave pass by, they will miss the most significant change to physical security since the inception of CCTV cameras. "The cost of doing nothing far exceeds the cost of doing something," said Lamb.

"We're still seeing the ripple effect of doing nothing the last time the industry had to adapt," he continued, citing the challenges with COVID and increased violence that has caused a spike in store closures.

Failure to act now might not lead to store closures, but it will mean playing catch up with other retailers who are riding the AI wave.

### *Becoming a Strategic Business Partner*

The effectiveness of any new technology, especially AI, is entirely dependent on those driving it. "We need AP and LP leaders who are curious and will be part of how AI is shaped instead of being fearful of what it will be," said Lamb.

Already security leaders in the retail space are being asked to not only secure their stores, but to increase profitability and operational effectiveness (i.e. reducing waste and shrink, improving inventory accuracy, decreasing administrative errors, etc.).

This involves doing their homework and working as more than just security personnel. "We need AP leaders who will position themselves as more than AP. Retailers need that type of leader and they are looking for those types of leaders," said Lamb.

> *"We're still seeing the ripple effect of doing nothing the last time the industry had to adapt."*
>
> —MIKE LAMB

But that doesn't mean they should jump blindly into AI products. That will result in wasted effort and investments. Instead, they need a plan that involves three steps:

1. Identify the problem you're trying to solve for. This includes collecting historical data so you know how big the problem is. "Don't confuse effort with results," said Lamb. "You could be working hard, but if it doesn't solve problems it doesn't matter."
2. Research solutions. Look into multiple solution providers. See how the solution can help long term to avoid procuring one that you set and leave. "You don't just get an idea on a solution and immediately run to senior leadership," said Lamb. "Each solution has to be vetted with your own team first. Does it help reduce shrink? Does it help increase the customer experience?"
3. Sell executives. As the expert in the problem and solution, you are responsible for selling any solutions to the executive team. "There needs to be a methodology of selling and advocating for solutions after vetting," said Lamb.

### *Securing Internal Buy-In*

To ensure maximum return on investment and successful adoption, leaders need to extend their focus beyond the technology and proactively engage the organization, especially their teams and the C-suite. This approach establishes the foundation for AP/LP leaders to drive immediate business value.

1. Approach the people side of it. Begin by showing the people side of the problem you are solving for. Show that the AI solution will not only increase safety and security (and give exact ROIs on both) but that it will also help your employees be more successful.
2. Sell internally. Build a case for the solution. You are responsible for showing how the solution works and how it will have a positive impact on the business. You have to be the internal advocate for the investment in additional technology.
3. Everyone has to buy in. This not only includes purchasing, the C-suite, and your own team, but it also includes those on the ground who will use the solution every day. You don't want to research a solution, invest in it, and set it up just to leave it, never using it to its full potential.

As AP/LP leaders fully embrace AI solutions, they will become successful leaders of tomorrow, helping their companies succeed now and in the future.

### *A Cross-Industry Solution*

AI in the physical security industry will impact more than just asset protection and loss prevention professionals. "This isn't just a retail issue," said Lamb. "Everyone has some sort of security needs. Even within retail there is distribution, warehouse, third-party logistics, and interactions with law enforcement."

We're in a critical time window for all stakeholders to actively collaborate, influence the trajectory of AI adoption, and ensure it meets the comprehensive needs of the entire physical security ecosystem. Now is the time to ride the AI wave. If you delay, it will sweep across the physical industry without your input or influence.

SHARE

Loved this piece? Scan the code to easily share the digital version. **lvt.com/elevate/ai-wave**

# ETHICS FIRST

## *Designing Unbiased Security AI*

BY
Steve Lindsey

Security is a necessary evil. Its purpose is to mitigate liability and, in its traditional setup, is purely a cost center. Businesses only invest the minimum amount to ensure their safety and security. It isn't profitable. In fact, security is there to stop the bleeding. But that is changing with the addition of AI.

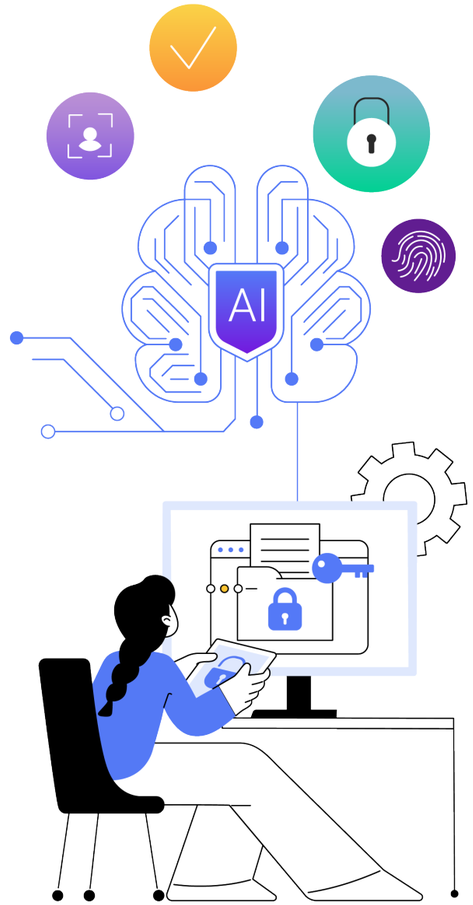
AI, particularly agentic AI, is going to change the whole of physical security. It's going to change how we gather data, interpret data, act on data, and even how we employ security professionals. In the past, physical security was about detecting an anomaly and alerting a human who does their best to respond. But agentic AI can move security towards prevention instead of reactionary with the goal to change threatening behavior as it's happening.

Naturally, as the industry moves away from only human decision making, it raises concerns about privacy, AI policies, and the ethical use of AI in physical security. Like all great technologies, agentic AI in physical security can be used for good but it can also be twisted to be used for bad. The direction the technology takes will all depend on the care in design, the thoughtfulness of long-term impacts, and ultimately the ethics and values of the companies that develop them; is it revenue and speed to market at all costs or is it doing the right thing for the right reasons even if it results in lower revenue?

*All **manufacturers** promise the moon and don't necessarily deliver. End users must understand the manufacturing, lifecycle costs, and where the data is **stored, retained, and protected.***

### THE CRITICAL ROLE OF DATA GOVERNANCE

Everything starts with data storage and handling even in the physical security industry. This component is often overlooked or deliberately ignored, but it needs to change. End users need to be aware of where their data is (is it on-prem, stored on the edge, or does it live on the cloud), how long their data is stored, how their data is transmitted, and they need to know how their data is used. It is the end user's responsibility to vet any manufacturer or service provider and to know their data policy. Of course, there are companies who will do anything to earn a buck, but if end users do their homework, they'll find security providers who share their values, have a solid data security policy, have proper governance to know that policy is followed, and who clearly communicate that policy and show evidence of following it. Mary Rose McCaffrey, a security expert with more than 30 years of experience, said, "All manufacturers promise the moon and don't necessarily deliver. End users must understand the manufacturing, lifecycle costs, and where the data is stored, retained, and protected."




This is vitally important because AI models use data to learn, and if end users aren't careful, their data sovereignty will be violated. Governance of the entire data pipeline from input to analysis to enrichment to reporting needs to be thoughtfully designed to ensure chain of custody. "The ubiquity of data doesn't have a bias per se, but where stored, how it is used, and who has access can introduce a bias," said McCaffrey. "Do your homework to avoid 'red flags.' What are your requirements? How do you vet your manufacturer? What are your options for remedy if it doesn't deliver against your requirements?"

*as AI is trained to recognize **behaviors**, it will naturally help remove biases.*

### SHIFTING THE FOCUS FROM IDENTITY TO BEHAVIOR

AI needs to be implemented in a way that does not violate privacy. The public does not like technology that can reveal their identity, especially if that technology can track their movements. Think about the concerns users have with cyber tracking and cookies. Those concerns are more pronounced in the physical world because there can be more serious consequences.

Because AI is trained on data input into the system, it will inherently have bias depending on the type and style of data input. Using AI technology that relies on matching gender, race, or any other human features or characteristics is fraught with problems and produces a lot of mistakes and false positives. Instead, AI should focus on behaviors as it is behavior that results in criminal activity.

The truth is, as security professionals we shouldn't care about who is committing a crime. We should care about the what, when, where, and why of criminal behavior. Agentic AI, if trained and implemented correctly, will be better at this than humans. We can't stop being human and can't remove our biases, but as AI is trained to recognize behaviors, it will naturally help remove biases.

## CONSCIOUSLY DESIGNING AI TRAINING TO MITIGATE BIAS

The best way to avoid bias as we're training the AI is to consciously exclude it from the models to ensure the data coming out is of the highest quality and relevance. Finding ways to identify potential crime is the holy grail of security. If we include racial and facial identifiers, we simply introduce bias with no improvement in recognizing criminal activity. That's why we need to understand human behavior in context before the crime occurs in order to create the sweet spot for AI modeling.

AI model development is also not a one-and-done type of thing. The sources of training data for AI models should thoroughly and continuously be vetted for lawful, ethical, and unbiased data sources. This includes proper monitoring and governance of those data sources ensuring chain of custody and security that it isn't tampered with. Never before has zero-trust architecture been a necessary pattern for physical security systems and the data pipelines they generate.

In the early days of agentic AI use, intentional use of deterministic vs. nondeterministic reasoning needs to be monitored carefully, erring on the side of determinism when AI behavior is still unproven. We don't need to boil the ocean when introducing agentic AI into physical security workflows nor should we throw the baby out with the bathwater. Instead, guardrails should be used to ensure outcomes are predictable and when outcomes fall out of acceptable guardrails, the appropriate circuit breakers need to be in place to suspend agentic automation and bring human monitors into the loop.

## GUIDING PRINCIPLES FOR ETHICAL AI IMPLEMENTATION

Now is the time for end users to start implementing AI ethically in their physical security plans.

Four guiding principles are:

- Have a values-based approach to data, personally identifiable information (PII), and AI
- Ensure policies reinforce those values throughout the organization
- Have monitoring and governance in place to ensure policies are being followed correctly
- Do business with trusted partners who share your values

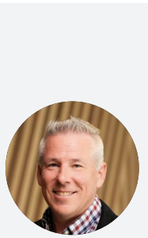
Thankfully, it isn't an all or nothing implementation. Start with a small area where the AI will have an impact on your security but one that is controllable, and ease into using it. See how AI can help your security and business and learn what guardrails you need to have in place to use it ethically. This includes vetting any potential providers and manufacturers and knowing how your data is stored and used.

## THE FUTURE OF SECURITY: HUMAN EFFORTS MULTIPLIED BY AI

In the next five years, security professionals must continue to innovate, become more cyber literate, and lean into technology, AI being the most prevalent. The world of security as a "fixed infrastructure" will continue to morph into a suite of tools, driven by requirements, but met by the utility of agentic AI to complement the security requirements of any business. Security professionals will need to become more knowledgeable about agentic AI and other cyber technologies to augment existing approaches to physical security.

Agentic AI will have such an impact on the physical security industry that all security practitioners need to keep an open mind and be willing to rewrite their physical security playbook. Thinking that agentic AI is another tool that is grafting into existing processes and procedures will be a big mistake.

AI will change how data is aggregated and how we consume it. It will change the way we think about physical security. With the correct guardrails in place to ensure the development and deployment and use cases of AI are ethical, AI will help us do more and multiply any human efforts.



*Steve Lindsey*

*Co-Founder and Chief Strategist*

*Steve was instrumental in designing, forming, and implementing the LVT Platform. Steve joined LVT in 2011 after leading technology, software, engineering, and development teams at multiple companies including i3 Technologies and Novell. He holds a bachelor's degree in electronic and information technology from Brigham Young University. Outside of all things tech, Steve loves mountain biking, music, food, sports, and especially his family. He and his wife Wendy have seven children and live in Utah County.*

If you enjoyed this article, be sure to share it online: **lvt.com/elevate/ethics-first**

SHARE

**LIVEVIEW TECHNOLOGIES**
802 E 1050 S, STE 300
AMERICAN FORK, UT 84003

ELEVATE

READ MORE ONLINE AT
**LVT.COM/ELEVATE**