ELEVATE

ISSUE 5

SUMMER 2026

THE BRADSHAW COLLECTION
A Curated Approach to Security Partnerships

8

PUBLISHER LiveView Technologies

EDITORIAL DIRECTOR Noelle Baldwin

ART DIRECTOR Olivia Juárez Knudsen

CONTRIBUTING DESIGNERS Brad Hoen, Felicity Lewit, Marlo Monteagudo, Andrea Portillo

WRITERS Noelle Baldwin, Matt Kelley, Oscar Nunez, Michael Riordan, Ash Roberts, Karl Schmae

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

LEGAL ADVISER John Thomas

ELEVATE

ISSUE 5 — SUMMER 2026

4 **Do More Than Just Make Do**
How Technology Solves Security's Capacity Crisis

2 **Security Landscape: The 11K-Foot View**
Inside the 2026 Safety and Security Summit

6 **Tectonic Plates**
LPR's Seismic Shift to Data Analytics

8 **The Bradshaw Collection**
A Curated Approach to Security Partnerships

13 **Buddy Cops**
Why Humans and AI Always Catch Their Guy

16 **Cutting Through the Noise**
How AI Sharpens Awareness

20 **The Invisible Tax of Visible Wins**
Prosecution Alone Won't Match the Dividends of Investing in Deterrence

SECURITY LANDSCAPE: THE 11K-FOOT VIEW

Inside the 2026 Safety and Security Summit

This past February, the fourth Safety and Security Summit (S3) took to the slopes of the Wasatch Mountains at Snowbird, Utah. The goal? To assemble a high-altitude think tank of the security industry's sharpest minds to solve the industry's most complex challenges and to plan for the future.

THE FUTURE IS PROACTIVE, NOT REACTIVE

The primary focus of S3 was the move from reactive monitoring to autonomous orchestration. In an era where integration is a baseline requirement, the summit explored what happens when we go further.

Through sessions led by industry experts like former CIA Director of Security Mary Rose McCaffrey, retired General William J. Walker from Allied Universal, and former CSO of Boeing Dave Komendat, the conversation centered around moving physical security into the world of AI. The takeaway was clear—the future belongs to systems that don't just alert us to trouble, but proactively manage perimeters, differentiate threats, and execute responses in real-time.

DEFINING MOMENTS AND SHARED CHALLENGES

For General Walker, S3 was a chance to gain exposure to the future of security technology. "As a 2 star general, I was always trying to think forward. And LVT has a way to see what's coming and how to get there," he said.

Mary Rose loved being part of the event, acting as a moderator for the breakout session titled "From F-47s to Servers: How Defense CSOs Master the Physical-Cyber Risk Balance." She said, "My personal benefit was two-fold; of the individuals I suggested to attend, they were all impressed with the capabilities. Secondly, I am re-energized about bringing new solutions to a different customer set. My passion for security solutions is as strong as ever."

Mike Lamb has been part of each Safety and Security Summit but said 2026 S3 was the best of the best, saying "My favorite part was the realization that no matter the vertical, safety and security challenges are very similar, both in scope and solutions to mitigate."

Steve Jensen is the Chair of the Board of Directors for the Utah Organized Retail Crime Association (UTORCA) and has more than two decades of experience in law enforcement and public safety. He said, "As the Chairman of UTORCA, I am always looking for ways to bridge the gap between law enforcement and private retail. S3 has a reputation for bringing the right people into the room to discuss how technology can facilitate those public/private partnerships."

Dr. Mike Perry, who served for more than 30 years with the U.S. Department of Defense and as a command chief and top first sergeant in the Air Force, said, "I think of defining times and defining moments, and I believe this is one of them. Conferences like S3 help us to make sure that we grab ahold of the tools that are out there at our disposal and use them to do what's good for society. The collaboration, innovation, and foresight we experienced at S3 was truly inspirational." Dr. Perry is currently the Dean of the College of Space, Intelligence, and Military Operations at Columbia Southern University.

HIGH-ALTITUDE DIALOGUE WITH REAL-WORLD IMPACT

The setting allowed industry experts and peers to debate and learn from each other without the typical trade-show noise. This resulted in an unfiltered dialogue on the future of AI in physical security—one focused on execution rather than just theory because at the end of the day, the goal of S3 isn't just about discussions or networking. It's about increasing safety and security at our businesses, in our communities, and throughout the world.

"As a 2 star general, I was always trying to think forward. And LVT has a way to see what's coming and how to get there."

—General William J. Walker

See this article online at **lvt.com/elevate/security-landscape**

SHARE

Do More Than Just Make Do

BY
Michael Riordan

The safety and security industry is reaching a breaking point—it is understaffed and overwhelmed. Private security has seen a turnover rate of 100% to 300%. And law enforcement isn't fairing any better with 70% of agencies reporting more difficulty recruiting officers. Each year, fewer people want to enter these high-risk jobs.

The result is a capacity crisis. Security teams are stuck in a constant reactive loop—chasing incidents, responding to alerts, putting out fires. When your people spend all their time reacting, they lose the bandwidth to get ahead of crime before it happens.

The best organizations have recognized this reality and instead of throwing more manpower at the problem, they use technology to increase their current workforce's capabilities.

Which Problems Need People?

Organizations are being forced to decide, explicitly or by default, where they need human judgment and where they don't need it. That's the framework for the decisions that follow. Do you deploy your people, bring in outside help, or let technology carry the load? Get the answer wrong, and you're either wasting expensive human attention on work that doesn't need it, or leaving critical decisions without the human judgment they require.

The most disciplined security teams know that the best use of technology is offloading the volume of low-priority events so that human operators can focus on what actually demands human judgment. The more you can see of the site, the more data you have to act on. Site coverage then becomes the floor and what you do with the information gathered is the ceiling.

This question of what the technology does versus what actual humans do is actively playing out in three areas security teams care about today: deterrence, people safety, and investigations.

› DETERRENCE

Let's start with deterrence. The ROI logic is straightforward—prevention of an incident is cheaper than responding to the incident. When nothing happens, it lowers costs in investigations, liability exposures, and reputational damage.

But criminals adapt, making deterrence hard to sustain. A static camera or fixed patrol stops working once a criminal figures out the patterns. Maintaining high deterrence requires constant variation, and that takes attention and time that most lean teams simply don't have. Which is why most teams default to post-incident response, not because it's the right strategic choice, but because it's the path of least resistance. Sometimes it's the only path open to them.

This is where AI-enabled dynamic deterrence changes the industry. Rather than a static presence, AI can generate real-time, context-specific responses—messages and interventions that are unique to what's actually happening at a site at that moment. It creates the perception of an active, attentive security force without requiring a human operator to be watching every feed at every moment. It makes it so deterrence is sustainable for an understaffed team. True deterrence isn't just about the cameras—it's about creating a dynamic environment with the perception of security presence.

› SAFETY

Your employees and customers deserve to feel safe on your property, and their safety is a huge responsibility for security leaders, and a costly one. In recent years, there has been:

- A 62% increase in workplace violence *(2025, NCCI)*
- 470 employee fatalities from violent acts *(2024, BLS)*
- 54,000+ assault-related injuries 2023–2024, median 6 days away from work *(NSC)*.

The problem is that a lean security team can't be everywhere at once. But what if technology can make staff feel more confident? Then the judgment call is back in their hands and they can activate the tech to intervene.

That's why safety needs to be shared across the organization, not just a security department. When frontline employees and customers have tools that put deterrence capabilities in their hands—triggering alerts, requesting a virtual escort, flagging a concern in real time—the perimeter expands without expanding headcount. Security teams move from being the sole owners of safety outcomes to being the coordinators of a much larger, distributed safety network.

› INVESTIGATIONS

Security teams can spend days, sometimes weeks, manually scrubbing through evidence to aid investigations. This is a security opportunity cost. Instead of team members helping prevent the next incident, they are buried reacting to the last one.

The strategic question isn't whether to invest in better investigative tools—it's whether you can afford not to. With correct coverage, you will have the data you need and can leverage the advancements in tech and AI to find the needed footage. Searching through evidence becomes a matter of minutes. You close cases faster, surface patterns earlier, and free your team up so they can focus on prevention.

From Security Asset to Business Platform

When you invest in full site coverage today, you're actually investing in intelligent site management (ISM) tomorrow. Improved deterrence, enhanced safety, and faster investigations are just the starting point. Today they mean preventing more crime, getting ahead of bad actors with dynamic deterrence, improving staff retention and morale, and closing cases faster as fewer incidents reach the investigative phase. All of it ladders up tomorrow to a broader, programmatic view of how your site and operations are performing. The smartest organizations are approaching their security challenges with this end in mind. They know that their security infrastructure is actually a future platform for their entire business.

The data that flows through your security infrastructure—foot traffic patterns, peak hours, parking utilization, incident trends—may be used by business intelligence, marketing teams, operations, and more. Marketing teams can use it to understand customer behavior. Operations can use it to optimize staffing and store layout. Real estate and facilities teams can make smarter decisions about space. Executives get a clearer picture of how their physical locations are actually performing.

Security's capacity crisis isn't going away. But the teams that respond by investing in intelligent technology aren't just surviving it—they're building organizations that are more capable, strategic, and future-ready.

SHARE

Loved this piece? Scan the code to easily share the digital version. **lvt.com/elevate/dont-make-do**

TECTONIC PLATES

LPR's Seismic Shift to Data Analytics

BY
Oscar Nunez

Physical security is shifting away from passive video recording and toward real-time intelligence. License plate recognition (LPR) is a big part of that change and as AI becomes more integrated into security technology, LPR is becoming less of a tool and more of an analyst.

From OCR to AI-Powered Intelligence

Early LPR systems relied on basic optical character recognition (OCR), which meant they only worked well under near-perfect conditions. Poor lighting, rain, glare, motion blur, or dirty plates could all impact accuracy. The real breakthrough came with advances in AI, edge computing, and large-scale training data. Modern systems can now accurately read plates at highway speeds, across multiple lanes, and in difficult conditions while simultaneously identifying vehicle make, model, and color.

But the biggest shift happens after the plate is captured. Real-time hotlist alerts, geospatial analytics, and behavioral pattern detection are where the technology delivers the most value. The camera collects the data; the software platform turns it into intelligence.

A Force Multiplier for Public Safety

LPR automates the reading and organizing of publicly visible, government-issued identifiers. Its real strength is efficiency. Instead of spending hours reviewing footage, investigators can search for specific vehicle details and narrow results in seconds. Even partial descriptions like color, make, and approximate model can quickly reduce a large volume of footage into a manageable set of leads, enabling faster investigations, more recovered stolen vehicles, and stronger cases.

Expanding Impact

While law enforcement remains the largest adopter, private organizations are increasingly leveraging LPR as well. Retailers use it to combat organized retail crime by connecting suspicious vehicle activity across multiple locations, patterns that traditional security systems would miss. Logistics operations use it for gate management and chain-of-custody tracking. Residential communities deploy it as both a deterrent and investigative tool.

Across sectors, LPR increasingly functions as an intelligence layer within broader security ecosystems, integrating with access control platforms, video management systems, and mobile surveillance units.

Privacy Through Control and Transparency

As adoption grows, data privacy remains critical. Organizations should maintain full control over their data, who accesses it, how long it's retained, and how it's shared. Strong audit trails, role-based permissions, and secure storage are essential. At Insight LPR, the focus is on giving agencies ownership of their own data rather than placing it into shared networks without oversight. Like any powerful technology, LPR works best when paired with clearly defined policies and safeguards.

The Next Leap

The next phase won't simply be about reading plates more accurately—it will be about understanding context and uncovering insights from massive amounts of vehicle data. As LPR integrates further with surveillance, access control, and geospatial analytics, it's becoming a more active analytical tool rather than a passive collector.

Oscar Nunez
Chief Product Officer, Insight LPR

Oscar Nunez is an executive recognized for driving innovation and operational excellence across the public safety technology, auto lending, and finance sectors. With a career anchored in strong leadership, Oscar previously served as VP of Product Development & New Markets at Motorola Solutions and led loss mitigation for Uber as a Senior Operations Department Manager. His expertise lies in bridging strategic vision with data-driven insights to launch market-leading products while scaling high-performing teams. A specialist in navigating highly regulated industries, Oscar has a proven track record of managing multi-million-dollar budgets, forging nationwide alliances with law enforcement and insurers, and delivering scalable technology solutions that sustain high performance and compliance.

SHARE

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

PHOTOS BY FELICITY LEWIT

The Bradshaw Collection

A CURATED APPROACH TO SECURITY PARTNERSHIPS

BY
Noelle Baldwin

It takes a village to run a modern business, and not just the employees inside its walls. Today's businesses thrive when they are connected to the communities around them. For Mark Bradshaw at DLC, bridging the gap between private enterprise and public safety isn't a line item in a budget or a box to check. It's a deliberate investment in relationships that strengthens both security and community trust.

For Bradshaw, relationships start long before a 911 call for help or a crisis with his tenants. Instead, they begin with a simple handshake and introduction, a shared business card, and a commitment to ongoing communication. By blending proactive engagement with cutting-edge technology, Bradshaw has proven that when businesses view themselves as part of a community, public safety becomes a shared—and highly successful—mission.

Starting Before the Sirens

Bradshaw is currently the Vice President of Property Management at DLC, a commercial real estate group that owns and operates shopping centers across the U.S. His focus throughout his career has been building public and private relationships, including his current position at DLC.

"At the end of the day, it's about putting in the time to build relationships," he said. Early in his career, Bradshaw made it a habit to introduce himself to officers patrolling the properties he managed. "When I see an officer at the shopping center, I thoughtfully approach them with one of my business cards," said Bradshaw. "I identify myself, give them a handshake, and go on my way. Most of the time, they will be very welcoming of the engagement." Rather than waiting until he needed assistance, it was critical to establish connections before issues arose.

Bradshaw and his team at DLC even go another step further and host meetings with local law enforcement. "We have quarterly meetings with officers to continue to grow the relationship and officers from different districts and ranks attend," said Bradshaw. The goal of these meetings is to keep their finger on the pulse of the community. They share with officers what they see on the ground while gaining insight into local concerns and trends from law enforcement. This creates a foundation of trust and collaboration making it easier to quickly coordinate when an issue does arise. "Police so often these days don't get this type of engagement. It is so warmly received when a manager or company takes this initiative," said Bradshaw.

The Handshake, 2026
Hand on hand contact

An essential moment of connection before a brush with crime. The simple handshake transforms safety and security from solitary pursuit into a shared objective.

An Exchange, 2026
Numerically etched connection

Two figures trade digits, and collaboration takes shape. Suddenly, the barrier between team, law enforcement, and community collapse—turning protection into something crafted together.

Building Beats Reacting

What begins as a handshake often evolves into a highly effective information-sharing network. The relationships Bradshaw and his team cultivate allow security personnel and law enforcement to communicate directly, identify concerns early, and address issues before they escalate.

"When something happens, my team will reach out to the officer and report what they're seeing. Traditionally, there is not always a close collaboration between police and private security," said Bradshaw. "But my guards have the police officers' numbers and vice versa. They are able to reach out and say 'This is what I'm seeing' and help them better police without calling 911 or dispatch."

The police frequently reach out to Bradshaw's teams. Sometimes if there is a crime nearby, police approach with a request. "They reach out asking if I have camera footage that I am willing to share," he said. Other times it is to simply get an update. "We've experienced very robust engagement with this," said Bradshaw. "We have calls from the guy on the street writing parking tickets, all the way up to the major who runs the district."

Not Just Law Enforcement

But public engagement isn't just about building relationships with local law enforcement. "We have HOAs and communities that routinely reach out to us," said Bradshaw. "We've had situations where the county representative wanted to walk our shopping center. Or we reach out to police, community members, church leaders, and politicians to talk about different shopping centers and what needs to be improved."

Frequently the feedback is constructive criticism. "Sometimes the feedback from the community is critical, but you listen to their concerns and take it to heart," he said. "This is about a willingness to engage, take the criticism and feedback, and better the communities you are in."

Bradshaw's teams also ensure they build relationships with their tenants, third-party vendors, other employees, and even neighboring businesses. For example, at many DLC locations, guards are required to check in with the tenants multiple times per day.

Does it Work?

Is it worth the time and effort to reach out to others in the community? Absolutely. Having a good relationship with local law enforcement enables them to do their jobs better and increase retail safety for both customers and employees. When working with HOAs and their neighborhoods, Bradshaw states that they are asking for an increase in safety and security. "In some of these communities they have been asking for these changes. These are welcome changes. They like that they feel safer. They like that no one is trying to panhandle or intimidate them," he said.

"It has already paid dividends that can be hard to quantify," said Bradshaw. "One huge improvement reported by our own tenants is that of feeling safer and of feeling heard."

Other ways are easy to track. "The easiest way to see if our approach is working is when it comes to renewal time, when the lease is expiring," Bradshaw said. "That is the time where this proactive approach shines. Tenant retention is the name of the game. If the environment is such that they are not seeing the sales they need and can't feel safe, they are going to go somewhere else."

> *"One huge improvement reported by our tenants is that of* ***feeling safer*** *and of* ***feeling heard.***"
>
> —MARK BRADSHAW

Is it Ever Too Much?

Bradshaw has never had someone tell him there is too much security. There are situations where landlords might fear adding additional security like armed and unarmed guards, mobile security units, or other security measures because they're afraid it will scare away customers.

But Bradshaw disagrees. "Every center that we have is unique. Some don't require any advanced security measures. This is a very subjective call and dependent on the neighborhood and necessity. Normally, for the areas where security may be needed, security additions are welcomed, and we know because we talk to people that are in that area daily."

There are other ways to increase safety and security without installing more cameras, ways that can help ease landlords' or HOA managers' concerns. The best way is to simply make the area uncomfortable for the bad actors. Focusing on creating environments that naturally discourage unwanted activity through visibility, activity, and thoughtful property maintenance. "Try power washing, moving scaffolding, or have janitorial services throughout the day. Think outside of the box. Make it hard to hide and uncomfortable for [bad actors]."

The Right People Make All the Difference

Technology only works when the people behind it are the right fit. Bradshaw looks for guards who are trained to engage thoughtfully without escalating a situation. "In the center where adding security guards is appropriate, I want a team of guards who are not afraid to engage and who are not afraid to do it without throwing gasoline on the fire. That's training and having the right security partner."

When the right guards are in place, police will stop and talk. "They're stopping to talk to the guards and asking, 'What have you seen today?'" said Bradshaw. That kind of informal intelligence-sharing is only possible when trust has already been established, and trust is only possible when the people on the ground have earned it.

Real Partnership, 2026
Composite vision on safety

A mixed palette of security partners, assembled around a shared mission. Meaningfully crafted connections unlock the secret to long-lasting safety and security.

A Blueprint for Community-Centered Security

For Bradshaw, everything comes back to the principle of community. DLC operates shopping centers where people buy their groceries, take their kids shopping, and go out to eat. “More so than any place I’ve been, DLC embraces that we’re part of a community and we strive to create a welcoming environment where people feel safe,” he said.

That mindset demands a willingness to be uncomfortable. It means sitting across from HOA managers and neighborhood residents who have complaints, listening without being defensive, and making changes.

The blueprint Bradshaw has developed over his career is remarkably simple, but it requires consistency. Show up before the crisis, build the relationship before you need it, invest in training and technology, and never stop listening to the people you serve. “At the end of the day,” he said, “it’s about relationships—with the police, our tenants, our vendors, our security staff, and our next-door neighbors. Knowing your neighbors, being part of a community, building trust. It’s taking criticism, being able to pivot, and being committed to that.”

It’s an approach that transforms security from a reactive function into a community-wide effort—one built on trust, communication, and shared accountability.

For any property manager wondering where to start, Bradshaw’s advice is as simple as it gets. Start with a handshake with an officer doing their rounds, walk over, and extend your hand. The rest builds from there.

Mark Bradshaw
Vice President of Property Management, DLC Management

At DLC, Mark is responsible for overseeing the strategy, operations, and capital management for a vast retail portfolio. With comprehensive experience in retail property leadership, he currently manages approximately 17 million square feet of retail assets across the U.S., focusing on driving operational efficiency and asset profitability. He has more than two decades worth of experience in property management and keeping them safe and secure. Prior to joining DLC Management Corp., he held leadership roles at The Loughlin Management Group, Inc. and Continental Reality Corporation.

SHARE

Spread the word.
Scan to get the digital article and share.
lvt.com/elevate/bradshaw-collection

Buddy Cops

Why Humans and AI Always Get Their Guy

BY
Ash Roberts

It is 2 AM. A security operator sits alone in front of a wall of screens. Thirty camera feeds. All quiet. All still.

Here is the problem. After about 20 minutes of watching screens like that, a person misses up to 90% of what happens on them. We are just not built for it. The one moment that matters slips right past.

Psychologists proved this years ago. In one famous study, viewers watched a video and counted basketball passes. Halfway through, a person in a gorilla suit walked into the frame and thumped their chest. Afterward, about half the viewers swore they never saw it. They were so locked on the ball that a gorilla turned invisible. Scientists call this inattentional blindness.

This is the gap that artificial intelligence promises to fill. But before we decide whether to trust it, we should ask a simpler question. What is AI, really?

A Quick, Honest Explanation

Most people meet AI through tools like ChatGPT. They are called large language models, and under the hood they do something almost boring. They predict the next word. You type a few words, and it guesses the next, then the next. That is it. No understanding. Just a very fast, very good guess.

The AI used in physical security works a little differently. It does not predict words. It predicts patterns in what a camera sees. Show it enough video and it learns to tell a person climbing a fence from a plastic bag blowing across a lot.

This AI no longer lives in a far-off server room. It continues to move onto the hardware itself. Cameras and field units carry the brains inside them. They watch, judge, and flag a problem right where they stand, then call a human. That continued shift, AI baked into the device, is quietly the biggest story in security.

Good AI systems do not replace your people. They augment them by pointing them toward the moments that count. Think of AI-enabled hardware as a teammate that never blinks. Not a replacement for judgment.

The real choice was never robots versus guards. It is whether to hand your team smart hardware that helps them see and act with extreme efficiency.

Why So Many Leaders Are Saying "Yes"

The pull toward AI is not hype. It is a hiring crisis and some hard math.

The security industry cannot keep people. Guard turnover runs between 100% and 300% a year. Many firms replace their entire team once or more every year. Pay is low. Benefits are thin. Nearly half of guards have no health insurance through work. When a better job shows up, people leave. You cannot build security on a revolving door.

The cost story is just as loud. Covering one post around the clock takes three to four full-time guards, once you count shifts, vacation, and sick days. In a big city, that one post can run $200,000 to over $300,000 a year. Smart cameras with remote monitoring cost a fraction of that. Many properties cut their security spend by 40% to 70%.

Now add the attention problem. A smart camera does not get bored, and it watches every feed at once. For a leader facing empty shifts and a tight budget, AI-enabled hardware is hard to ignore.

Why "Yes" is Not the Whole Story

But hardware is only as good as the AI inside it and the human behind it.

In October 2022, a student walked into a high school in Utica, New York. The school relied on an AI weapons scanner built to catch threats. It missed a seven-inch knife. That knife was used to stab a student. Turn up the sensitivity, and the same scanner flagged laptops, lunchboxes, even a bag of chips as a gun. The FTC later took action against the maker for overstating what its system could do. Smart hardware that promises everything and cries wolf can be worse than none at all.

Bias is the other trap. Facial recognition does not work the same for everyone, with higher false match rates for women, older people, and people of color. That is not just a statistic. It has a face. In January 2020, police arrested Robert Williams in his Detroit driveway, in front of his wife and daughters, after a camera matched his face to a watch thief. The match was wrong. Porcha Woodruff was arrested for carjacking while eight months pregnant. The suspect on camera was not. More than a dozen people, most of them Black, have been wrongly arrested this way. The machine guessed, and people trusted it without checking.

The law is watching too. Face scans count as biometric data, and Texas just won a $1.4 billion settlement over face data collected without consent. Skip clear permission and a real policy and the legal risk can swallow any savings.

This AI no longer lives in a far-off server room. It continues to move onto the hardware itself. Cameras and field units carry the brains inside them. They watch, judge, and flag a problem right where they stand, then call a human.

So, to AI or not to AI? That is the wrong question. The better one is how.

The Smarter Middle Path

So, to AI or not to AI? That is the wrong question. The better one is how.

The best security programs do not pick AI or people. They blend them. The hardware does the tireless watching. People make the judgment calls and decide when to act. Keep a person in the loop on every real decision and you get the speed of the machine with the wisdom of a person.

For years, the AI story was all software. Smarter algorithms. Better analytics. Fancier dashboards. The real breakthrough now is putting that intelligence into rugged hardware you can drop anywhere, with no permanent power or cable required.

A new class of security units is rewriting the rules. They roll onto a site and go live within the hour. They run on solar and cellular. No trenching, no grid hookup. They pair on-site cameras and edge AI with live human monitoring, so the device watches everything and a real person steps in when it counts. And they cover ground old-school guarding never could. Construction sites. Parking lots. Remote yards. Corners that never justified a full-time post.

That is the real promise. Not replacing people, but extending them. One operator backed by smart cameras can now cover ground that used to take a dozen guards in places that used to have none. The labor crisis and the budget crisis ease at the same time.

AI is not a magic guard, and it is not a monster to fear. It is a tool. Paired with hardware built for the real world and a human hand on the wheel, it can fill the gaps that have stretched security teams thin for years.

Ash Roberts
Staff Product Manager, LVT

Ash Roberts is a Staff Product Manager at LiveView Technologies (LVT), overseeing a diverse portfolio that includes Alert and Video Management, GuardGate, SafeNow, and the LVT Mobile App. With over a decade of product management experience across FinTech, business communications, and peer-to-peer recognition platforms, he specializes in dissecting foundational user workflows to pinpoint root problems and drive collaborative solutions. Ash holds a B.S. in Psychology from Brigham Young University and is currently pursuing a Master's in Applied Artificial Intelligence at Utah Valley University.

SHARE

Pass it on.
Scan to share the online version:
lvt.com/elevate/buddy-cops

CUTTING THROUGH THE NOISE

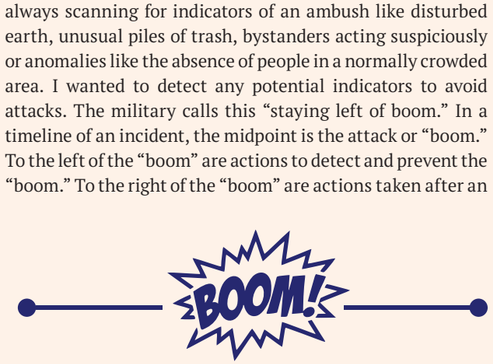
HOW AI SHARPENS AWARENESS

By Karl Schmae

When I was in the FBI we didn't just view situational awareness as a skill—it was a mindset necessary to survive and to stay one step ahead of threats. Situational awareness is the continuous process of identifying threat indicators in your surroundings, recognizing the significance, and then assessing the risk. This enables you to make informed decisions about possible courses of action. The gold standard for a security team is to use situational awareness to prevent an incident rather than to just defend and respond. With correct training and application of technology, they can detect the pre-attack indicators before a threat fully materializes, saving time, money, and potentially even lives.

Cutting Through the Noise

My first time operating in a combat environment was during my deployment to Afghanistan. Even driving was risky because of potential ambushes or hidden improvised explosive devices (IEDs). I had hyper vigilance when driving, always scanning for indicators of an ambush like disturbed earth, unusual piles of trash, bystanders acting suspiciously or anomalies like the absence of people in a normally crowded area. I wanted to detect any potential indicators to avoid attacks. The military calls this "staying left of boom." In a timeline of an incident, the midpoint is the attack or "boom." To the left of the "boom" are actions to detect and prevent the "boom." To the right of the "boom" are actions taken after an incident like response and investigation. How do corporate security teams stay left of "boom?" Security team members can be distracted by their phones, coworkers, or computers. People monitoring security systems can overlook legitimate threats because they are overwhelmed by too many false alarms or too much information. When most alerts amount to nothing substantive, a sense of complacency develops—nothing bad is ever going to happen. It's like the boy who cried wolf. He called out so many false alerts that when he finally called out a real warning, it was ignored, and the opportunity to prevent an attack was missed.



A guard needs to learn how to triage incoming information—what is important, what is irrelevant. They must be trained to recognize false alarms and which alerts require further investigation.

Artificial intelligence can help sort through the large haystack of incoming information and help to highlight the potential needles that represent the threat. AI-enabled security cameras can distinguish between a person and an animal. A human can then respond and investigate alerts that need more attention.

Spotting the Pre-Attack Indicators

Situational awareness is key to staying "left of the boom." This requires security teams to operate with a prevention mindset—looking for potential indicators of danger and analyzing information for trends, anomalies, or clues that indicate something is not right. Preventing incidents requires an understanding of your adversaries/threats and their tactics, techniques, and procedures (TTPs).

Every organization faces unique threats. For the retail sector your primary threat may be retail theft. Your adversaries—thieves—have their own TTPs. They may wear oversize clothing, carry backpacks, enter in groups, cause distractions, loiter, or visit on certain days or times. You should conduct a security assessment to identify and prioritize potential threats and to understand their TTPs. These provide clues for early warning of impending action.

Offenders conduct certain preoperational activities prior to incidents or "booms." They may take photos and videos to gather information about security measures such as guard patrols, locks, and security cameras. The offender may test security measures by attempting to enter locations without a badge or timing a guard's response to an alert. They may elicit information by asking seemingly innocuous questions about the facility. Your adversary is looking for gaps in your security coverage so they can evade your security measures. During the October 2025 art heist at the Louvre Museum, the thieves exploited security vulnerabilities by finding an access point with no camera coverage. Their heist was the result of careful planning.

Security team members need training to recognize "pre-boom" behaviors early so you can stay left of "boom." They should document suspicious activity in suspicious activity reports (SARs) so these can be analyzed to connect the dots. Was there a plausible explanation for an alert? Does the activity reveal a plan to commit mayhem or mischief against your organization? Has the same person tried to enter multiple locations? Has the same suspicious vehicle been observed at different times?

Your situational awareness can also be boosted by your employees, who can be another set of eyes and ears. They may see something the security team wasn't aware of. Creating a strong security culture needs robust security awareness training so people know what to look for and to encourage them to say something if they see something suspicious. This organizational situational awareness increases the chances of detecting potential preoperational indicators. Each report is a data point, a dot in a mosaic of ambiguity. When a security team has more data points to examine, they are better positioned to connect the dots to see if a more clear picture of a potential threat emerges. The security team can then assess risk levels to make informed decisions that prevent bad outcomes. These actions may include increasing their security posture, notifying law enforcement, warning company leaders, and advising employees how to stay safe.

Creating a Unified Front

Building strong partnerships strengthens your security team's situational awareness and effectiveness because it promotes information sharing. No security team has all the resources to respond to critical incidents or to get results like successful prosecutions. A security team may detain a person stealing merchandise, but local police need to make the actual arrest, conduct the investigation, collect evidence, and present the case to a prosecutor.

Build relationships with police prior to any incident or "boom." Meet frequently with law enforcement to discuss what they need to facilitate their response to your company. How do they obtain security camera footage? Where can they interview witnesses? How do they subpoena records? Streamlining this investigative process removes friction, leading to faster police responses and more efficient investigations. Identify all law enforcement agencies you'll work with and invite them to tour your facility. Local law enforcement generally are the first responders, but some crimes may violate federal laws, which then involve federal agencies like the FBI. Be proactive to meet police before the "booms" happen. Meeting regularly with police builds trust and encourages reciprocity. Ask for local crime trend data to improve your understanding of threats and their TTPs, and ask for introductions to other industry security personnel facing similar threats as you.

Meeting with security teams from other organizations in your area will also increase your situational awareness. You may have common threats such as organized retail theft crime groups. Sharing information about suspicious individuals or crime trends can help your security team sharpen their situational awareness skills. Sharing information contributes to your TTP knowledge base, which improves your situational awareness and your ability to stay left of "boom."

The threat landscape is constantly changing, because your adversaries are constantly changing their TTPs to exploit your vulnerabilities. Successful TTPs used in other regions will likely be used against you. Technology can help you but may also be used against you. Adversaries may use AI to plan operations against you or use drones for surveillance. Strong partnerships are a key element for staying situationally aware about evolving threats.

The Bottom Line

At the end of the day, you don't rise to the occasion—you sink to the level of your training. Developing a mindset that prioritizes situational awareness based upon an understanding of your threats is crucial to prevent incidents from happening. True security is built in the muscle memory developed during realistic drills and the gut instinct sharpened by a culture of vigilance. You want to build those law enforcement bridges and sharpen your team's eyes long before the radio goes quiet and the adrenaline hits. By the time the "boom" happens, it's too late to start wondering if you're ready. In this business, the ability to use situational awareness, trust your training, and act can make all the difference.

Karl Schmae

Former FBI Agent,
Law Enforcement/Intelligence Consultant,
President/Owner—Apex Security Advisors

Karl Schmae is a highly accomplished security expert and the Founder/President of Apex Security Advisors, dedicated to advising and training clients on mitigating risks. He draws upon a 22-year career with the FBI, where he served as a Supervisory Special Agent. Now in the private sector, he brings this expertise to clients, and appears on media outlets to discuss current events involving sensitive security issues.

SHARE

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

THE INVISIBLE TAX OF VISIBLE WINS

PROSECUTION alone won't match the dividends of investing in DETERRENCE.

BY MATT KELLEY

To all the security leaders out there—in the past month, how many times have you had to make a decision that:

- Would affect the safety of customers or employees?
- Had to be made with incomplete information?
- Had to be made under time pressure?

In all cases, I'd bet your answer is higher than that of your non-security peers.

Security leaders tend to be well-acquainted with the world of high-stakes decision-making under uncertainty and pressure. It's just part of the job. As a result, they also tend to understand the value of a decision-making framework to make quality decisions quickly.

In that spirit, I'd like to offer a framework for a decision that security leaders often face, but may not fully account for: deterrence vs. prosecution.

Defining Deterrence and Prosecution

Let's start with some rough definitions:

> **Deterrence** capabilities refer to an organization's ability to prevent would-be criminals from accomplishing a crime or to persuade them that it would be too difficult, too risky, or that the payoff would be too small to justify the effort.
>
> **Prosecution** capabilities refer to an organization's ability to adequately identify a criminal, collect sufficient evidence to build a case, and provide that case to law enforcement in a way that they are able to prioritize and successfully apprehend and prosecute the criminal.

I'll rely on the above definitions throughout the article knowing that, in practice, the lines between the two typically blur (many deterrence investments also support some aspects of the prosecution funnel, and many prosecution investments support deterrence). I separate them to provide a model that helps with strategy formulation and investment decisions.

Which is a Better Investment?

The TLDR (too long; didn't read) is that there isn't a universal right answer, but an optimal system likely has a mix of the two. Which investment will yield a better return depends largely on:

> **Industry** In certain industries, prosecution efforts have add-on benefits beyond just taking one criminal out of circulation for a certain amount of time (e.g. when retailers document crimes, their data can often help build cases for other locations and even other retailers). In others, this effect is limited (e.g. a federal defense contractor may decide not to prosecute a vandal because of the attention it could draw and the consequences to their brand).
>
> **Severity of incidents** Higher severity incidents lend themselves to prosecution better than lower severity incidents do. A low severity incident is unlikely to gain the necessary support from law enforcement to take action. On the flip side, deterrence capabilities can often deter high severity incidents just as well as low severity incidents.
>
> **Current capabilities** Capabilities often face diminishing returns. For example, the first $1 you spend on a capability might yield a 20x return, but the $1 millionth might only yield a 1.1x return. Accounting for your organization's current capabilities will help you evaluate the marginal return of each set.

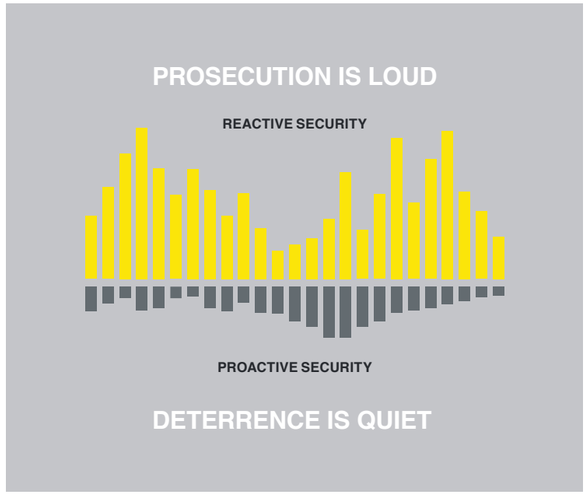
But I won't leave you hanging with an, "It depends on..." answer. Here are three insights that you might find useful:

1 PROSECUTION IS LOUD, WHILE DETERRENCE IS QUIET

Many security leaders skew their resources toward prosecution-related tactics. Why is this? We believe it comes down to human psychology.

When a criminal is arrested, you have tangible evidence of success. And the sheer volume of work required for this (reviewing footage, filling reports, coordinating with law enforcement) can reinforce the feeling of productivity. However, a successfully deterred crime is generally silent. It doesn't give the satisfaction of a successful arrest or conviction. And because it is usually a result of upfront rather than ongoing work, it may give the illusion that nothing is happening, even when it is working exactly as designed.

This visibility bias often leads organizations to over-invest in tools to improve documentation, investigation, and prosecution. For decades this has been the traditional approach to physical security countermeasures. These tactics offer visible gratification, even in scenarios where deterrence would yield a higher marginal return on investment.



2 PROSECUTION IS A VARIABLE COST, WHILE DETERRENCE IS FIXED

Prosecution requires manual work throughout the process (reviewing and organizing evidence, investigating suspects, and working with law enforcement) and tends to be a 1:1 or 1:few motion. This means the cost of prosecution tends to be variable—the more criminals you investigate and prioritize, the more it costs.

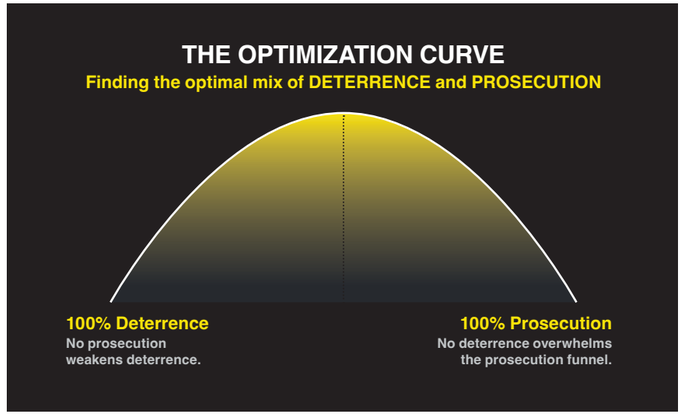
Deterrence on the other hand tends to require more up-front work (designing and implementing deterrents), but when done well, it is always working (1:many). This makes deterrence more of a fixed cost—regardless of how many criminals are deterred, the costs are stable.

3 DETERRENCE VS. PROSECUTION IS AN OPTIMIZATION PROBLEM

All things being equal, it's better to deter the crime than to catch the criminal after the crime. However, it isn't about choosing one over the other.

Robust prosecution reinforces deterrence, and effective deterrence allows investigators and prosecutors to focus on high-priority cases. Conversely, with no prosecution, deterrence loses its effectiveness, and with no deterrence, there are too many incidents to effectively prosecute. Capital allocators need to find the right mix.

By estimating the incremental return of your next dollar spent, capital allocators can reduce the noise and bias influencing the tradeoffs and make higher quality decisions.



How Do I Measure Them?

This is where many teams get stuck, but a few simple, low-cost measures can yield a meaningful reduction in uncertainty.

MEASURING PROSECUTION

To measure prosecution, it can be helpful to think of a funnel:

- At the top of the funnel are all those who follow through with a crime
- The next tier down are those who are accurately identified by investigators
- The next tier down are those whose case is accepted by law enforcement
- The next tier down are those who are arrested by law enforcement
- Then those who are convicted

If you want, you can round out the funnel with those who don't return to crime.

Think of every step in that funnel as a conversion rate. The value of any improvement to one of those conversion rates can be estimated with simple math. Keyword: estimated. If you are seeking greater levels of precision, as with most things, it requires more than simple math. Fortunately, the simple math is often sufficient to make much more informed tradeoff decisions between investments.

MEASURING DETERRENCE

Because deterrence is less visible than prosecution, many organizations don't measure it. But it can be measured—it just has to be measured differently. You often quantify deterrence by looking for changes in patterns over time and differences across comparable environments. For example:

- Before/after staff surveys about feeling of safety and crimes observed
- Before/after pictures of sites (if vandalism, property damage, or vagrancy are issues)
- Before/after customer surveys or interviews about feelings of safety
- Change in guard spend after making deterrence investment
- Capture success stories when available from those on site
- Changes in guard dispatches or manual interventions
- Trespass, vandalism, shrink, or after-hours activity trends
- Incident frequency/severity before and after deployment
- Number of activations, alerts, or escalations (depending on what is available from your deterrent system)

Lastly, for organizations with many sites, it is often possible to design the rollout of deterrent capabilities in a way that allows for some form of A/B testing, using similar sites as a control group for treated sites.

Selling the Strategy to Leadership

While security leaders often have their own discretionary budget, which they can allocate as they see best, sometimes they don't. And even if they do, it's important they share and gain buy-in from their leaders and colleagues for their security strategy—the time usually comes, if it hasn't yet, when they need support from others.

A great first step is to translate security outcomes into business language. Cash flow is often the universal shared outcome. Whenever possible, estimate the cash flow impact of various security outcomes. Precision may not be possible, but even wide estimate ranges can be helpful.

Second, identify opportunities for your security investments to benefit your non-security colleagues. We have been surprised to find how often security teams are sitting on what other teams would consider a gold mine (e.g. data on customer traffic, visibility into remote locations, real-time footage of locations), and the other teams are completely unaware. This is a missed opportunity, which can often be quickly and easily resolved (e.g. by picking up the phone).

Lastly, be strategic in how you pilot new capabilities. Involve non-security colleagues and leadership so they can personally experience the changes you are making in the business, and so they can identify opportunities where the investments will benefit them as well. Further, piloting new capabilities, especially if they generate video footage, can go viral within an organization—video clips are easily sharable storytelling tools.

A New Standard for Physical Security

Ultimately, the goal of a world-class security strategy is to contribute to the success of the business. By identifying the optimal balance between investments in prosecution and deterrence, security teams can operate in a way that builds trust from the rest of the organization.

Matt Kelley
SVP of Business and Market Development, LVT

Matt joined LiveViewTechnologies (LVT) in 2022. Previously, he was Sr. Manager of Asset Protection Resources, Innovation, and Technology at The Home Depot, overseeing physical security, asset protection technology, security guards, cash logistics, alarms, and CCTV. He served on the Loss Prevention Research Council's Advisory Board and led projects there. Matt holds a business degree from Georgia Southern and an MBA from Georgia State.

CALCULATOR

Wish there was a way to quantify the invisible wins of deterrence? Check out this online calculator tool.
lvt.com/elevate/deterrence-roi

How Legacy Becomes Legendary

5 min read

Using AI to Enhance Your Existing Security Systems

Augmented is the New Reality

7 min read

How Agentic AI Makes Security Faster, Cheaper, and More Efficient

Unleashing Intelligent Site Mangement

5 min read

How to Breed Security Into Your Business Strategy

Drones on the Rise

5 min read

What Eyes in the Sky Mean for Boots on the Ground

The Future of Physical Security

9 min read

Moving Beyond the Era of the Scarecrow to Solve the Safety Crisis

Want More Elevate?

Dive deeper into extended articles, bonus content, and expert insights at **lvt.com/elevate.**

Catching the AI Wave

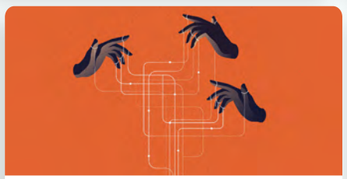
5 min read

Catching the Wave and Positioning Teams for the AI Shift

Cat Track Fever

3 min read

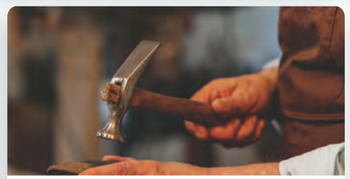
The Purr-suit of Everyone's Favorite Calico



Organized Crime Has Entered the Chat

7 min read

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



Leading with Human Agency in the Age of Autonomous Technology

6 min read

Strategic Leadership and the Future of Security

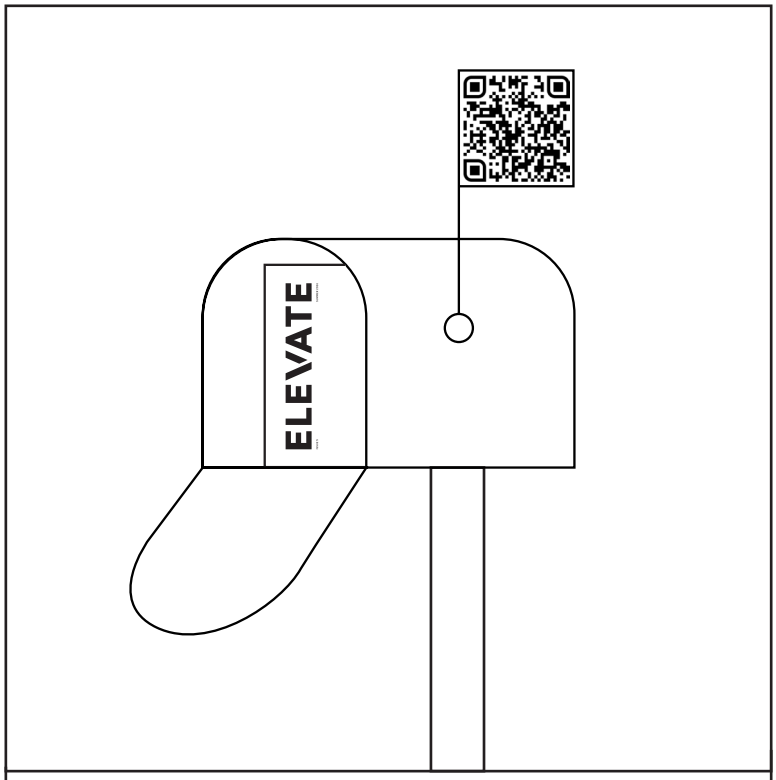
A Simple Framework for Complex Security

7 min read

The Essential Guidelines for Physical Security and Risk Assessment

LIVEVIEW TECHNOLOGIES

802 E 1050 S, STE 300
AMERICAN FORK, UT 84003



ELEVATE is LVT's thought leadership publication that explores the evolving challenges of safety and security across multiple industries. It features expert commentary, investigative reporting, frontline perspectives, and collaborative solutions to inform and empower security professionals, business leaders, and community stakeholders.

SUBSCRIBE *Get Elevate in physical and digital formats!*