

# SECURITY BUSINESS

Powered By



SECURITY  
INFOWATCH.COM



The Path to Greater Profits for Security Integrators

Vol. 44 No. 11 • November 2022

## Security Takes the Reins at WEC

A robust video surveillance system  
integrates with advanced door and  
access solutions to protect the  
World Equestrian Center

Page 42



Brian Remington of SmartWatch Security & Sound (a division of Sciens Building Solutions), oversaw much of the World Equestrian Center project.

THE  
PATENTED  
**CX-EPD1289L**  
PRELOAD RIM STRIKE  
NOW AVAILABLE!



**CAMDEN**  
DOOR CONTROLS

See Our Ad on Page 3

# StarLink Goes 5G to the MAX 5G LTE-M Is Here!

Introducing New **StarLink MAX 5G Universal Cell Communications Solutions**, Maximum Reliability & Labor-Savings - *Still the Dependable, Low-Cost Leader*



- 5G MAX** Speed & Next-Level Coverage 5G LTE-M, Fastest Networks & Longest Cellular Lifespan Available
- MAX** Account Protection For Any Panel Brand, Any Central Station & Any Application
- MAX** Reliability Proven to Work Even Where Others Won't 2 Antennas Are Better Than 1 + Signal Boost\*
- MAX** Ease of Installation Installs in Minutes; Panel-Powered & Preactivated. Connect models with Native Panel Downloading
- MAX** Pro Tradeup Incentive in the Industry For Lowest Cost Solution - **Save \$100 on all models**

## The New Dealer's Choice Just Got Better!

### TRADEUP OLD RADIOS & NETWORKS

StarLink **MAX**



as low as **FREE**

**APP OPTION: StarLink Remote On/Off**

### TRADEUP DISAPPEARING POTS LINES

StarLink **MAX FIRE**



Cell/IP Comm. Only  
**\$5795\***  
 net

**APP OPTION: FACP-Saver Tool**  
 Demos Savings v. POTS

### TRADEUP NEW INSTALLATIONS

StarLink **MAX Connect**



Radio from **\$1995\***  
 net

**APP OPTION: Gemini Security/Video/Access**



StarLink®, StarLink\*Max, Signal Boost™ are trademarks of Napco. Other marks trademarks of their respective cos. \*Sugg. Net equipment pricing quoted in USD with StarLink Tradeup Incentive Program™. \$100 Incentive credit on your StarLink Account, applicable to all models. See full details [www.napcosecurity.com/starlink/starlink4upgrade](http://www.napcosecurity.com/starlink/starlink4upgrade). Promotions subject to change without prior notice.

**Here's How To Get All StarLinkMax Radios FREE or \$100 Off**

\*See full details online at [www.napcosecurity.com/starlink/starlink4upgrade/](http://www.napcosecurity.com/starlink/starlink4upgrade/) or scan QR Code.



1.800.645.9445 [www.StarLinkMax5G.com](http://www.StarLinkMax5G.com)

Request information: [www.SecurityInfoWatch.com/10215125](http://www.SecurityInfoWatch.com/10215125)



# FINALLY, A RIM STRIKE DESIGNED FOR EVERY INSTALLER!

Whether you've installed a hundred RIM strikes or just one, Camden's remarkable preload strike is designed to get you off the job faster and can even avoid future service calls!

The patented design of CX-EPD1289L RIM strikes will release with up to 15lbs. of preload pressure, caused by differences in air pressure, inexact installation, or misaligned doors (during or after installation).

## Features:

- Patented Preload Feature, up to 15lbs.
- UL Security and 3Hr. UL Fire Listings
- 3/4" Latch Projection
- Grade 1 'Universal' 12/24V, AC/DC, Fail Safe/Fail Secure
- Included Latch Monitor
- Metal Marking Jig Included

Contact us for more information or to request a product demonstration today!

CX-EPD1289L



Opening New Doors to Innovation, Quality and Support!

1.877.226.3369 / 905.366.3377 | [camdencontrols.com](http://camdencontrols.com)

Request information: [www.SecurityInfoWatch.com/10213140](http://www.SecurityInfoWatch.com/10213140)

# November 2022 Contents

## FEATURE ARTICLES

### 30

TRAINING

#### Q&A: Inside SIA's New Apprenticeship Program

SIA director of learning and development Dr. Elli Voorhees outlines the early goals for the program, set to launch in 2023  
**Paul Rothman**

### 32

VIDEO SURVEILLANCE

#### The Democratization of AI

As the applications for surveillance devices expand beyond traditional security capabilities and into business intelligence and operations, interest in the technology has expanded among both developers and consumers  
**Fredrik Nilsson**

### 40

INDUSTRY INFLUENCER Q&A

#### The Evolution of Optical Turnstiles

An evolved new look also comes with increased functionality, technology integrations, and much more  
**Sponsored by dormakaba**

### 56

ACCESS CONTROL

#### How PACS Improve the Commercial Tenant and Building Experience

Commercial Real Estate (CRE) customers can leverage cloud-based and physical access control to modernize the buildings they own or lease  
**Troy Johnston**

### 60

INDUSTRY OUTLOOK

#### Q&A: New ESA Chairman John Loud

Coming off a long-awaited victory against false alarm fines in Georgia, the renowned security business owner looks ahead to two years at the helm of the Electronic Security Association  
**Paul Rothman**

## COVER FOCUS:



# 42

TOP PROJECT

#### Security Takes the Reins at WEC

2022 Security Vanguard Award Project of the Year: A robust video surveillance system integrates with advanced door and access solutions to protect the World Equestrian Center  
**Steve Lasky & Paul Rothman**

Cover Photos: Cara Dezzo

### 48

HONORABLE MENTION

#### Massive Upgrade in Harris County, Texas

Multi-year retrofit project involved security technology upgrades in more than 150 buildings in the downtown Houston area

**John Dobberstein**



48

### 54

HONORABLE MENTION

#### Keeping 350K Anime Expo Attendees Safe

A unique combination of screening technologies, video surveillance and human/canine patrols made impossibly long lines a thing of the past at the annual event

**John Dobberstein**



54

# The Partner Pros Trust

Snap One is the one-stop shop for all your needs, combining pro feedback and expertise with high-quality products and reliable technical support to deliver exceptional smart solutions.

## Price-Protected

We only sell to pros like you, which means you'll never get shopped by your customers.

## Free same day shipping

All orders over \$1,000 ship free, and Partner Rewards members get free shipping on every order.

## Shop Locally

Visit one of our 35 stores across the U.S. for same-day products, demos, and in-person training opportunities.

## High-quality Products

Bringing you trusted brands in technology categories like audio, video, surveillance, control, networking, conferencing, and remote management.

## Brands You Trust

We manufacture and distribute preferred brands including:



Ready to become a Snap One Partner?  
Visit [snapav.com/security](https://snapav.com/security) to learn more.



Request information: [www.SecurityInfoWatch.com/21090092](https://www.SecurityInfoWatch.com/21090092)

# November 2022 Contents

## COLUMNS

8

EDITOR'S NOTE

### The War on Lines

Unchecked queues can lead to impatience, despair, and even violence and injury – but there are emerging and time-tested ways to alleviate them

Paul Rothman

18

TECH TRENDS

### Everything as a Service

A closer look at the pros and cons of going “aaS”

Paul F. Benne

22

LEGAL BRIEF

### Consumer Fraud Lawsuits

Acquiring and storing sensitive data is simply part of most integration businesses, thus it is vital to be diligent and responsible with business and sales practices

Timothy J. Pastore

24

MODERN SELLING

### Four Steps to Turning Around Poor Sales Performers

Just saying “you really need to pick it up” never works

Chris Peterson

26

RECRUITING ROADMAP

### When to Go Temporary

There are many situations where a short-term contracted employee makes more sense than a long-term hire

Ryan Joseph

28

THE SMART MONEY

### Three Hot Trends in Residential Security

From inflation to product innovation and MDU expansion, residential integrators have a lot to pay attention to in the fourth quarter

Jennifer Kent

74

INSIDER INTELLIGENCE

### What's Keeping You up at Night?

Four of the hottest topics from last month's PSA Annual Convention

Kristie Kidder

## SECURITY WATCH

Industry News and Trends

10

TOP STORY

### The Sullivan Verdict Fallout for Security

Uber CSO's conviction stemming from a cyber-breach cover-up has put security directors, C-Suites on notice

Paul Rothman

12

RESIDENTIAL

### Matter 1.0 Released

Smart homes take the first big step to true intelligent device interoperability

Paul Rothman

14

### Fresh off the Wire

- CTSI Relaunches as Pavion
- Tech Systems Merges with Cyber Provider Securitronics
- RapidFire Makes First Buy-and-Build Move

16

### Headlines from SecurityInfoWatch.com

## DEPARTMENTS

64 NEW PRODUCTS

67 CORPORATE PROFILES 2022

71 MARKETPLACE

73 ADVERTISER INDEX

Vol. 44 • No. 11

# SECURITY BUSINESS



Published by Endeavor Business Media, LLC  
1233 Janesville Ave  
Fort Atkinson WI 53538  
(800) 547-7377

### EDITORIAL

**Editor-in-Chief** | Paul Rothman  
(847) 454-2731  
prothman@securitybusinessmag.com

**Editorial Director** | Steve Lasky  
(847) 454-2719  
steve@securityinfowatch.com

### Expert Columnists & Regular Contributors

Ray Bernard, *RBCS Inc.*  
Paul Benne & Jon Polly – *Tech Trends*  
Ryan Joseph – *Recruiting Roadmap*  
Timothy Pastore – *Legal Brief*  
Chris Peterson – *Modern Selling*  
Parks Associates – *The Smart Money*  
PSA Security Network – *Insider Intelligence*

### SALES

**Group Publisher** | Jolene Gulley-Bolton  
(480) 524-1119  
jgulley@endeavorb2b2.com

**Northeast US & Eastern Canada** | Janice Welch  
(224) 324-8508  
janice@securityinfowatch.com

**Midwest** | Brian Lowy  
(847) 454-2724  
brlowy@endeavorb2b.com

**Western US & Western Canada** | Bobbie Ferraro  
(310) 800-5252  
bobbie@securityinfowatch.com

**Classified Marketplace** | Amy Stauffer  
(920) 259-4311  
astauffer@endeavorb2b.com

### PRODUCTION

**Production Manager** | Jane Pothlanski  
jpothlanski@endeavorb2b.com

**Ad Services Manager** | Carmen Seeber  
cseeber@endeavorb2b.com

**Art Director** | Eric Van Egeren  
evanegeren@endeavorb2b.com

**Audience Development Manager** | Delicia Poole  
dpoole@endeavorb2b.com

### ENDEAVOR BUSINESS MEDIA, LLC

**Chief Executive Officer** | Chris Ferrell

**President** | June Griffin

**Chief Operations Officer** | Patrick Raines

**Chief Administrative and Legal Officer** | Tracy Kane

**EVP/Group Publisher** | Lester Craft

**Subscription Customer Service**  
PO Box 3257, Northbrook, IL 60065-3257  
Toll-Free 877-382-9187; Local 847-559-7598  
Circ.SecDealer@omeda.com

### Article Reprints

To purchase article reprints, please email  
reprints@endeavorb2b.com.

**List Rental** | InfoGroup

**Michael Costantino** | (402) 836-6266  
Michael.Costantino@infogroup.com

**Kevin Collopy** | (402) 836-6265  
Kevin.Collopy@infogroup.com

# Our Tech and Customer Support Teams are on Top of Our Entire Product Line



**The first step is to build a great product, the second is to support it after it goes out our door.**

A team founded on dedication and loyalty, DKS is made up of hardworking people who have been with us designing, testing, building, and handling DKS products for 10, 20, and even 40 years. Those values extend to our Customer Service and Tech Support teams, staffed with great people who know our products backwards and forwards and strive to support our customers every day. When you call DKS, you'll receive support from someone who knows the ins and outs of each product and how they work together. Seamless integration and seamless support, that's the DKS way.



[doorking.com/ontop](http://doorking.com/ontop)  
800-673-3299 • [info@doorking.com](mailto:info@doorking.com)





# The War on Lines

Unchecked queues lead to impatience, despair, and even violence – but there are emerging and time-tested ways to alleviate them

**I** once stood in a two-and-a-half-hour line because my 8-year-old wanted to ride the Seven Dwarfs Mine Train at Disneyworld.

I think pretty much every parent has been in this spot: We sat whenever possible; we shared snacks; we quickly depleted the battery power of every electronic device within reach; we moaned; we complained; and of course, we all questioned whether a nearly three-hour wait for a little less than three minutes of entertainment was actually worth it in the end.

I think many would argue that the three-hour wait was exactly what we signed up for when we entered the gates of the Orlando theme park – but do you know what we *weren't* doing throughout that time? We weren't buying anything, for one, and we were confined to a tight area as we weaved through the maze of crowd control barriers and rope stanchions.

Ask anyone who is running late for a flight at a major U.S. airport what they think about working their way through a maze of rope stanchions...I would bet that most of the responses are not fit for reprint here.

Bottom line, lines are bad! They are terrible for business, they can create anxiety and anger among those who are stuck in them – often leading to violence – and they can leave throngs of people in an extremely vulnerable situation with no easy route of escape. In all honesty, lines may be one of the most hated things in America.

Stadiums and indoor venues like convention centers have long been on the front lines of the war on lines.

“First of all, nobody likes to stand in line,” Jim Mercurio, Executive Vice President and General Manager of Levi's Stadium – home to the NFL's San Francisco 49ers – pointed out during a recent SecurityInfoWatch webinar on special events and sports facility security. “When you reduce time in a line, it does a whole bunch of things from a revenue-generation standpoint. Waiting in line means losing sales.”

The entire premise of the Vanguard Award honorable mention Anime Expo project (see page 54) was the fact that the 2019 event – as well as previous iterations – was given the unfortunate nickname of “LineCon,” and management was intent on improving what was reported as four-hour waits just to enter the venue. Expo patrons – many of whom were fully outfitted in cosplay in 90-degree heat – swore they would never return.

“When you're standing in line to get into a venue, that increases the potential threat to folks who are in that line,” Mercurio said. “We want to get people screened as quickly as possible and into the facility.”

Thankfully, integrators can come to the rescue here, with frictionless and mobile technologies that enable these venues to vastly increase throughput of patrons at entrances. From threat screening solutions to wave-and-go ticketing, a combination of

technologies is proving to be the primary defense in the war on lines.

“In most cases, you are [catching] the things that are giving you pause or keeping you up at night,” Mercurio said. “But you have to be careful when you are using technology that you don't solve one problem and create another. The answer is not 100-percent technology driven – it [should be] a part of securing people and process.”

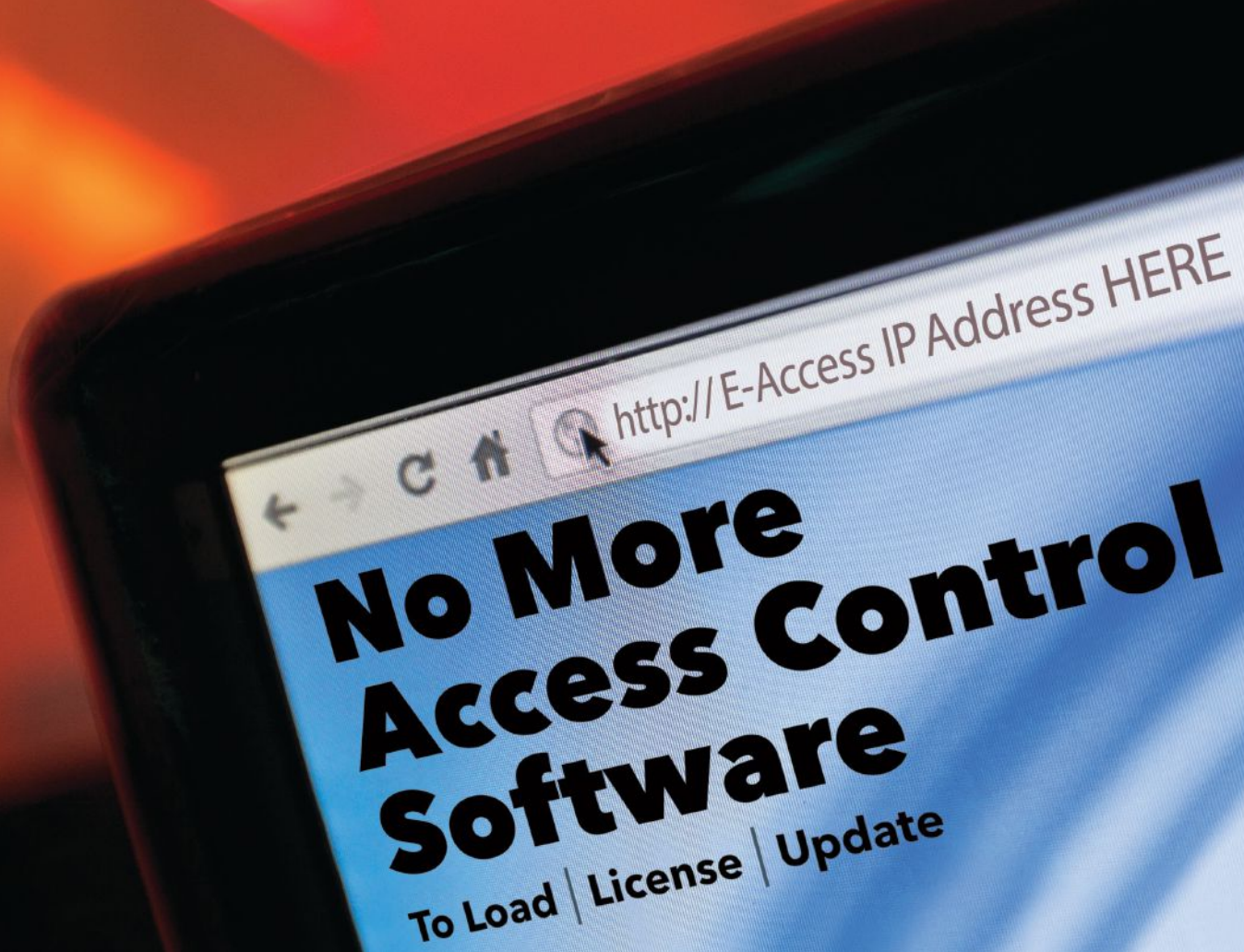
Indeed, beyond the cutting-edge technology to combat lines, integrators and security executives should also always be cognizant of the people who are standing in them. As an example, I was recently in a long line to enter a special party. It was taking quite a while, and folks were growing impatient. Just as voices began to rise and tempers were about to flare, a man pushing a cart with free water and snacks appeared, and everything calmed down again. A little understanding and compassion surely goes a long way to shortening a long line.

Listen to the full, archived SecurityInfoWatch webinar on special events and sports facility security at [securityinfowatch.com/21281197](https://securityinfowatch.com/21281197). ■

Paul Rothman, Editor-in-Chief

Email me your comments/questions at [prothman@securitybusinessmag.com](mailto:prothman@securitybusinessmag.com)





## Smart Access Control Made Simple by Napco

Now there's no more software to load or update & super-fast setup, with new **E-Access® Embedded Self-Contained Controllers**. Web-browser-based access from anywhere; the Panel's IP address is the URL. Stop software hassles & additional costs\*, while still getting all of the advanced features and flexibility you and accounts want: Cool App with dashboard and Free easy-issue Bluetooth mobile credentials; embedded Linux Operating System and 256 bit encryption; choice of slick readers (BLE, NFC, Prox, MiFare), easy configuration wizard, bulk ID uploads, Napco Gemini Security System integration and more. Simply scalable with choice of 1-, 2- or 4-Door Embedded Access Control Panels – for hundreds of doors and users.



\* No charge after one-time cloud activation

Now Available at all Napco Distributors.  
Ask about FREE Training Classes too.



1.800.645.9445  
[www.napcosecurity.com/products/e-access](http://www.napcosecurity.com/products/e-access)

Request information: [www.SecurityInfoWatch.com/10215125](http://www.SecurityInfoWatch.com/10215125)



© Hesu01/bigstockphoto.com

# The Sullivan Verdict Fallout for Security

Uber CSO's conviction stemming from a cyber-breach cover-up has put security directors, C-Suites on notice

**The conviction of Joseph Sullivan, the former Chief Security Officer (CSO) of Uber, sent shockwaves throughout the security industry –**

for companies' cybersecurity postures, as well as for the general career path of your average CSO. Sullivan was convicted in federal court in October for his attempted cover-up of a 2016 hack of private consumer information.

"[It] highlights the importance of disclosure and information sharing in fighting cybercrime," says noted cybersecurity consultant Chuck Brooks, who also serves as a cybersecurity professor at Georgetown University. "This case will hopefully be a wake-up call for companies to not only be forthcoming in alerting victims of breaches, but also calling attention to the new sophisticated and often automated cyber-threats that need to be addressed by all operating in the global digital ecosystem."

Sullivan, who will be sentenced at a later date by U.S. District Court Judge William H. Orrick, faces up to 8 years in prison for "obstruction of proceedings of the Federal Trade Commission" and concealing a felony.

"Security people have always been subject to criminal and civil risk,

because people, companies, information, or brand get damaged when security isn't managed well," explains Bob Hayes, managing director of the Security Executive Council and former CSO of Georgia Pacific and 3M. "This is just a high-visibility incident with a different twist."

## Security Best Practices: A Must

So how can an otherwise law-abiding security director stay clear of federal prosecution? First and most obvious is to understand the law. Each vertical has its own rules and regulations regarding cyber-breach notification. There is a HIPAA breach notification rule for healthcare, for example, and President Biden signed a new federal data-breach notification requirement in March 2022 for the vast majority of the critical infrastructure sector.

According to the U.S. Attorney's Office in the Northern District of California, "the evidence demonstrated that, shortly after learning the extent of a 2016 breach, rather than reporting it to the FTC, any other authorities, or Uber's users, Sullivan executed a scheme to prevent any knowledge of the breach from reaching the FTC...Sullivan then arranged

to pay off the hackers (100,000 in bitcoin) in exchange for them signing nondisclosure agreements in which the hackers promised not to reveal the hack to anyone."

## Effect on the Industry

No matter the sentence, a high-profile case such as Sullivan's will have an effect on the C-Suite, as well as current – and future – CSOs. It also likely will alter their stances on hiring best practices, as well as cybersecurity in general.

"Cyber is one of the biggest risks a corporation faces. From that standpoint, it is a good thing that people will have a greater understanding of the importance of [cybersecurity]," Hayes says. "In many of these breach cases, security has repeatedly warned that more needs to be done. Probably the most difficult question to ask coming out this is: When [the CSO] has made management aware of the business case [for security] and the consequences of [inaction], and they say no, then what?"

Thus, Hayes says the Sullivan case will have a significant effect in the boardroom and on executive behavior. "It is a high-impact event. It could have a negative impact, but it could also be a positive, because people are going to say to themselves, 'I better learn about this, and I better be pretty darn professional about what I do.' I think it will change behaviors for some people; for others it will reinforce what they have been doing all along," he says.

"I think security people will be more determined than ever to do the right thing," Hayes concludes. "Security people who are surprised by this better get busy, because if they didn't think these kinds of things can happen, then they probably shouldn't have been in the business in the first place...and this won't be the last time." ■



Read the full analysis:

[www.SecurityInfoWatch.com/21283224](http://www.SecurityInfoWatch.com/21283224)

# MAKE ROOM!

NOW... MORE CHANNELS OF POWER DISTRIBUTION – by ALTRONIX



Introducing **ACMS12(CB)** 12-Output Access Power Controllers with Fire Alarm Interface, and **PDS16(CB)** 16-Output Power Distribution Modules.

These new stackable sub-assemblies further increase access control capacity when integrated with Altronix Trove Series or virtually any wall/rack mount application - reducing overall equipment and installation costs.

Both feature dual inputs providing selectable 12 or 24VDC from any output with bi-color voltage LEDs for visual identification.



YOUR LEADER IN POWER | BACKED BY A LIFETIME WARRANTY

Request information: [www.SecurityInfoWatch.com/10212790](http://www.SecurityInfoWatch.com/10212790)



© MongtaStudio/bigstockphoto.com

# Matter 1.0 Released

Smart homes take the first big step to true intelligent device interoperability

**After several false starts and delays, the Connectivity Standards Alliance (CSA) announced in October the much-anticipated release of the Matter 1.0 specification** and

the opening of the Matter certification program, which many predict will revolutionize the smart home and residential security technology markets.

As *Security Business* reported in February, Matter is a proprietary, royalty-free home automation connectivity standard. First announced on Dec. 18, 2019, it aims to reduce fragmentation across different vendors, and achieve interoperability among smart home devices and Internet of things (IoT) platforms from different providers.

As part of Matter 1.0, authorized test labs are open for product certification, the test harnesses and tools are available, and the open-source reference design software development kit (SDK) is complete. Further, CSA members with devices already deployed and with plans to update their products to support Matter can now do so, once their products are certified.

## What does it mean for the residential security market?

"It is too soon to tell how the integrations between the security panels and Matter devices will shake out," says Avi Rosenthal, managing partner for smart

home and security consulting firm Bluesolve Partners LLC. "One of the features of the standard is something that allows for multiple 'managers' of a device. This gives control of a specific sensor to both the security panel and the Matter 'controller' (Google Home or Amazon Alexa, for example). But it is unclear how that data will pass from a security panel if they have not allowed this feature."

The initial release of Matter, running over Ethernet, Wi-Fi, and Thread, and using Bluetooth Low Energy for device commissioning, supports a variety of common smart home products, including lighting and electrical, HVAC controls, window coverings and shades, safety and security sensors, door locks, and media devices like TVs, controllers, and bridges.

"This release is the first step on a journey our community and the industry are taking to make the IoT more simple, secure, and valuable," Tobin Richardson, CSA President and CEO, explained in a press release.

The Matter 1.0 standard launches with test cases and comprehensive test tools for CSA members and a global certification program – including eight authorized test labs who are primed to test not only Matter, but also Matter's underlying network technologies, Wi-Fi and Thread.

Wi-Fi enables Matter devices to interact over a high-bandwidth local network and allows smart home devices to communicate with the cloud. Thread provides an energy efficient and highly reliable mesh network within the home. Both the Wi-Fi Alliance and Thread Group partnered with CSA to help realize the complete vision of Matter.

"Matter and Thread resolve interoperability and connectivity issues in smart homes so manufacturers can focus on other value-adding innovations," Thread Group president Vividh Siddha said in the release. "Thread creates a self-healing mesh network which grows more responsive and reliable with each added device, and its ultra-lower power architecture extends battery life."

Matter is also striking new ground with security policies and processes using distributed ledger technology and Public Key Infrastructure to validate device certification and provenance. This will help to ensure users are connecting authentic, certified, and up-to-date devices to their homes and networks.

"There are still lots of questions, but it is going to be very exciting to see how they are solved," Rosenthal says. "I hope to learn more at the launch in Amsterdam [in November]."

The CSA is spearheaded by some of the heaviest hitters in the smart home and residential security technology space, with its Board of Directors including executives from Amazon, Apple, ASSA ABLOY, Comcast, Google, Huawei, Latch, Legrand, Lutron Electronics, Resideo, Samsung SmartThings, Schneider Electric, and others.

"We would not be where we are today without the strength and dedication of the Alliance members who have provided thousands of engineers, intellectual property, software accelerators, security protocols, and the financial resources," Bruno Vulcano, Chair of the CSA Board and R&D Manager for Legrand Digital Infrastructure, said in the release. ■

CONNECT.  
COMMUNICATE.  
CONTROL.



MYALARM.CHAT®

Exclusively at COPS Monitoring



Most people prefer  
SMS to phone calls

## MyAlarm.Chat® is the fastest and easiest way to resolve alarms and improve customer satisfaction.

Instant text notification and secure web chat room experience bring your customers together like never before to make informed decisions about their security.

MyAlarm.Chat **works with every monitored account** and the intuitive interface is compatible with all modern smartphones without the need to download an app.

For more information, visit: [copsmonitoring.com/MyAlarmChat](http://copsmonitoring.com/MyAlarmChat)

Request information: [www.SecurityInfoWatch.com/10552071](http://www.SecurityInfoWatch.com/10552071)

Providing nationwide professional alarm monitoring and dealer services from  
New Jersey | Florida | Arizona | Tennessee | Texas | Maryland  
800.367.2677 | Fax: 856.629.4043 | [info@copsmonitoring.com](mailto:info@copsmonitoring.com) | [copsmonitoring.com](http://copsmonitoring.com)

CA: ACO6132 • DE: 05-85 • FL: EF20000481 • IL: 127-001299 • MD: 21PLU-SS1051 • TN: 632/1626 • TX Burg: B11561/17961 • TX Fire: ACR-2215 • VA: 11-1941



**COPS**  
Monitoring  
Your Hometown Central Station



## CTSI Relaunches as Pavion

After 10 acquisitions in 15 months, the integrator is uniting them all under the rebranded umbrella

Corbett Technology Solutions Inc. (CTSI) and its portfolio of recently acquired companies have relaunched as Pavion, saying it is now the third-largest safety and communications systems integrator in the United States.

The shift from CTSI to Pavion is the result of significant growth over the past 15 months – most of it via acquisitions. In all, CTSI has acquired 10 companies in that timespan: The Security Division of EC&M Electrical, DavEd Fire Systems, Collaborative Technology Solutions, The Protection Bureau, Star Asset Security/Ion247, AFA Protective Systems, Structure Works, Enterprise Security Solutions, Systems Electronics and Firecom.

Uniting under the Pavion umbrella allows each company to continue delivering core offerings while expanding services, impact and geographic reach,” a press release explains. It goes on to outline how CTSI and the acquired companies have already begun successfully integrating IT, enterprise resource planning (ERP), quoting, payroll, HR information systems (HRIS), safety and other management systems to optimize business operations.

“We are excited for the formation of Pavion, as it will allow us to accelerate our strategic growth,” Pavion President and CEO Joe Oliveri said in the release. “We felt it was time to introduce a new brand and vision that more accurately represents the direction we’re heading.”

CTSI is a portfolio company of Wind Point Partners, a Chicago private equity investment firm. Pavion combines the word pavise, a full-body shield used by warriors in the 14th-16th centuries, and ion, an electrically charged atom that drives forward momentum. ■

## RapidFire Makes First ‘Buy-and-Build’ Move

Acquisition of Security & Access Systems the “first of many,” according to CEO Mike McLeod

RapidFire Safety & Security has made its first acquisition since its March 2022 formation of a “Buy & Build” partnership with Concentric Equity Partners (CEP), by acquiring Security & Access Systems (SAS), an Albuquerque, NM-based provider of commercial security and fire alarm system design, installation, maintenance, monitoring, test, inspection, and repair services. “It is exciting to get the first one done, with many more to come,” RapidFire CEO Mike McLeod wrote in a post on LinkedIn, adding that the company is poised to acquire more businesses in California, Arizona, Texas, Missouri, and adjacent states.

RapidFire acquires SAS from Chris and Molly Ipiotis, who will briefly facilitate the transition. All other SAS employees will remain with the company. ■

Read the full story at [www.securityinfowatch.com/21282734](http://www.securityinfowatch.com/21282734).



## Tech Systems Merges with Cyber Provider Securitronics

Terry Rivet, CEO/President of Securitronics has been a long-time friend of Tech Systems CEO Darryl Keeler; in fact, they both served together on the Board of PSA Security Network for seven years.

Prior to the pandemic, Rivet acknowledged to Keeler that he was weighing potential exit options, and while Keeler admitted Tech Systems wasn’t looking at acquiring a company now, he asked his colleague to give him the first right of refusal when he firmed up his plans.

In October, both parties pulled the trigger. Tech Systems – one of the largest employee-owned (ESOP) systems integration firms in the security industry – announced a merger with Securitronics.

“Terry was aware of us becoming 100% employee owned in 2015 and felt that would be a huge benefit to his team for their years of service,” says Keeler, adding that TSI brought the Securitronics team into the ESOP based on their tenure with Securitronics, which resulted in anyone who been there for five or more years being 100% vested in the ESOP their first day with Tech Systems.

From an operational perspective, the merger is expected to be seamless as the two companies become one under the Tech Systems brand.

“Our companies’ culture [will] create an incredible force together,” Keeler says. ■

Read Steve Lasky’s full story at [www.securityinfowatch.com/21282542](http://www.securityinfowatch.com/21282542).



# Your first line of defense



Protect people and property by upgrading perimeter access control.

HES electric strikes are windstorm resistant, certified for outdoor use, and leverage existing hardware.

Securitron's integrated suite of products works seamlessly together, making your access control system easier to setup, customizable, and more reliable to operate.

[hesinnovations.com](http://hesinnovations.com) | [securitron.com](http://securitron.com)

**ASSA ABLOY**  
Opening Solutions



HES 1500



HES 1600



HES 9400



HES 9600



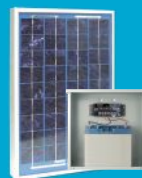
HES 9800



Securitron DK-37  
Digital Keypad  
System



Securitron GL1  
Force Gate Lock



Securitron BPSS  
Boxed Power Supply  
Solar – 10W or 20W



Request information: [www.SecurityInfoWatch.com/10213861](http://www.SecurityInfoWatch.com/10213861)

Experience a safer  
and more open world



The Milestone Systems Partner Summit (MIPS) in Minneapolis featured CEO Thomas Jensen, who unveiled the Milestone Kite offering.

## CENTRAL MONITORING

AvantGuard acquires Armstrong's National Alarm Monitoring of Canada  
[www.SecurityInfoWatch.com/21283505](http://www.SecurityInfoWatch.com/21283505)

## VIDEO SURVEILLANCE

Milestone Systems unveils Kite VSaaS solution based on Arcules technology at annual MIPS event  
[www.SecurityInfoWatch.com/21285095](http://www.SecurityInfoWatch.com/21285095)  
i-PRO rolls out EZ-2 Partner Portal  
[www.SecurityInfoWatch.com/21283686](http://www.SecurityInfoWatch.com/21283686)

## MANUFACTURER M&A

Alarm.com acquires Noonlight's connected safety platform  
[www.SecurityInfoWatch.com/21284771](http://www.SecurityInfoWatch.com/21284771)

Teledyne acquires X-ray technology provider ETM-Electromatic  
[www.SecurityInfoWatch.com/21285125](http://www.SecurityInfoWatch.com/21285125)

Volaris Group acquires, renames Hitachi ID Systems as Bravura Security  
[www.SecurityInfoWatch.com/21283932](http://www.SecurityInfoWatch.com/21283932)

Knightscope announces acquisition of CASE Emergency Systems  
[www.SecurityInfoWatch.com/21283425](http://www.SecurityInfoWatch.com/21283425)

March Networks acquires data analytics platform from DoIT Software  
[www.SecurityInfoWatch.com/21283119](http://www.SecurityInfoWatch.com/21283119)

Velodyne Lidar acquires AI software company Bluecity  
[www.SecurityInfoWatch.com/21284777](http://www.SecurityInfoWatch.com/21284777)

## MANUFACTURER NEWS

ASSA ABLOY readies sale of Emtek, Yale in response to DOJ complaint  
[www.SecurityInfoWatch.com/21284345](http://www.SecurityInfoWatch.com/21284345)

Snap One joins ONVIF, gains certification for multiple product lines  
[www.SecurityInfoWatch.com/21284664](http://www.SecurityInfoWatch.com/21284664)

Aiphone integrates IX Series with Genetec Security Center  
[www.SecurityInfoWatch.com/21283796](http://www.SecurityInfoWatch.com/21283796)

Ambient.ai achieves SOC 2 Type II certification for its software  
[www.SecurityInfoWatch.com/21284739](http://www.SecurityInfoWatch.com/21284739)

Cognyte sells portion of threat intelligence analytics offering to Volaris  
[www.SecurityInfoWatch.com/21284703](http://www.SecurityInfoWatch.com/21284703)

## DISTRIBUTORS

Arcules announces global distribution partnership with Wesco  
[www.SecurityInfoWatch.com/21284593](http://www.SecurityInfoWatch.com/21284593)

ADI's Electronic Custom Distributors opens Austin, Texas branch  
[www.SecurityInfoWatch.com/21285242](http://www.SecurityInfoWatch.com/21285242)

## INTEGRATOR M&A

Security Services Holdings/Protos acquires MG Security Services  
[www.SecurityInfoWatch.com/21283308](http://www.SecurityInfoWatch.com/21283308)

Pye-Barker Fire & Safety acquires Metro Fire & Safety Equipment  
[www.SecurityInfoWatch.com/21283230](http://www.SecurityInfoWatch.com/21283230)

Lone Star Communications acquires CareSight for hospital alarm tech  
[www.SecurityInfoWatch.com/21282976](http://www.SecurityInfoWatch.com/21282976)

## INTEGRATOR NEWS

Eastern Bank welcomes CPSS of Florida as commercial customer  
[www.SecurityInfoWatch.com/21283903](http://www.SecurityInfoWatch.com/21283903)

## PEOPLE IN THE NEWS

Camect names Sean Miller as CEO  
[www.SecurityInfoWatch.com/21283794](http://www.SecurityInfoWatch.com/21283794)

Omnigo Software announces Kevin Lafeber as new CEO  
[www.SecurityInfoWatch.com/21284028](http://www.SecurityInfoWatch.com/21284028)

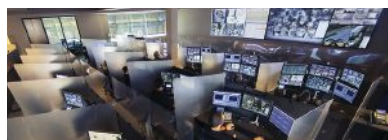
Managed services provider Protos Security names Mark Hjelle as CEO  
[www.SecurityInfoWatch.com/21285156](http://www.SecurityInfoWatch.com/21285156)



## Online Exclusives

### School Security Roundtable Discussion

Our recent school security roundtable webinar has generated a lot of buzz and is a must-listen in our archives. Hear the heart-wrenching story of **Noel Glacier**, parent of Parkland shooting survivor **Jake Glacier**, as well as expert opinions from industry luminaries including **Michael Dorn** of **Safe Havens Intl.**, integrator **Shaun Castillo** of **Preferred Technologies** and **Andy Phelps** of **Napco Security Technologies**.  
[www.SecurityInfoWatch.com/21273771](http://www.SecurityInfoWatch.com/21273771)



### In-Depth: Proactive Video Monitoring

Learn more about the central monitoring trend of Proactive Video Monitoring – which allows a monitoring provider to intervene and notify local authorities before a crime can occur – from **Woodie Andrawos** of **National Monitoring Center (NMC)**.  
[www.SecurityInfoWatch.com/21283626](http://www.SecurityInfoWatch.com/21283626)

### Has Security Reached a Watershed Moment?



In his latest *Real Words or Buzzwords* column, expert consultant **Ray Bernard** says We have reached a physical security industry watershed moment, in which we are making a complete break in security technology capabilities from the products and deployments of the past. The next 10 years of physical security, he says, will be a radical transformation from the previous 50.  
[www.SecurityInfoWatch.com/21284519](http://www.SecurityInfoWatch.com/21284519)

Follow SecurityInfoWatch on Social Media



facebook.com/SecInfoWatch

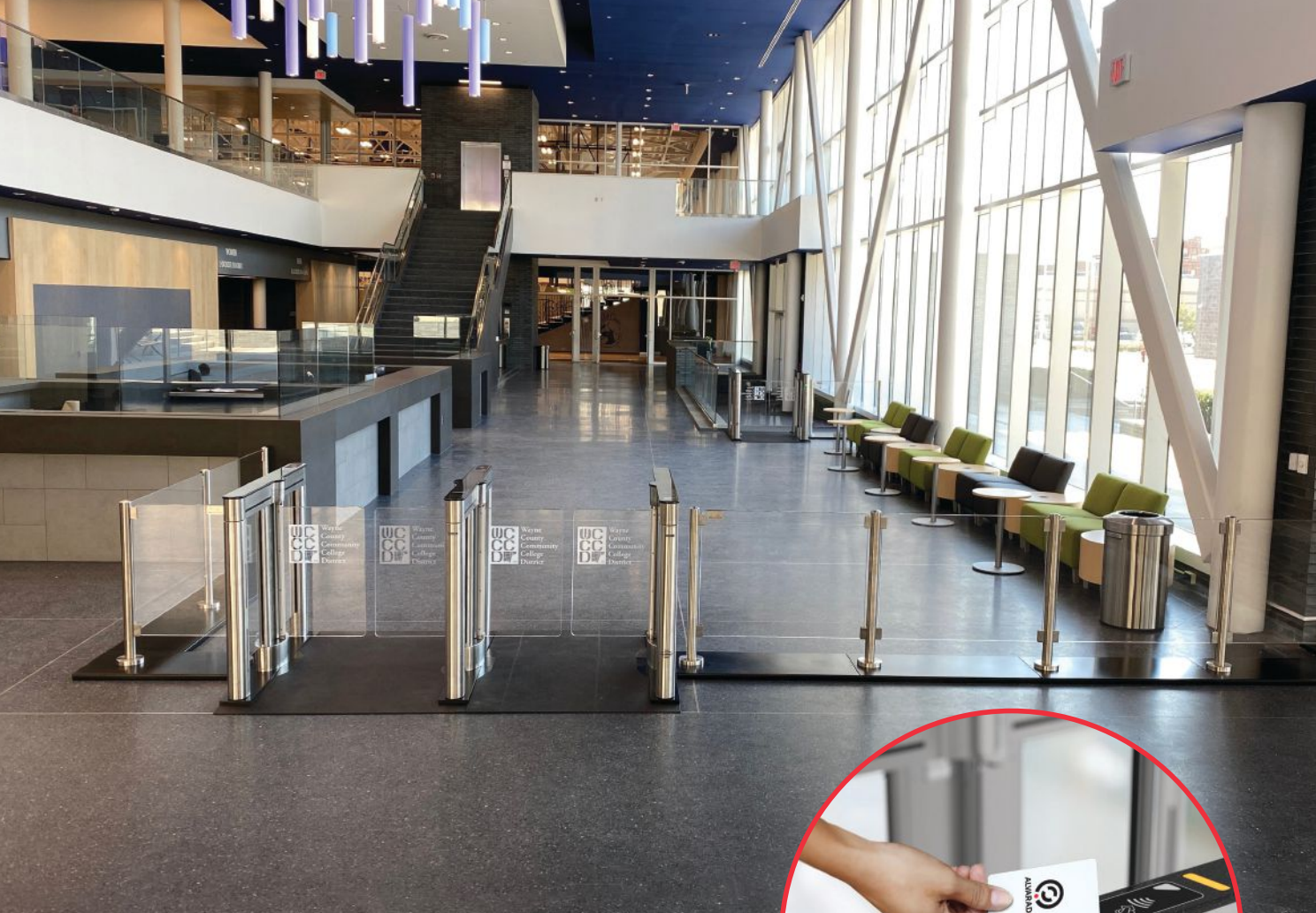


@SecInfoWatch



linkedin.in/company/securityinfowatch.com





# Access the Exceptional.

For over 65 years, customers have trusted Alvarado and our U.S.-manufactured products to protect their assets and control the seamless flow of people. Now, with the added resources and support of dormakaba, we are a turnkey partner with the power to make your next project exceptional.

Contact us today and let our solutions experts bring your vision to life.

[ALVARADOMFG.COM](http://ALVARADOMFG.COM)

Request information: [www.SecurityInfoWatch.com/10212792](http://www.SecurityInfoWatch.com/10212792)

 **ALVARADO**  
dormakaba Group



# Everything as a Service

A closer look at the pros and cons of going “aaS”

**J**ust about every vendor, software platform, and service provider are figuring out how to convert single-item sales into “as a Service” recurring revenue models.

If you are considering this as a service provider or an end-user, you will need to look beyond the sales pitch to see the true value – and the drawbacks – of this technology trend.

At first pass, the “aaS” model can be annoying to me as a consumer. I used to go into a store or browse online at the software available and buy it outright. If I elected to upgrade to a newer version in the future I could, but my hand was seldom forced, and the power was all mine.

Now, you are hard-pressed to find a software platform that is not offered in some type of subscription or SaaS model, and this trend is moving from the software world into hardware, systems and services. It is like you cannot “buy” anymore, only rent – but is that all bad?

## The Pros and Cons

Understanding some of the pros and cons of this trend can help you understand its value, both to yourself individually and to an overall organization. While there are many aspects of the “aaS” sales model, here are five considerations you should evaluate prior to making the commitment – keeping in mind that one person’s pro may be another person’s con. Thus, consider these points under your own application and circumstances.

“Many **construction projects have deeper CapEx budgets** to allow for the initial procurement and installation of expensive security technology; however, buying ‘aaS’ typically gets expensed through OpEx budgets and is a recurring monthly or annual expense – which can be more highly scrutinized.”

**1 Limits expensive server hardware:** When using platforms like Ava Security, Brivo, OpenEye, IronYun, etc., certain configurations can be cloud-based. This can reduce or eliminate the need for on-premises servers, which are costly and have a limited lifespan.

If your customer is considering a traditional deployment of security technology, they should consider that the servers installed on premises will come at a high cost and will need to be replaced in 5-8 years. They will also need to consider that they will likely need a Software Service Agreement (SSA) and a preventive maintenance contract to keep the system updated with patches, fixes and version releases. With an “aaS” model, this is all included.

**2 CapEx vs OpEx:** While evaluating “aaS” options, take into consideration how the customer will buy the technology. Many construction projects have deeper CapEx budgets to allow for the initial procurement and installation of expensive security

technology; however, buying “aaS” typically gets expensed through OpEx budgets and is a recurring monthly or annual expense – which can be more highly scrutinized. Having a thorough understanding of how “aaS” is funded and working out the details with the end-user’s finance department is critical to resolving push-back regardless of what solution is up for consideration.

**3 Critical facilities, SOCs and uptime requirements:** For facilities that operate in a critical capacity and have an on-site SOC, GSOC, or other real-time point of aggregating security information, close attention to “aaS” features are mandatory. Most “aaS” offerings have some or all features that are entirely dependent on outbound network connectivity; therefore, if the network fails, the security operation loses the ability to access and use the “aaS” product. When evaluating “aaS,” ask your customer pointed and hard questions about what services operate and if there are critical services that will not work in the event that outbound network connectivity is severed.

**4 Bandwidth and network:** The “aaS” sales pitch is typically a good one when it is well-perfected and delivered, but there are some downsides to consider, and integrators will need the end-user’s IT department or a non-biased third party like a consultant to help navigate the sales pitch and dig into the tech requirements of the network.

Having 10, 50, 100, or 1000 cameras at a facility that are going to a cloud-based “aaS” will have big implications on network architecture and bandwidth. Be sure this is fully understood before making a commitment to the “aaS” technology.

**5 Proprietary equipment:** Some “aaS” platforms openly accept cameras and edge technology from multiple manufacturers; others have cameras that can be used on other systems should you elect to stop using those systems in the future. That said, be warned that this is not the case for all “aaS” providers; in fact, some providers’ cameras are as good as a brick should your customer stop using the “aaS” platform. This could be a costly and embarrassing mistake.

### Best Practices

Here are key takeaways for considering any type of “aaS” model for software, systems, or services:

- Thoroughly understand what your customer’s needs are before calling “aaS” companies in to do a sales pitch. Not having this will distract you with sales presentation sparkles, bells, and whistles that may be great features, but can deviate from the core performance objectives required to serve the business.

- Understand the points of failure in “aaS” models and be willing to accept the risks they present. Knowing exactly where the points of failure are enables the integrator

and end-user to build operational processes to stopgap the vulnerability should a failure occur.

- Know the total cost of ownership (TCO) of both the “aaS” and traditional deployment of the software, systems, and services you are evaluating.

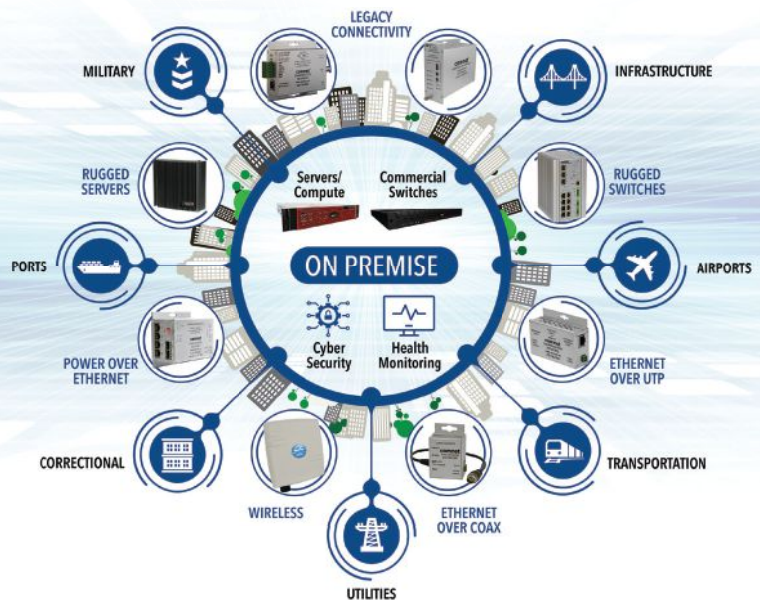
- Don’t go it alone. Bring in IT, Finance, and other major

stakeholders of the business to help evaluate the solution from their areas of expertise. ■

» **Paul F. Benne** is a 35-year veteran in the protective services industry. He is President of Sentinel Consulting LLC, a security consulting and design firm in based in New York City. Connect with him at [www.linkedin.com/in/paulbenne](http://www.linkedin.com/in/paulbenne) or visit [www.sentinelconsulting.us](http://www.sentinelconsulting.us).

# comnet

The Single-Source Solution  
for All Your Transmission Challenges



## COMNET CONNECTS

Offering the most comprehensive line of products, **ComNet is a single source solution for all your transmission challenges.** Choose ComNet Products today and you’ll **guarantee the performance of your network tomorrow.**

- Video, audio, data, Ethernet, over fiber optic, copper, and wireless media and servers
- Customer care specialists with the experience and understanding to support your application
- Cost-effective solutions to meet every performance standard
- Working 24/7 to get you the transmission products you need when you need them

Contact the Design Center Now for Free Design Assistance

Call 1-888-678-9427 or email [designcenter@comnet.net](mailto:designcenter@comnet.net)

[www.comnet.net](http://www.comnet.net) | [info@comnet.net](mailto:info@comnet.net) | 1-203-796-5300 | Toll Free 1-888-678-9427

**ACRE**  
Intelligent Security. Simplified

LIFETIME WARRANTY ∞  
MADE IN THE USA

Visit ACRE at ISC East  
New York City | Booth 1228  
16 - 17 Nov, 2022

Request information: [www.SecurityInfoWatch.com/10215705](http://www.SecurityInfoWatch.com/10215705)

# WHAT !F

## SMART SECURITY

**gave you more freedom**

**to focus on what**

**matters most!?**



**BOBBY MCGRILL**

**CSO (CHIEF SUPERGRILL OFFICER)**



Find out more

[www.stid-security.com](http://www.stid-security.com)

Request information: [www.SecurityInfoWatch.com/12266353](http://www.SecurityInfoWatch.com/12266353)

**STiD**

SMARTER SECURITY ANSWERS

# SPECTRE NANO



## Innovative SPECTRE nano Simplifies and Improves Vehicle Security



### Flexible and Durable

SPECTRE nano is the most compact UHF and Bluetooth® reader on the market for vehicle and driver identification. Nano uses contactless technologies to expedite entry and exit from parking garages, fleet lots, or corporate campuses. It can recognize either the driver, the vehicle or both by using UHF windshield tags, a badge or even the driver's Bluetooth smartphone with integration of the STid Mobile ID® ecosystem. These capabilities allow organizations to differentiate access control for vehicles and drivers with multiple profiles (e.g., visitors, employees, tenants). In addition, SPECTRE nano is housed

in a durable, anti-vandal shell that's resistant to shock, heavy precipitation, vibration, dust or even sea water. Maintenance is minimal, and no batteries are required.

### High Security

SPECTRE nano offers the highest levels of security, using encryption methods recommended by independent security organizations such as ANSSI and FIPS. In addition, OSDPTM and SSCP® protocols provide secure end-to-end, bi-directional communication. Key storage is certified EAL5+. Encrypted and signed credentials prevent cloning, and managers have the capability to quickly erase security keys.

### Easy & Intuitive

But, don't be intimidated by its robust features. SPECTRE nano is easy to install, easy to use, and can interface with most existing access controllers. The shell can be customized with your branding. After all, STid's objective is to simplify your security management.

---

Experience unprecedented efficiency for vehicle security and management. SPECTRE nano offers a more fluid and seamless access control process that is intuitive for its users without compromising on security requirements.



# Consumer Fraud Lawsuits

Acquiring and storing sensitive data is simply part of most integration businesses, thus it is vital to be diligent and responsible with business and sales practices

**F**raud. It sounds serious, right? It can be, when credibly alleged in a lawsuit. Google learned this the hard way recently – when, after nearly two years of hard-fought litigation, it agreed to pay \$85 million to settle claims brought by the Attorney General of the State of Arizona under the Arizona Consumer Fraud Act.

The lawsuit alleged that Google misled and deceived consumers about the collection and use of their personal location data by tracking smartphones even when consumers disabled the “location history” setting. Among other remedies, the Arizona act allows for civil penalties of up to \$10,000 per violation (*i.e.*, per impacted user), which was among the reasons for the size of the settlement.

Every state has one or more consumer protection laws that prohibit deceptive trade practices such as false or misleading advertisements, bait-and-switch tactics, and other fraudulent marketing methods. Since the Arizona suit, Washington, Texas, Indiana, and the District of Columbia have also filed lawsuits against Google.

In addition to these general consumer protection laws, there are laws that target specific industries or practices, such as telemarketing, predatory lending, health or travel club memberships, in-person solicitations, etc.

If a State Attorney General launches an investigation or files a lawsuit under a state consumer protection law (also sometimes known as a deceptive

or unfair trade practices law), they have the power and resources of the state behind them. Depending on the state, they also may have the authority to dissolve the offending company and/or to impose monetary or even criminal penalties. That puts your company at an immediate disadvantage – even if you are Google.

## When the FTC Intervenes

State Attorneys General often share consumer complaints and other information with each other as well as with the Federal Trade Commission (FTC).

As the most powerful consumer protection agency in the country, the FTC’s Bureau of Consumer Protection collects complaints and conducts investigations into unfair, deceptive and fraudulent business practices – bringing lawsuits, developing rules to maintain a fair marketplace, and educating consumers and businesses about their rights and responsibilities.

Only the FTC has the authority to enforce Section 5 of the FTC Act – a federal statute that prohibits “unfair methods of competition” and “unfair or deceptive acts or practices.” Conduct that violates the FTC Act will often violate state laws; thus, states sometimes bring consumer protection actions in coordination with the FTC against the same defendant(s).

## Private Litigants (*i.e.*, Consumers)

In addition to regulators such as the FTC and State Attorneys General, individual consumers can file private

lawsuits under most state consumer protection laws. Many laws allow the consumer to recover heightened damages *and* attorneys’ fees, which makes them attractive to plaintiffs’ lawyers.

While private lawsuits should be taken seriously and could pose a meaningful risk to your company, private litigants generally cannot obtain the full range of remedies available to Attorneys General. Also, a private litigant may have a higher evidentiary burden – because the private litigant may have to prove that they relied on and were proximately damaged by the specific business practice that gave rise to the lawsuit.

Over the years, I have defended several private consumer fraud actions brought against my security clients in various states. While none of those cases succeeded, because security integrators often acquire and store sensitive information and, ultimately, are sales organizations who market their products and services to commercial and residential consumers, it is important to be diligent and responsible with your business and sales practices – with the guidance of capable counsel – lest you find yourself facing a consumer fraud claim. ■

» **Timothy J. Pastore, Esq.**, is a Partner in the New York office of Montgomery McCracken Walker & Rhoads LLP ([www.mmwr.com](http://www.mmwr.com)) where he is Vice-Chair of the Litigation Department. Before entering private practice, he was an officer and Judge Advocate General (JAG) in the U.S. Air Force and a Special Assistant U.S. Attorney with the DOJ. Reach him at (212) 551-7707 or at [tpastore@mmwr.com](mailto:tpastore@mmwr.com).



# 40

YEARS

## EXCEPTIONAL MONITORING

With 40 years of experience providing our customers with exceptional monitoring services, UCC employees know what it takes to help our dealers succeed. In addition to quality, caring monitoring services to our dealers and their customers, we invest our time and resources into providing industry leading dealer support and training and implementing new technologies and value add services.

- ✓ Over 260 years of combined leadership experience
- ✓ Over 112 years of operation management experience
- ✓ 63,000 Dealer Training Workshops, Webinars, one on one sessions, support outreach calls, and in person office visits
- ✓ 3 year average tenure of alarm dispatcher
- ✓ 2.5 million+ dollars invested in upgrades & expansions

For more information on UCC and our 40 years in the industry, go to [www.teamucc.com](http://www.teamucc.com)



**JOIN UCC TODAY**  
[www.teamucc.com](http://www.teamucc.com) | 888.832.6822





# Four Steps to Turning Around Poor Sales Performers

Just saying “you really need to pick it up” never works

**T**urning around struggling salespeople is one of the most unsuccessful ventures in business. After facing this scenario dozens of times in my consulting work with clients, we have developed four critical steps as a process for sales leaders to turn around poor performing salespeople:

## 1 Catch it before it's too late.

A key to most challenges in life is catching them early. Most sales leaders know that they should track Key Performance Indicators (KPI), but many track the wrong ones. Here are the two types of activity all sales leaders should track:

- **Short-Term Quote Activity:** Don't simply track outstanding quotes that are on the street, but also track week-to-week quoting activity.
- **Early-Stage Activity:** Although calculating quotes is important, tracking the activity that leads to quotes can be an eye-opener. I am not suggesting that you create a cold call report, but your salespeople should have a targeted list of new prospects that you can review with them during your one-to-one meetings. You will learn quickly whether they're working or not.

## 2 Work on opportunities together.

Stating “you really need to pick it up” never works. The good ones know they need to pick it up, and they are looking for help. When you realize that one of your salespeople is performing poorly, use the greatest four words a sales leader can say: “*Let's figure it out.*” These are magical words to the good ones and may even inspire the bad ones.

## 3 Develop short-term, realistic goals.

One of the biggest time-wasters that I see is the Performance Improvement Plan (PIP). It usually looks like this: The sales leader says, “*You're at 30% of your quota, and we're halfway through the year. I need you to catch up by the end of the third quarter, or we will have to make some hard decisions around here.*”

(Translation: Brush up your resume and go find a job while we pay you for the next few months).

Instead, enact the two steps above and then establish short-term and realistic goals, for example: Schedule appointments with three of your top 50 prospects in the next week; generate 110% of your quoting goal in the next two months; or, schedule and execute successful vision meetings with your two Tier 1 clients in the next quarter.

Focus on activity that matters and set mini-short-term goals aligned with this activity.

## 4 Continue to coach.

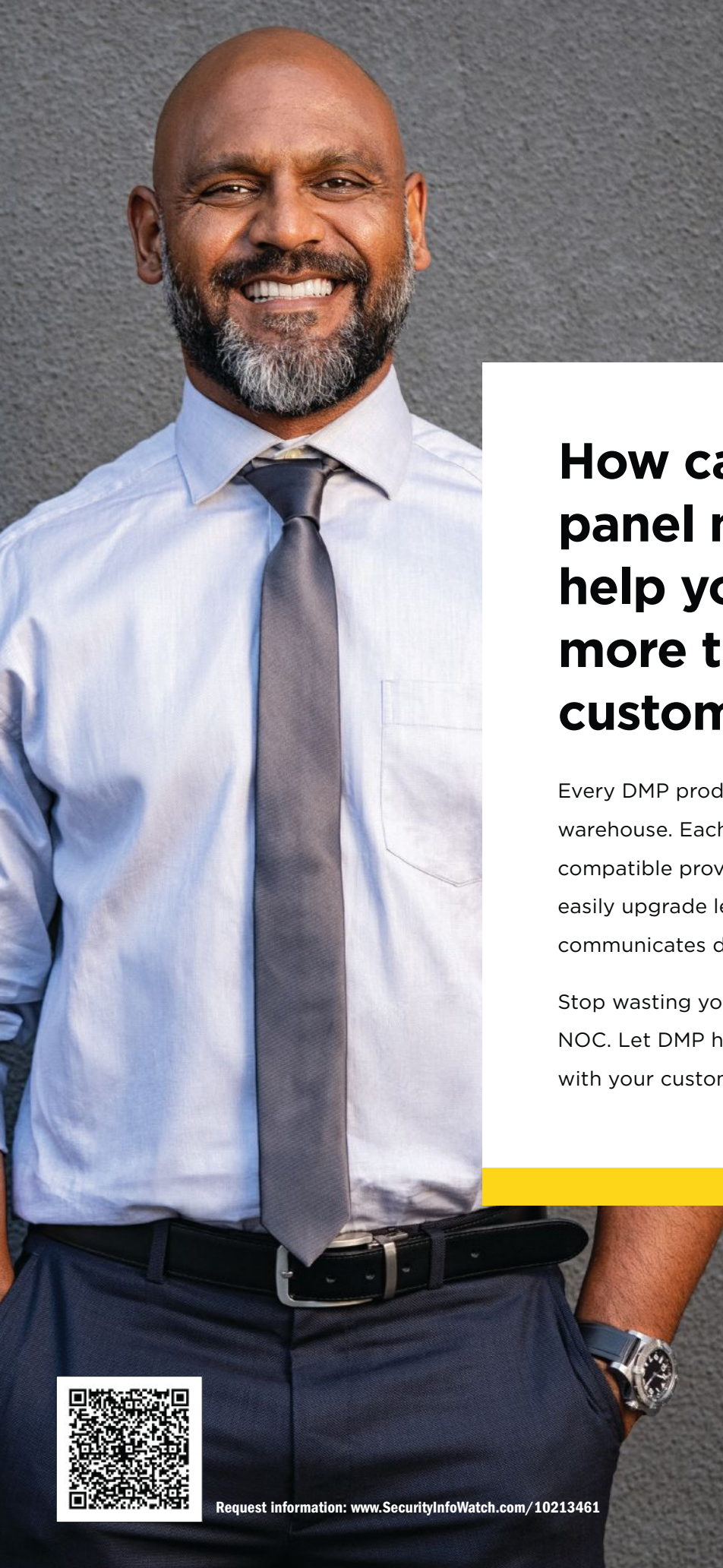
Have you seen *The Biggest Loser* – the reality television show that brought obese people together in a competition of losing weight? Some of the transformations were so drastic that it seemed unhealthy. After a few years of *The Biggest Loser*, multiple stories arose about contestants gaining back much of the weight they lost (to be fair, there are some long-term success stories, too).

For months, these contestants are surrounded by coaches, nutritionists, and supporting peers. Even though the show does a great job of providing support structure for them after the season, it pales in comparison to the support they receive while filming the show.

Of course, some of them are going to slip back into their old habits, and it is the same with your salespeople. You cannot be as active with them as you were during your short-term goal stage, but you must continue coaching them. Ride in the field with them, hold them accountable to their activity, and keep an extra eye in their direction – at least for the six months following your short-term goal work. ■

» **Chris Peterson** is the founder and president of Vector Firm ([www.vectorfirm.com](http://www.vectorfirm.com)), a sales consulting and training company built specifically for the security industry. Use “Security Business” as a coupon code to receive a 10% lifetime discount at [www.vectorfirmacademy.com](http://www.vectorfirmacademy.com). To request more info about the company, visit [www.securityinfowatch.com/12361573](http://www.securityinfowatch.com/12361573).





## How can an alarm panel manufacturer help you build even more trust with your customers?

Every DMP product is tested before leaving the warehouse. Each product is forward and backward compatible providing the flexibility for you to easily upgrade legacy equipment. And, each panel communicates directly with your monitoring center.

Stop wasting your money building someone else's NOC. Let DMP help you build a better relationship with your customers.



Request information: [www.SecurityInfoWatch.com/10213461](http://www.SecurityInfoWatch.com/10213461)





# When to Go Temporary

There are many situations where a short-term contracted employee makes more sense than a long-term hire

**W**hile many companies call on recruiters to bring on full-time employees, far fewer utilize a contract workforce to its fullest potential. Contract employees – while generally hired to complete short-term projects or services – can provide a lot of value to organizations and fill gaps in skillsets when they arise.

In addition to long-term, full-time candidates, many recruiting companies will offer organizations contract employees in a multitude of fields – ranging from office administration to warehouse workers and even up to the CFO level.

While many prefer the stability of full-time employment, some people prefer to learn different industries, companies, or skills and will take on contract positions to do so.

Contract employees have the opportunity to work on new projects in different industries for a relatively short period of time. With contract work, there is often more flexibility when it comes to scheduling, and it is a great way for skilled laborers to find part-time work as well.

Lastly, many people find contract work to hold them over after a layoff while they are searching for a new full-time position.

## When Contract Employees Make Sense

Supplementing your workforce with contracted employees is a great way to quickly scale your organization when needed. It is also an excellent way to find hidden gems

“Supplementing your workforce with contracted employees **is a great way to find hidden gems**...and you might gain some great new employees who are too impactful to just be part-timers.”

in the workforce. Who knows you might gain some great new employees who are too impactful to just be part-timers.

There are multiple scenarios and methods to using temp employees in a way that will provide both short- and long-term success to a business. Here are four of the most popular:

### 1 Maternity or paternity leave:

Using a contractor to fill a gap while a key employee is out on leave can prevent a lot of headaches; in fact, with enough planning, companies can avoid any pain during the transition. If done correctly, the employee going on leave can actually train the contractor to make for a smooth transition. This will keep your departments functioning even with a change.

**2 Test drive:** Are there positions that would be opportunistic within your organization? Meaning, if the right candidate came along, would it take a lot of work off your (or someone else's) plate? Are you held back by tasks preventing you from getting to the next level? Imagine what other tasks you could take on as a leader if other tasks were taken off of your plate!

A contracted worker will help you try it out. Utilizing a contractor will allow you to test drive not only the level of necessity of the position, but

also if the candidate is the right fit culturally and skillfully.

### 3 Easing growing pains:

Sometimes companies are in a transition phase and need to scale but aren't quite there yet. Sound familiar? For example, many companies may be fine using a bookkeeper or go without an HR person until they reach a certain size; however, once they reach that pain point, it is often too late.

Hiring a contracted consultant to come in can be a cheaper alternative to bringing in an expert. Doing this allows companies to have the skilled expertise of a veteran in that field without the big-ticket salary that comes with it.

### 4 Seasonal employment:

Is there a “busy season?” Hiring seasonal employees – such as for the summer security selling season – can help combat full-time employee burnout by sharing some of the heavy workload. This is particularly helpful for companies smaller in size or who have recently lost an employee that was critical to the team. ■

» **Ryan Joseph** is an Executive Recruiter for Recruit Group (<https://recruitgrp.com>), with a focus on security industry operations, sales, and sales leadership. For help with your security recruiting efforts, contact her at [ryan@recruitgrp.com](mailto:ryan@recruitgrp.com) or call (954) 278-8286.

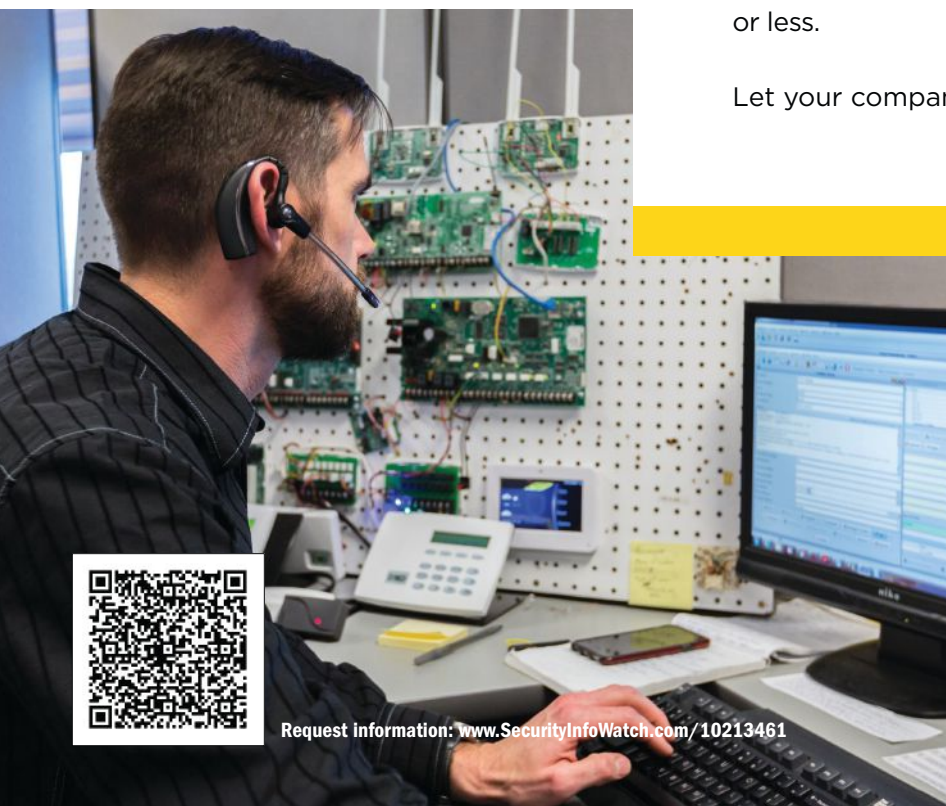


# Does your manufacturer have your back?

When technology issues occur, how fast does your manufacturer respond?

DMP not only provides superior products, advanced training and tools to help support your customers, but also leading-class U.S.-based technical support, addressing your questions, on average in two minutes or less.

Let your company rely on DMP to have your back!



Request information: [www.SecurityInfoWatch.com/10213461](http://www.SecurityInfoWatch.com/10213461)





# Three Hot Trends in Residential Security

From inflation to product innovation and MDU expansion, residential integrators have a lot to pay attention to in the fourth quarter

**A**s we enter the fourth quarter of 2022, several trends are having an immediate effect on the residential security industry. Integrators serving this market are navigating inflation as much – if not more – than their own customers. In addition, new technology innovations are coming, along with a push into emerging markets.

Here's a look at three of the top residential security trends as we head into the holiday season:

## 1 Inflation forces integrators to raise monitoring fees and diversify services.

The cost of living has increased in 2022, as inflation recently broke a 40-year high; and there are few indications that consumers can expect a decrease in the cost of goods and services in the near future. Meanwhile, security integrators must find ways to increase revenue to compensate for the higher prices of materials, overhead and wage inflation of employees.

Parks Associates research reveals that a good portion of these integrators are raising professional monitoring fees or including new opt-in services for consumers to compensate for the rising expenses.

The research firm reports that price hikes for security monitoring may impact adoption rates throughout the rest of 2022 or shift market share to less-costly competitors.

Security solutions have enjoyed high demand – even under the economic uncertainty of the pandemic –

but it is unclear if growth will continue with higher pricing and tighter consumer wallets.

## 2 Security players make moves in the MDU market.

The National Apartment Association (NAA) reports demand for apartments is at an all-time high, driven by factors such as the increase in adults aged 18 to 24 who are delaying home ownership, as well as an aging population choosing apartment living.

Technology product and service providers are increasingly targeting the multi-family space, offering services focused on both MDU residents and rental property owners.

In June, ADT acquired IOTAS, a leading smart home automation platform for the multi-family space, for just this purpose.

From a new product perspective, Brivo's new interoperable smart credentials enable property managers to issue a single keycard or fob that operates multiple locks, eliminating the need to replace existing lock hardware with compatible devices or using unencrypted, insecure proximity cards for access control.

Parks Associates research finds that 80% of property managers plan to introduce smart home devices in their units within the next 12 months, indicating high demand. This also reflects MDU operators' and owners' need to remain competitive in order to secure top rental candidates.

As security providers offering professional installation and monitoring services feel the pressure of

competition from low-cost DIY players, the MDU market is an attractive play.

## 3 Product introductions focus on video and deterrence.

Smart cameras and video doorbells are the top-adopted smart home device product categories (other than smart speakers). Security system owners adopt these products at dramatically higher rates, and they are the top devices that security owners *add* to their systems if they didn't include them in the original system purchase.

Manufacturers are fighting for an edge in this competitive market. In Q2 2022, Bosch, Swann, Arlo, Vivint, and Alula each announced new cameras. Whether a video doorbell or free-standing camera, manufacturers are improving pixel quality, night/thermal vision, as well as camera view, durability, battery life, and AI capabilities. These new features improve deterrence for intruders or porch pirates.

The Arlo Go 2 release is notable for its improved features – including 1080p, Wi-Fi and LTE support, longer battery life, GPS, a spotlight, and real-time 2-way communication – but also for lower pricing – \$150 cheaper – than the previous model. ■

» **Jennifer Kent** is VP of Research for Parks Associates. Parks Associates analyst **Ryan Hulla** also contributed to this article. Access a special virtual roundtable "*Tech-Enabled Buildings: Driving Next-Gen Services*," in partnership with Alarm.com focusing on the current state of property tech, broadband requirements, system integration and more at [www.parksassociates.com/webcasts/spaces2022-virtual-sessions](http://www.parksassociates.com/webcasts/spaces2022-virtual-sessions).



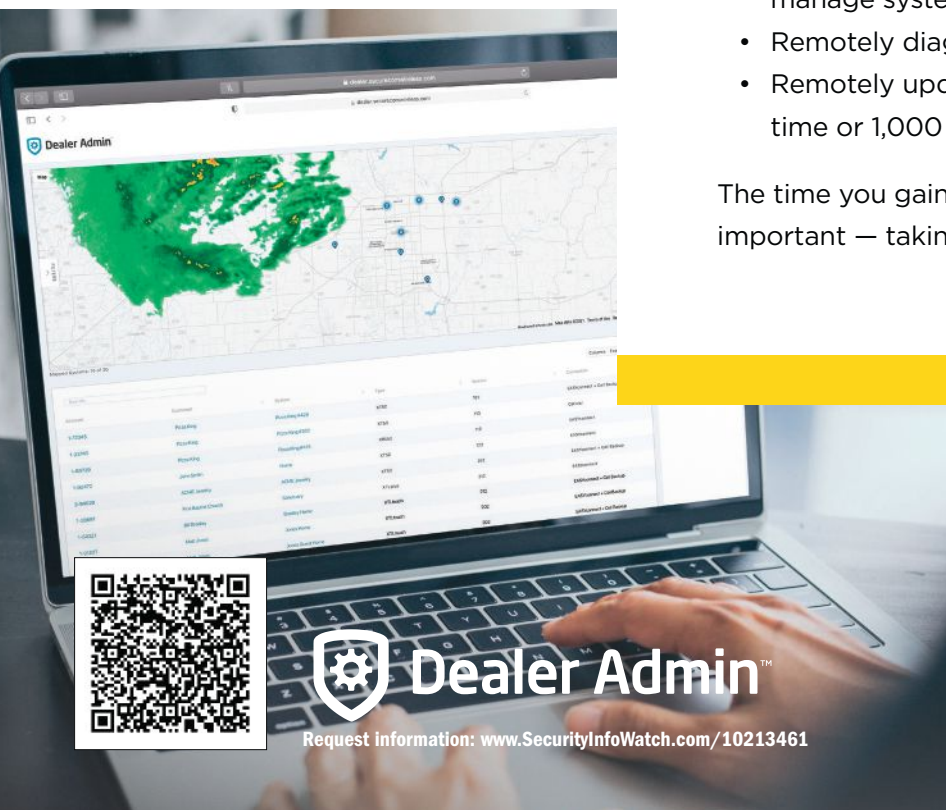
## How can I have peace of mind that my business won't suffer when good help is hard to find?

Like so many businesses, alarm companies are having a tough time finding people.

You don't have a personnel shortage — you have a time shortage. Your current staff can accomplish more in the same time by doing more with Dealer Admin™.

- Account management
- Automatically program panels without installers/technicians
- View, search and pull dashboard analytics to manage systems and serve customers proactively
- Remotely diagnose late-to-test signals
- Remotely update panel programming — one at a time or 1,000 at a time

The time you gain can be used to focus on what's most important — taking care of your customers!



**Dealer Admin™**

Request information: [www.SecurityInfoWatch.com/10213461](http://www.SecurityInfoWatch.com/10213461)



# Q&A: Inside SIA's New Apprenticeship Program

© cynhzl/1096464132/Getty Images

SIA director of learning and development Dr. Elli Voorhees outlines the early goals for the program, set to launch in 2023

By Paul Rothman

**I**n September, the Security Industry Association (SIA) announced it is developing an apprenticeship program to help address security integrator workforce challenges.

According to a press release ([www.securityinfowatch.com/21284772](http://www.securityinfowatch.com/21284772)), the initiative is set to launch in June 2023 as a one-year pilot program. *Security Business* caught up with Dr. Elli Voorhees, SIA director of learning and development, for the early details:

**Will the pilot be a limited or full program to start, and how will it work once it is finalized?**

**Voorhees:** The pilot program will include participation from several large security integrator companies and their end-user partners. Together, they will implement the program and align their apprentice onboarding and training to the competency framework developed by SIA.

**What will be the focus of the curriculum, and is it still under development?**

The program is designed for security systems technicians and covers elements of physical security device installation, configuration, networking and cybersecurity, as well as general employability skills in customer service, business acumen, time management and communication.

**Are integrators contributing to the curriculum?**

A group of security integrators helped identify skills needed for entry-level system technicians and contributed



“The pilot program will include participation from several large security integrator companies.”

— Dr. Elli Voorhees, SIA

to the development of the framework for the program. SIA is working collaboratively with manufacturers and integrators to identify related training curriculum to support apprentice learning and development.

**Who is the ideal candidate(s) for this type of program?**

The target audience for this program includes security system technicians, installers and field service technicians. The program is designed to expedite the learning and on-the-job training journey for new, entry-level techs at integrator companies.

**How is it being marketed to people outside of the industry?**

The program will be registered with the U.S. Department of Labor and listed publicly on RAPIDS, the national apprenticeship programs registry. Though collaborative efforts with employer partners, SIA will share program information with job placement agencies, non-profit organizations and schools in targeted hiring localities.

**How will it connect students with integrator jobs?**

SIA will partner with participating companies on recruitment efforts to target local schools, employment

organizations, special interest groups (i.e., nonprofits) and government agencies to attract applicants. Fostering diversity, equity and inclusion (DE&I) is an important tenant of the program, and outreach efforts will focus on reaching non-traditional students as well as communities that historically have not had access to well-paying jobs.

**What will integrators need to do to be able to participate?**

Following the pilot program, security integrators can elect to participate in the program by adopting the competency-based framework and fulfilling certain program reporting requirements. Companies will be responsible for assisting in recruitment, hiring apprentices and supplying resources to support apprentice onboarding, learning and on-the-job training.

**Who will teach the classes? Do you need volunteers?**

The program includes both classroom learning (technical instruction) and on-the-job training. SIA and its members will offer both free and fee-based programs to support competency development and skill attainment. We are not currently recruiting instructors or volunteers. ■



## One customer, 102 locations, 5 installers, 30 days to finish the job. Who can help?

Large jobs generate revenue, but logistical issues and shortages in experienced technicians impact time and your bottom line.

DMP gives you everything you need to complete the job at the right place and at the right time.

- Equipment arrives where you need it and when you need it
- Custom auto programmed from the factory

What you thought was your time and people problem became your DMP advantage.



Request information: [www.SecurityInfoWatch.com/10213461](http://www.SecurityInfoWatch.com/10213461)





# The Democratization of AI

© monajji/1181535674/Getty Images

As the applications for surveillance devices expand beyond traditional security capabilities and into business intelligence and operations, interest in the technology has expanded among both developers and consumers **By Fredrik Nilsson**

**A**rtificial intelligence (AI) has come so far so quickly that the public perception of AI remains heavily influenced television or movie portrayals, even as its real-life capabilities have begun to match and even exceed many of those depictions.

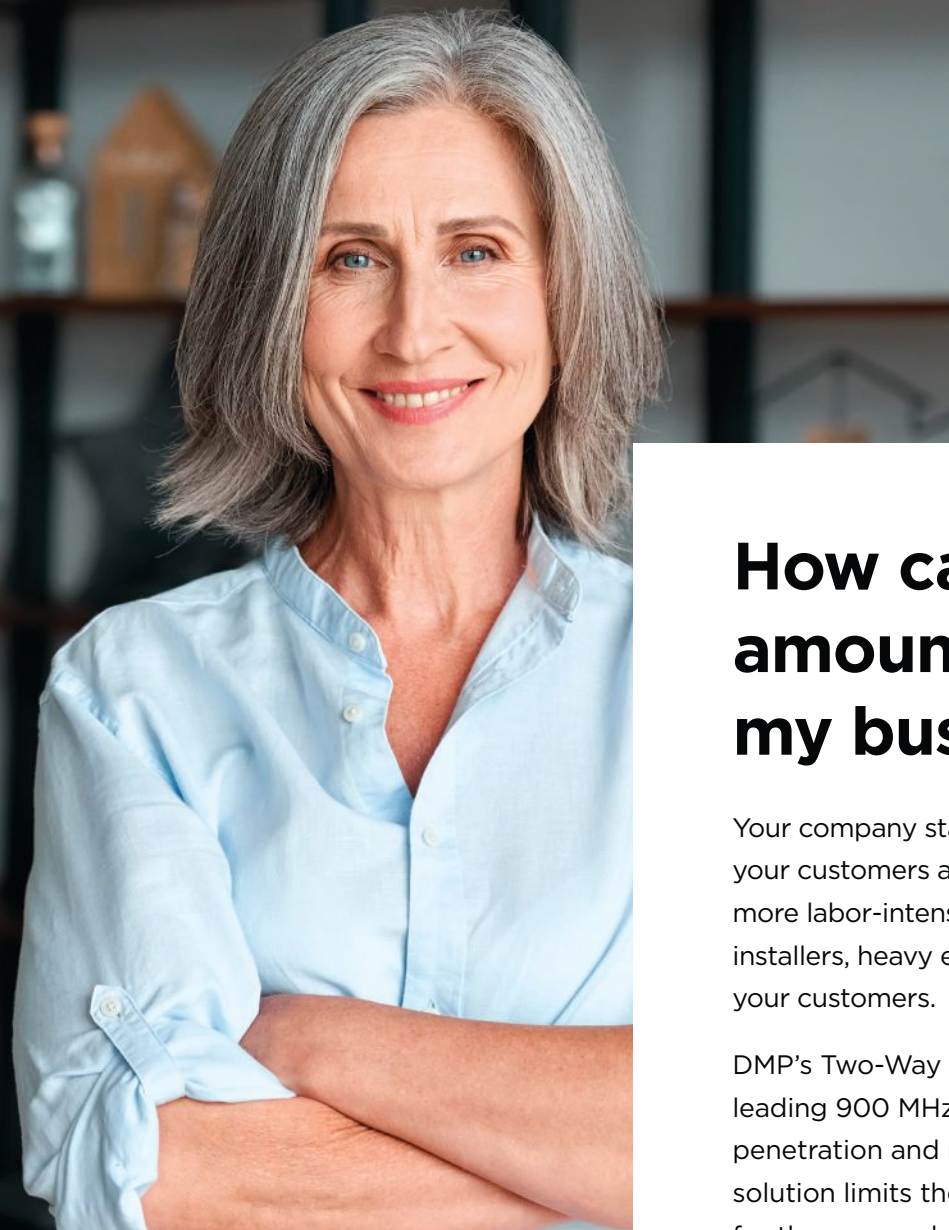
Never fear, a rogue AI is not going to form Skynet or create an army

of Austrian-accented Terminators, nor does it mean you are likely to be having a conversation with an AI companion anytime soon. That said, it does mean that working with artificial intelligence technology is no longer the exclusive practice it once was. Today, different forms of AI are being used in a wide range of devices and for a variety of different business and consumer applications.

For the security industry, this is wonderful news. Today's security devices – such as internet protocol (IP) surveillance camera and audio solutions – are increasingly capable of leveraging AI technology natively, at the network edge.

This means that more powerful analytics can be run on the devices themselves, keeping bandwidth and data storage needs in check.





## How can I reduce the amount of stress on my business?

Your company starts making money the moment your customers are up and running. However, larger, more labor-intensive installations may require multiple installers, heavy equipment and can be disruptive to your customers.

DMP's Two-Way Wireless™ features an industry-leading 900 MHz spread spectrum for superior penetration and range. This reliable and robust solution limits the number of technician hours needed for those complex installations, reducing the stress on you and your customers.

---

*Add wireless devices to your installation with the snap of a picture with Tech APP™.*



 **Tech APP™**  
AUTOMATIC PANEL PROGRAMMING

Request information: [www.SecurityInfoWatch.com/10213461](http://www.SecurityInfoWatch.com/10213461)



This means that not only are more developers capable of creating AI-based solutions, but those solutions are becoming available – and valuable – for an increasing number of consumers as well.

This growing democratization of AI technology is enabling valuable new applications, both within the security industry and beyond.

### Where AI Stands, and How We Got Here

Artificial intelligence is a scientific term with a scientific definition: it applies to digital systems capable of performing tasks that normally require human intelligence.

If that sounds like a broad definition, that's because it is – AI is essentially an umbrella term that encompasses everything from chatbots to self-driving vehicles. But under that umbrella, there are other, more specific terms: machine learning and deep learning.

Machine learning (ML) is more complex, and it applies to technology that shows signs of basic cognition, or the ability to learn. Deep learning (DL) adds even more complexity, helping machines perform tasks like pattern recognition and information classification.

Based on that definition, it should come as little surprise that the advent of deep learning – and the deep learning processing units (DLPUs) that power today's advanced cameras – has been a boon

for the security industry.

It is impossible to overstate how critical these DLPUs have been for the democratization of AI. It is important to note that video analytics are not a “new” technology – they have been around for many

the cameras themselves, analyzing and classifying data so that only the relevant metadata needs to be sent to the cloud. This vastly reduces the amount of both bandwidth and storage needed to use advanced new analytics while also decreasing the

on-site hardware footprint, making the technology much more accessible to a broader range of potential customers.

On top of that, the platforms on edge devices have become much more capable and easier to develop for. This has inspired more and more developers to create new analytics, result-

ing in expanding use-cases that go far beyond traditional security applications. This explosion of interest in AI-based analytics has expanded the security market in fascinating new ways.

### Expanding into New Areas

Analytics, both video and audio, have traditionally been very security-focused – detecting trespassing, theft, assault, and other potential crimes was paramount. Analytics could help a security team know if someone crosses a certain line or enters an area at night. If someone is behaving aggressively or the sound of breaking glass is heard, the security team probably needs to know that, too.

Rather than watching recorded video to look for evidence, security teams can now launch an immediate response the moment suspicious or alarming behavior is detected. In many cases, this can prevent situations from escalating, allowing secu-



With AI technology much more accessible and easier to develop on edge platforms, it has inspired developers to create new analytics, resulting in expanding use-cases that go far beyond traditional security applications.

years – but they tended to suffer from both poor accuracy and a generally cumbersome and expensive user experience. Movement detection was possible, but prone to false alarms. Object detection was possible, but not always accurate.

As the image quality of cameras improved over time, some of these issues were lessened, but the higher quality the image, the greater the need for pricey storage space, either on premises or in the cloud.

And while powerful DLPUs have been available in larger servers for some time, granting the ability to run analytics in the cloud, both the servers themselves and the bandwidth needed to transmit high quality images or entire video clips could be extremely expensive. As a result, early AI-based analytics were limited in both their scope and their use.

Now, thanks to DLPUs, these AI-based analytics can be run on



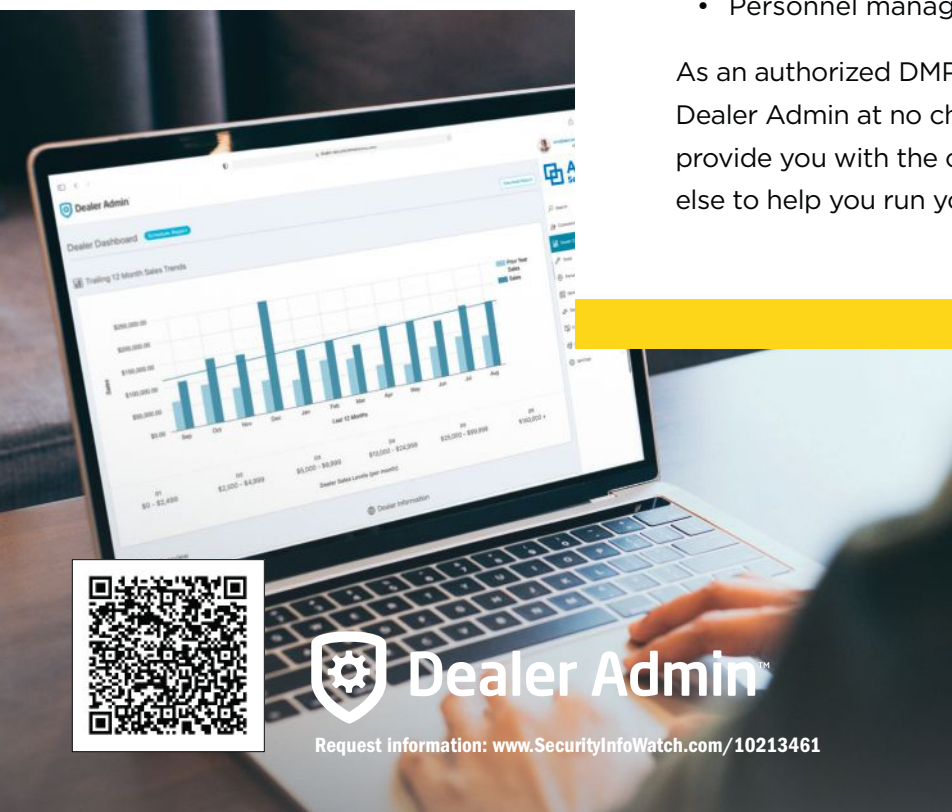
## How can I get more time back to focus on my business?

Running a successful business takes dedication, risk taking and information. Business data is difficult to track on a regular basis, but it helps you make critical decisions.

DMP's cloud-based administrative tool – Dealer Admin™ – provides real-time information available at your fingertips, including:

- Sales trends
- Customer reports & analytics
- Tech support calls
- Personnel management

As an authorized DMP dealer, you get all this and more from Dealer Admin at no charge. Let DMP's Dealer Admin tool provide you with the critical insights you can't get anywhere else to help you run your business more efficiently.



Dealer Admin™

Request information: [www.SecurityInfoWatch.com/10213461](http://www.SecurityInfoWatch.com/10213461)



rity to be proactive vs. reactive.

Those applications will always be valuable. But as a wider range of companies enter the analytics space – both on the developer side and the customer side – a growing number of them are exploring other applications. Many are looking at their camera deployments and wondering whether they can add additional functionality to increase the value of their hardware investment.

Manufacturing companies, for instance, are not just interested in keeping trespassers out of facilities, they are also interested in analytics that can monitor assembly lines and identify opportunities for improvement. Are employees following proper procedures? Are things moving too fast? Too slow? Are there

opportunities to improve workflow process on the factory floor?

In the past, those questions could only be answered using an extremely high-end machine vision camera – one that might cost tens of thousands of dollars per device.

Today, that same functionality can be achieved using the same DLPU-equipped cameras that many organizations may already have installed as part of their security setup – and a growing number of them are realizing that they have capabilities they have not been using.

### **New Developers, New Possibilities**

Because of this, and platforms that are very easy and effective to develop

AI code for, developers of all types have jumped at the chance to create new applications for broader use-cases. And it isn't just a case of security analytics developers expanding into other areas – a wave of new developers has entered the fray.

In fact, the need for powerful new analytics has even inspired developers with complementary skills to work together.

People counting technology is valuable from a security perspec-

traffic is impacted by weather, season, sales promotions, or point of sale data. It might be important to know that on Saturdays during the summer, there tends to be a 40% uptick in customers between 11 a.m. and 1 p.m., so a similar 40% uptick in staff is needed.


This has nothing to do with safety and security – it simply serves to make the customer experience better by avoiding big lines, long wait times, and unavailable staff

members. It makes the entire process more seamless, and the customer has no idea it is made possible by AI-based technology built off security and surveillance software.

It is also interesting to note that the benefits of this democratization actually do circle back

around to improve security, as well. For example, a company that makes long-distance detection and tracking software might have quite a bit to offer a company that focuses on license plate recognition. A camera mounted on the side of a building might have a limited vantage point, only able to read license plates on cars that drive up to the entrance. But with the help of long-distance tracking analytics, that same technology might be deployed on a rooftop camera able to see read the plates on vehicles at the edge of the facility or far into the parking lot.

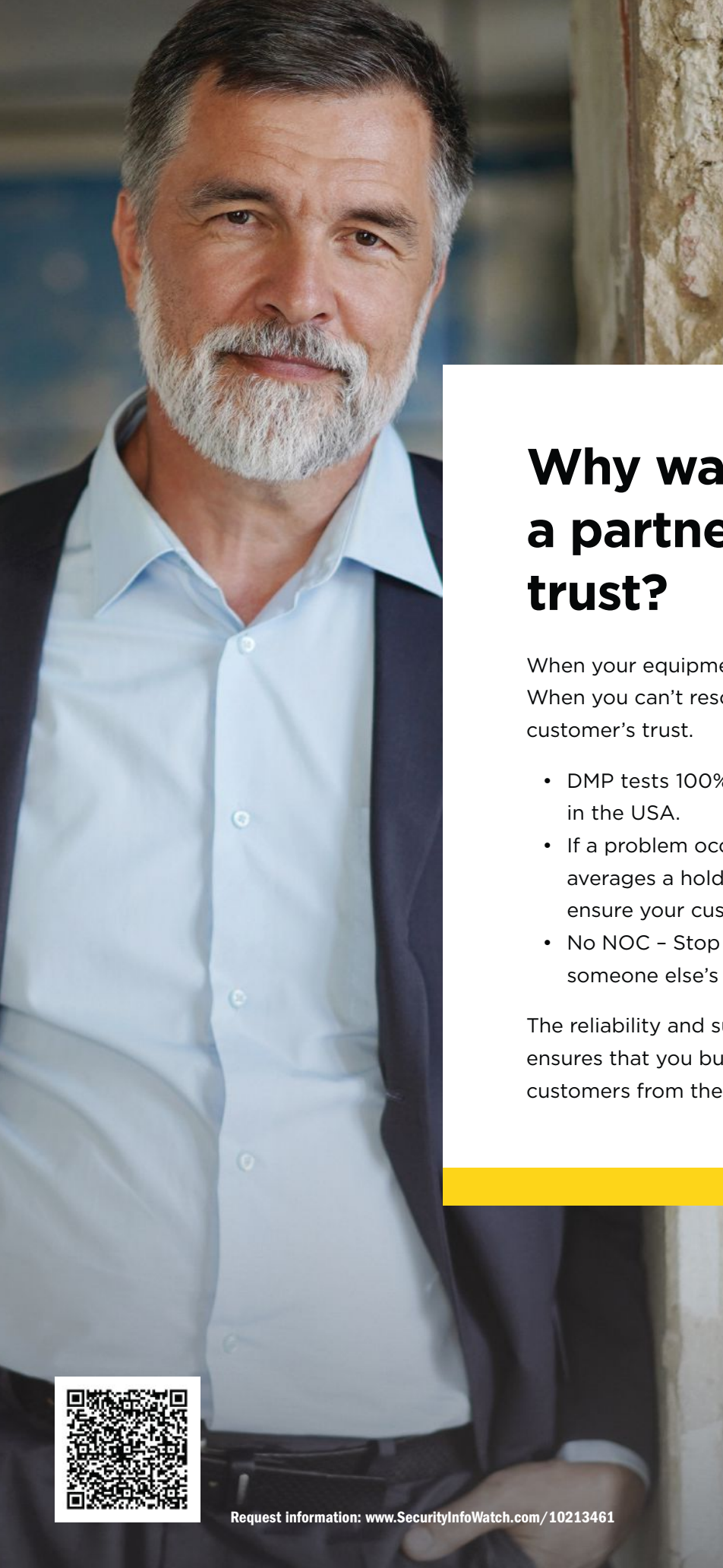
That same technology could also be applied to gun detection instead of license plate recognition, enabling security systems to identify



**Because many modern cameras come equipped with the deep learning capabilities needed to run advanced new analytics – along with platforms that are easy to develop code for – AI-based technologies have reached a vast array of new customers.**

ive, but it can be combined with other analytics to grant businesses new insights. A hardware store might be interested in knowing how many customers walk through its doors on a daily basis so they can better plan around the peaks and valleys of foot traffic. But chances are their own employees are also coming and going frequently – how can they avoid counting them? Is there another data set to cross reference, such as shirt color?

That might not matter from a security perspective, but today's developers have become good at understanding the relationship between discrete data sets and using them to identify and solve new problems. That same store might want to know how foot



## Why waste time on a partner you can't trust?

When your equipment doesn't work, you lose credibility. When you can't resolve an issue quickly, you lose your customer's trust.

- DMP tests 100% of your equipment, manufactured in the USA.
- If a problem occurs, DMP's technical support averages a hold time of less than two minutes to ensure your customers are up and running - FAST.
- No NOC - Stop wasting your money building someone else's NOC.

The reliability and support you receive from DMP ensures that you build a strong foundation with your customers from the start!



Request information: [www.SecurityInfoWatch.com/10213461](http://www.SecurityInfoWatch.com/10213461)



an armed assailant further from the building, granting them extra time that can potentially save lives.

Without new developers delivering analytics with greatly expanded capabilities and use cases, none of this would be possible. And without deep learning technology becoming more readily available, fewer consumers would be able to take advantage.

### Democratization of Data

It is important to avoid the hype train. Because of AI's promise, there is a tendency to assume that the technology can solve any problem, or that it will sweep through the security industry overnight and allow end-users to do whatever they want. That is not exactly the case. It will take time and incremental improvement before AI, ML, and

DL technologies reach full maturity, and both integrators and consumers should be wary of manufacturers and developers who overpromise.

That said, the democratization of AI isn't the only thing having an impact. The democratization of data is helping, too.

AI-based technology requires vast amounts of training data to improve its accuracy, and countless organizations have been gathering data for years and years, whether they are actively using it or not. A company might have 10 or 15 years of license plate data gathering dust on a server somewhere, unused. This is an invaluable resource when it comes to training modern license plate rec-

ognition analytics, and that company might be willing to share that data with partners looking to improve the accuracy of their own analytics. Even going from 85% accuracy to 95% accuracy is huge. That might not seem like a significant jump, but it can eliminate a considerable number of false alarms, which in turn can allow security teams to investigate each actual incident more thoroughly.

Thirty alarms in a day are a lot, but reducing that to 10 might enable staff to respond to each one more



Because of AI's promise, there is a tendency to **assume the technology can solve any problem**, or that it will sweep through the security industry and allow end-users to do whatever they want. That is not exactly the case.

thoroughly. AI is not a magic wand, but the incremental improvements it enables make a real difference.

Don't underestimate the importance of the democratization of data when it comes to making AI more valuable and desirable. It is neither desirable nor feasible for every company to master every AI application, which encourages companies to partner with others who have a different type of expertise.

Sharing data between them is a win for everyone, and it improves the quality of AI solutions across the board. As in the long-distance tracking example, different companies with different specialties can come together to create something better.

This helps customers see the value of AI grow over time, encouraging further adoption and, in turn, further development.

### Democratization Inspires Innovation

Because many modern cameras come equipped with the deep learning capabilities needed to run advanced new analytics – along with platforms that are easy to develop code for – AI-based technologies have reached a vast array of new customers.

As the applications for surveillance devices expand beyond traditional security capabilities and into business intelligence and operations, interest in the technology has expanded both on the developer side and the consumer side, creating a feedback loop of

positive reinforcement: as developers create exciting new applications, customers become more interested, and as customer become more interested, developers are spurred to further innovation.

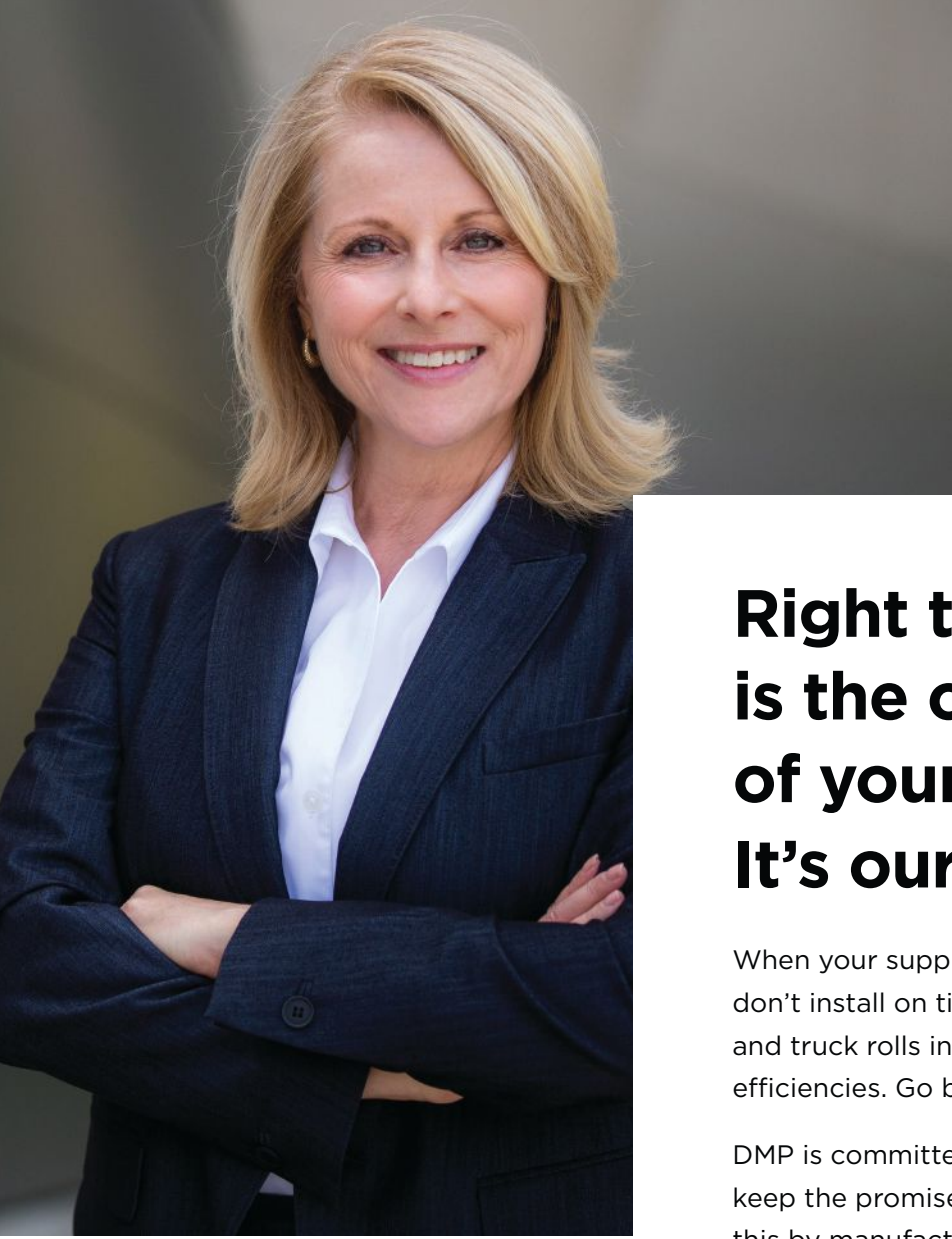
As AI becomes further democratized, expect to see that innovation continue – or even accelerate. ■



» **Fredrik Nilsson** is VP of the Americas for Axis Communications, and is the author of "Intelligent Network Video: Understanding

Modern Video Surveillance Systems" published by CRC Press and now in its second edition.

Request more info about Axis at [www.securityinfowatch.com/10212966](http://www.securityinfowatch.com/10212966).



## Right the first time is the cornerstone of your business. It's ours as well.

When your supplier doesn't have equipment — jobs don't install on time, customers become frustrated and truck rolls increase — your business loses its efficiencies. Go backs kill profits.

DMP is committed to our customers so that you can keep the promises made to your customers. We do this by manufacturing our panels in the USA.

Having equipment when you need it enables you to keep your promises to customers, maintain your reputation and continue being profitable.



Request information: [www.SecurityInfoWatch.com/10213461](http://www.SecurityInfoWatch.com/10213461)





Today's optical turnstiles can be integrated with a variety of technologies, including biometric facial recognition.

Additionally, modern optical turnstiles offer a higher level of security violation detection and faster throughput than their predecessors. Added intelligence and superior optical technology now allows for better detection, including identifying the difference between tailgaters and roller bags or luggage.

# The Evolution of Optical Turnstiles

An evolved new look also comes with increased functionality, technology integrations, and much more

**F**rom its humble beginnings as an access control and people counting device, the turnstile has undergone a multitude of technological evolutions, where today's aesthetically pleasing optical turnstiles – while similar in function – have almost no resemblance to their three-armed predecessors. An evolved new look also comes with an evolution of functionality, technology integrations, and much more. In this exclusive Industry Influencer Q&A sponsored by dormakaba, Nick Simon, National Security Sales Manager for Alvarado, takes a closer look.

## How have optical turnstile technologies evolved in recent years?

**Simon:** There has been an increase in the integration with what was, at one time, emerging technologies. Facial recognition, biometric devices, elevator dispatch screens, dual-use readers and QR readers are all commonplace now, where they were the exception many years ago. The migration to non-traditional means of accessing the turnstile lanes is exciting and provides manufacturers with an in-house software and development team the ability to ensure all devices are properly integrated for the best client experience.

## What are the ideal use-cases for optical turnstiles?

Ideal use-cases have not varied much over time. Facilities and clients that need resolution to the challenge of knowing who, when and where the people are in the building is still a very real security concern, and optical turnstiles help resolve those issues immediately. Reporting tailgating attempts and restricting access to authorized personnel is critical to our clients and the primary reason why systems are implemented.

As turnstile manufacturers have streamlined their designs, optical turnstiles are no longer seen as a burden to the aesthetics of the facility. Building owners, architects, and end-users are very cognizant of the corporate culture that they are looking to convey. They want security, while also having an open and inviting work environment. Optical turnstiles are thoughtful in their design, and can be provided in custom finishes, panel etching, ambient lighting, etc., to match the required security needs with the facilities desire for equipment that blends into their environment.

As optical turnstiles have matured in the security market-



place, there are increased opportunities for retrofitting or replacing equipment that is 15-plus-years old. Baseplates and risers allow for turnstile lanes to sit on top of existing turnstile conduit openings, allowing for an easy path to update the lobby without having to invest in what can be expensive or impossible core drilling of the floor.

### What makes optical turnstiles more effective than alternative technologies?

The effectiveness will vary depending on what alternative technology the turnstile is being compared to. Normally, optical turnstiles (with physical barriers) are used in place of either traditional doors, attendants surveying/securing the area, or card readers. All those technologies rely heavily on the honor system and may not be capable of limiting access to single users.

While a reader and lock require a valid credential to unlock the door, it cannot control how long the door is open or how many people enter. Unauthorized individuals can follow authorized personnel through the secured door, resulting in a common security issue referred to as "tailgating." Additionally, a door cannot isolate the direction of an authorized passage. If a door is activated for exit, it will not prevent entering at the same time while open.

Optical turnstile lanes will only unlock upon presentation of a valid credential, and the unit tracks the user as they pass through the lane. The device will trigger an alarm for tailgating attempts, unauthorized passage, or forced entry, making them a more effective means of secured entry.

The functionality noted above also allows for additional monitoring that is not possible with the alternative solutions. Optical



“As turnstile manufacturers have streamlined their designs, optical turnstiles are no longer seen as a burden to the aesthetics of the facility.”

– Nick Simon, Alvarado

turnstiles have numerous outputs that fully integrate with the facilities access control system. That means that clients are instantly notified upon unauthorized passage attempts, forced entry, door held open, authorized passage, and many others. Monitoring these outputs provides not only a log of activity, but also enables users to create procedures for security staff to respond to the alarms to ensure that the facility is fully secure.

The outputs can also be integrated with third party systems such as cameras to time stamp specific activity at the turnstile lane. This is invaluable information for clients and helps make their facility more secure and responsive.

### What technologies can be effectively integrated with optical turnstiles?

There are not many limits to what can effectively be integrated. The security industry moves fast, and new products, upgrades and improvements are always on the horizon. As noted above, we have seen increased use of facial recognition, biometrics, Bluetooth-enabled, QR codes, detection systems (metal detectors, for example) and many more. Most commonly, optical turnstiles will integrate with the facilities access control system and life safety system. Clients do not need to

invest in a new access control system or life safety system to create a safe and secure environment.

### How much time and technical know-how does a technician need to complete the install process?

Install times vary; however, Alvarado recommends having experience with these solutions before completing an installation and "turning the keys over" to the end-user. Our documentation is very concise, and we have experts at Alvarado that are a constant resource for our partners.

Remote and on-site training and commissioning is available. Additionally, Alvarado has partners throughout the world that are certified and have been trained on how to install and service our equipment – some of which stock parts. Our partners are valuable to our success, and we can offer recommendations to meet installation needs to ensure that the installation process is smooth.

### How can optical turnstiles provide integrators with an RMR stream?

The RMR for optical turnstiles would be in the form of providing service contracts for preventative maintenance.

**To learn more about Alvarado optical turnstiles from dormakaba, visit [www.alvaradomfg.com/product-c/optical-turnstiles](http://www.alvaradomfg.com/product-c/optical-turnstiles).**



Photo: World Equestrian Center

# Security Takes the Reins at WEC

**2022 Security Vanguard Award Project of the Year:** A robust video surveillance system integrates with advanced door and access solutions to protect the World Equestrian Center

By Steve Lasky, Paul Rothman

**T**he premise for any successful security systems buildout is that it is flexible and designed with future expansion in mind. While these were certainly factors that were prime drivers for operators of the World Equestrian Center (WEC) in Ocala, Fla., even the on-site security management team and the systems integration group that oversaw this expansive project could not have anticipated the whirlwind of complexity the job would entail.

Because of the strong collaboration between user and integrator within such a high-stress and diverse project, it has been named the 2022 Security

Vanguard Award Project of the Year by *Security Business*, *SecurityInfoWatch* and *Security Technology Executive* (STE) magazine.

“Because of the sheer size of the project and the number of cameras and access control points, it takes a lot of people working together to come up with a cohesive project at the end, even though it is being done piecemeal and in phases,” explains Brian Remington, the account executive for Fla.-based integrator SmartWatch Security and Sound, who has overseen the project from its beginning.

The WEC is a one-of-a-kind equestrian center designed for world-class breeders and competitors. It is a

veritable maze of venues that features not only areas reserved for the world’s top equine competitors – showcasing climate-controlled stables for 2,000-plus horses, five arenas and a large veterinary clinic – the resort-like property also includes an RV park, an expo center and a first-class hotel on nearly 380 acres of sprawling horse country, with an additional 300 acres set aside for future expansion.

From its inception, security management staff and developers agreed that a facility destined to house the world’s most majestic and valuable livestock also needed a security system with a blue-ribbon pedigree.

◀ The WEC is the largest equestrian center in the United States, featuring a maze of venues including five equestrian arenas, climate-controlled stables, veterinary clinic, resort hotel, RV park, expo center and more.

### Collaboration was Key

The job of securing this sprawling first-in-show property nestled among the gently rolling hills of central Florida fell to Security Director Kevin O'Rourke, who in 2017 hand-selected integrator SmartWatch Security & Sound – which was actually acquired by Sciens Building Solutions mid-project – for the job.

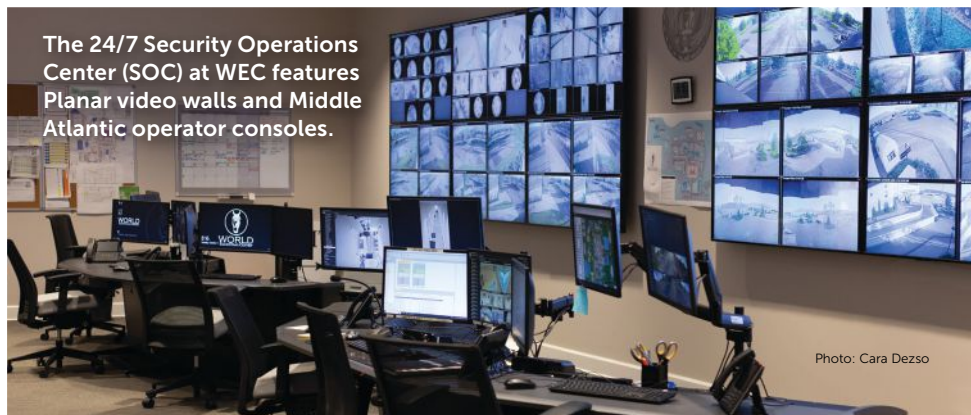
The WEC project has morphed beyond the original blueprints as new venues on the property have come online and others have been retrofitted. This quirk has required a constant balancing act between end-user and systems integrator, as the footprint has grown to more than 900 cameras and 145 doors of integrated access control.

O'Rourke, who has a law enforcement background, realized early on that SmartWatch brought invaluable experience to the project from years of close working relationships with Orlando's Universal Studios and other large outdoor entertainment venues.

"At the end of the day, you've literally got people whose livelihoods depend on us," O'Rourke explains. "A good portion of them have horses that, quite frankly, could be more expensive than [most] people's houses. When you look at it strictly from a liability standpoint, being able to make accurate determinations – not just a guess as to what [event] may have transpired – was a crucial element of this security [framework]."

The dilemma O'Rourke faced was that although everything management wanted to do from a security perspective was realistic, the project continued to expand over myriad months, forcing numerous change orders.

"This particular layout is not where we initially started – it was not nearly at this scale," O'Rourke says. "Once we



## Project Overview: World Equestrian Center

- **Project submitted by:** Sciens Building Solutions
- **End-User:** World Equestrian Center (WEC), Ocala, Fla.
- **Integrator:** SmartWatch Security & Sound (a Division of Sciens Building Solutions)
- **Access Control Management System:** Gallagher
- **Electrified Door Hardware:** Von Duprin (ASSA ABLOY)
- **IP Cameras:** Axis Communications
- **Video Management Software (VMS):** Milestone Systems
- **Data Servers:** Seneca Data
- **Video Walls:** Planar
- **SOC Consoles:** Middle Atlantic Products

were into it, we had to continue to follow that path for the entire campus. Once we recognized that, we looked at the layouts of the barns, for example, and we came up with a game plan for minimizing the number of cameras and hardware required – but at the same time covering an area that would have required four different cameras."

### Video Surveillance is the Foundation

Video surveillance and storage has played a significant role in the WEC security footprint, especially around the barns, horse stalls, staging areas at the equine arenas, and parking areas. Remington emphasizes that because of

liability issues to horse, rider and owners, video systems had to be ubiquitous.

"The number-one concern was injury to the livestock," Remington explains. "Usually, we think of slip-and-falls in a mall where someone falls and bangs their head, and they file a big lawsuit. If somebody pulls a million-dollar horse out of a barn and it stumbles because the floor is wet, and the horse can no longer perform or get stud fees – the implications are enormous."

Looking to alleviate liability issues around the barns while also creating a streamlined security operation for staff in the 24/7 Security Operations Center (SOC) mandated that strategic camera placement, adequate storage

and an intuitive VMS were essential. Remington's integration team installed more than 30 IP video cameras from Axis Communications in each of the 26 barns, with each being placed at a key intersection point for full coverage using minimal devices.

"You have to see as much as possible, so I focused on coverage," O'Rourke explains. "That's the mindset we tried to follow, understanding that efficiency [was also important]. We were able to do that with technology [such as] 360-degree fisheye cameras that can [cover an area] where you would [ordinarily] need three fixed cameras."

O'Rourke says the sprawling WEC campus currently uses around 940 cameras with nearly 1,680 corresponding video streams flowing into the SOC. This requires a vast amount of connectivity and storage, which Remington says is handled by an array of data servers from Seneca.

"There are 19 servers overall, at 124 terabytes [of storage] each," Remington says, adding that they are arrayed both in a main server farm and at the edge. "The network is so robust, you

can literally hang a server anywhere and it will perform, so we didn't have to worry about bandwidth."

"We try to keep our archive at a usable number, which has worked pretty well, because economically speaking, you can't store [video] forever," O'Rourke adds. "Typically, for an event or an issue that we are reviewing, we are usually aware of it within hours, days or at most, a week – and we have the capability to go back and do a productive review."

While many of the cameras are covering the stables and other equine

areas, the RV park, show venues and hotel also require a great deal of video technology. Remington admits that he and O'Rourke decided early in the project that it would be impossible to economically issue individual event badges or task a manned guard force with crowd control on such a massive scale.

"It is definitely what we would consider a hospitality project, because there is a resort on property, but it is also very unique in that it's an entertainment complex with the show arenas," Remington says. "The back-of-house stables were the original concern



“ [WEC management] operates a number of large corporations, so at the end of the day, **they understand security and the need for it** from a business standpoint.”

— Kevin O'Rourke, WEC Director of Security

## M&A Catastrophe Avoided

### How SmartWatch Security & Sound kept an award-winning project on track despite being acquired at the halfway mark

Putting together an ever-growing but award-winning security project is never easy for an integration firm – now try doing it in the midst of being acquired by another integrator. Such was the case for Brian Remington and SmartWatch Security & Sound, which was acquired by Sciens Building Solutions in 2019 – at roughly the halfway mark of the World Equestrian Center (WEC) project.

"It probably went as well as any acquisition of a small company by a large organization – I have never been a part of it before, so it was a new experience for me," Remington says. "I would say that the Sciens takeover really had no impact on the overall growth, or modifications to the WEC project. They were very

hands-off and understanding of our relationships with our existing customers, and they continue to be so. Obviously [Sciens] has its own policies and procedures, and we are working those into our system. That has affected some of our business, but not in a negative way – it just changes how we do things."

Still, one of the first orders of business in this situation is communication. Remington says he had sit-down meetings with all his major customers to communicate the transition.

"We had principals from Sciens come out and attend large meetings wherever it was appropriate," he explains. "But to be honest, if you are the general contractor or the electrical contractor [on a project], they just want to know that I'm going to pick up the phone when they call, and that my project manager is going to be the same guy they've been dealing with for years, and when we get on-site, the parts get delivered when they are supposed to."

# BATTLE-TESTED SECURITY



When it comes to security and communication, strength matters. At Viking Electronics, we combine the industry-leading innovation of today with the tough-as-nails durability of the past.

Whether your system calls for analog or VoIP, multiple access points, or color video...

**YOU NEED A VIKING.**

 **DESIGNED  
MANUFACTURED  
& SUPPORTED**

## **VIKING**

**715.386.8861**  
vikingelectronics.com

Request information: [www.SecurityInfoWatch.com/10556843](http://www.SecurityInfoWatch.com/10556843)



for the owners of the property, but it turns out that theft, operations – all those typical worries that anybody in a hotel or resort or theme park would have – also became items of interest for the security staff.”

Remington adds that the sheer size of the property means often covering multiple events at once. “It is so big that you could literally have 30 different events going on throughout the weekend,” he says. “At one arena, you’ve got a car show; in another arena, you have a craft fair. It would be too problematic to try to control access in and out of the property, so the decision was made to just blanket the area with [surveillance] coverage.”

Facilitating an ability to integrate open technology with an eye towards economy of scale led WEC to choose solutions from companies like Axis, Seneca and Milestone Systems (VMS), as well as Gallagher for the access control systems and Von Duprin for the electronic door hardware.

### Inside the Security Operations Center

Within the 2,000-square-foot SOC, operators at custom consoles provided by Middle Atlantic can monitor two Planar video walls as well as desktop monitors for up-close viewing.

The SOC is staffed 24/7 and serves as the WEC security dispatch center as well the video monitoring hub. A two-way radio system enables O’Rourke and his security team to reach out to any officer at any moment, anywhere on the property. O’Rourke adds that the SOC had to be large enough so his team could not only monitor ongoing events – which he admits is almost



Photo: Cara Dezzo

World Equestrian Center Director of Security Kevin O’Rourke (center), is flanked by Brian Remington (left) of SmartWatch Security & Sound, and Vinnie Card (right), WEC’s Director of Operations.

impossible to do in real-time given the scale of the video surveillance system – but also accommodate security staff that were reviewing older video and those performing forensics.

“We view all the main hot spots or intersecting areas, and that basically takes up three workstations and one video wall,” O’Rourke says. “We then have a second video wall with three workstations assigned to that video wall, so when we have a specific event – a home and garden show going on in expo one, for example – it allows us to simultaneously concentrate on that. We’re not giving up our normal operations and strictly focusing on one event because we have [the capability to monitor] multiple things going on the property at once.”

### Lessons Learned

The key to success on a project of this scale, according to both O’Rourke and Remington, was a top-down understanding of what would be involved, and then making the commitment to

achieving it on the WEC campus.

“[WEC management] operates a number of large corporations, so at the end of the day, they understand security and the need for it from a business standpoint,” O’Rourke says. “There was going to be some investment required, but then the project kept expanding.”

In fact, Remington chuckles when thinking back to the number of times “the project kept expanding” – after all, what started at a 30-building project morphed into 330 acres of facilities. Still, he stresses that having a solid working relationship with a customer and serving as a trusted advisor is the key to success.

“Know your customer, and listen to what they have to say,” Remington says. “That’s what I have learned most from dealing with Kevin, because he is a smart guy, and he always has a lot of great points to offer. But in the end, he always relied on our knowledge and expertise to make the decision on which products to go with and whether they were appropriate or not.” ■



**The Security Vanguard Award** is an industry accolade given by *Security Business*, *Security Technology Executive* and *SecurityInfoWatch.com* – with support from the Security Industry Association (SIA) – that recognizes the most impressive integrated technology and solutions projects of the previous year. Read more about the award and the 2022 Honorable Mention projects at [www.securityinfowatch.com/vanguard](http://www.securityinfowatch.com/vanguard).

# Securitron®

SECURITRON  
ASSA ABLOY

*The premier supplier of  
electromagnetic locking solutions.*

When you choose a genuine Securitron Magnalock®, you get quality solutions for high traffic and high security applications plus MagnaCare® Lifetime Replacement No-fault Warranty.

Experience a safer  
and more open world



## Intelligent & Sustainable Magnalocks

- Available with PIR REX, BondSTAT® and DPS reducing the number of devices to buy and install at the door.
- Sleek and low profile for aesthetically demanding applications.
- Patent-pending template and bracket mounting system enable accurate alignment of magnet and armature plate for maximum holding force.
- Reduces energy consumption by up to 80%.

## Durable Magnalocks

- Lower power usage than competitor locks. Securitron Magnalocks consume less energy, generate less heat and outlast the competition.
- Water resistant design, shock absorbing polyurethane, stainless steel casing and plated lock face, for outdoor applications.
- Instant release circuit with no residual magnetism and no inductive kickback.

## Delayed Egress Magnalocks

- For applications meant to prevent peril or property loss to persons and businesses.
- Highly configurable, strong, easy-to-mount.
- DEM680E standard model is HUGS-compliant with specific code compliant models available.



Visit [Securitron.com](http://Securitron.com) for complete product details  
and available installation and support tools.

Request information: [www.SecurityInfoWatch.com/10214963](http://www.SecurityInfoWatch.com/10214963)



MagnaCare  
Warranty



HONORABLE MENTION

# Massive Upgrade in Harris County, Texas

Multi-year retrofit project involved security technology upgrades in more than 150 buildings in the downtown Houston area **By John Dobberstein**

**W**ith more than 150 buildings, hundreds of video cameras and access control points to monitor, and lots of unknowns to factor in, security operations for Harris County in the Houston Metro area – the most populous county in Texas and the third most populous county in the United States – must perform well every day.

But after years of building an enterprise security system in a piecemeal fashion, the county was left with clunky, inefficient and outdated technology to track more than 17,000 employees and support more than 4 million residents with services ranging from public safety and jails to libraries and licensing facilities.

Harris County, along with Texas-based integration partner ESI Fire & Security Protection and primary vendor Honeywell, embarked on a multi-year journey to streamline and modernize the county's vast security needs, culminating in the project's completion in June 2021. The enterprise project has been named as an **honorable mention in the 2022 Security Vanguard Awards** from *Security Business*, *SecurityInfoWatch* and *Security Technology Executive* (STE) magazine.

## The Backbone

Each of the 150-plus buildings that fall under Harris County jurisdiction previously used different security products that did not communicate to one another, creating an overly complicated network and increasing work for employees, as well as driving down efficiency.

County administrators decided to contract with Honeywell and ESI Fire & Security Protection to identify the county's needs and streamline technology platforms.

ESI, which became the county's primary security contractor in 2014, recommended an integrated system from Honeywell and other security manufacturers that would tie together the disparate security systems, facilitate better business decisions, and enable Harris County security and other officials to streamline operations.

At the time, there was little or no standardization, with four different access systems, at least four different video management systems and two different intrusion detection and alarm systems. And it cost taxpayers a lot of money to have multiple employees manage all the different systems.

The primary goal was to replace those various access control and security components and consolidate them into



## Project Overview: Harris County Overhaul

- **Project submitted by:** Honeywell Building Technologies
- **End-User:** Harris County, Texas
- **Integrator:** ESI Fire & Security Protection

### Security Products

- **Security Management System:** Honeywell Pro-Watch Intelligent Command
- **IP Cameras, NVRs and VMS:** Honeywell MAXPRO
- **Intrusion Panels:** Honeywell 120 and 250
- **Visitor Management Platform:** IDEMIA
- **Thermal cameras:** Silent Sentinel
- **Intercoms:** Commend USA
- **Optical Turnstiles:** Smarter Security
- **Smart Cards and Readers:** HID Global
- **Mobile Surveillance Trailers:** ESI Fire & Security

a single system. The county opted to go with Honeywell's Pro-Watch Intelligent Command security management system as its backbone, uniting video surveillance, alarm events, access and safety "under one pane of glass," says Bruce Montgomery, strategic account manager for Honeywell.

"We couldn't start from day one with a full integration, but we took it one step at a time, and it was well thought out," explains James Humbert, ESI's president and business development manager. "We knew they couldn't change everything overnight, but we needed them to see what they have and what it could be. Once we showed them [the benefits of] one uniform platform, it made it so much easier for them to move forward and change it out building-by-building."

Harris County's Security Operations Center enables security personnel to monitor incidents "without having to jump through a lot of hoops to figure out what's going on," explains Nemiah McGee, senior manager of security technology for Harris County.

The county's Security Technology Services division feeds all IP cameras, access control, body-worn cameras, intrusion detection systems and fire monitoring into its SOC, which includes a 24/7 emergency response call center.

The upgrade project launched its first phase in early 2017. In addition to upgrading the access control on doors in all buildings, ESI installed the Pro-Watch

# Solutions to Enhance Your Business



- **Video Analytics**
- **Reduce False Alarms**
- **Priority Response**

# QUICK RESPONSE



Your trusted partner

800-462-5353

info@quickresponse.net  
quickresponse.net



Request information: [www.SecurityInfoWatch.com/10746329](http://www.SecurityInfoWatch.com/10746329)



## HONORABLE MENTION

backbone, Honeywell MAXPRO cameras and NVRs, Silent Sentinel thermal cameras, as well as third-party access control components such as Inxium access control terminals, optical turnstiles from Smarter Security and intercoms from Commend.

The technology, of course, is all designed to help Harris County accomplish its goals:

- Save taxpayer dollars through better analytics that reduce false alarms and help first responders.
  - Monitoring from a single central control station for improved situational awareness.
  - Creating healthier building environments by leveraging people-counting technologies and analytics to manage health and safety compliance, such as social distancing.
  - Streamlined systems to create operational efficiencies and save the county resources that can be redirected to other infrastructure or services.
- “Everyone understands that we were all working together on this, and that we all have the same goals,” Humbert says, underscoring the synergy between Harris County officials, Honeywell and his company.

### Surveillance Systems

The first phases of the project involved replacing all access control and video camera systems in the county, which took nearly four years. There were built-in challenges for this phase, as the central station – which is staffed 24/7 – had to monitor multiple, disparate systems while ESI and Honeywell were building and configuring the new system.

There was also some pushback from security and monitoring team members who were accustomed to the legacy systems, but that is not to be unexpected with major changeovers, McGee says, adding that he explained how much faster they would be able to respond to incidents with a more



The ESI Fire & Security Protection team includes: Robby Burleson, Head of MST Division; John Copeland – Head of Security Operation; Lorenzo Cuellar – Head of Fire Division; and James Humber – Head of the Harris County Account. Not pictured is Matt Betancourt – Harris County Project Manager.

adequate alerting system that includes screen pop-ups, lights, sounds and visual messages that inform them what’s happening and when.

“That makes it easier on the operators and they can give the proper location to law enforcement or any responding agency when an event happens,” McGee says.

County officials say the incorporation of analytics in the central station has increased intelligence provided by the integrated equipment, dramatically reducing false alarm events. Video analytics also provides a clear image from a specific camera that corresponds with movement causing the alarm – enabling central station operators to see what’s happening and determine instantly whether an alarm is caused by an intruder or, perhaps, just an animal.

### Access Control and Visitor Management

In most buildings, the county uses Smarter Security optical turnstiles integrated with either HID smart readers or the Idemia visitor management system to create a frictionless access and visitor management procedure that enables employees

and visitors to enter the buildings. In some cases, the system can recognize employees and frequent visitors, such as judges and lawyers, using data stored in the ProWatch system without the need to physically scan a badge or remove facial coverings.

McGee says that the county uses Honeywell analytics capabilities in concert with the visitor management system, enabling the SOC to search for someone in one of the many buildings based on attributes such as height, color, hairstyle, the clothes they were wearing and cross-reference that with entry and exit data from the visitor management system.

McGee recalled an incident where someone got into a facility with a weapon. The suspect was eventually caught, but during the incident post-mortem, security officers wanted to know how and when the suspect got into the building with a weapon in the first place.

“[It was] a building with tens of thousands of people moving through it in and out in the morning time-frame, so it was like trying to find a needle in a haystack,” McGee says. “We were able to narrow the time-frame where they believed the per-

# Perfect Match

Black maglocks for black door frames



UL294, UL864, UL1034, and UL10C Listed



**SECO-LARM  
maglocks**  
are now  
available in  
**black**



600-lb Maglock



600-lb Double-door Maglock



1,200-lb Maglock



1,200-lb Double-door Maglock

**SECO-LARM® U.S.A., Inc.**

16842 Millikan Avenue, Irvine, CA 92606

**Tel:** (800) 662-0800 **Email:** sales@seco-larm.com

**Fax:** (949) 261-7326 **Website:** www.seco-larm.com

Request information: [www.SecurityInfoWatch.com/10214926](http://www.SecurityInfoWatch.com/10214926)



Copyright © 2022 SECO-LARM U.S.A., Inc. All rights reserved.  
All trademarks are the property of SECO-LARM U.S.A., Inc. or their respective owners.  
The SECO-LARM policy is one of continual development. For that reason, SECO-LARM reserves the right to  
change prices and specifications without notice. SECO-LARM is not responsible for misprints.

**SECO-LARM® ENFORCER® CRIMEBUSTER® CBA® SLI®**



## HONORABLE MENTION

son came in, [the officers] gave us a description of the person's clothing, and we ran that through the analytics software and the visitor management system. It came back with the exact timestamp of the individual and when they got in and how, within two to three hours."

Another advantage to the Honeywell access control is that users can be easily created or deleted in the system, and automatically be deleted under certain parameters – such as an employee who is no longer with the county but still had a user profile in the system, McGee explains.

Security personnel can also lock down a building according to specific groups of users, or an entire building can be locked down in a matter of minutes.

### Upgrades and Maintenance

The shift to the unified security management system is complete, although Harris County is constantly upgrading and performing maintenance, as the system continues to grow from 10 to 15 percent every year. In addition to phased projects that are part of the main upgrade, pop-up projects continue – for example, the county bought another building last year and awarded a \$2.5 million contract to ESI to upgrade the turnstiles and intercom systems in the building and install speed gates in the garages.

There are monthly firmware updates as well, primarily focused on the 300-plus NVRs in use. McGee says the software updates are tested for up to a month in an internal lab built by the county before being pushed out ensure there are no problems.

For the ESI integration team, which includes Harris County Project Manager Matt Betancourt, as well as Humbert, Robby Burleson (head of ESI's mobile surveillance tower division), John Copeland (head of ESI's security operation, and Lorenzo Cuellar (head



**Harris County's Security Technology Services division feeds all IP cameras, access control, body-worn cameras, intrusion detection systems and fire monitoring into its SOC, which includes a 24/7 emergency response call center.**

of ESI's fire division), the lessons learned on this project are many; however, ironically, one of the biggest was creating a human "single pane of glass" with the County – more specifically, having a single point of contact for all things project-related.

"When we started, there were so many different departments and divisions and they were all coming to us for upgrades," Humbert explains. "It was a big challenge, but we overcame that by building a relationship with a main source at the county, Anthony Bean [the Enterprise Program Manager for Public Safety Technology Services with Harris County Central Technology Services]. It was 'one pane of glass' from a personal contact point of view, and it makes our process a lot easier."

Humbert explains that Bean has outlined a standard configuration for each of the buildings, which has made a uniform deployment much smoother. "The standard tells us exactly what they are looking for in every building, and the first step is to always make sure the standard is covered."

Humbert adds that over the course of a 7-year ongoing project, if the

integrator wants to keep that contract, you can never take it easy.

"You have to bring your A game every single day," Humbert says. "When you have a customer for 5 or 10 years, some guys get too comfortable – they think, 'I've had this for so long, so I can slow it down a bit.' There's none of that [with Harris County]. We are going at the same pace on day one as we are right now. That's how we set ourselves apart from the competition. It takes that same mentality every day. There's no time or day to bring the B game."

Humbert adds that constantly being available helps to establish the integration team as a long-term and trusted partner. "You can actually become the customer's go-to security person – not just the company that sells and installs something, but somebody they actually trust when there's an issue," he says. "If you can build that kind of relationship – that trust with a customer – then you are more than just their salesperson; you are more than just their integrator; you've simply become part of their team." ■

» John Dobberstein is managing editor of SecurityInfoWatch.com.

# Your Fire/Security/ Integration/Wholesale Monitoring Company is WORTH MORE THAN YOU THINK!

*We have qualified buyers  
ready to purchase your  
Security, Fire, Integration  
business and/or accounts.*

- FIRE ALARM/SECURITY
- INTEGRATION/CCTV
- WHOLESALE MONITORING
- BUSINESS OR ACCOUNTS



**CALL RORY'S CELL  
AT 1-800-354-3863**

Talk to Rory Russell to get the most recent and complete Business Valuation for your company and see for yourself how much your business is currently worth.

Request information: [www.SecurityInfoWatch.com/10744814](http://www.SecurityInfoWatch.com/10744814)

**Don't Wait! We Are Closing Deals Now! (over \$100 million):**

Ponoma, NY	\$575,000
Detroit, MI	\$600,000
Los Angeles, CA	\$810,000
Mt. Vernon, NY	\$1 Million
Boston, MA	\$1 Million
Northern GA	\$1.3 Million
Jackson Hole, WY	\$1.8 Million
Clifton, NJ	\$1.8 Million
Fort Pierce, FL	\$2.8 Million
Orlando, FL	\$11 Million

<b>MOST RECENT CLOSINGS 2021:</b>	
Lafayette, LA	\$8 Million
Houston, TX	\$1.5 Million
Edison, NJ	\$10 Million
Providence, RI	\$2.5 Million
Memphis, TN	\$4.2 Million
Tampa, FL	\$6.8 Million
Los Angeles, CA	\$10.4 Million
Philadelphia, PA	\$12 Million
Fort Myers, FL	\$21.5 Million

**A F S**  
ACQUISITION &  
FUNDING SERVICES

**CALL  
RORY RUSSELL  
FOR A COMPLETE  
BUSINESS VALUATION  
1-800-354-3863**



HONORABLE MENTION



Photo: Anime Expo

# Keeping 350K Anime Expo Attendees Safe

A unique combination of screening technologies, video surveillance and human/canine patrols made impossibly long lines a thing of the past at the annual event **By John Dobberstein**

**T**he Anime Expo (AX), an annual celebration of all things “Anime,” is one of the largest conventions of its type in North America; in fact, the size and popularity of AX has grown exponentially since its humble beginnings in 1991, from about 10,000 people to more than 350,000.

For years, AX – formally known as Anime Con – earned the unfortunate nickname of “line-con” due to massive crowds that formed just to gain entrance, which meant headaches for security and operations staff.

Thanks to a unique combination of weapons screening technology, guard and canine services, and temporary security technology – all coordinated by security firm Sentinel Consulting – AX 2022 was a rousing success. The

project has been named has been named as an **honorable mention in the 2022 Security Vanguard Awards** from *Security Business*, *SecurityInfoWatch* and *Security Technology Executive (STE)* magazine.

## **The Crowd Control Challenge**

Based on turnstile counts at entrances, more than 350,000 people attended Anime Expo during three days at multiple venues, including the Los Angeles Convention Center, Novo (an indoor club), and the Microsoft Theater.

Efficient screening was the first challenge for Michael Grossman, a senior advisor at New York City-based Sentinel Consulting, who was responsible for all security planning and operations, including the preparation of a comprehensive operations plan

and the management of the overall on-site security operations.

A massive crowd is one thing, but the vast majority of these attendees came to the AX venues in full costumes – many that included imitation weapons. The Society for the Promotion of Japanese Animation (SPJA), the event organizer, also required COVID-19 checkpoints.

“We were getting people into the buildings, but the crowding on the outside [creates] a soft target,” explains Matthew Thomas, SPJA’s senior director of operations.

Thankfully, Grossman and the Sentinel team came up with a multi-faceted solution, combining high-throughput weapons screening technology with good, old-fashioned security officers – provided by Ayvar Security, JRM Security and Executive

Event Services – and canine teams from MSA Security Services, a division of Allied Universal. Additionally, RFID badging implemented at the show helped with counting attendees and protected against people getting in without the proper credentials.

“It is not all high-tech, but when you use all those things to your advantage and integrate their use, that makes a system more efficient and there are a lot fewer problems,” Grossman says.

As for the technology aspect of the crowd control technology, Thomas and Grossman zeroed in on the Evolv Express, a high-throughput walk-through weapons screening system that uses digital sensors and artificial intelligence to spot concealed weapons and other threats.

Evolv claims a single unit can screen 4,000 people per hour, and that the technology has been successfully used at stadiums, theme parks, hospitals, schools and other busy venues. Ideally, the technology is accurate enough that people are not required to stop, empty their pockets or remove bags as they are screened.

2022 was the first year that AX used the screening technology, and Thomas – who held previous security operations roles at Universal Studios and Westfield malls – says it enhanced the throughput of patrons from 55 people per hour to 300 people per hour at each entry point.

“Honestly, I think it was a little *too* quick, and we slowed that down on site just to be very thorough,” Thomas admits. “That was due to my thinking that it was impossible. I am used to the metal detector going off on every belt buckle.”

### **Achieving Situational Awareness**

Grossman – who retired from the Los Angeles County Sheriff’s Department in 2013 as chief of the Homeland

## **Project Overview: Anime Expo**

- **Project submitted by:** Sentinel Consulting
- **Weapons Screening:** Evolv Technology
- **Temporary Surveillance System:** Unified Command
- **Video Management System:** Milestone
- **Guard Services:** Ayvar Security, JRM Security and Executive Event Services
- **Canine Services:** MSA Security Services

Security Division and later served as SVP of U.S. National Security for Westfield Corp., where he oversaw security operations for 32 malls across the nation – assembled a security command center at AX that coordinated the activities of all security and life safety agencies, including convention center security, private contractors, the Los Angeles Police Department, and many others.

Through the assistance of Las Vegas-based Unified Command, a temporary surveillance system was also deployed, with cameras placed at strategic locations to maintain situational awareness at key points throughout the venue. The temporary system focused on areas outside the venues, since the buildings had their own cameras.

“We were working with the existing Convention Center security with their technology and adding on our technology to complement,” Thomas says. “That really helps us get good angles to manage crowds and respond to certain things from the [security monitoring] perspective.”

Those working in the Unified Command post could monitor cameras, zoom in on nearly any area or focus on certain cameras. “They know exactly the things that need to be seen

and where to put cameras,” Grossman says, adding that the command post at AX was similar to one that he might set up for a large wildfire or other major event.

“You have representatives from all the agencies that do security or emergency response in the same room, and they monitor for 24 hours a day through the entire event,” he explains. “If you don’t have adequate and documented planning, a clear organizational chart, clear lines of communication, and contingency plans, [if] something comes up, it is pretty tough to manage,” Grossman says.

In reviewing the successful AX 2022 security operations, Thomas says “the secret sauce is there right now” to maintain an effective security program for AX in the future. As for similar events, he implores event security managers to take advantage of all the technology and tools available, even if the cost is hard to swallow.

“All it could take is one situation, and you no longer have an event anymore,” Thomas says. “I like spending a bunch of money on security...because [it means] we’ve done the most that we can to protect everybody.” ■

.....  
» **John Dobberstein** is managing editor of SecurityInfoWatch.com.

# How PACS Improve the Commercial Tenant and Building Experience

© CHUNWIP WONG/134528585/Getty Images

Commercial Real Estate (CRE) customers can leverage cloud-based and physical access control to modernize the buildings they own or lease **By Troy Johnston**

**S**ecurity integrators serving clients in the Commercial Real Estate (CRE) industry are seeing a recurring theme: from the car park to the office suite, and across countries and regions, there is a common need to ensure a building's people and assets are safe and secure while reducing friction at all access control touchpoints. Most importantly, CRE providers need to offer meaningful amenities

and experiences that employees and visitors value.

Building tenants are also innovating new ways to work that require integrators to help their CRE clients accommodate additional needs. Tenant employees want flexible, multi-location, and hybrid work styles that include work-from-home and in-office hot-desking. They want contact-free access to doors and elevators, and intuitive features and amenities that make their journey to

and from the office easier. And the ubiquitous mobile phone has become the command center for their lives; a single device that consolidates both work and life.

To address these needs, security professionals need to help those managing the building to deploy a modern physical access control system (PACS) that enables robust experiences, mobile adoption across systems, and future-ready, touchless access control.



## What Tenants Want

From their home to the office suite, tenants interact daily with a vast array of disparate systems as they access a consistent set of services, having to manage multiple keys, cards, fobs, passwords, and other credentials, creating friction and frustration.

“The challenge as a landlord is to provide tenants and their guests the ability to come into an owner-controlled perimeter (e.g., turnstile), interact with a destination elevator system and then get into their office space in a seamless manner, with one credential,” says James Whalen, SVP and Chief Information and Technology Officer for Boston Properties. “They don’t want to have two cards. That’s the most basic definition of a seamless experience: through space, with least friction. You think about New York, some of these buildings have thousands of employees and get up to 19,000 visitors a month. Our goal is to move that queue in a quicker way through innovation.”

In addition to these requirements, the pandemic surfaced a new social awareness of health and safety, driving tenants to seek solutions that meet the requirements of today and tomorrow. With contactless check-points and advanced visitor management capabilities including unattended self-serve check-in, they want to enhance the workplace experience and its management by:

- Reducing surface touches;
- Understanding who is accessing the facilities;
- Keeping common areas free of crowds and congestion;
- Support for appropriate social distancing measures;
- Balancing a mix of work-from-home and in-office working styles;
- Offering broad amenities and services for tenants; and
- Capturing data for better systems management and decision-making.

## How Integrators Can Help with Cloud-Based PACS

Today’s buildings range from a managed, multi-tenant property to a company-owned headquarters facility with many satellite operations worldwide. In any scenario, it can be difficult to scale access control deployments without large infrastructure investments.

Organizations can solve this problem by working with a security integrator who understands how to leverage cloud-based PACS technology as the flexible, easily scalable and future-proofed foundation of a modern building experience.

Hosted in the cloud (off-premise data center) and often procured on a subscription model, cloud-based PACS enable centralized management of cloud-connected access control devices, applications and trusted mobile identities. This, in turn, enables remote management of PACS systems in multi-tenant and multi-location environments with the high level of integration needed to deliver a seamless experience across systems.

This approach also facilitates a comprehensive tenant experience – including access to the turnstile, the elevator, the seventh floor, the ninth floor, and the data center in the basement. It links all of these entitlements as part of one digital identity.

Cloud-based PACS provide end-to-end information security, compliance, and data privacy, while also enabling data-driven decision-making.

In support of a seamless experience, it enables integrations with a range of access use cases as well as centralized control over property technology solutions.

Tight integration of these various technologies can help overcome key access control challenges and make it easier to manage through the lifecycle of an identity while offering key amenities and services.

Access control is very important, especially adopting mobile credentials. As an engagement model, mobile access defines active users and grounds them in daily interactions that help with all the other interactions, whether they are amenities and services, food and beverage, events, or building communications. It creates the fabric of the daily engagement model at home or in the office.

## Mobile Access is a Key Enabler

One of the biggest areas where integrators can deliver value is in providing their clients’ building tenants with a mobile experience. Mobile devices are ubiquitous and inherently secure – a perfect form factor for access control. Because people are never without their phones, these devices can serve as a central component for improving the experience of interacting with and moving through buildings. They offer a higher level of convenience and greater security than is possible with plastic cards – so many of which today’s employees have lost or misplaced during such a long period of working from home.

From the administrator’s perspective, cloud-based PACS mobile enables over-the-air provisioning and remote administration while empowering credential management across multiple tenants and locations. It alleviates much of the administrative burden associated with management of physical credentials, which involves archaic workflows and face-to-face time involved with each of what can be hundreds or thousands of individuals. It also supports the short-term credentialing needed in a hybrid workforce model.

Mobile devices can readily integrate with a visitor management solution, simplifying the credentialing process for administrators and end-users. Credentials can be

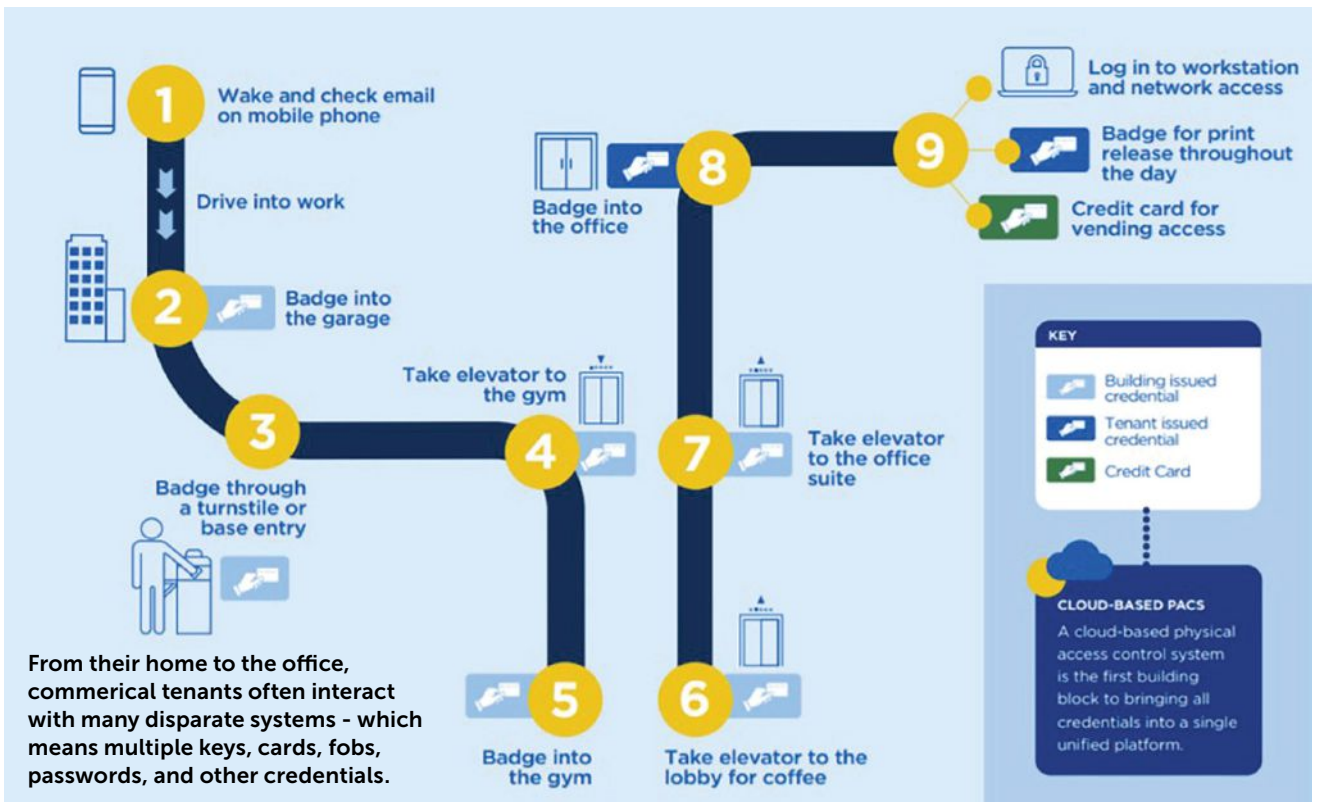


Illustration: H2D Global

delivered by email and downloaded to the device without a face-to-face interaction with the front desk. Tenants no longer have to wait for shipping of cards or come into a building to physically collect a card. With mobile, thousands of credentials can be issued remotely to users' phones through a few mouse clicks, enabling tenants to walk straight into the building on Monday morning.

For the end-user, the benefits of mobile include a single device for access control and other integrations, a more seamless experience, and touchless functionality in support of health and safety. Integrations beyond physical access control support things like tenant engagement, logical access systems, and mobile-friendly access to building amenities.

Meanwhile, mobile's ease of management gives building owners and operators transparency in the system that did not previously exist. As an added bonus, these solutions are eco-friendly, taking plastic cards out of

the access control ecosystem. This can be a boon to resident satisfaction, in addition to helping the environment.

## Taking the Next Step with a Tenant Experience Platform

The modern tenant experience is inherently complex. Each property is used for an array of purposes with a distinct assortment of tenants, visitors, and contractors. Each user requires access to a unique set of services, and each access point has its own functionality. Tenants want a seamless experience for their employees, with a single device for access to all touchpoints, and a frictionless experience across disparate systems.

People also have grown fatigued from having so many passwords, and different apps on their phone when they only use a few. They want more convenience and to improve their day-to-day life. They want the right information at their fingertips and interoperability among the differ-

ent systems they engage with. By leveraging PACS in support of the modern tenant experience, tenant companies can integrate technologies across their workplaces into a single interface, creating an attractive and innovative environment.

One way security professionals can help their clients address these issues is with a tenant experience platform – a desktop or mobile application that brings together all the things that companies should look for when exploring properties to house their operations – all in a single solution.

The application acts as a remote control for how a tenant interfaces with the physical space around them, from wayfinding, local restaurants and available fitness classes to weather, and traffic updates, along with mobile access. Being able to have one seamless, organized interface versus needing to potentially download eight to 10 different applications to use in the building on a day-to-day basis is extremely valuable.

Serving as a “single source of truth,” tenant experience platforms integrate access control, visitor management, building operations (maintenance requests, broken elevator alerts, etc.), shared asset management (booking shared rooms or spaces), as well as custom experiences like local dining options, yoga schedules, and café specials.

## What the Future Looks Like

One example of what’s ahead can be seen in the February 2022 announcement from Silverstein Properties that it had added contactless access to its 7 World Trade Center office building through an employee badge in Apple Wallet.

To help create this experience, HID partnered with Silverstein and SwiftConnect, whose Access Cloud manages and connects disparate access control systems across owner and enterprise portfolios with mobile credential platforms, user directories, and other systems that influence physical access requirements. SwiftConnect Access Cloud and Silverstein’s Inspire app integrate with HID Origo, a cloud platform that enables lifecycle management of mobile credentials. This tenant experience platform also leverages HID’s Seos credential technology to deliver an intuitive, private, and secure access transaction when a user presents their iPhone or Apple Watch to HID Signo Readers.

With Silverstein’s solution, tenants can easily access the company’s office buildings and their tenant floors, fitness centers and amenity spaces using their iPhone or Apple Watch. First, they add their employee badge to Apple Wallet after an initial set-up through an app. They can then hold their device near the door’s NFC-enabled lock to

access secured areas. To deliver this access experience in even the most extreme circumstances, employee badges stored in Apple Wallet works in Power Reserve mode when the iPhone needs a charge.

Solutions like these will also address the shift in what employees expect from their work environment. Those who return to the office have a new mindset forged during a lengthy period of working from home. Some will want the same digital conveniences of their home environment.

Others will need the assurances of touchless access, social-distancing, and hygiene measures that can only be efficiently managed through a tenant experience platform that integrates with beacon-based location services technologies and other automated solutions to these challenges.

Still others will need to operate in both worlds – seamlessly moving between each of the two environments and expecting the same experience in either one.

Delivering these experiences in a world where someone’s identity is the new – and often only – perimeter will put pressure on those owning and leasing their buildings to implement multi-factor authentication and other measures associated with a Zero Trust security model. This, too, will rely on the solid foundation of a cloud-based, mobile-first tenant experience platform. ■



» **Troy Johnston** is Global Business Director and CRE Vertical Lead for HID Global. Request more info about the company at [www.securityinfowatch.com/10213866](http://www.securityinfowatch.com/10213866).

## WE KEEP UP WITH THE INDUSTRY’S LATEST TRENDS



JLM Wholesale stocks a vast inventory of the industry’s biggest name brands, including SECO-LARM. We now stock SECO-LARM’S ENFORCER® Bluetooth® Access Controllers. This line of key pads and proximity readers provides easy access control with streamlined app-based set up management using integrated Bluetooth® wireless technology.

For more information, call (800) 522-2940 and our sales representatives will help you today!



SECO-LARM®



423.JLM.HELP  
704.509.2940

[www.jlmwholesale.com](http://www.jlmwholesale.com)

Request information: [www.SecurityInfoWatch.com/10214128](http://www.SecurityInfoWatch.com/10214128)



John Loud, right, with Kirk MacDowell and outgoing ESA Chairman Jamie Vos during the ESA Board Meeting at ESX.

Photo: ESA

# Q&A: New ESA Chairman John Loud

Coming off a long-awaited victory against false alarm fines in Georgia, the renowned security business owner looks ahead to two years at the helm of the Electronic Security Association

By Paul Rothman

**J**ohn Loud, president of Georgia-based LOUD Security Systems, is no stranger to the spotlight in the alarm and security industry. A business owner who has become famous for not only making public, but *actively giving out* his personal cellphone number to any customer who may need it, Loud most

recently spearheaded a difficult but successful effort in his state to outlaw the fining of alarm companies for a customer's false alarms.

The 2022 Electronic Security Expo (ESX) saw Loud confirmed as the new Chairman of the Electronic Security Association (ESA) for the next two years, taking over after the end of Jamie Vos's two-year term. On

top of that, Loud received the prestigious William N. Moody Award at ESX for his leadership and work with the fight against alarm company fines for false alarms in Georgia.

Created in 2004 by the Security Industry Alarm Coalition (SIAC), the Moody Award is given annually to an individual who demonstrates a passion for advancing positive alarm management and best industry practices. "John's leadership roles in ESA and the Georgia Electronic Life Safety & Systems Association (GELSSA) demonstrate a career-long commitment to helping our industry protect life and property through cooperation with public officials and public safety organizations," SIAC's Stan Martin said.

A few months after his ESX tour de force, I caught up with Loud during

the recent GSX show in Atlanta for this exclusive 1-on-1 interview.

**Rothman: What's your vision for ESA moving forward?**

**Loud:** I have been an independent security guy for 27 years and have been watching these different leadership roles in many ways. I really want to expose more of the value of what ESA does on a national level. There have been decades – almost 75 years – of folks who have worked collaboratively, whether it is codes, standards, or false alarm reduction.

I want folks to understand that they can have a seat at the table on all the committees that ESA has – some that many members might not even know of. We are also going to roll out a new membership campaign drive.

**How is ESA taking a leading role in false alarm reduction?**

We just passed unanimously a resolution about false alarm reduction, and this is going to be an issue I will be beating the drum on for the next two years. I've been involved with SIAC and the Georgia False Alarm Reduction Committee, and our model ordinance from day one.

When I was at ISC West in 2019, I saw advertising from some central stations about this new technology that's coming, and it was all about text chat [alarm] cancellation.

We want to make dealers aware that their monitoring centers are investing in this technology, and just about every software has this technology [now]. So at no cost to the dealer, they now can enroll subscribers. Not

every customer will do text chat, and most centrals are actually still calling; but, when we were talking to many of the third-party centrals out there, they don't have high adoption rate yet [for text cancellation], but they've invested a lot of money in it.

We did about 4,000 customers for a trial and then we put everybody on there. Within the first week, we had 171 folks cancel a false dispatch just on their phone. We realize as an industry, people aren't answering their phones anymore. You've got to meet them where they are.

I hope that as chair of ESA, we can bring awareness [of alarm cancellation technology] to the dealers, who can have less false alarm fees and fines to deal with their subscribers, netting lower attrition.

# 25% Project Discount\*

## 14" Residential Plastic Wiring Enclosure



**\$43** ~~\$58~~  
Model E

Typical installer's cost from ICC distributors

Available at:

**JENNE**

Ohio  
800.422.6191

**TD**  
TELEDYNAMICS

Texas  
800.847.5629

**TARGET**  
DISTRIBUTING

Maryland  
888.792.7463

**Beach**  
wire and cable

California  
800.309.2322

**Coleman's**  
ELECTROM

Utah  
801.484.5238

**font@I**

Nebraska  
800.238.0787

**Pirate Wire**

California  
800.590.0115

**Codale Electric**

Utah  
800.300.6634

**EarthBend Distribution**

South Dakota  
605.777.7005

**Systems Distributors**

Georgia  
800.452.8588

**Tristate Supply**

New York  
800.223.4534

**Brooklyn Supply**

New York  
718.298.4000

\*1. Valid on all 14-inch Plastic Residential Enclosures (Model E, W & K). 2. Offer ends 12/31/22. 3. Minimum 50 Units per shipment. 4. May be eligible for Free Freight. 5. Limit to Stock only, no backorder. 6. Discount does not apply to tax and fees. 7. Must mention this promo at the time of order; no retroactive credit. 8. Cannot be combined with any other discount or promotion. 9. Void where prohibited. Please visit [icc.com/resi-promo](http://icc.com/resi-promo) for complete details. © 2022, ICC

Request information: [www.SecurityInfoWatch.com/10213923](http://www.SecurityInfoWatch.com/10213923)

***With so many alarm dealers and integrators dealing with huge project backlogs, which will require more training and hiring, what is ESA doing to help with workforce development?***

Along with false alarm reduction, that is another one of the biggest challenges. Both are vital. Even though workforce development has been a challenge for quite a while, it might be a short-term need, where false alarm reduction needs to be solved for the long-term viability of our industry.

As far as workforce development, to me that is one of those challenges that we have to really think about differently. My example is Holly Thomas, who I have known for over five years and has been with KPMG almost 30 years. Her job for the last 25 years has been to bring in new college graduates to the firm. Along with her team

around the country, they have a very strategic and organized effort to hire more than 8,500 annually for their tax advisory and audit division.

On the other hand, alarm dealers in many aspects are just putting an ad on Indeed and just thinking the phone is going to ring and valuable people are just going to come running in. Then, once you find someone and you schedule an interview, and they are a no-show.

So, what can we do beyond just paying \$500 for an ad or whatever? We are not doing anything formalized as a recruiting process. Where are we working with our technical college students? Where are we working with the high schools?

We've got to go back to the whiteboard and say, "here's the way we have been doing it for the last 3, 5, 7

years, but here's a new way we should consider." To go write a print ad and a classified ad and say, "Oh, for 500 bucks it's going to work" – you've got to change and be different.

For example, we've had success on Facebook where employees put things out because now [that recruit] is getting a mentor within the company.

Another one is, should we be doing video ads – having a technician or an office staff or a salesperson doing kind of a testimonial – because at the same time you are looking to recruit, you are doing an advertisement for the company, as well as shining the light on an awesome employee.

Those are some examples of thinking differently. There are many reasons people join a company, including competitive compensation packages, but that is just one of the

Together we can



Inspire



Nourish

reasons. People look at the culture of a company and the people they meet and connect with – the people they will be working with day in and day out. That cannot be underestimated. People join other people.

I recently attended a DMP executive roundtable discussion, and the light bulb went off and I connected it to Holly. They have a massive team that does nothing but recruit. We've got to get into that kind of recruiting.

You are going to see a lot more attention and focus on the FAST [Foundation for Advancing Security Talent, launched in 2020 by the ESA and the Security Industry Association (SIA)] program. We've got to get that funded better to be able to really get that out there. We are in talks with a technical school campus in Louisville and we have great relationships in



“ I hope that as chair of ESA, we can bring awareness [of alarm cancellation technology] to the dealers, who can have less false alarm fees and fines to deal with their subscribers, netting lower attrition.” – **John Loud**

Georgia exploring models that we can create with curriculum and so forth that can then spread across the nation.

Workforce is one of those challenges that while there are many steps in process, I encourage alarm dealers to ask themselves: What can I do in my community to invest in or investi-

gate or partner with different schools, churches and other organizations? We need somebody who can help identify candidates or allow alarm dealers to give people an opportunity to be exposed to our industry via an apprentice role on the technician side, or even entrepreneurial or sales training. ■



Educate



Heal

By supporting Mission 500, you'll join the legions of security professionals who are already contributing their time and resources to help children in need across the US. Your contributions provide food and educational support where little or none is available. Please make an investment in our collective future. Together with Mission 500 we can make a difference.

**Learn more by visiting [Mission500.org](https://Mission500.org)**



Request information: [www.SecurityInfoWatch.com/10487869](https://www.SecurityInfoWatch.com/10487869)

## NEW PRODUCTS

The Latest From Security Product Manufacturers



### DMP 711S Pre-Programmable Zone Expansion Modules

The less time technicians spend programming panels, the quicker they can finish the job and move on to the next one. DMP's 711S Zone Expansion Modules are now programmed into the panel via a 10-digit serial number, giving integrators the ability to pre-program the modules ahead of time. Once at the job site, technicians just install and test the equipment without having to waste time programming any information. If programming on-site, simply scan the barcode into Zone Information with the DMP Tech APP, and the modules are ready to go.

Request more info at [www.SecurityInfoWatch.com/21284916](http://www.SecurityInfoWatch.com/21284916)



### Vivotek's Vortex VSaaS Solution

Vortex from Vivotek is an end-to-end surveillance solution

for VSaaS – the company's first step in transitioning to a subscription-based model. Its hybrid cloud architecture means that dedicated video management software or centralized management systems are no longer required to manage and process video data. The line includes many cameras ranging from 2-12 MP resolution in bullet, dome, turret, and 360-degree fisheye configurations. Intelligent object recognition technology accurately detects intrusion, line-crossing, and loitering detection of people and vehicles; with real-time notifications.

Request more info at [www.SecurityInfoWatch.com/21260455](http://www.SecurityInfoWatch.com/21260455)

### AXIS D3110 Connectivity Hub

The AXIS D3110 Connectivity Hub from Axis Communications enables secure integration of sensors and audio equipment into network systems. With a microphone, a speaker, or both connected, this cost-efficient device



helps increase scene awareness through high-quality audio. The product can be integrated with a broad range of non-visual sensors to trigger alarms and events in the system. Supporting audio recording, streaming, and audio analytics, it is ideal for systems that don't have or require additional audio capabilities.

Request more info at [www.SecurityInfoWatch.com/21284909](http://www.SecurityInfoWatch.com/21284909)

### SDC EA Series Door Prop Alarms

SDC door prop alarms are compatible with all access control systems but can also function as a stand-alone solution. All of the door prop alarms feature audible sirens with adjustable timer settings, two outputs, bypass status indicator light, and vandal-resistant aluminum construction. Available to install in single gang or double gang enclosures, they also offer optional keylock and mortise cylinder reset/bypass switches. Models include: EA-SN Single Gang Door Prop Alarm; EA-728V Double Gang Door Prop Alarm, Keylock Reset/Bypass; and EA-708V Double Gang Door Prop Alarm, Mortise Key Cylinder Reset/Bypass Prep.



Request more info at [www.SecurityInfoWatch.com/21284914](http://www.SecurityInfoWatch.com/21284914)



### Vicon Roughneck Pro LPR Cameras

Vicon's new Roughneck

Pro License Plate Recognition Network Cameras (V2008-WNL-LPR and V2000B-W310LPR) are NDAA/GSA/TAA compliant and available in bullet or box form factors. Supporting license plates from more than 70 countries, the cameras use 8 MP of resolution to see crisp vehicle details, such as vehicle color, make and model, even in the dark. The LPR technology is embedded in the camera, so storage and bandwidth are not compromised. They are ideal for single-lane, stop-and-go use-cases to control access, grant permissions and manage privacy in applications such as drop-off/pick-up lines, gated entrances, parking garages, drive-thrus and more.

Request more info at [www.SecurityInfoWatch.com/21284905](http://www.SecurityInfoWatch.com/21284905)

### SRL-1 Single Line Loud Ringer from Viking Electronics

Viking Electronics has introduced the SRL-1, a single line loud ringer with built in LEDs that quickly notifies employees of incoming calls and visitors with four traditional ringing sounds and doorbell tones, while also flashing the built-in LEDs for added visibility. The unit generates ringing and LEDs from an analog ringing line or from a dry contact closure. A second set of contact inputs will trigger a door chime sound, which can be used to notify that a door has opened or used as a doorbell or push for assistance button.



Request more info at [www.SecurityInfoWatch.com/21283791](http://www.SecurityInfoWatch.com/21283791)



## DedroneDefender Counter-Drone Jammer

DedroneDefender is a connected gun for targeted precision Radio Frequency (RF) jamming, to be used as part of a counter-drone mitigation strategy for civilian, state and local law enforcement in urban environments.

It can be operated in traditional handheld mode supported by a phone-based app for targeting. By Q1 2023, it will also be available mounted on a pan-tilt-positioner for automated targeting as directed by DedroneTracker software, resulting in an autonomous Pan-Tilt-Jammer (PTJ) solution.

Request more info at [www.SecurityInfoWatch.com/21283915](http://www.SecurityInfoWatch.com/21283915)



## SightLogix SightSensor Dual-Imager Camera

The SightSensor TC4 from SightLogix is a dual-imager smart camera that combines thermal detection and visible color to detect targets on critical infrastructure, industrial and commercial perimeters. Featuring a 384x288 high-clarity thermal array, it offers 44% more pixels and a higher resolution than standard 320x240 thermal cameras. Long-range and wide area detection means fewer cameras are needed to protect large outdoor areas. One device means one camera on the pole instead of two, with a single network drop, one mounting bracket, and simpler installation.

Request more info at [www.SecurityInfoWatch.com/21284885](http://www.SecurityInfoWatch.com/21284885)



## CMOS Image Sensor from Omnivision

Omnivision's OS05B CMOS image sensor combines pixel technology and quantum efficiency in a 5-megapixel design for professional and high-end consumer security cameras. With a 1/2.78-inch optical format and 2.0-micron BSI pixel based on PureCel Plus technology, it also features near-infrared (NIR) technology for clear images in low-light conditions. Other features include signal-to-noise ratio (SNR1) improvement of 32% over the OS05A, and NIR QE at 940nm is improved by 24%.

Request more info at [www.SecurityInfoWatch.com/21283934](http://www.SecurityInfoWatch.com/21283934)



# SecurityInfoWatch On-Demand Webcasts

## New Tech in Physical Perimeter Protection

As threats to physical perimeters proliferate, security professionals must design end-to-end, future proofed PIDS capable of detecting, classifying and deterring threats long before they are able to reach an end user's perimeter. Our panel of experts will discuss some of the more advanced and emerging technologies systems integrators are implementing for end-user organizations, including: **radar, multi-spectral cameras, video analytics and AI**, and **counter-drone technologies**.

Sponsors:



[www.SecurityInfoWatch.com/21283898](http://www.SecurityInfoWatch.com/21283898)

Earn  
CEU  
Credits!

## More Archived Events:

- **Special Event and Sports Facility Security**  
(sponsors: dormakaba, Everbridge, Evolv, Salient Systems)
- **School Security & Safety Trends Roundtable**  
(sponsors: Aiphone, Bold Group, Evolv, Genetec, Milestone Systems, Napco)
- **Active Shooter Prevention & Response**  
(sponsors: Aiphone, Bold Group, Evolv, Genetec, Milestone Systems, Napco)
- **Security Technologies on Campus**  
(sponsors: Aiphone, Bold Group, Evolv, Genetec, Milestone Systems, Napco)
- **K-12 Security & Safety Planning**  
(sponsors: Aiphone, Bold Group, Evolv, Genetec, Milestone Systems, Napco)

Access them all (and more) at [www.SecurityInfoWatch.com/webinars](http://www.SecurityInfoWatch.com/webinars)

## NEW PRODUCTS

The Latest From Security Product Manufacturers

### Fire-Rated Strikes from Camden Door Controls

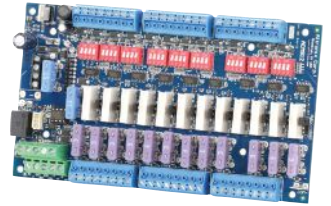
Camden Door Controls' 1500 line of fire-rated electric strikes for mortise and cylindrical locksets includes a CX-ED1500LP low-profile strike with one latch monitor, as well as a CX-ED1500L2 strike with two latch monitors. They are available in a range of faceplate packs for both deadbolts and latchbolts. UL1034 and UL 294 listed, the strikes also carry a three-hour fire listing. A universal design includes selectable fail safe/fail secure and 12/24 V AC/DC operation. Additional features include a magnetic door position switch, keeper position switch, power monitor and easy fit connectors.



Request more info at [www.SecurityInfoWatch.com/21282318](http://www.SecurityInfoWatch.com/21282318)

### Access Control and Power Distribution Sub-Assemblies from Altronix

Altronix ACMS12 series Access Power Controllers and PDS16 Power Distribution Modules further increase access control system capacity in Altronix Trove Access and Power Integration Solutions, and any other wall or rack mount solution – reducing overall equipment and installation costs. The sub-assemblies deliver up to twice the outputs and feature the same stackable mounting footprint. More outputs in less space means more room for controllers inside an enclosure.



Request more info at [www.SecurityInfoWatch.com/21276090](http://www.SecurityInfoWatch.com/21276090)



### Gallagher Command Centre v8.80 Security Management Software

The latest version of Gallagher's Command Centre v8.80 site management software comes with a new web-based system, Command Centre Web, reducing costs and operational downtime by removing the need to maintain a full workstation on the operator's computer. The first component introduced in Command Centre Web focuses on cardholder management, and allows administrators to view cardholder history, view activity of cardholder, manage cards and credentials (excluding printing/encoding cards), manage cardholder access/assign access, and general personal data field (PDF) management.

Request more info at [www.SecurityInfoWatch.com/21284908](http://www.SecurityInfoWatch.com/21284908)



### Sensormatic Computer Vision for Retail

Created through collaboration with Intel and optimized for retail using proprietary Sensormatic IQ artificial

intelligence (AI) algorithms, Johnson Controls' Sensormatic computer vision analytics offering can be deployed using a smart hub device in conjunction with existing camera infrastructure to facilitate streamlined, cost-effective adoption of next-generation AI in retail environments. Capabilities include: Shelf sweep detection (monitors shelf activity for large-scale item removal); unauthorized and abandoned vehicle alert; loitering monitoring; group detection alerts; traffic pattern insights; slip-and-fall detection; dwell time measurement, and more.

Request more info at [www.SecurityInfoWatch.com/21284898](http://www.SecurityInfoWatch.com/21284898)

### Luma x20 Surveillance Line from Snap One

The new Luma x20 family of surveillance products from Snap One are fully NDAA-compliant and include AI-powered security features and full OvrC integration.

Available by early January 2023, products include a variety of cameras, NVRs, the Luma View mobile app and more. Professional setup procedures are provided via OvrC and gives users a state-of-the-art experience with for system control and live monitoring. The app features AI-filtered events, allows saving and sharing clips, lets users scrub synchronized event footage and provides them with enhanced connectivity security between mobile devices and the surveillance system.



Request more info at [www.SecurityInfoWatch.com/21284901](http://www.SecurityInfoWatch.com/21284901)

### License Plate Capture Camera from IDIS

The 2MP IDIS DC-T6224HRXL NDAA-compliant license plate capture camera has a detection range of over 325 yards (100m) in full light and advanced IR to capture flawless images at up to 66 feet (20m) to accurately capture the license plates of vehicles worldwide traveling up to 50 mph. Ideal for single-lane traffic monitoring, the camera also features analytics, including motion detection, active tampering, and trip zones, and can be quickly and easily connected to IDIS DirectIP NVRs to ensure rapid installation and secure connectivity. The DC-T6224HRXL is and crime prevention.



Request more info at [www.SecurityInfoWatch.com/21284912](http://www.SecurityInfoWatch.com/21284912)



## Altronix – Powered by People

Founded in 1984, Altronix provides the security industry with more reliable and efficient power solutions. For nearly four decades, Altronix continues to deliver the quality, innovation and unparalleled customer support that has earned the company a global reputation as being the gold standard in power and data transmission solutions.

Altronix corporate headquarters, which includes manufacturing, encompasses more than 200 thousand square feet at the Brooklyn Army Terminal in Brooklyn, New York, employing approximately 300 people.

A true design and manufacturing powerhouse from board level up, Altronix's boasts the latest advancements in technology across every phase of operations. Altronix is an ISO registered firm and part of the UL Client Test Data Program – now referred to as DAT. This capability benefits Altronix and its partners by shortening development time and getting products to market expediently.

Altronix has been a longtime supporter of numerous professional security associations, including but not limited to the SIA, ASIS, ESA, TMA and AIREF to name a few. Altronix also has a vested interest in corporate social responsibility and provides funding for charitable causes.

Altronix's lifetime warranty is also a testament to the extreme quality and confidence that the company places in every product that leaves its facility. Packaged in the recognizable blue box, Altronix products are all NDAA and TIA compliant.

For more information, visit <http://altronix.com>



TOUCHLESS WIRELESS LOCKING CONTROL

## Innovation, Quality & Support for Any Access Control or Automatic Door Project!

Camden Door Controls designs and manufactures door activation, control, and locking products that provide better performance and the best value in the industry. For over 30 years, Camden has been the right source for any access control or automatic door installation.

### TOUCHLESS!

Camden offers a family of 'NO-TOUCH' solutions for automatic door or access control applications. Our no-touch switch options include line power or battery power, wired or wireless, 1 or 2 relays, and a range of models, from narrow, single gang, square, round, or 36" tall configurations!

### WIRELESS!

Only Camden offers a family of 915MHz spread spectrum wireless products that include wall switch transmitters, 1, 2, & 4 button fobs, touchless switches, and even weather and vandal-resistant keypads!

### LOCKING!

Camden offers a huge selection of electric strikes, including the new CX-ED1500 strikes for mortise and cylindrical locksets.

### DOOR CONTROL!

A new addition to our product lineup is our CV-603 BLE two door access control system that comes ready to support each system user with the credential of their choice, including mobile Apple® or Android® smartphone credential, a prox card/tag, or two button wireless key FOB.

5502 Timberlea Blvd.  
Mississauga, ON L4W 2T7

Phone: 1-877-226-3369

Fax: 1-888-436-8739

E-Mail: [david.price@camdencontrols.com](mailto:david.price@camdencontrols.com)

[www.camdencontrols.com](http://www.camdencontrols.com)



## COPS Monitoring

### Not just different. Better.

Let us show you how we stand out from the rest and why thousands of dealers trust COPS to help safeguard over 3.5 million of their customers.

**100% Wholesale Monitoring:** COPS Monitoring does not sell, install, own accounts, or compete with our dealers the way other monitoring companies do. 100% wholesale monitoring means COPS is 100% focused on properly supporting your company.

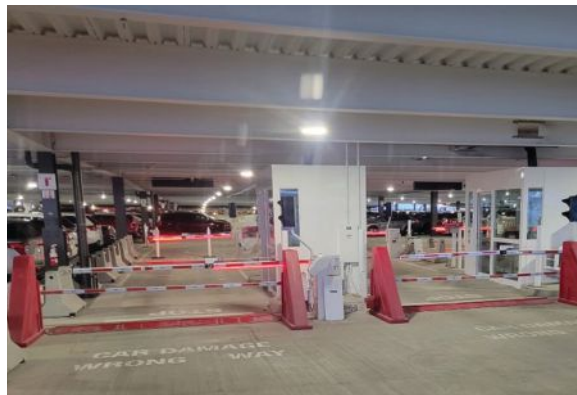
**Reliability:** COPS has been improving redundant monitoring since we opened our second site in 2004. Our network of real-time load sharing monitoring centers is trusted by thousands of alarm dealers to safeguard more than 3.5 million subscribers across the US, Canada, and the Caribbean. Our average response time to more than 6 million alarm signals received over the past 12 months remained under 24.8 second. COPS is UL listed, FM approved, IQ certified, has more TMA Five Diamond certified monitoring stations than any other company, and we are proud to have been recognized as TMA Central Station of the Year.

**Technology:** We are the only wholesale monitoring company with its own UL listed proprietary monitoring platform. Generations® was written and continues to be developed by our staff of in-house programmers, which gives COPS the unique ability to tailor our system to meet the demands of our quickly evolving industry and our Dealers the ability to capitalize on the next generation of revenue-creating services.

**Stability:** In an industry flush with acquisition, COPS has been a leader in high-quality third party monitoring services for more than 44 years. Our ongoing commitment to reinvest in our employees, central stations, and dealer base has made COPS the #1 professional monitoring company in the industry.

**People:** What qualities make the best dispatchers? It is a critical question because that person on the phone is representing your company! Learn how COPS utilizes psychology and science and its rigorous Gradation process to ensure only the best people serve your customers: [cops-monitoring.com/people](http://cops-monitoring.com/people).

[www.copsmonitoring.com](http://www.copsmonitoring.com)



DoorKing®, Inc. was established in 1948 and is one of the country's leading manufacturers of single and multi-door access control systems, telephone entry systems, vehicular gate operators, parking control products and vehicular barrier products in the United States. Based in Inglewood, California, DoorKing operates from seven buildings and is located less than three miles from Los Angeles International Airport (KLAX).

DoorKing manufactures a variety of single and multi-door access control systems, telephone entry and video entry systems, secure MicroPLUS® RF transmitters and receivers, and digital keypads. Our ProxPlus™ Secure card readers are encrypted with a unique identifier offering an extremely high degree of security and making the duplication of cards almost impossible.

Our vehicular access control products include slide, swing and barrier gate operators and systems. For areas requiring a higher degree of perimeter control, such as airports, military installations, industrial sites, sea ports, infrastructure facilities (chemical, electrical, water treatment plants, etc.), DoorKing's maximum security gate operators are equipped with special features that help to insure that the perimeter gate system is secured as quickly as possible. Our vehicle barrier systems insure that traffic lanes cannot be breached.

<http://doorking.com>

120 S. Glasgow Avenue

90301 Inglewood, CA

800-826-7493

[info@doorking.com](mailto:info@doorking.com)



Speco Technologies has been dedicated to providing the latest innovations in video surveillance, access control, and audio products for over sixty years. We provide affordable, dependable merchandise, and deliver exceptional customer service, extensive product training, and complimentary technical and marketing support to all our partners. We will continue to be innovators in residential and commercial solutions and want our customers to grow with us and move forward.

**Innovation** – Speco’s patented Digital Deterrent® technology can actively deter crime before it happens. Utilizing advanced analytics including facial recognition, people detection, vehicle detection, and now visually and audibly alert would-be criminals that they are under surveillance. Our Digital Deterrent IP cameras house extremely bright red and blue LED lights and a built-in speaker to cast a loud audible message to any detected area. This technology can be used in any application to actively prevent crime from occurring such as parking lots after hours, catalytic converter theft, and more.

**World-Class Support** – we know what it takes to run a business and how critical it is to have a manufacturer that can be relied upon. Our mission is to provide a customer and technical support team that is as reliable as our products. Utilize our S.E.A.L. Team for project design of any size. They can walk you through each step of integrating video surveillance, access control, and audio equipment. Our award-winning marketing department is always ready to assist with website support, digital marketing, custom catalogs, and anything else you can think of to separate you from the pack.

**Speco Technologies**  
200 New Highway  
Amityville, NY 11701

[www.specotech.com](http://www.specotech.com)



SMARTER SECURITY ANSWERS



STid is an award-winning developer of contactless identification solutions for high-security access control as well as Automatic Vehicle Identification. Using RFID, NFC, Bluetooth®, and IoT technologies, STid develops intelligent, non-proprietary identification solutions for flexibility and custom integrations.

Headquartered in France with offices worldwide, STid has over 25 years of experience in providing businesses, residences, and governments with the means to safeguard their people, assets and data. Its mission is to simplify digital identity management, so organizations can focus on their core competencies.

The company has seen unprecedented growth worldwide as clients immediately see value from STid’s expertise in hardware development, offering complete, consistent solutions as well as effective support. The corporate policies of STid for product development and data storage are based upon open technology standards and public cryptography standards. This approach allows all the company’s products to meet the highest security requirements. To ensure interoperability and compatibility with legacy systems, STid’s solutions offer several secure hosting options which can be matched to network architecture, corporate security policies, and the applicable legislation in specific regions.

A recognized pioneer in its field, STid was the first manufacturer to obtain First Level Security Certification (CSPN) from the French government agency ANSSI for its access control solutions. With thirteen awards, STid’s flagship Architect® series of readers is the most awarded in the world by security experts. STid recently launched the new SPECTRE nano UHF and Bluetooth® reader for easy vehicle and driver access control.

Learn more at <https://stid-security.com>



## United Central Control

With 40 years of experience providing our customers with exceptional monitoring services, UCC employees know what it takes to help our dealers succeed. In addition to high quality, caring monitoring services for our dealers and their customers, we invest our time and resources into providing industry leading dealer support and training and implementing new technologies and value add services.

Our monitoring centers in San Antonio and Lewisville, TX are home to highly trained, seasoned professionals that have been certified by the TMA Central Station Operator Level 1 online course, earning UCC the TMA Five Diamond Central Station rating. UCC is fully licensed, UL listed for burglary, fire, UL2050 and is the first contract monitoring center to participate in the TMA's ASAP program.

UCC's cutting edge "Stages" monitoring platform is widely considered the "Best in Class" monitoring and account management platform and it provides the tools dealers need to manage their alarm accounts, including multiple CRM integrations, a 2 way chat feature for end users to communication with the monitoring center, and more.

UCC provides a wide array of monitoring services including alarms of all types, elevator and emergency telephones, two-way voice, PERS/mPERS units, and video verification. We also support several interactive home solutions, funding partnership options and we are continuously seeking out, evaluating, and investing in the newest products and services that are beneficial to our dealers and their customers.

Our Dealer Support and Dealer Development teams have provided over 63,000 dealer training workshops, webinars, one on one sessions, outreach calls, and in person office visits to provide dealers with customized training and education designed to help them grow and manage their business.

UCC's Grow Your Business workshop series is designed with the individual alarm dealer in mind to EDUCATE managers with expert training using proven techniques that help create more than 300,000 accounts, ENABLE owners to make informed business decisions that increase their bottom line and EMPOWER companies with in-demand services and technologies to help build their business portfolios.

Make the move today and experience the UCC difference.

[www.teamucc.com](http://www.teamucc.com)

## VIKING

SECURITY & COMMUNICATION



Viking Electronics designs and manufactures over 500 security and communication products right here in the United States. We made the decision a long time ago to keep all engineering, production, and shipping in Hudson, Wisconsin. It's more than just a "Made in the USA" policy - it's our way of keeping close to our customers.

Established in 1969, Viking is a long-standing leader in the industry. With more than 50 years of experience, Viking has developed an extensive product line; including Emergency Phones, Entry Systems, Paging Interfaces, Amplifiers, Mass Notification Systems, Hot Line Phones, Auto Dialers, Enclosures, and more. The majority of our products are "problem solvers," designed to fix or add unique features to other manufacturers' telephone or security systems. We also manufacture several stand-alone telephone and security products.

In addition to our analog solutions we also offer numerous IP based options. Viking VoIP products are SIP compliant, with features such as superior audio quality, built-in relays, and automatic noise canceling. We provide IP options for Emergency Phones, Entry Systems, Paging Interfaces, and more.

If you have questions about a Viking product, or maybe you're not even sure what you're looking for, we want to hear from you. Since the beginning, we've been telling our customers to "Ask Us First." If we don't make it, we'll do our best to direct you to someone that does.

Learn more about how Viking can help you by visiting:

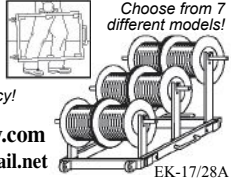
[www.vikingelectronics.com](http://www.vikingelectronics.com)

**Viking Electronics, Inc.**  
1531 Industrial Street  
Hudson, WI 54016

Call: 715-386-8861

E-Mail: [info@vikingelectronics.com](mailto:info@vikingelectronics.com)

**Easy Kary®**  
Wire Reel Holders



Choose from 7 different models!

Second to none in durability and efficiency!

www.musicupply.com  
musicupply@airmail.net

EK-17/28A

Info: [www.SecurityInfoWatch.com/10744798](http://www.SecurityInfoWatch.com/10744798)

**MAKE THE  
RIGHT CALL**

Advertise in

**SECURITY  
BUSINESS**

The Path to Greater Profits for Security Integrators



**CONTACT AMY STAUFFER  
FOR MORE INFORMATION:**

(920) 259-4311

[astauffer@endeavorb2b.com](mailto:astauffer@endeavorb2b.com)



**DA™** **Dakota Alert**

**NEW**

**PIR-4000**

- Small indoor passive infrared sensor
- Works with any Dakota Alert 4000 Series receiver
- 110° Field of view
- Operates on one CR-2 battery
- Perfect addition to any 4000 Series kit
- Wireless range of up to 1 mile

**[www.dakotaalert.com](http://www.dakotaalert.com)**

**605-356-2772**

Request info: [www.SecurityInfoWatch.com/10215782](http://www.SecurityInfoWatch.com/10215782)

**SECURITY  
BUSINESS**

The Path to Greater Profits for Security Integrators

**Advertise in  
Security Business**

Contact Amy Stauffer  
[astauffer@endeavorb2b.com](mailto:astauffer@endeavorb2b.com)

(920) 259-4311



# PowerStream

24VAC UPS



INPUT AND OUTPUT 24VAC  
EXTERNAL 12V BATTERY  
UNINTERRUPTIBLE 24VAC POWER SUPPLY

24VAC TO 24VDC  
CONVERTER



50 WATTS OR 2 AMPS

24VAC TO DC CONVERTER



1V TO 18V USER ADJUSTABLE OUTPUT  
3 TO 7 AMPS

CALL US FOR A  
CONSULTATION  
**(801) 764-9060**



[www.powerstream.com](http://www.powerstream.com)

Request info: [www.SecurityInfoWatch.com/10744755](http://www.SecurityInfoWatch.com/10744755)



*Regional Firm. National Presence.*

100+ Attorneys • 108 Years of Experience • 5 Offices

**Timothy J. Pastore**  
Vice-Chair, Litigation Department  
212.551.7707  
[tpastore@mmwr.com](mailto:tpastore@mmwr.com)

[WWW.MMWR.COM](http://WWW.MMWR.COM)

PENNSYLVANIA • NEW YORK • NEW JERSEY • DELAWARE

ATTORNEY ADVERTISING © 2021 Montgomery McCracken Walker & Rhoads LLP

Request info: [www.SecurityInfoWatch.com/21209650](http://www.SecurityInfoWatch.com/21209650)



CREATING  
**SECURE**  
ENVIRONMENTS



**PLAN**

Security Assessment and  
Planning Services



**DESIGN**

Security Design and  
Engineering



**DEPLOY**

Procurement and Project  
Management Services



**MANAGE**

Comprehensive Security  
Program Management

888-793-9380  
[info@sentinelgroup.us](mailto:info@sentinelgroup.us)

50 Tice Blvd. Suite 340,  
Woodcliff Lake, NJ 07677

[www.sentinelgroup.us](http://www.sentinelgroup.us)

Request info: [www.SecurityInfoWatch.com/12435458](http://www.SecurityInfoWatch.com/12435458)

**VECTOR FIRM**  
Sales Academy

Sales Training built  
exclusively for the  
Security Industry

Save 10% Lifetime Membership  
Use Coupon Code  
**security business**



LEARN MORE

**VECTORFIRMACADEMY.COM**

Request info: [www.SecurityInfoWatch.com/12361573](http://www.SecurityInfoWatch.com/12361573)



ADVERTISER NAME	PAGE	WEB SITE URL
Acquisiton & Funding Services	53	www.securityinfowatch.com/10744814
Altronix Corporation	11	www.securityinfowatch.com/10212790
Alvarado by dormakaba Group	17	www.securityinfowatch.com/10212792
Camden Door Controls	1, 3	www.securityinfowatch.com/10213140
ComNet by ACRE	19	www.securityinfowatch.com/10215705
COPS Monitoring	13	www.securityinfowatch.com/10552071
Digital Monitoring Products (DMP)	25, 27, 29, 31	www.securityinfowatch.com/10213461
Digital Monitoring Products (DMP)	33, 35, 37, 39	www.securityinfowatch.com/10213461
DKS DoorKing Systems	7	www.securityinfowatch.com/10213482
HES	15	www.securityinfowatch.com/10213861
ICC	61	www.securityinfowatch.com/10213923
JLM Wholesale	59	www.securityinfowatch.com/10214128
Mission 500	62-63	www.securityinfowatch.com/10487869
NAPCO Security Technologies	2, 9	www.securityinfowatch.com/10215125
Quick Response Monitoring	49	www.securityinfowatch.com/10746329
Seclock	1, 75	www.securityinfowatch.com/10215009
Seco-Larm	51	www.securityinfowatch.com/10214926
Securitron	47	www.securityinfowatch.com/10214963
Snap One	5	www.securityinfowatch.com/21090092
Speco Technologies	76	www.securityinfowatch.com/10215180
STid	20-21	www.securityinfowatch.com/12266353
United Central Control Inc.	23	www.securityinfowatch.com/10215459
Viking Electronics	45	www.securityinfowatch.com/10556843

This index is supplied as a service to our readers. The publisher assumes no liability for omissions or errors.



**ADVERTISING REPRESENTATIVES**

**Jolene Gulley-Bolton** | Group Publisher  
(480) 524-1119  
jgulley@endeavorb2b2.com

**Janice Welch** | Sales Manager  
(224) 324-8508 • Fax: (888) 507-2310  
Janice@SecurityInfoWatch.com

**Bobbie Ferraro** | Sales Manager  
(310) 800-5252 • Fax: (310) 545-3019  
Bobbie@SecurityInfoWatch.com

**Brian Lowy** | Sales Manager | Midwest  
(847) 454-2724  
brlowy@endeavorb2b.com

**DISPLAY/CLASSIFIED**

**Amy Stauffer**  
(920) 259-4311  
astaufer@endeavorb2b.com

**LIST RENTAL**

**Michael Costantino**, InfoGroup  
Michael.Costantino@infogroup.com  
(402) 836-6266

**Kevin Collopy**, InfoGroup  
Kevin.Collopy@infogroup.com (402) 836-6265

**REPRINTS**

To purchase article reprints please email  
reprints@endeavorb2b.com.

**CIRCULATION & SUBSCRIPTIONS**

PO Box 3257, Northbrook, IL 60065-3257  
Phone: (877) 382-9187 or (847) 559-7598  
fax (800) 543-5055  
Circ.SecDealer@omeda.com

**RENEW  
OR SUBSCRIBE**  
to *Security Business*  
today!



**GO TO**

[www.SecurityInfoWatch.com/subscribe](http://www.SecurityInfoWatch.com/subscribe)

and enter priority code 2020MAG

**INFORMATION IS  
POWER**

**Security Business** (USPS 460-650), (ISSN 1941-0891, print; ISSN 2688-058X, online) is published monthly by Endeavor Business Media, LLC, 1233 Janesville Avenue, Fort Atkinson, WI 53538. Periodicals postage paid at Fort Atkinson, WI 53538 and additional mailing offices. POSTMASTER: Send address changes to Security Business, PO Box 3257, Northbrook, IL 60065-3257, Canada Post PM40612608. Return undeliverable Canadian addresses to: Security Business, PO Box 25542, London, ON N6C 6B2.

Subscriptions: Individual subscriptions are available without charge in the U.S. to qualified subscribers. Publisher reserves the right to reject non-qualified subscriptions. Subscription prices: U.S. \$54 per year, \$101 two year; Canada/Mexico \$74 per year, \$143 two year; All other countries \$106 per year, \$202 two year. All subscriptions payable in U.S. funds, drawn on U.S. bank. Canadian GST#842773848. Back issue \$10 prepaid, if available. Printed in the USA. Copyright 2022 Endeavor Business Media, LLC.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recordings or any information storage or retrieval system, without permission from the publisher.

Endeavor Business Media, LLC does not assume and hereby disclaims any liability to any person or company for any loss or damage caused by errors or omissions in the material herein, regardless of whether such errors result from negligence, accident or any other cause whatsoever. The views and opinions in the articles herein are not to be taken as official expressions of the publishers, unless so stated. The publishers do not warrant, either expressly or by implication, the factual accuracy of the articles herein, nor do they warrant any views or opinions offered by the authors of said articles.





# What's Keeping You up at Night?

Four of the hottest topics from last month's PSA Annual Convention

In October, more than 80 integrators gathered in Hilton Head, S.C., for the PSA Annual Convention to discuss their most significant business concerns – among them being supply chain challenges, employee retention, M&A and cybersecurity. The integrators shared solutions and collaborated on creative ways to address their challenges.

## Supply Chain Concerns

As reported in depth by *Security Business* in its September issue, integrators continue to report that many “go-to” manufacturers are experiencing shipping delays and product shortages ranging up to two years out due to supply chain issues.

Often, integrators redesign systems to accommodate similar products; however, sometimes the products are also not available. On rare occasions, manufacturers are reengineering their products to omit the specific chip or part that is hindering production.

Integrators agreed that transparent communication from manufacturers is essential during these challenging times. From manufacturer to distributor to integrator, the group recognized that open lines of communication will not resolve the issue but will go a long way to helping manage expectations and frustrations for end-users.

## Employee Retention

Similarly, lack of manpower is a concern facing integrators. Specifically, recruiting and retaining workers was top of mind when the integrators discussed workplace culture.

“Some integrators hold **employee trainings and meetings regarding cybercrime**, send test emails to employees to mimic a cyber-attack, and document process improvements to include mandated phone verification to confirm the legitimacy of certain transactions.”

According to HR consultant April Simpkins, SHRM, millennials will be the majority of the workforce in 2025, with Generation Z comprising more than 25% of the workforce. With Generation X and baby boomers holding most of the executive roles, the workplace is diverse in worker expectations and values.

Simpkins highlighted characteristics of the up-and-coming Generation Z. Understanding generational differences can help employers retain talent while making the employees feel valued and acknowledged.

## Industry Consolidation

Another hot topic for integrators is the consolidation of competitors, manufacturers or a combination of both. There has been significant M&A activity in the security industry in the past two years, and the integrators agreed that staying up to date on these moves is essential to any business.

Michael Morabito, partner of Houlihan Lokey, shared during a speaking panel that security M&A isn't slowing down, and was even bullish during the pandemic when it was expected to shrink. He said this is also the case with the next stage of the hybrid workplace, with new buildings

and redesigned commercial systems driving growth in cloud-based managed services, convergence of point products and the increasing enterprise focus on workplace security and safety.

## Cybersecurity Awareness

An increase in cybersecurity threats – especially to integrators' own businesses – were also discussed. Email phishing attacks are used by attackers to try to gain access to critical business information or extract money through email-based fraud. The FBI reported losses from business email compromise attacks cost companies \$1.7 billion last year – over half of all losses due to cybercrime – and that number is dramatically growing each month.

To mitigate attacks, some integrators hold employee trainings and meetings regarding cybercrime, send test emails to employees to mimic a cyber-attack, and document process improvements to include mandated phone verification to confirm the legitimacy of certain transactions. These strategies will hopefully save companies millions. ■

» **Kristie Kidder** is Director of Marketing and Communications for PSA Security Network. Request more info about PSA at [www.securityinfowatch.com/10214742](http://www.securityinfowatch.com/10214742).



## You're the best at what you do. So are we.

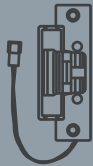
When it comes to sourcing the right parts for the job—any job—no one comes close to SECLOCK. Our team of technical service reps is unrivalled in the industry, meaning you get exactly what you need exactly when you need it, every time.

You have other things to worry about. Let us take care of the hardware.

Visit [SECLOCK.com](http://SECLOCK.com) to see how we can help.

dormakaba 

BEST 



[info@SECLOCK.com](mailto:info@SECLOCK.com)

800.847.5625

# DON'T JUST WITNESS A CRIME. DETER IT!

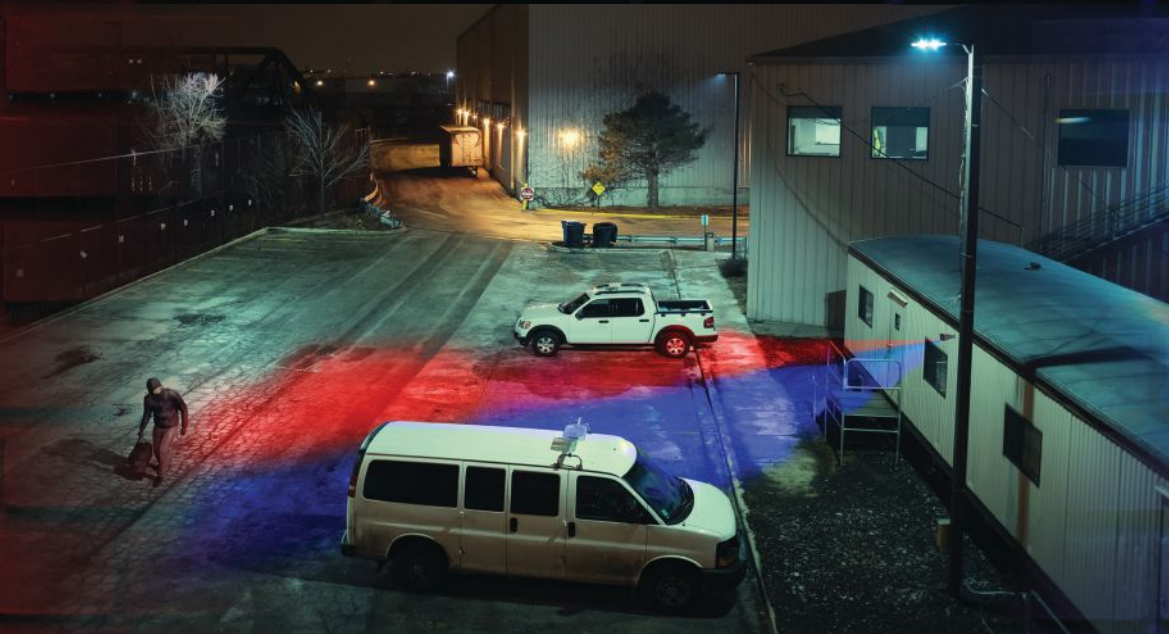
## A CAMERA WITH BARK & BITE



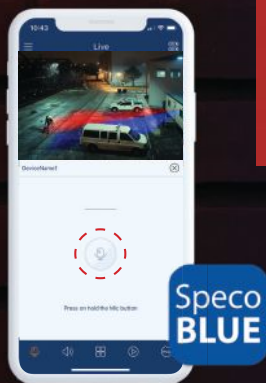
AVAILABLE IN BULLET  
AND TURRET HOUSINGS  
2.8-12MM MOTORIZED LENS  
O4BDDIM & O4TDDIM



**THIS IS A  
PRIVATE  
AREA!**



- Line crossing, region intrusion and video blurring detection
- People/Vehicle detection
- 2-way audio with talk-back feature enables voice communication through the built-in speaker
- Manually trigger audio messages via app!



## DIGITAL DETERRENT

### LOUD AUDIBLE MESSAGE

Built-in speaker emits a siren and custom or preset warning messages.

### BRIGHT VISUAL DETERRENCE

High-powered Blue and Red flashing lights trigger a flight response and draws attention to the scene.

**NDAA**  
COMPLIANT



Follow us at  
Speco Technologies

Call us at 1.800.645.5516 to learn more!

\*Products are in compliance with NDAA Section 889 Part B Guidelines

Request information: [www.SecurityInfoWatch.com/10215180](http://www.SecurityInfoWatch.com/10215180)

**speco**  
technologies

# SCHOOL SECURITY & SAFETY

*Supplement to American Schools  
& Universities, Locksmith Ledger  
International, Security Business,  
Security Technology Executive*

## COVER STORY

**Campuses Strive to  
Strike a Balance  
Between Technology  
and Policy – Page 6**

## CAMPUS SECURITY FEATURES:

**Modern Systems for  
Enhanced Campus  
Security – [Page 4](#)**

**Schools Must As-  
sess Risk Prior to  
Implementing  
a Plan – [Page 10](#)**

**K-12 Security and  
Technology Expert  
Q&A – [Page 14](#)**

**How School Active-  
Shooter Myths Can  
Increase Casualties –  
[Page 18](#)**



**Most Affordably Meets  
New Classroom Codes:**  
*Locks from Either Side;  
Always Provides  
Unrestricted Exit*

## LocDown® Any Door from Safely Inside with Budget-Friendly Classroom Locks by Marks



Keep teachers, staff and students safer in the classroom with **Marks LocDown® Locks**. In the old days, with a standard lock, someone would have to go outside into the hall to lock up a classroom, but **LocDown Locks** uniquely lock from the inside, so no one has to potentially face an external threat. **Created in conjunction with, and spec'd by, one of the largest school districts in the country (LAUSD) and used by many more nationwide, Marks LocDown Locks have an inner door key and lock-down indicator, and easily & super-affordably replace any standard door lock.**

- **Lock Down in seconds, with a simple key, safely from inside** the classroom, without having to step foot into the hall or danger
- **Lockdown indicator** gives visual peace of mind
- **Retrofits any standard lock** easily & very economically
- **Classroom Locks in cylindrical or mortise lock styles**, with unique double cylinder locking mechanism
- **ALSO Ultra-Affordable Code-Compliant Marks F-Function Models**, as previous, but without indicator
- **All Durable for Life -** Lifetime warranty; exceeds ANSI/BHMA Grade 1 standard



 **MARKS USA**

1.800.645.9445 • salesinfo@marksusa.com • [www.marksusa.com](http://www.marksusa.com)

LocDown is a trademark of Marks USA/ Napco Security Technologies, Inc. For full warranty details, consult manual or see terms online.

Request information: [www.SecurityInfoWatch.com/10215125](http://www.SecurityInfoWatch.com/10215125)

See us at ISC East, Napco Booth 903

 **NAPCO**  
SECURITY TECHNOLOGIES

# CONTENTS

## COVER STORY

- S6** **Campuses Strive to Strike a Balance Between Technology and Policy**  
– Tim Kridel

## SCHOOL SAFETY & SECURITY

- S4** **Modern Systems for Enhanced Campus Security**  
– Rick Taylor
- S10** **Schools Must Assess Risk Prior to Implementing a Plan** – Tim Kridel
- S14** **K-12 Security and Technology Experts Weigh in on Strategic Security Planning and Organization**  
– Steve Lasky
- S18** **How Dangerous Myths About School Active Shooters Increase Casualties** – Michael Dorn

## COLUMNS

- S22** **My Point of View**  
What Can We Do to Fix a Broken School Security Blueprint? – Steve Lasky

## AD INDEX

Company Name	Page	Web Site URL
Access Hardware Supply	S13	<a href="http://www.securityinfowatch.com/10722906">www.securityinfowatch.com/10722906</a>
Aiphone Communications Systems	S9	<a href="http://www.securityinfowatch.com/10212724">www.securityinfowatch.com/10212724</a>
ASSA ABLLOY DSS	S11	<a href="http://www.securityinfowatch.com/10212899">www.securityinfowatch.com/10212899</a>
Bold Group	S15	<a href="http://www.securityinfowatch.com/10215780">www.securityinfowatch.com/10215780</a>
Evolv Technology	S17	<a href="http://www.securityinfowatch.com/21214371">www.securityinfowatch.com/21214371</a>
Genetec Security Center	S24	<a href="http://www.securityinfowatch.com/10213771">www.securityinfowatch.com/10213771</a>
IP Video Corporation	S21	<a href="http://www.securityinfowatch.com/10239527">www.securityinfowatch.com/10239527</a>
Milestone Systems	S23	<a href="http://www.securityinfowatch.com/10214397">www.securityinfowatch.com/10214397</a>
NAPCO Security Technologies	S2	<a href="http://www.securityinfowatch.com/10215125">www.securityinfowatch.com/10215125</a>

This directory is provided as a service. The Publisher assumes no liability for errors and/or omissions.

Cover photo: SDI Productions / 1221435875 / Getty Images

# SCHOOL SECURITY & SAFETY



## PUBLISHED BY

1233 Janesville Ave  
Fort Atkinson WI 53538  
800-547-7377

School Security & Safety is a supplement to American Schools & Universities, Locksmith Ledger, Security Business and Security Technology Executive magazines.

## EDITORIAL

**Editorial Director** | Steve Lasky  
**Editor, American Schools & Universities** | Joe Agron  
**Editor, Locksmith Ledger** | Will Christensen  
**Editor, Security Business** | Paul Rothman  
**Editor, Security Technology Executive** | Steve Lasky  
**Editor, SecurityInfoWatch.com** | John Dobberstein

## SALES

**Group Publisher** | Jolene Gulley-Bolton  
480-524-1119  
[jjulley@securityinfowatch.com](mailto:jjulley@securityinfowatch.com)

### Northeast US & East Canada

**SB, STE, SecurityInfoWatch** | Janice Welch  
(224) 324-8508  
[janice@securityinfowatch.com](mailto:janice@securityinfowatch.com)

### Midwest

**Locksmith Ledger, SB, STE, SecurityInfoWatch** | Brian Lowy  
(847) 454-2724  
[brlowy@endeavorb2b.com](mailto:brlowy@endeavorb2b.com)

### Western US & Western Canada

**SB, STE, SecurityInfoWatch** | Bobbie Ferraro  
310-800-5252  
[bobbie@securityinfowatch.com](mailto:bobbie@securityinfowatch.com)

## PRODUCTION

**Production Manager** | Brenda Wiley  
[bwiley@endeavorb2b.com](mailto:bwiley@endeavorb2b.com)  
**Audience Development Manager** | Delicia Poole  
[dpoole@endeavorb2b.com](mailto:dpoole@endeavorb2b.com)  
**Art Director** | Eric Van Egeren  
[evanegeren@endeavorb2b.com](mailto:evanegeren@endeavorb2b.com)

## ENDEAVOR BUSINESS MEDIA, LLC

**Chief Executive Officer** | Chris Ferrell  
**Chief Revenue Officer/CMO** | June Griffin  
**Chief Financial Officer** | Mark Zadel  
**Chief Operations Officer** | Patrick Raines  
**Chief Admin and Legal Officer** | Tracy Kane  
**EVP/Group Publisher** | Lester Craft  
**EVP Marketing Solutions** | Jacquie Niemiec

## Subscription Customer Service

Toll-Free 877-382-9187; Local 847-559-7598  
[Circ.SecDealer@omeda.com](mailto:Circ.SecDealer@omeda.com)

## Article Reprints • Brett Petillo

Wright's Media 877-652-5295, ext. 118  
[bpetillo@wrightsmedia.com](mailto:bpetillo@wrightsmedia.com)



Photo: Robert Hoetink / 82058978 / Bigstockphoto.com

# Modern Systems for Enhanced Campus Security

Upgrading a security system may feel daunting but there are options to fit most retrofit budgets **By Rick Taylor**

**M**ost schools today have adopted electronic access control and video surveillance systems as part of their campus security. However, since many schools have added these systems over several years, they often have multiple different systems that do not share information or use outdated technologies that now have known vulnerabilities. This results in systems that are complicated, expensive to maintain, and difficult to use. After a while, the technology becomes obsolete and needs to be replaced. Campuses can spend significant time fixing their system or implementing workarounds, and maintaining the status quo becomes very expensive.

Keeping campus security systems up to date with modern security

standards is easier when you implement a unified security platform. A unified platform is easier to use, more effective, and may even cost less over time, thanks to lower maintenance costs.

## Actionable Insights for Faster Responses and Efficient Operations

Disparate security systems make it hard to see the big picture of your campus security operations. With a unified platform, you can view and interact with data from all of your systems in a unified platform dashboard.

When all components of your security system, including access control, video surveillance, sensors, and license plate readers, are monitored and controlled within the same intuitive software interface, security

***Schools are counting on security technology more than ever to help them mitigate risk to students and staff.***

teams can respond quickly and work more efficiently.

Nuisance alarms, for example, can be reduced with a unified platform that combines data from door sensors with live and recorded video from the cameras. With the additional information from these systems, your team can have more control over when the system should alert staff. Both systems may tell you that a door has been opened for longer than usual, but only the system with unified video surveillance and analytics can let you quickly see if there's an obvious reason why. With more context about what's happening, you can decide whether or not someone needs to investigate in person.

If certain kinds of nuisance alarms are especially common you can even configure the system to be more selective about when to sound the alarm. For example, automated alerts



can be set if a door is left open for more than a specified number of seconds or only if the door is open and no person is present within the field of view of a camera positioned at that door.

Intelligent analytics can help you optimize security, allocate resources more effectively, and reduce the load on staff. You can see which doors or sensors set off alarms most frequently, and pull in data from video cameras, sensors, and other systems such as license plate recognition, to get a better understanding of why this is happening. You can also set up automated reports to identify hardware that isn't working properly or behavioral trends on campus that help your facilities managers address recurring or potential problems.

### **Video Surveillance Balanced with Privacy Protection**

When there is an event that requires investigation, such as vandalism or a report of an assault on campus, intelligent analytics allows security teams to go back and reconstruct what happened by pulling recorded video from that time and location, as well as any other relevant data from access control or license plate readers that might help identify the people involved. If the event is happening in real-time, security personnel can use this data to guide first responders, so they have real-time situational awareness before they arrive on the scene.

With so much data available at your fingertips, modern security systems must also consider privacy protection as a fundamental aspect of operations. Privacy isn't just important in sensitive areas on campus such as locker rooms and residence halls. Nobody wants to feel "watched" while moving through their daily routines.

Thankfully, it is possible with today's technology to protect individuals' right to anonymity. Campuses don't have to compromise security for privacy. Instead, modern video management software (VMS) can be configured to pixelize or mask individual

identities by default. Permissions can be granted to select staff members to depixelate the footage if the video needs to be reviewed for an investigation. The system can require multiple people to sign off on the request as a further check to ensure personally identifiable information is protected, the unified platform will report on which personnel retrieved the recorded video.

If video footage must be shared with police investigators, media, or members of the public, faces can also be unmasked for officers with the appropriate permissions. For example, the version shared with the public may have almost all faces blurred, while police or legal teams can be assigned secure credentials to view the original unaltered version. By requiring the video to be viewed only through a secure platform, your campus security can keep track of who has seen, downloaded, or shared the video, and can adjust permissions on a dynamic basis.

### **Access Control Management Through Automation**

Another important aspect of modern security systems is access control. In a unified system, access can be defined by role and can be granted or revoked easily as needs change. For example, access control can be linked to faculty, staff, and student profiles. When a student changes majors or residence halls, or a staff member changes office locations or roles, their permissions are reassigned automatically.

On college campuses, professors can even be given the authority to temporarily grant after-hours access to labs, libraries, or practice spaces to students as needed. If a student drops a class or graduates, the system can automatically remove access as well.

For visitors, access can be granted on a temporary or location-specific basis. For example, a guest speaker may have access to select campus spaces for the day they are scheduled to present, but this access will automatically be removed after the allotted time has expired.

### **Upgrading with Scalable Security Systems**

Unified platforms are built to be scalable and modular so you can upgrade or scale gradually as your campus's needs change. A unified system can serve a small K-12 school with a couple of hundred cameras and dozens of access points or a sprawling university complex with 20,000+ cameras and hundreds of access points — and everything in between.

Furthermore, a unified platform allows you to integrate elements such as automatic license plate recognition, sensors, and video analytics that monitor the outer perimeter of your campus. This helps you expand a "net of safety" beyond the walls of the building. The sooner you can detect something out of the ordinary, the more time your team has to respond to potential threats.

Upgrading to a modern security system may feel daunting but the good news is that in many cases, you won't need to replace the equipment you've invested in over the years. With a unified, open-architecture software solution, you can often reuse many hardware components you already have in place. This allows you to prioritize upgrades or plan a gradual transition one step at a time. The result will be not only a safer campus but also a more efficient and effective security operations team. «



**About the author:** Rick Taylor is the National Director of the Public Sector for Genetec. Rick joined Genetec in April 2013 as a Regional Sales

Manager. He was then promoted to Regional Sales Director for the Central U.S. before moving into the position of National Sales Director for Public Sector in November 2020. In his current role, Rick is responsible for leading his team in developing strategic plans within the public sector. Prior to his start at Genetec, Rick gained nearly a decade of experience in the security field, including positions as District Manager at both UTC Fire & Security and GE, and as Vice President at Esscoe for the company's Security Practice.



# Campuses Strive to Strike a Balance Between Technology and Policy



Photo: SDI Productions / 482576863 / Getty Images

Experts agree that technology is useless unless properly implemented with a comprehensive security strategy **By Tim Kridel**

***Districts, colleges and universities must strike a balance between responding to parents' and students' concerns about the latest headline-grabbing incident while still devoting enough resources to other risks.***

**T**here's something to be said about a two-way radio blaring in a hallway or classroom — and it's not all good. On the one hand, the chatter continually reminds students that their safety is a top priority. But on the other, the cacophony disrupts the learning and teaching environment.

Radios are just one example of how schools and higher-ed institutions have to weigh the additional

security of technology or policy against side effects such as disruptions and restrictions that faculty and students find onerous.

"PreK-12 school administrators have walked a tightrope for decades trying to balance having reasonable security and emergency preparedness measures with a welcoming, supportive climate conducive to their mission as child-oriented educational community centers," says Kenneth S. Trump,

National School Safety and Security Services president. "This challenge has intensified as mass school shootings, as well as other 'unknown unknowns,' present growing challenges to creating and maintaining secure and prepared campuses."

Those considerations prompted Olathe Public Schools to issue CrisisAlert badges to faculty and staff, which they can use to put their entire building on lockdown. This enables

them to respond immediately rather than waiting minutes to reach an administrator, explain the situation and finally get a lockdown.

“Obviously, our No. 1 priority is to keep our students and staff safe, but student learning is right behind that,” says Jim McMullen, the Olathe assistant superintendent who oversees safety services. “Finding that balance of a welcoming environment for kids and teachers while also providing the safest environment that you can is really our end goal. That’s why we felt this product was great.”

And unlike a radio, the alert is shared silently.

“We were a district that was very heavily reliant upon building radios, especially at the elementary level,” McMullen says. “This takes the place of the need for as many radios within a building. If a teacher needed assistance, anyone in the building could hear who needed assistance and why. That can be a disruption and a privacy issue, as well.”

Districts, colleges and universities also must strike a balance between responding to parents’ and students’ concerns about the latest headline-grabbing incident — such as a mass shooting — while still devoting enough resources to other, more everyday vulnerabilities. That’s another reason why Olathe chose CrisisAlert: Eight pushes trigger a lockdown, but fewer ones send an alert to the office.

“[We have] the ability to utilize this product not only in a worst-case active shooter scenario but also on crises that happen every day in schools across the country: behavioral, medical, the occasional fight, that sort of thing,” says Brent Kiger, Olathe executive director of safety services.

Besides CrisisAlert and walkie-talkies, districts also can leverage a device that every member of the faculty and staff already owns: a smartphone. In theory, which sounds like a great idea because means the security budget doesn’t have to fund thousands of specialized devices. In reality, their effectiveness is at the

mercy of coverage: the mobile operator that each employee uses and the district’s Wi-Fi network. Dead spots can become — literally and unfortunately — dead spots.

“There are a lot of things that pretty quickly rule out certain products for me,” Kiger says. “Some of those are if it’s heavily reliant upon Wi-Fi or cell phone coverage. Those are huge barriers for me.”

## Security Obscurity

Olathe uses CrisisAlert to control a locking mechanism on the bottom of doors that drops a pin into a floor plate.

“It really provides an opportunity for staff members with vulnerable kids to lock down quickly and provides a barricade without having to move furniture, file cabinets, etc.,” McMullen says. “No one really even knows it’s there.”

Hidden locking mechanisms and badges that look like ordinary ones are ways to hide new security and safety tools, so they don’t disrupt the learning experience. But doesn’t “out of sight, out of mind” also make students feel vulnerable? Possibly, but opting for high-profile measures such as metal detectors can backfire.

“A skewed focus on security products, hardware and technology often result in more ‘security theater’ than it does a meaningful, comprehensive school safety strategy,” Trump says. “Target hardening may make people feel more emotionally secure, but it doesn’t necessarily mean that it will actually make them safer. As a civil litigation expert witness on school safety lawsuits, while the facts and merits of each case vary, a common theme is that they involve allegations of failures of human factors — training, policies, procedures — than they do alleged failures of security hardware and equipment.”

## Cameras Shouldn’t Be the Only Eyes

People are another example of how the most effective security measures often are hiding in plain sight.

“We like to recommend technologies to enhance school safety, but

you can’t replace that human factor in awareness,” says Bob Klausmeyer, education safety coordinator at the Missouri School Boards’ Association (MSBA) Center for Education Safety. “First and foremost, it has to be that change in culture to where everybody makes themselves more aware of what’s going on.”

One example is training faculty and staff about how not to inadvertently undermine technologies and policies.

“You can put lockdown devices in doors, but if somebody props it open, then what good is it?” Klausmeyer says. “They become so reliant upon it [that] they become less aware because they believe that’s going to keep them safe, and it doesn’t.”

Another example is creating an environment that facilitates trust and is thus willing to share information, such as with SROs.

“The first and best line of defense is a well-trained, highly alert staff and student body,” Trump says. “The No. 1 way we find out about weapons, kids who have plotted to cause harm and individuals who are considering self-harm is from students who come forward and tell an adult that they trust.”

Olathe agrees.

“When they have a trusted adult, they will report things that they’ve seen online,” McMullen says. “We have students send things on to teachers or coaches that they see online at night. We get that to Brent and our safety services division, and they work with local law enforcement. We get things taken care of well before school starts the next day.

“The welcoming environment and the relationship pieces are critical. Without that, you just lose that communication and trust, which is essential to preventing the crisis in the first place.”

Faculty, staff and administrators also should be encouraged to say something when they see something.

“I’ve got five board members that live on social media,” says Mark Skvarna, Montebello Unified School District interim superintendent. “They’ll say: ‘Such and such said this. This group said that.’”

## Bring in the Experts

All security/safety technologies and policies share one vulnerability: If people are unwilling or unable to use them, they'll look for ways around them, which can result in even greater risks. To avoid that problem, get input from all types of end users.

"When they're developing emergency operation plans, we recommend that they bring teachers, custodians, everybody in as a part of that development process to get their ideas and their experience," Klausmeyer says. "Make it so it works for everybody because it's not going to be good if they're uncomfortable with it or if it inhibits their jobs."

For example, teachers might ferret out problems with a technology's user interfaces and other aspects that otherwise would remain hidden until after implementation.

"If you're an administrator, and you haven't been in a classroom for 15 years, your teachers might think of something that you hadn't thought about," says Amy Roderick, director of the MSBA's Center for Education Safety.

But others caution against extending the feedback process with a trial, such as a couple of schools or a handful of campus buildings.

"I have been in law enforcement 38 years and director here for 17," says Kevin Grebin, University of Sioux Falls director of campus safety/security. "I learned early on that if we would float out the trial balloon, the process would get delayed and most likely never applied. We do look at other universities for information on new technologies and processes to hopefully see what problems to avoid on our end."

Finally, scrutinize feedback and other input instead of simply incorporating it at face value. That's one lesson learned from Columbia College's panic button implementation.

"Everybody wanted panic buttons on their desk," says Klausmeyer, who was head of campus safety before joining MSBA. "We put a few and we were very careful where we put them. But even so, we received so



Photo: gradyreese / 909472296 Getty Images

**Olathe Public Schools have issued CrisisAlert badges to faculty and staff, which they can use to put their entire building on lockdown.**

many false alarms because somebody either knocked them with their knee or just played with them. It became that cry wolf situation: 'Here we go again.'"

Some districts and colleges also look at other professions for ideas. For example, Montebello's Skvarna consulted his brother, who is the police chief at Burbank Airport.

"I did a lot of research on how they were handling open spaces, entrances, exits, hallways, and what type of locking equipment they use," he says.

Many hospitals require visitors to wear a badge, which enables staff to identify at a glance people who have snuck in. Some districts are applying this model. For example, about four years ago, Olathe implemented the Raptor visitor management system. When visitors check in at the front office, the system scans their driver's license so it can add the person's picture to a badge that they must wear. At the same time, Raptor also runs a check against the sex offender registry list.

"That's another layer of security," McMullen says. "It allows us to catch them on the front end. When a staff member sees an adult in the building that they don't recognize, they need to have a badge on."

## Shuffling Priorities

Another balancing act is prioritizing budgets, staff and other resources. For example, shootings are relatively rare,

but they also can dominate to the point of distraction.

"It's easier for them to lose focus on other potential threats or hazards that could occur — and might be more likely to occur — than an event like an active shooter," Klausmeyer says. "There are other things as simple as a gas leak or a fire that could be just as devastating. They need to focus on the broad spectrum of potential hazards and threats instead of just one area — even as devastating as that one event could be."

High-profile events can completely upend how a district or college looks at security.

"Funding school safety initiatives and strategies usually isn't number one in the budget," Roderick says. "So then when you respond to situations such as Uvalde, now it's become important, and you're trying to figure out how to fund what you want to do without having previously thought about that."

"Whether a major event triggers that or not, it just needs to be in the normal course of your annual budgeting: what our needs, whether it's perimeter fencing or radios or fire sprinkling systems. If you're doing renovations or adding on to the structure, you've got to think about those safety measures and budget for that."

Similar considerations and challenges apply at the collegiate level.

"The administration will be reactive to such events, but they also are

very supportive of my introduction of preventive measures, too, [such as] increased staffing, collaborating with our Neighborhood Watch groups, increased training, new surveillance techniques," Grebin says.

Even so, it's not necessarily a bad thing when high-profile events push certain upgrades up the priority list. For example, in August, a sex offender scaled a chain-link fence around a Riverside, Calif., elementary school and attempted to assault a student in a restroom. That prompted Montebello to replace its fences with ones that can't be scaled.

"It actually looks better than your standard chain link," Skvarna says. "It doesn't make it look like an institution, yet you can't get over it."

Uvalde also prompted Montebello to make changes — major ones.

"I believe that there was such a lesson with the failures in Texas that it

couldn't be ignored," Skvarna says. "I didn't believe it to be an overreaction to consider this. I think it's in our best interest to be proactive, and it's going to cost money: \$6 million or \$7 million.

"The board did not get involved where they said, 'We want you to do this.' I went to the board and said, 'We need to consider an emergency resolution.'"

One initiative is a complete overhaul of Montebello's surveillance network. That's also an example of how a major event can lead to funding for long-overdue projects that might otherwise continue to languish.

"We had cameras that were very, very old," Skvarna says. "We had ones that weren't working. We just had a hodgepodge of a bunch of junk. All of that is being replaced. We're also adding new cameras where they're needed."

Whether it's new cameras, new fencing or something else, it also helps

to educate the public about how their votes directly affect safety.

"We're very fortunate our community supported a bond issue last March," says Olathe's McMullen. "We had four threads to that bond, and one was safety. It has been on every bond we've passed in recent memory, so our community really supports safety measures and initiatives. We've also received some state grants, and we're currently looking at a couple on the national level. I think you have to be creative." ◀◀



**About the author:** *Tim Kridel is a freelance writer who has been covering a wide variety of technologies since 1998, including enterprise IT, video collaboration, cellular and Wi-Fi. For more information, visit [www.timkridel.com](http://www.timkridel.com).*

# AIPHONE

## Dynamic Security Solutions for Campuses and Commercial Properties



Our commercial IP intercoms provide campus-wide **communication, convenience, and controlled access.**



Scan QR code.

Look for the play button and watch our video to see how an intercom can help secure your campus.



Request information: [www.SecurityInfoWatch.com/10212724](http://www.SecurityInfoWatch.com/10212724)



*If the school district has not conducted a risk and vulnerability assessment, a security consultant can educate the school district on the importance of conducting a threat, risk and vulnerability assessment prior to making any physical security technology changes to their security program.*

Photo: gradyreese / 903472296 / Getty Images

# Schools Must Assess Risk Prior to **Implementing a Plan**

Creating a strategic security roadmap helps administrators understand critical shortcomings needing to be addressed

by **Jim Townzen, PSP, CPP**

**W**e are often contacted by school administrators with a Request for Proposal (RFP) to provide professional physical security consulting services. When we review the RFP, we learn that they want to add some type of physical security technology enhancements for their school district. Once we have been selected as the consulting firm for the project, one of the first questions we ask is, "Can we review the most recent threat, risk and vulnerability assessment?"

Often, we learn that the school district has not conducted a threat, risk and vulnerability assessment to ascertain what the real threats, risks and vulnerabilities are to their district. In other words, we are being asked to specify and design physical security technologies for their district without understanding first what risks we are mitigating. This process of not knowing what the true needs of the school district are can be expensive for the district when poor decisions are made and oftentimes does not address the real

issues for “we do not know what we do not know” at this point. Oftentimes, school districts are reacting to public opinion to do “something quickly” following a recent catastrophic event. The Uvalde School District incident in Uvalde, Texas is a recent example.

If the school district has not conducted a risk and vulnerability assessment, we do our best to educate our contact with the school district on the importance of conducting a threat, risk and vulnerability assessment prior to making any physical security technology changes to their security program. All too often we are told that the money set aside for the physical security technology enhancements does not include funding for a district-wide threat, risk and vulnerability assessment. We are usually told that an assessment has already been conducted by the school administration, and they just need someone to assist them in the creation

of an RFP, hire a contractor, and project manage the installation and testing of the systems. In our thirty-plus years in this industry, we have rarely seen this scenario turn out well.

**Why should a school district conduct a district-wide threat, risk and vulnerability assessment prior to making changes to their existing security program?**

A threat, risk and vulnerability assessment is an evaluation by a physical security professional of the district’s current security program. This process includes a careful and methodical process to identify the district’s risks through a thorough fact-finding and evaluation process that includes the identification of the district’s tangible and intangible assets including people (in the eyes of the public, particularly the parents, the number one asset are the children and the families.), facilities,

equipment, intellectual, critical issues, applicable standards and reputation as a community resource, as well as the development of mitigation strategies that are appropriate for the district’s culture and capabilities and the risks within their environment.

The consultant will review the district’s security program to identify those threats, risks and vulnerabilities faced by the district that are either not optimally addressed or addressed at all. Once these risks are identified, the consultant will analyze the potential effect of these threats and exploited vulnerabilities in terms of likelihood of occurrence and severity of impact to determine and prioritize the most effective actions for mitigating risk. Other critical aspects of the assessment process include taking a holistic approach to evaluate the entire program from security technologies, the people involved in keeping

**ASSA ABLOY**  
Opening Solutions

Experience a safer  
and more open world

## Creating access *for the future*

Today it may feel more difficult than ever to ensure an ideal learning environment. However, with an approach that balances safety, security and wellness, you can create an atmosphere that provides peace of mind for students, faculty and staff.

Helping schools create a safe and secure learning environment is a top priority for ASSA ABLOY. We are here to help you evaluate your safety and security needs and assist with any questions or concerns you may have.

Learn more:  
[assaabloydss.com/SIW-K12](https://assaabloydss.com/SIW-K12)



Copyright © 2022, ASSA ABLOY Sales and Marketing Group, Inc., an ASSA ABLOY Group company. All rights reserved. 545 - A 10/22

Request information: [www.SecurityInfoWatch.com/10212899](http://www.SecurityInfoWatch.com/10212899)

the district safe, and the processes/ training in place to ensure everyone knows their roles and responsibilities in emergency situations.

**What should your school district expect during an assessment and what involvement will be required from your staff?**

- The firm that is selected will take a deep dive into your existing security policies and procedures looking for any improvements that can be made based on current best practices.
- Stakeholder interviews are very important in understanding if security practices currently in place are working/not working as well as get a firsthand understanding of the real-life implementation of district security policies.
- Physical review of the schools before, during and after school hours to get an understanding of circulation patterns (people and vehicles) from the outermost part of school property into the classroom.

The assessment team will review the physical security technologies in place to see what is in use and what gaps may be inherent in the design of the system and if there are any opportunities for improvement. Systems that would be reviewed include:

- Electronic Access Control
- Visitor Management
- Video Surveillance
- Intrusion Detection
- Mass Notification
- Metal Detection
- Weapons Detection

Last, but certainly not least, is a thorough review of the property to assess lighting, sightlines, perimeters, areas of concealment, remoteness, accessibility, surrounding properties, fencing and public access after school hours.

**What is the value of a risk and vulnerability assessment for your school district?**

Plain and simple – it serves as a road-map. Once the team has conducted a thorough assessment, the district will receive a report that goes into detail identifying the security gaps found and recommendations on how to mitigate those gaps. The assessment report

## A threat, risk and vulnerability assessment are an evaluation by a physical security professional of the district's current security program.

provides a holistic view of the district's entire current security program and not just one aspect of the program. A successful security program consists of the right mix of people, policy, and technology.

The road map will prioritize the recommendations to help the district determine short-term, mid-term and long-term planning needs that can be incorporated into their overall district master plan. Although it is tempting to use internal staff, local law enforcement, parents, or an online tool to conduct an assessment of the security program, the benefit of using a firm that does this every day and has the expert knowledge on how to best mitigate risk in a school environment brings tremendous benefit to the district.

### Conclusion

By reacting to pressure and not taking a holistic view of your security program you are, albeit inadvertently, doing a disservice to students, staff, parents and visitors who enter one of your campus buildings. A security program is a multi-dimensional approach to addressing your known threats, risks and vulnerabilities so without conducting a threat, risk and vulnerability assessment you're not looking at the entire picture.

Invest in a professional security consulting firm with experience commensurate with your school district. Pay close attention to the credentials of their team and make sure you hire a firm that specializes in physical security consulting. Keep your threat, risk and vulnerability assessment report

separate from your facility master planning as you may have information in the report that needs to remain confidential for the protection of students, staff, and visitors. Make sure that any plans that require construction or construction enhancements are shared with the architect who is implementing your facility master plan so that they can be executed as part of other budget items in the facility master plan.

As administrators, be honest and open with your assessors and encourage your staff to do the same. Bringing outsiders into your 'house' and sharing your known vulnerabilities is and can be uncomfortable but keep in mind the more honest you are the better solutions your assessors can provide you with mitigation methods and best practices. It is in your best interest that you use an outside firm to conduct this assessment as it will bring merit to those items you have been bringing up for years, but it also could bring to light other items of which you were unaware.

In conclusion threat, risk and vulnerability assessments are a vital part of every security program and should be used to guide your security program as well as your security budget. Hire an experienced firm, be open and honest, integrate your security plan into your facility master plan as necessary, and conduct these assessments at regular intervals every three to five years. ☞



**About the author:** Jim Townzen, PSP, CPP is a Staff Consultant for Security Risk Management Consultants, LLC in Ohio.



# THREE OF THE BEST



# CLOSERS

## AT INCREDIBLE PRICES

Ready to ship today at [accesshardware.com/nortonrixson-closer-sale](https://accesshardware.com/nortonrixson-closer-sale)

Request information: [www.SecurityInfoWatch.com/10722906](https://www.SecurityInfoWatch.com/10722906)



Where Service Meets Expertise.  
[accesshardware.com](https://accesshardware.com) | (800) 348 - 2263



# School Security **INSIGHTS:** Project Planning and Implementation

K-12 security and technology experts weigh in on strategic cybersecurity planning and organization **By Steve Lasky**



*The best place to start a security program is to seek out help from others for planning. This can mean professionals from other districts, security integrators as well as academics, and IT from within the district.*

Photo: Rawpixel.com / 121244216 / Bigstockphoto.com

**H**ave you ever gotten “Google Overload”? Have you ever searched for a symptom and found out that you’re dying of a real disease? If you’ve ever tried searching online for advice on security planning, your experience was most similar. The best advice always comes directly from industry professionals. Two K-12 security experts were asked to give advice on starting a security plan from the ground up.

We talked to Chris Montgomery, who is the Network Services Manager for Tomball, Texas ISD and has been with the school district for more than 26 years, along with Troy Neal, currently the Executive Director of Cybersecurity and Operations for Spring Branch, Texas ISD. Neal has worked as a cybersecurity professional in the K-12 school sector for more than 13 years.

The first step to building a security plan is to figure out the scope of your project.

**If a new school district approached you, how would you advise them on the best way to start a security program?**

**Chris Montgomery:** “You need a scope. Realize that you are not a security professional and that you will need help to develop a comprehensive security program. Reach out to other local school districts and ask

about systems and partners. Reach out to your local law enforcement as they often have resources dedicated to helping develop these programs. Reach out to the other departments and your administration to ensure cohesion and integration with the different parts and systems in the plan. A good partner will help you determine your technology needs, such as camera types, video storage, switching ports, and bandwidth

## Alarm Monitoring and Business Management Software for the Security Industry



For **over 40 years**, Bold Group has empowered security organizations with the most comprehensive array of alarm monitoring and integrated business management solutions tailored to achieve optimal outcomes and growth for security teams, central monitoring stations, dealers, and integrators.

**BOLD**  
GROUP

TO LEARN MORE VISIT [BOLDGROUP.COM](http://BOLDGROUP.COM)

Request information: [www.SecurityInfoWatch.com/10215780](http://www.SecurityInfoWatch.com/10215780)



requirements. A good partner will also assist with knowledge of any federal/state money that can be used to implement your plans.”

**Troy Neal:** “You have to have a philosophy first. Take physical security and cameras in general. What are you trying to solve? Is it just building security? Physical security, technology, academ-

*from other districts, security integrators as well as academics, and IT from within the district. All parties involved should be on the same page and meet regularly to ensure the security program is meeting the needs of everyone. The next step is working within the budget. Funding for K-12 is limited, so accounting for needs versus wants also requires the help of everyone at the table.*

And some of those are not built to an enterprise standard. They don’t develop it, they don’t have the life cycle and so you’re dealing with some of this great-looking software, but you can’t get data out of it. You can’t move data. Data drives everything; same with security. The more data points I have, the better holistic view I have of the organization. Our biggest challenge in K-12 is money. Especially with so much of this cloud-based software. We are not funded to pay for that. The subscription-based software is the hardest thing for me to pay for because that comes from general funds. In schools, 85% of your budget is spent on salaries. It’s people which are the most important piece of education. How do you find those mechanisms?”

*The first step to building a security plan is to figure out the scope of your project. Then verify the legal requirements. Next, move to planning for the basics like cameras, access control and fire alarms. Make decisions now that will solve your current needs, but also continue to work in the future without compromising your philosophy.*

## Storage upgrade requirements and yearly pricing increases in subscription-based software are limited by the strict budgets of K-12 schools.

ics, and operations all have to be on the same page and discuss it together versus one person making all the decisions. That’s where a lot of failures happen between academics and technology. We should be true partners. From there, then, what’s your strategy? How do you want to get there? What are your long-term costs? Can you scale it? Can you manage it? Who’s going to own it? The biggest problem we have in technology alone is, “Who owns it?” If somebody doesn’t own it, it’s always going to fail. Who’s your executive sponsor? It’s true project management from the start. All of our projects are done by a project charter. Bring in industry experts. Talk to other school districts and find out what they do. Find out what fits the organization and then plan where you want to go with it. Size means a lot. Run it like an enterprise. From a technology and security standpoint, you’re never in the way of things. And I think that’s where it starts.”

*The best place to start a security program is to seek out help from others for planning. This can mean professionals*

### If money were no object, how would you build out your security plan and in what order would you implement it?

**Montgomery:** “Develop a thorough scope that will solve your security needs. Choose a partner that understands your needs and has resources available to assist you. Determine which systems you will use to solve your needs and build an infrastructure that will support them now and in the future.”

**Neal:** You’ve got to look at local policy and legal policy because we have to follow all of that. You have state laws and federal laws. You have to figure out those parameters first. What are your basics? Cameras, you want to be able to see who comes in and out. You want people to badge in and out. Fire alarms, all the mandatory stuff. Then, how do you start tying in other things? The problem in K-12 is that there are certain systems we have to use, whether we like them or not.

### What changes have you seen over the last few years after security upgrades and integration?

**Montgomery:** “The number of resources used by our security devices (storage, bandwidth) has increased greatly on a scale that we have found ourselves unprepared for.”

**Neal:** “A lot of security software has gone cloud-based and subscription-based. This is where schools are really struggling. The way our budget cycles and planning is, we start budget conversations in October for the next school year. The biggest problem is the cloud part of it. Second, is the complexity of the software. You need a certain level of talent to get people to be able to own it and manage it. If you don’t have a philosophy or roadmap, someone is going to want this shiny object. Then it’s this next siloed system that you’ve got to manage and maintain. So, you start building

out these cool things, but then they become despaired again. Ideally, there would be a holistic integrated kind of system from the start. You have to have a different model for us to pay for things, especially in regard to the licensing for K-12."

"In regard to changes in physical security, a lot has helped because a lot of it now talks together. The hurt is, they still don't have industry standards. Just like we update standards in education and in the world, you've got to have very basic standards that things talk to one another. Especially in physical security, things don't talk to each other by design, and that's a problem. We need industry standards that force organizations and companies to say, "look you need to be able to talk based on this protocol." So, then I can take this information and use it in another system. Going

back to data and physical security, the most important part is protecting the entrance of a building and ensuring there is no unwanted person or thing coming through a building. Access control technology and simple things like badging and turning off alarms have all grown. In schools, a lot of them are not there yet. You've got schools built in the '50s and up. The cost to redo all of this even from a cabling standpoint is a lot. Standards are the number one thing. Just build it to an industry standard that's then safe and secure."

*Planning, and planning early is of the utmost importance when considering upgrades in security. Storage upgrade requirements and yearly pricing increases in subscription-based software are limited by the strict budgets of K-12 schools. Avoid getting caught up in buying software that can cost more money than originally budgeted for. Although many*

*improvements have been made, more efforts should be made to push for industry standards in physical security that would benefit everyone.*

*Schools have always been the place where members of the community come together to collectively educate and protect children, and their futures. Having a plan for creating a safe school starts with designing and building out a security plan. Planning should involve communities coming together from local school districts, law enforcement agencies and security integrators alike. When these groups can have vulnerable, productive conversations, real changes can be made for everyone's benefit. Involving voices from many spheres to share their successes, and more importantly, failures will only strengthen security in schools to protect our future generations to come. Now go, be vulnerable and reach out; build the security program your school needs. ❧*



The world is growing increasingly unsafe and incidents at schools are rapidly on the rise. If you are responsible for the safety of your students, faculty, staff, and visitors, now is the time to familiarize yourself with the benefits of transforming your physical security screening.

**Learn how Evolv is helping schools take a proactive stance against the threat of violence and ensure a safe learning environment.**

**evolvtechnology.com**

Request information: [www.SecurityInfoWatch.com/21214371](http://www.SecurityInfoWatch.com/21214371)

**evolv™**



# How Dangerous School Active-Shooter Myths **Can Increase** **CASUALTIES**

Schools must be able to identify and implement proper training procedures and policy to make security work

By Michael Dorn

*Poor active shooter training programs have thus far been a contributing factor in school shootings where more than \$130 million in out-of-court settlements have been paid by school systems and law enforcement agencies*



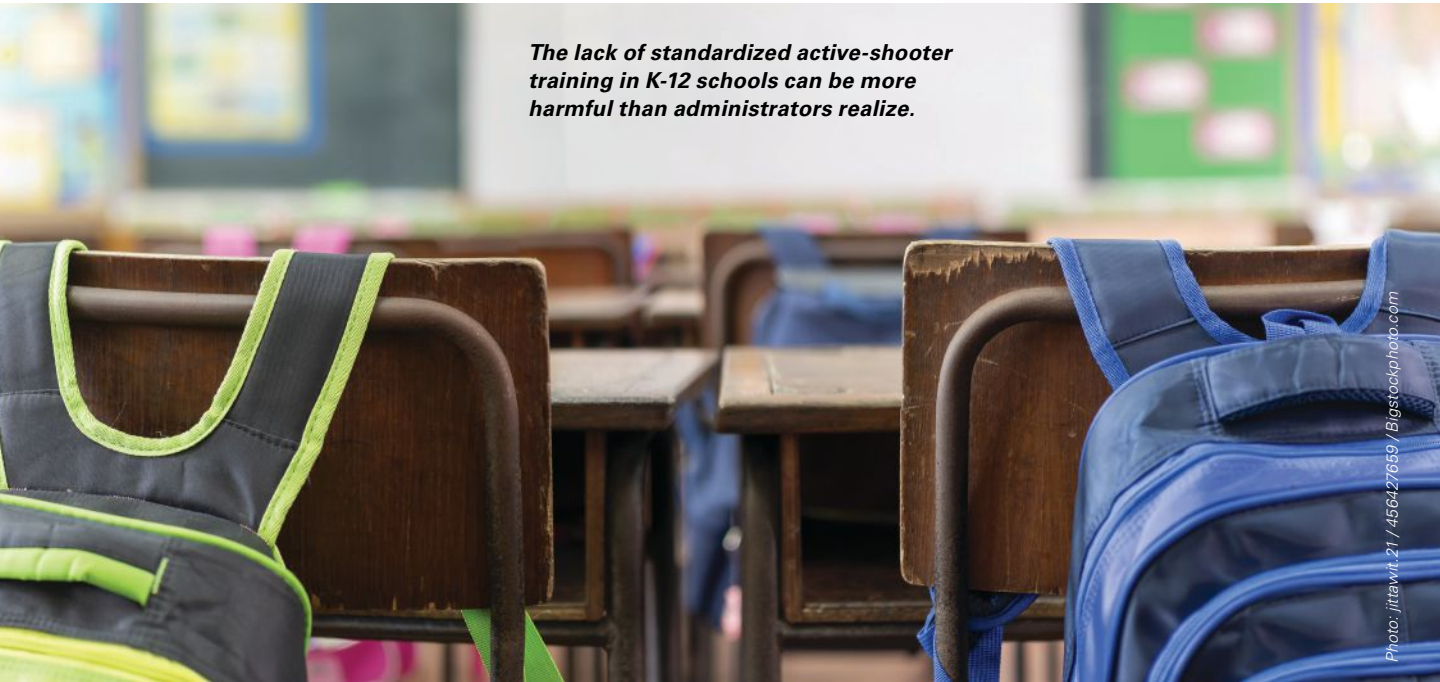
Upon hearing the instructions to lock down, a teacher and students move briskly to place chairs, desks and tables in front of the door to their classroom to prevent an active shooter from forcing entry to their classroom. Next, the students and teacher arm themselves with books and other objects to throw at the attacker's face and prepare to "swarm" the attacker. Sadly, this is not just a hypothetical example of how some schools with the best of intentions are spending precious time, energy and budget to increase rather than decrease the risk of harm to students and staff.

The various active shooter training programs that teach these types of approaches that have increased casualties in multiple school shootings provide but one example of the types of popular but dangerous approaches that are causing increased fatalities in U.S. K-12 schools. In fact, these types of active shooter training programs have thus far been a contributing factor in school shootings where more than \$130 million in out-of-court settlements have been paid by school systems and law enforcement agencies – in just a few of the school shootings our center's analysts have worked with litigation for other shootings ongoing.

Unfortunately, our experience providing official post-incident assistance for 23 active assailant and targeted shootings in K-12 schools in three countries, show that actions such as these clearly increase rather than decrease the danger to students and staff in most K-12 school shootings. But how could these alleged "best practice" approaches increase rather than decrease danger?

### **Know The Drill!**

For starters, having timed well-practiced teachers and high school students who barricade in this fashion, we have found that it takes an average of more than 120 seconds to accomplish the above actions, which keeps occupants in an exposed position for longer periods than it took the attacker at Marjorie-Stoneman Douglas High School to shoot his first 24 victims



***The lack of standardized active-shooter training in K-12 schools can be more harmful than administrators realize.***

Photo: jittawit.21 / +56427659 / Bigstockphoto.com

worked on were shot in less than 90 seconds with many victims shot within the first seven to 43 seconds of a gun being observed.

The reality is that there has only been one K-12 school shooting in the United States where an attacker has forced entry into a locked classroom and subsequently killed occupants. In fact, the approaches taught in several of the more popular active shooter training programs fail to mitigate predominant attack patterns. Even though the “mega study” of school shootings recently conducted by the National Institute of Justice found that more than 50% of the people shot on K-12 school campuses around the country in the last 25 years, more than 650 that occurred were *outdoors* when they were shot, these training programs fail to address the far more important reverse evacuation tactics.

This severe training disconnect resulted in a catastrophic failure in a shooting on an elementary playground that personnel from our center observed as an expert witnesses. The litigation following this tragedy resulted in five sizeable out-of-court settlements in state and

federal jurisdictions. There are no easy answers to this complex problem in a nation with more students in school each day than the combined populations of Canada and Australia. Continuing to seek simple solutions to complex and challenging societal problems that lead to on-campus shooting ensure that more tragedies will occur unless realistic active-shooter strategies are embraced.

### **Misguided Active Shooter Training and Security Technology Implementation**

Flawed active shooter training programs are not the only critical problem seen from well-intentioned, but misguided school safety efforts. Oversimplified and canned emergency preparedness plans, unreliable emergency phone apps, dangerous emergency door locking devices, gun detection systems that do not work as advertised, incredibly expensive wearable panic buttons that are prone to malfunction and an array of other unsafe solutions have created havoc on school safety as fear-based mitigation methods have become more popular.

Our staff has also noticed school officials who are implementing security technologies that exceed the fiscal and staff resources over the long term. One extremely expensive and unreliable wearable duress button system incurs a yearly cost close to the initial installation cost. Most school districts or non-public schools will be unable to maintain the system over time. Many schools are less safe because precious limited time, energy and budget are being expended on solutions that are unreliable or fail to provide a viable benefit in relation to cost and staff time.

The time, energy and budget wasted on marginal types of security and safety solutions may also lead to preventable serious injuries and fatalities. Technology solutions that don't work are increasingly being used as powerful objective evidence against school officials in litigation. Common examples of solutions that fail to address significant risks are as simple as improving student supervision with training and electronic hall-pass systems or enhanced pre-employment screening and properly confronting traffic safety in parking lots. Other



boxes that can be checked include proper implementation of student threat assessment and management processes, use of effective self-harm prevention measures, upgrades to facilitate more rapid reverse evacuation from outdoor areas (if it is not safer to move away from the school in a particular event) and improving internal and internal public address capabilities.

### Misconceptions

One of the most critical observations derived from our more than seven decades working full-time in the field is that many of the perceptions surrounding school safety are seriously out of balance with reality. These misconceptions have been systemic since the tragic shooting at Columbine High School in 1999 and have become even more pervasive with every inaccurately publicized mass casualty attack.

Much too often, the severe disconnect between perceptions and facts that have given birth to the common refrain that there is an "epidemic of school shootings" in the United States, is an objectively false descriptor that can have serious ramifications in litigation if relied upon for determining school safety priorities. An "epidemic" is a public health term that defines a dramatic and rapid increase in a public safety threat over a short period of time. To be historically accurate, we would require an increase of thousands of school shootings in one or two school years to be truly considered a health crisis. This is not the case and among the reasons, the public health community has not declared school shootings to be an epidemic.

Much of the discussion and debate about reducing school violence oversimplifies complex societal problems. Comprehensive, locally tailored, assessment based and data-driven solutions to school safety may not make good media sound bites or be easy to implement but they are the most efficient way to create safe, welcoming and

The reality is that there has only been one K-12 school shooting in the United States where an attacker has forced entry into a locked classroom and subsequently killed occupants.

effective schools. In a nation with more quality free training, assessment and school safety planning tools than any place on earth, American school and public safety officials should not be negligent in utilizing them to develop practical and sustainable school safety strategies. «



**About the author:** The author of 28 books in his field, Michael Dorn serves as the Executive Director of Safe Havens International, the world's largest K12 school safety center. Michael's work has taken him to eleven countries during his 41-year career in the campus safety field.

**HALO SMART SENSOR**

**The Award Winning HALO 3C Device Protects Schools with Advanced Health, Safety & Vape Detection.**

- Chemical and Gas Detection
- Gunshot Detection
- Emergency Escape Lighting
- Air Quality Monitoring
- Aggression Detection and Calls for Help
- Disease Prevention with Health Index
- Motion & Occupancy Detection
- Vape and THC Detection
- Panic Button

**HALO SMART SENSOR**

[www.halodetect.com](http://www.halodetect.com)  
[info@ipvideocorp.com](mailto:info@ipvideocorp.com) | 631.969.2601

Request information: [www.SecurityInfoWatch.com/10239527](http://www.SecurityInfoWatch.com/10239527)



By Steve Lasky

# What Can We Do to Fix a Broken School Security Blueprint?

I have been writing about school shootings for more than two decades. As heinous and bone-crushing as each of them are, the most recent (up until this writing that is) in Uvalde, Texas seems to have shaken most security professionals to the core. Count me among them. The epic failure of local and state law enforcement during and after the shooting to address the threat, the utter confusion of school administrators to assess and react, combined with the shocking lack of basic security technology countermeasures created the perfect storm of chaos, coverup and carnage.

Over the years there has evolved a dual path of thinking related to school shootings, active-shooter protocols and preemptive security. One is couched in training and response and the other embraces technology implementation. My assessment is that both are critical to mitigating campus crime and violence, but there must be a symbiotic relationship between policy and hardware.

In the wake of the Uvalde shootings, this past June, Carnegie Mellon University's Biometrics Center hosted an online forum of experts in school security, law and technology for a special "School Safety Emergency Summit." (<https://vimeo.com/723133604/3e34e1c42c>). While one of the technology sponsors discussed the benefits of facial recognition as a lead element in a burgeoning AI-based technology environment for school and campus security solutions, veteran security professionals like Guy Grace, Vice-Chairman of the Partner Alliance for Safer Schools and a Unified K12 Life Safety consultant, was a bit more holistic.

"There is tremendous aftermath for years after a shooting. Uvalde is going to be dealing with this for the rest of their life. It's a cascading effect and it's all about how we mitigate that. Our mitigation is an all-hazards-type response [including] technologies that we use to support the response but also to support the aftermath of how we deal with these situations. Technology that empowers, it's a tool that we use to deal with the aftermath of these situations. It's multi-faceted when we're dealing with these emergencies. The technology measures... are there to detect, deter and deny... there are other security components that we need to have in place to nullify the effects or impact of a failure of one component. We have to be comprehensive when we're putting in these technologies not to just address an active threat situation, so we have to be thinking in an all-hazards sense in schools," stresses Grace.

Michael Matranga, the CEO of M6 Global security consultancy, a former U.S. Secret Service agent and a past director of security for Texas City ISD was adamant that the first responder to these types of events is not necessarily the law enforcement officer or the medical professional

"It's the person in the classroom right next door or in the hallway; we have to empower them for self-sustainability because we know that seconds matter in all of these things, whether it be in a school, whether it be in a grocery store, or in a shopping mall," he says.

Grace continues: "Everything we implement and purchase for schools, they are tools. They are going to be a unified life and safety system. The most important piece is going to be

the people and how do the people use those tools that we as security practitioners provide to our school districts and our communities to protect them."

Carnegie Mellon Bossa Nova Robotics Professor of Artificial Intelligence, Electrical and Computer Engineering Director Marios Savvides, Ph.D., provided an insight into the value of video surveillance used to help the FBI apprehend the Boston Marathon terrorist bombers. He laments that the data supplied was after-the-fact information and that today's goals are to prevent such incidents before they occur.

"While the killings are unacceptable no matter what you term them and are an unspeakable tragedy for the impacted families and communities, we have yet to acknowledge and clearly state: the senseless murder of Americans going about their daily lives should be addressed with the same focused and coordinated determination that our national security enterprise exhibits in preventing transnational and domestic terrorist attacks on the homeland. Let us not forget, the whole concept of homeland security gained prominence after 9/11 because of the need to protect Americans against the terror of attack as we went to work, traveled, and lived our lives," says Dr. Savvides.

He concludes: "It has been 10 years since the carnage at Sandy Hook elementary school. Following that mass shooting... we were part of the interagency team working at the White House, contributing to the President's plan to protect our children and our communities by reducing gun violence. Sadly, a decade later, mass shootings have increased exponentially. We have reached a point where this epidemic needs to be addressed as a significant risk to the homeland." «



# Safeguarding Moments for K-12 & Higher Education Campuses

Milestone Systems open video technology platform empowers administrators, security professionals, and IT leaders in our schools and universities to safeguard joyous moments, major turning points, and everything in between.



Scan here to  
learn more

**MAKE THE  
WORLD SEE**

Request information: [www.SecurityInfoWatch.com/10214397](http://www.SecurityInfoWatch.com/10214397)



© 2022 Genetec Inc. Genetec and the Genetec logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.



# Unified security, unlimited possibilities.

Securing your organization requires more than video surveillance. To be successful, you need access control, intercom, analytics, and other systems too. This is why our Security Center platform excels. It delivers a cohesive operating picture through modules that were built as one system. So, whether you're securing an airport, a parking structure, a multi-site enterprise, public transit, or an entire city, you can access all the information you need in one place.



To learn about the benefits of unifying your security operations visit [genetec.com](https://www.genetec.com)



Request information: [www.SecurityInfoWatch.com/10213771](https://www.SecurityInfoWatch.com/10213771)

# SCHOOL SECURITY & SAFETY

*Supplement to American Schools  
& Universities, Locksmith Ledger  
International, Security Business,  
Security Technology Executive*

## COVER STORY

**Campuses Strive to  
Strike a Balance  
Between Technology  
and Policy – Page 6**

## CAMPUS SECURITY FEATURES:

**Modern Systems for  
Enhanced Campus  
Security – [Page 4](#)**

**Schools Must As-  
sess Risk Prior to  
Implementing  
a Plan – [Page 10](#)**

**K-12 Security and  
Technology Expert  
Q&A – [Page 14](#)**

**How School Active-  
Shooter Myths Can  
Increase Casualties –  
[Page 18](#)**



**Most Affordably Meets  
New Classroom Codes:**  
*Locks from Either Side;  
Always Provides  
Unrestricted Exit*

## LocDown® Any Door from Safely Inside with Budget-Friendly Classroom Locks by Marks



Keep teachers, staff and students safer in the classroom with **Marks LocDown® Locks**. In the old days, with a standard lock, someone would have to go outside into the hall to lock up a classroom, but **LocDown Locks** uniquely lock from the inside, so no one has to potentially face an external threat. **Created in conjunction with, and spec'd by, one of the largest school districts in the country (LAUSD) and used by many more nationwide, Marks LocDown Locks have an inner door key and lock-down indicator, and easily & super-affordably replace any standard door lock.**

- **Lock Down in seconds, with a simple key, safely from inside** the classroom, without having to step foot into the hall or danger
- **Lockdown indicator** gives visual peace of mind
- **Retrofits any standard lock** easily & very economically
- **Classroom Locks in cylindrical or mortise lock styles**, with unique double cylinder locking mechanism
- **ALSO Ultra-Affordable Code-Compliant Marks F-Function Models**, as previous, but without indicator
- **All Durable for Life -** Lifetime warranty; exceeds ANSI/BHMA Grade 1 standard



 **MARKS USA**

1.800.645.9445 • salesinfo@marksusa.com • [www.marksusa.com](http://www.marksusa.com)

LocDown is a trademark of Marks USA/ Napco Security Technologies, Inc. For full warranty details, consult manual or see terms online.

Request information: [www.SecurityInfoWatch.com/10215125](http://www.SecurityInfoWatch.com/10215125)

See us at ISC East, Napco Booth 903

 **NAPCO**  
SECURITY TECHNOLOGIES

# CONTENTS

## COVER STORY

- S6** **Campuses Strive to Strike a Balance Between Technology and Policy**  
– Tim Kridel

## SCHOOL SAFETY & SECURITY

- S4** **Modern Systems for Enhanced Campus Security**  
– Rick Taylor
- S10** **Schools Must Assess Risk Prior to Implementing a Plan** – Tim Kridel
- S14** **K-12 Security and Technology Experts Weigh in on Strategic Security Planning and Organization**  
– Steve Lasky
- S18** **How Dangerous Myths About School Active Shooters Increase Casualties** – Michael Dorn

## COLUMNS

- S22** **My Point of View**  
What Can We Do to Fix a Broken School Security Blueprint? – Steve Lasky

## AD INDEX

Company Name	Page	Web Site URL
<b>Access Hardware Supply</b>	S13	<a href="http://www.securityinfowatch.com/10722906">www.securityinfowatch.com/10722906</a>
<b>Aiphone Communications Systems</b>	S9	<a href="http://www.securityinfowatch.com/10212724">www.securityinfowatch.com/10212724</a>
<b>ASSA ABLLOY DSS</b>	S11	<a href="http://www.securityinfowatch.com/10212899">www.securityinfowatch.com/10212899</a>
<b>Bold Group</b>	S15	<a href="http://www.securityinfowatch.com/10215780">www.securityinfowatch.com/10215780</a>
<b>Evolv Technology</b>	S17	<a href="http://www.securityinfowatch.com/21214371">www.securityinfowatch.com/21214371</a>
<b>Genetec Security Center</b>	S24	<a href="http://www.securityinfowatch.com/10213771">www.securityinfowatch.com/10213771</a>
<b>IP Video Corporation</b>	S21	<a href="http://www.securityinfowatch.com/10239527">www.securityinfowatch.com/10239527</a>
<b>Milestone Systems</b>	S23	<a href="http://www.securityinfowatch.com/10214397">www.securityinfowatch.com/10214397</a>
<b>NAPCO Security Technologies</b>	S2	<a href="http://www.securityinfowatch.com/10215125">www.securityinfowatch.com/10215125</a>

This directory is provided as a service. The Publisher assumes no liability for errors and/or omissions.

Cover photo: SDI Productions / 1221435875 / Getty Images

# SCHOOL SECURITY & SAFETY



## PUBLISHED BY

1233 Janesville Ave  
Fort Atkinson WI 53538  
800-547-7377

School Security & Safety is a supplement to American Schools & Universities, Locksmith Ledger, Security Business and Security Technology Executive magazines.

## EDITORIAL

**Editorial Director** | Steve Lasky  
**Editor, American Schools & Universities** | Joe Agron  
**Editor, Locksmith Ledger** | Will Christensen  
**Editor, Security Business** | Paul Rothman  
**Editor, Security Technology Executive** | Steve Lasky  
**Editor, SecurityInfoWatch.com** | John Dobberstein

## SALES

**Group Publisher** | Jolene Gulley-Bolton  
480-524-1119  
[jjulley@securityinfowatch.com](mailto:jjulley@securityinfowatch.com)

## Northeast US & East Canada

**SB, STE, SecurityInfoWatch** | Janice Welch  
(224) 324-8508  
[janice@securityinfowatch.com](mailto:janice@securityinfowatch.com)

## Midwest

**Locksmith Ledger, SB, STE, SecurityInfoWatch** | Brian Lowy  
(847) 454-2724  
[brlowy@endeavorb2b.com](mailto:brlowy@endeavorb2b.com)

## Western US & Western Canada

**SB, STE, SecurityInfoWatch** | Bobbie Ferraro  
310-800-5252  
[bobbie@securityinfowatch.com](mailto:bobbie@securityinfowatch.com)

## PRODUCTION

**Production Manager** | Brenda Wiley  
[bwiley@endeavorb2b.com](mailto:bwiley@endeavorb2b.com)  
**Audience Development Manager** | Delicia Poole  
[dpoole@endeavorb2b.com](mailto:dpoole@endeavorb2b.com)  
**Art Director** | Eric Van Egeren  
[evanegeren@endeavorb2b.com](mailto:evanegeren@endeavorb2b.com)

## ENDEAVOR BUSINESS MEDIA, LLC

**Chief Executive Officer** | Chris Ferrell  
**Chief Revenue Officer/CMO** | June Griffin  
**Chief Financial Officer** | Mark Zadell  
**Chief Operations Officer** | Patrick Raines  
**Chief Admin and Legal Officer** | Tracy Kane  
**EVP/Group Publisher** | Lester Craft  
**EVP Marketing Solutions** | Jacquie Niemiec

## Subscription Customer Service

Toll-Free 877-382-9187; Local 847-559-7598  
[Circ.SecDealer@omeda.com](mailto:Circ.SecDealer@omeda.com)

## Article Reprints • Brett Petillo

Wright's Media 877-652-5295, ext. 118  
[bpetillo@wrightsmedia.com](mailto:bpetillo@wrightsmedia.com)



Photo: Robert Hoetink / 82058978 / Bigstockphoto.com

# Modern Systems for Enhanced Campus Security

Upgrading a security system may feel daunting but there are options to fit most retrofit budgets **By Rick Taylor**

**M**ost schools today have adopted electronic access control and video surveillance systems as part of their campus security. However, since many schools have added these systems over several years, they often have multiple different systems that do not share information or use outdated technologies that now have known vulnerabilities. This results in systems that are complicated, expensive to maintain, and difficult to use. After a while, the technology becomes obsolete and needs to be replaced. Campuses can spend significant time fixing their system or implementing workarounds, and maintaining the status quo becomes very expensive.

Keeping campus security systems up to date with modern security

standards is easier when you implement a unified security platform. A unified platform is easier to use, more effective, and may even cost less over time, thanks to lower maintenance costs.

## Actionable Insights for Faster Responses and Efficient Operations

Disparate security systems make it hard to see the big picture of your campus security operations. With a unified platform, you can view and interact with data from all of your systems in a unified platform dashboard.

When all components of your security system, including access control, video surveillance, sensors, and license plate readers, are monitored and controlled within the same intuitive software interface, security

***Schools are counting on security technology more than ever to help them mitigate risk to students and staff.***

teams can respond quickly and work more efficiently.

Nuisance alarms, for example, can be reduced with a unified platform that combines data from door sensors with live and recorded video from the cameras. With the additional information from these systems, your team can have more control over when the system should alert staff. Both systems may tell you that a door has been opened for longer than usual, but only the system with unified video surveillance and analytics can let you quickly see if there's an obvious reason why. With more context about what's happening, you can decide whether or not someone needs to investigate in person.

If certain kinds of nuisance alarms are especially common you can even configure the system to be more selective about when to sound the alarm. For example, automated alerts



can be set if a door is left open for more than a specified number of seconds or only if the door is open and no person is present within the field of view of a camera positioned at that door.

Intelligent analytics can help you optimize security, allocate resources more effectively, and reduce the load on staff. You can see which doors or sensors set off alarms most frequently, and pull in data from video cameras, sensors, and other systems such as license plate recognition, to get a better understanding of why this is happening. You can also set up automated reports to identify hardware that isn't working properly or behavioral trends on campus that help your facilities managers address recurring or potential problems.

### **Video Surveillance Balanced with Privacy Protection**

When there is an event that requires investigation, such as vandalism or a report of an assault on campus, intelligent analytics allows security teams to go back and reconstruct what happened by pulling recorded video from that time and location, as well as any other relevant data from access control or license plate readers that might help identify the people involved. If the event is happening in real-time, security personnel can use this data to guide first responders, so they have real-time situational awareness before they arrive on the scene.

With so much data available at your fingertips, modern security systems must also consider privacy protection as a fundamental aspect of operations. Privacy isn't just important in sensitive areas on campus such as locker rooms and residence halls. Nobody wants to feel "watched" while moving through their daily routines.

Thankfully, it is possible with today's technology to protect individuals' right to anonymity. Campuses don't have to compromise security for privacy. Instead, modern video management software (VMS) can be configured to pixelize or mask individual

identities by default. Permissions can be granted to select staff members to depixelate the footage if the video needs to be reviewed for an investigation. The system can require multiple people to sign off on the request as a further check to ensure personally identifiable information is protected, the unified platform will report on which personnel retrieved the recorded video.

If video footage must be shared with police investigators, media, or members of the public, faces can also be unmasked for officers with the appropriate permissions. For example, the version shared with the public may have almost all faces blurred, while police or legal teams can be assigned secure credentials to view the original unaltered version. By requiring the video to be viewed only through a secure platform, your campus security can keep track of who has seen, downloaded, or shared the video, and can adjust permissions on a dynamic basis.

### **Access Control Management Through Automation**

Another important aspect of modern security systems is access control. In a unified system, access can be defined by role and can be granted or revoked easily as needs change. For example, access control can be linked to faculty, staff, and student profiles. When a student changes majors or residence halls, or a staff member changes office locations or roles, their permissions are reassigned automatically.

On college campuses, professors can even be given the authority to temporarily grant after-hours access to labs, libraries, or practice spaces to students as needed. If a student drops a class or graduates, the system can automatically remove access as well.

For visitors, access can be granted on a temporary or location-specific basis. For example, a guest speaker may have access to select campus spaces for the day they are scheduled to present, but this access will automatically be removed after the allotted time has expired.

### **Upgrading with Scalable Security Systems**

Unified platforms are built to be scalable and modular so you can upgrade or scale gradually as your campus's needs change. A unified system can serve a small K-12 school with a couple of hundred cameras and dozens of access points or a sprawling university complex with 20,000+ cameras and hundreds of access points — and everything in between.

Furthermore, a unified platform allows you to integrate elements such as automatic license plate recognition, sensors, and video analytics that monitor the outer perimeter of your campus. This helps you expand a "net of safety" beyond the walls of the building. The sooner you can detect something out of the ordinary, the more time your team has to respond to potential threats.

Upgrading to a modern security system may feel daunting but the good news is that in many cases, you won't need to replace the equipment you've invested in over the years. With a unified, open-architecture software solution, you can often reuse many hardware components you already have in place. This allows you to prioritize upgrades or plan a gradual transition one step at a time. The result will be not only a safer campus but also a more efficient and effective security operations team. «



**About the author:** Rick Taylor is the National Director of the Public Sector for Genetec. Rick joined Genetec in April 2013 as a Regional Sales

Manager. He was then promoted to Regional Sales Director for the Central U.S. before moving into the position of National Sales Director for Public Sector in November 2020. In his current role, Rick is responsible for leading his team in developing strategic plans within the public sector. Prior to his start at Genetec, Rick gained nearly a decade of experience in the security field, including positions as District Manager at both UTC Fire & Security and GE, and as Vice President at Esscoe for the company's Security Practice.



# Campuses Strive to Strike a Balance Between Technology and Policy



Photo: SDI Productions / 482576863 / Getty Images

Experts agree that technology is useless unless properly implemented with a comprehensive security strategy **By Tim Kridel**

***Districts, colleges and universities must strike a balance between responding to parents' and students' concerns about the latest headline-grabbing incident while still devoting enough resources to other risks.***

**T**here's something to be said about a two-way radio blaring in a hallway or classroom — and it's not all good. On the one hand, the chatter continually reminds students that their safety is a top priority. But on the other, the cacophony disrupts the learning and teaching environment.

Radios are just one example of how schools and higher-ed institutions have to weigh the additional

security of technology or policy against side effects such as disruptions and restrictions that faculty and students find onerous.

"PreK-12 school administrators have walked a tightrope for decades trying to balance having reasonable security and emergency preparedness measures with a welcoming, supportive climate conducive to their mission as child-oriented educational community centers," says Kenneth S. Trump,

National School Safety and Security Services president. "This challenge has intensified as mass school shootings, as well as other 'unknown unknowns,' present growing challenges to creating and maintaining secure and prepared campuses."

Those considerations prompted Olathe Public Schools to issue CrisisAlert badges to faculty and staff, which they can use to put their entire building on lockdown. This enables

them to respond immediately rather than waiting minutes to reach an administrator, explain the situation and finally get a lockdown.

“Obviously, our No. 1 priority is to keep our students and staff safe, but student learning is right behind that,” says Jim McMullen, the Olathe assistant superintendent who oversees safety services. “Finding that balance of a welcoming environment for kids and teachers while also providing the safest environment that you can is really our end goal. That’s why we felt this product was great.”

And unlike a radio, the alert is shared silently.

“We were a district that was very heavily reliant upon building radios, especially at the elementary level,” McMullen says. “This takes the place of the need for as many radios within a building. If a teacher needed assistance, anyone in the building could hear who needed assistance and why. That can be a disruption and a privacy issue, as well.”

Districts, colleges and universities also must strike a balance between responding to parents’ and students’ concerns about the latest headline-grabbing incident — such as a mass shooting — while still devoting enough resources to other, more everyday vulnerabilities. That’s another reason why Olathe chose CrisisAlert: Eight pushes trigger a lockdown, but fewer ones send an alert to the office.

“[We have] the ability to utilize this product not only in a worst-case active shooter scenario but also on crises that happen every day in schools across the country: behavioral, medical, the occasional fight, that sort of thing,” says Brent Kiger, Olathe executive director of safety services.

Besides CrisisAlert and walkie-talkies, districts also can leverage a device that every member of the faculty and staff already owns: a smartphone. In theory, which sounds like a great idea because means the security budget doesn’t have to fund thousands of specialized devices. In reality, their effectiveness is at the

mercy of coverage: the mobile operator that each employee uses and the district’s Wi-Fi network. Dead spots can become — literally and unfortunately — dead spots.

“There are a lot of things that pretty quickly rule out certain products for me,” Kiger says. “Some of those are if it’s heavily reliant upon Wi-Fi or cell phone coverage. Those are huge barriers for me.”

## Security Obscurity

Olathe uses CrisisAlert to control a locking mechanism on the bottom of doors that drops a pin into a floor plate.

“It really provides an opportunity for staff members with vulnerable kids to lock down quickly and provides a barricade without having to move furniture, file cabinets, etc.,” McMullen says. “No one really even knows it’s there.”

Hidden locking mechanisms and badges that look like ordinary ones are ways to hide new security and safety tools, so they don’t disrupt the learning experience. But doesn’t “out of sight, out of mind” also make students feel vulnerable? Possibly, but opting for high-profile measures such as metal detectors can backfire.

“A skewed focus on security products, hardware and technology often result in more ‘security theater’ than it does a meaningful, comprehensive school safety strategy,” Trump says. “Target hardening may make people feel more emotionally secure, but it doesn’t necessarily mean that it will actually make them safer. As a civil litigation expert witness on school safety lawsuits, while the facts and merits of each case vary, a common theme is that they involve allegations of failures of human factors — training, policies, procedures — than they do alleged failures of security hardware and equipment.”

## Cameras Shouldn’t Be the Only Eyes

People are another example of how the most effective security measures often are hiding in plain sight.

“We like to recommend technologies to enhance school safety, but

you can’t replace that human factor in awareness,” says Bob Klausmeyer, education safety coordinator at the Missouri School Boards’ Association (MSBA) Center for Education Safety. “First and foremost, it has to be that change in culture to where everybody makes themselves more aware of what’s going on.”

One example is training faculty and staff about how not to inadvertently undermine technologies and policies.

“You can put lockdown devices in doors, but if somebody props it open, then what good is it?” Klausmeyer says. “They become so reliant upon it [that] they become less aware because they believe that’s going to keep them safe, and it doesn’t.”

Another example is creating an environment that facilitates trust and is thus willing to share information, such as with SROs.

“The first and best line of defense is a well-trained, highly alert staff and student body,” Trump says. “The No. 1 way we find out about weapons, kids who have plotted to cause harm and individuals who are considering self-harm is from students who come forward and tell an adult that they trust.”

Olathe agrees.

“When they have a trusted adult, they will report things that they’ve seen online,” McMullen says. “We have students send things on to teachers or coaches that they see online at night. We get that to Brent and our safety services division, and they work with local law enforcement. We get things taken care of well before school starts the next day.”

“The welcoming environment and the relationship pieces are critical. Without that, you just lose that communication and trust, which is essential to preventing the crisis in the first place.”

Faculty, staff and administrators also should be encouraged to say something when they see something.

“I’ve got five board members that live on social media,” says Mark Skvarna, Montebello Unified School District interim superintendent. “They’ll say: ‘Such and such said this. This group said that.’”

## Bring in the Experts

All security/safety technologies and policies share one vulnerability: If people are unwilling or unable to use them, they'll look for ways around them, which can result in even greater risks. To avoid that problem, get input from all types of end users.

"When they're developing emergency operation plans, we recommend that they bring teachers, custodians, everybody in as a part of that development process to get their ideas and their experience," Klausmeyer says. "Make it so it works for everybody because it's not going to be good if they're uncomfortable with it or if it inhibits their jobs."

For example, teachers might ferret out problems with a technology's user interfaces and other aspects that otherwise would remain hidden until after implementation.

"If you're an administrator, and you haven't been in a classroom for 15 years, your teachers might think of something that you hadn't thought about," says Amy Roderick, director of the MSBA's Center for Education Safety.

But others caution against extending the feedback process with a trial, such as a couple of schools or a handful of campus buildings.

"I have been in law enforcement 38 years and director here for 17," says Kevin Grebin, University of Sioux Falls director of campus safety/security. "I learned early on that if we would float out the trial balloon, the process would get delayed and most likely never applied. We do look at other universities for information on new technologies and processes to hopefully see what problems to avoid on our end."

Finally, scrutinize feedback and other input instead of simply incorporating it at face value. That's one lesson learned from Columbia College's panic button implementation.

"Everybody wanted panic buttons on their desk," says Klausmeyer, who was head of campus safety before joining MSBA. "We put a few and we were very careful where we put them. But even so, we received so



Photo: gradyreese / 909472296 Getty Images

**Olathe Public Schools have issued CrisisAlert badges to faculty and staff, which they can use to put their entire building on lockdown.**

many false alarms because somebody either knocked them with their knee or just played with them. It became that cry wolf situation: 'Here we go again.'"

Some districts and colleges also look at other professions for ideas. For example, Montebello's Skvarna consulted his brother, who is the police chief at Burbank Airport.

"I did a lot of research on how they were handling open spaces, entrances, exits, hallways, and what type of locking equipment they use," he says.

Many hospitals require visitors to wear a badge, which enables staff to identify at a glance people who have snuck in. Some districts are applying this model. For example, about four years ago, Olathe implemented the Raptor visitor management system. When visitors check in at the front office, the system scans their driver's license so it can add the person's picture to a badge that they must wear. At the same time, Raptor also runs a check against the sex offender registry list.

"That's another layer of security," McMullen says. "It allows us to catch them on the front end. When a staff member sees an adult in the building that they don't recognize, they need to have a badge on."

## Shuffling Priorities

Another balancing act is prioritizing budgets, staff and other resources. For example, shootings are relatively rare,

but they also can dominate to the point of distraction.

"It's easier for them to lose focus on other potential threats or hazards that could occur — and might be more likely to occur — than an event like an active shooter," Klausmeyer says. "There are other things as simple as a gas leak or a fire that could be just as devastating. They need to focus on the broad spectrum of potential hazards and threats instead of just one area — even as devastating as that one event could be."

High-profile events can completely upend how a district or college looks at security.

"Funding school safety initiatives and strategies usually isn't number one in the budget," Roderick says. "So then when you respond to situations such as Uvalde, now it's become important, and you're trying to figure out how to fund what you want to do without having previously thought about that."

"Whether a major event triggers that or not, it just needs to be in the normal course of your annual budgeting: what our needs, whether it's perimeter fencing or radios or fire sprinkling systems. If you're doing renovations or adding on to the structure, you've got to think about those safety measures and budget for that."

Similar considerations and challenges apply at the collegiate level.

"The administration will be reactive to such events, but they also are

very supportive of my introduction of preventive measures, too, [such as] increased staffing, collaborating with our Neighborhood Watch groups, increased training, new surveillance techniques," Grebin says.

Even so, it's not necessarily a bad thing when high-profile events push certain upgrades up the priority list. For example, in August, a sex offender scaled a chain-link fence around a Riverside, Calif., elementary school and attempted to assault a student in a restroom. That prompted Montebello to replace its fences with ones that can't be scaled.

"It actually looks better than your standard chain link," Skvarna says. "It doesn't make it look like an institution, yet you can't get over it."

Uvalde also prompted Montebello to make changes — major ones.

"I believe that there was such a lesson with the failures in Texas that it

couldn't be ignored," Skvarna says. "I didn't believe it to be an overreaction to consider this. I think it's in our best interest to be proactive, and it's going to cost money: \$6 million or \$7 million.

"The board did not get involved where they said, 'We want you to do this.' I went to the board and said, 'We need to consider an emergency resolution.'"

One initiative is a complete overhaul of Montebello's surveillance network. That's also an example of how a major event can lead to funding for long-overdue projects that might otherwise continue to languish.

"We had cameras that were very, very old," Skvarna says. "We had ones that weren't working. We just had a hodgepodge of a bunch of junk. All of that is being replaced. We're also adding new cameras where they're needed."

Whether it's new cameras, new fencing or something else, it also helps

to educate the public about how their votes directly affect safety.

"We're very fortunate our community supported a bond issue last March," says Olathe's McMullen. "We had four threads to that bond, and one was safety. It has been on every bond we've passed in recent memory, so our community really supports safety measures and initiatives. We've also received some state grants, and we're currently looking at a couple on the national level. I think you have to be creative." ◀◀



**About the author:** *Tim Kridel is a freelance writer who has been covering a wide variety of technologies since 1998, including enterprise IT, video collaboration, cellular and Wi-Fi. For more information, visit [www.timkridel.com](http://www.timkridel.com).*

**AIPHONE**

## Dynamic Security Solutions for Campuses and Commercial Properties



Our commercial IP intercoms provide campus-wide **communication, convenience, and controlled access.**



Scan QR code.

Look for the play button and watch our video to see how an intercom can help secure your campus.



Request information: [www.SecurityInfoWatch.com/10212724](http://www.SecurityInfoWatch.com/10212724)



*If the school district has not conducted a risk and vulnerability assessment, a security consultant can educate the school district on the importance of conducting a threat, risk and vulnerability assessment prior to making any physical security technology changes to their security program.*

Photo: gradyreese / 903472296 / Getty Images

# Schools Must Assess Risk Prior to **Implementing a Plan**

Creating a strategic security roadmap helps administrators understand critical shortcomings needing to be addressed

by **Jim Townzen, PSP, CPP**

**W**e are often contacted by school administrators with a Request for Proposal (RFP) to provide professional physical security consulting services. When we review the RFP, we learn that they want to add some type of physical security technology enhancements for their school district. Once we have been selected as the consulting firm for the project, one of the first questions we ask is, "Can we review the most recent threat, risk and vulnerability assessment?"

Often, we learn that the school district has not conducted a threat, risk and vulnerability assessment to ascertain what the real threats, risks and vulnerabilities are to their district. In other words, we are being asked to specify and design physical security technologies for their district without understanding first what risks we are mitigating. This process of not knowing what the true needs of the school district are can be expensive for the district when poor decisions are made and oftentimes does not address the real

issues for “we do not know what we do not know” at this point. Oftentimes, school districts are reacting to public opinion to do “something quickly” following a recent catastrophic event. The Uvalde School District incident in Uvalde, Texas is a recent example.

If the school district has not conducted a risk and vulnerability assessment, we do our best to educate our contact with the school district on the importance of conducting a threat, risk and vulnerability assessment prior to making any physical security technology changes to their security program. All too often we are told that the money set aside for the physical security technology enhancements does not include funding for a district-wide threat, risk and vulnerability assessment. We are usually told that an assessment has already been conducted by the school administration, and they just need someone to assist them in the creation

of an RFP, hire a contractor, and project manage the installation and testing of the systems. In our thirty-plus years in this industry, we have rarely seen this scenario turn out well.

**Why should a school district conduct a district-wide threat, risk and vulnerability assessment prior to making changes to their existing security program?**

A threat, risk and vulnerability assessment is an evaluation by a physical security professional of the district’s current security program. This process includes a careful and methodical process to identify the district’s risks through a thorough fact-finding and evaluation process that includes the identification of the district’s tangible and intangible assets including people (in the eyes of the public, particularly the parents, the number one asset are the children and the families.), facilities,

equipment, intellectual, critical issues, applicable standards and reputation as a community resource, as well as the development of mitigation strategies that are appropriate for the district’s culture and capabilities and the risks within their environment.

The consultant will review the district’s security program to identify those threats, risks and vulnerabilities faced by the district that are either not optimally addressed or addressed at all. Once these risks are identified, the consultant will analyze the potential effect of these threats and exploited vulnerabilities in terms of likelihood of occurrence and severity of impact to determine and prioritize the most effective actions for mitigating risk. Other critical aspects of the assessment process include taking a holistic approach to evaluate the entire program from security technologies, the people involved in keeping

**ASSA ABLOY**  
Opening Solutions

Experience a safer  
and more open world

## Creating access *for the future*

Today it may feel more difficult than ever to ensure an ideal learning environment. However, with an approach that balances safety, security and wellness, you can create an atmosphere that provides peace of mind for students, faculty and staff.

Helping schools create a safe and secure learning environment is a top priority for ASSA ABLOY. We are here to help you evaluate your safety and security needs and assist with any questions or concerns you may have.

Learn more:  
[assaabloydss.com/SIW-K12](https://assaabloydss.com/SIW-K12)



Copyright © 2022, ASSA ABLOY Sales and Marketing Group, Inc., an ASSA ABLOY Group company. All rights reserved. 545 - A 10/22

Request information: [www.SecurityInfoWatch.com/10212899](http://www.SecurityInfoWatch.com/10212899)

the district safe, and the processes/ training in place to ensure everyone knows their roles and responsibilities in emergency situations.

**What should your school district expect during an assessment and what involvement will be required from your staff?**

- The firm that is selected will take a deep dive into your existing security policies and procedures looking for any improvements that can be made based on current best practices.
- Stakeholder interviews are very important in understanding if security practices currently in place are working/not working as well as get a firsthand understanding of the real-life implementation of district security policies.
- Physical review of the schools before, during and after school hours to get an understanding of circulation patterns (people and vehicles) from the outermost part of school property into the classroom.

The assessment team will review the physical security technologies in place to see what is in use and what gaps may be inherent in the design of the system and if there are any opportunities for improvement. Systems that would be reviewed include:

- Electronic Access Control
- Visitor Management
- Video Surveillance
- Intrusion Detection
- Mass Notification
- Metal Detection
- Weapons Detection

Last, but certainly not least, is a thorough review of the property to assess lighting, sightlines, perimeters, areas of concealment, remoteness, accessibility, surrounding properties, fencing and public access after school hours.

**What is the value of a risk and vulnerability assessment for your school district?**

Plain and simple – it serves as a road-map. Once the team has conducted a thorough assessment, the district will receive a report that goes into detail identifying the security gaps found and recommendations on how to mitigate those gaps. The assessment report

## A threat, risk and vulnerability assessment are an evaluation by a physical security professional of the district's current security program.

provides a holistic view of the district's entire current security program and not just one aspect of the program. A successful security program consists of the right mix of people, policy, and technology.

The road map will prioritize the recommendations to help the district determine short-term, mid-term and long-term planning needs that can be incorporated into their overall district master plan. Although it is tempting to use internal staff, local law enforcement, parents, or an online tool to conduct an assessment of the security program, the benefit of using a firm that does this every day and has the expert knowledge on how to best mitigate risk in a school environment brings tremendous benefit to the district.

### Conclusion

By reacting to pressure and not taking a holistic view of your security program you are, albeit inadvertently, doing a disservice to students, staff, parents and visitors who enter one of your campus buildings. A security program is a multi-dimensional approach to addressing your known threats, risks and vulnerabilities so without conducting a threat, risk and vulnerability assessment you're not looking at the entire picture.

Invest in a professional security consulting firm with experience commensurate with your school district. Pay close attention to the credentials of their team and make sure you hire a firm that specializes in physical security consulting. Keep your threat, risk and vulnerability assessment report

separate from your facility master planning as you may have information in the report that needs to remain confidential for the protection of students, staff, and visitors. Make sure that any plans that require construction or construction enhancements are shared with the architect who is implementing your facility master plan so that they can be executed as part of other budget items in the facility master plan.

As administrators, be honest and open with your assessors and encourage your staff to do the same. Bringing outsiders into your 'house' and sharing your known vulnerabilities is and can be uncomfortable but keep in mind the more honest you are the better solutions your assessors can provide you with mitigation methods and best practices. It is in your best interest that you use an outside firm to conduct this assessment as it will bring merit to those items you have been bringing up for years, but it also could bring to light other items of which you were unaware.

In conclusion threat, risk and vulnerability assessments are a vital part of every security program and should be used to guide your security program as well as your security budget. Hire an experienced firm, be open and honest, integrate your security plan into your facility master plan as necessary, and conduct these assessments at regular intervals every three to five years. ☞



**About the author:** Jim Townzen, PSP, CPP is a Staff Consultant for Security Risk Management Consultants, LLC in Ohio.



# THREE OF THE BEST



# CLOSERS

## AT INCREDIBLE PRICES

Ready to ship today at [accesshardware.com/nortonrixson-closer-sale](https://accesshardware.com/nortonrixson-closer-sale)

Request information: [www.SecurityInfoWatch.com/10722906](https://www.SecurityInfoWatch.com/10722906)



Where Service Meets Expertise.  
[accesshardware.com](https://accesshardware.com) | (800) 348 - 2263



# School Security **INSIGHTS:** Project Planning and Implementation

K-12 security and technology experts weigh in on strategic cybersecurity planning and organization **By Steve Lasky**



*The best place to start a security program is to seek out help from others for planning. This can mean professionals from other districts, security integrators as well as academics, and IT from within the district.*

Photo: Rawpixel.com / 121244216 / Bigstockphoto.com

**H**ave you ever gotten “Google Overload”? Have you ever searched for a symptom and found out that you’re dying of a real disease? If you’ve ever tried searching online for advice on security planning, your experience was most similar. The best advice always comes directly from industry professionals. Two K-12 security experts were asked to give advice on starting a security plan from the ground up.

We talked to Chris Montgomery, who is the Network Services Manager for Tomball, Texas ISD and has been with the school district for more than 26 years, along with Troy Neal, currently the Executive Director of Cybersecurity and Operations for Spring Branch, Texas ISD. Neal has worked as a cybersecurity professional in the K-12 school sector for more than 13 years.

The first step to building a security plan is to figure out the scope of your project.

**If a new school district approached you, how would you advise them on the best way to start a security program?**

**Chris Montgomery:** “You need a scope. Realize that you are not a security professional and that you will need help to develop a comprehensive security program. Reach out to other local school districts and ask

about systems and partners. Reach out to your local law enforcement as they often have resources dedicated to helping develop these programs. Reach out to the other departments and your administration to ensure cohesion and integration with the different parts and systems in the plan. A good partner will help you determine your technology needs, such as camera types, video storage, switching ports, and bandwidth

## Alarm Monitoring and Business Management Software for the Security Industry



For **over 40 years**, Bold Group has empowered security organizations with the most comprehensive array of alarm monitoring and integrated business management solutions tailored to achieve optimal outcomes and growth for security teams, central monitoring stations, dealers, and integrators.

**BOLD**  
GROUP

TO LEARN MORE VISIT [BOLDGROUP.COM](http://BOLDGROUP.COM)

Request information: [www.SecurityInfoWatch.com/10215780](http://www.SecurityInfoWatch.com/10215780)



requirements. A good partner will also assist with knowledge of any federal/state money that can be used to implement your plans.”

**Troy Neal:** “You have to have a philosophy first. Take physical security and cameras in general. What are you trying to solve? Is it just building security? Physical security, technology, academ-

*from other districts, security integrators as well as academics, and IT from within the district. All parties involved should be on the same page and meet regularly to ensure the security program is meeting the needs of everyone. The next step is working within the budget. Funding for K-12 is limited, so accounting for needs versus wants also requires the help of everyone at the table.*

And some of those are not built to an enterprise standard. They don’t develop it, they don’t have the life cycle and so you’re dealing with some of this great-looking software, but you can’t get data out of it. You can’t move data. Data drives everything; same with security. The more data points I have, the better holistic view I have of the organization. Our biggest challenge in K-12 is money. Especially with so much of this cloud-based software. We are not funded to pay for that. The subscription-based software is the hardest thing for me to pay for because that comes from general funds. In schools, 85% of your budget is spent on salaries. It’s people which are the most important piece of education. How do you find those mechanisms?”

*The first step to building a security plan is to figure out the scope of your project. Then verify the legal requirements. Next, move to planning for the basics like cameras, access control and fire alarms. Make decisions now that will solve your current needs, but also continue to work in the future without compromising your philosophy.*

## Storage upgrade requirements and yearly pricing increases in subscription-based software are limited by the strict budgets of K-12 schools.

ics, and operations all have to be on the same page and discuss it together versus one person making all the decisions. That’s where a lot of failures happen between academics and technology. We should be true partners. From there, then, what’s your strategy? How do you want to get there? What are your long-term costs? Can you scale it? Can you manage it? Who’s going to own it? The biggest problem we have in technology alone is, “Who owns it?” If somebody doesn’t own it, it’s always going to fail. Who’s your executive sponsor? It’s true project management from the start. All of our projects are done by a project charter. Bring in industry experts. Talk to other school districts and find out what they do. Find out what fits the organization and then plan where you want to go with it. Size means a lot. Run it like an enterprise. From a technology and security standpoint, you’re never in the way of things. And I think that’s where it starts.”

*The best place to start a security program is to seek out help from others for planning. This can mean professionals*

### If money were no object, how would you build out your security plan and in what order would you implement it?

**Montgomery:** “Develop a thorough scope that will solve your security needs. Choose a partner that understands your needs and has resources available to assist you. Determine which systems you will use to solve your needs and build an infrastructure that will support them now and in the future.”

**Neal:** You’ve got to look at local policy and legal policy because we have to follow all of that. You have state laws and federal laws. You have to figure out those parameters first. What are your basics? Cameras, you want to be able to see who comes in and out. You want people to badge in and out. Fire alarms, all the mandatory stuff. Then, how do you start tying in other things? The problem in K-12 is that there are certain systems we have to use, whether we like them or not.

### What changes have you seen over the last few years after security upgrades and integration?

**Montgomery:** “The number of resources used by our security devices (storage, bandwidth) has increased greatly on a scale that we have found ourselves unprepared for.”

**Neal:** “A lot of security software has gone cloud-based and subscription-based. This is where schools are really struggling. The way our budget cycles and planning is, we start budget conversations in October for the next school year. The biggest problem is the cloud part of it. Second, is the complexity of the software. You need a certain level of talent to get people to be able to own it and manage it. If you don’t have a philosophy or roadmap, someone is going to want this shiny object. Then it’s this next siloed system that you’ve got to manage and maintain. So, you start building

out these cool things, but then they become despaired again. Ideally, there would be a holistic integrated kind of system from the start. You have to have a different model for us to pay for things, especially in regard to the licensing for K-12."

"In regard to changes in physical security, a lot has helped because a lot of it now talks together. The hurt is, they still don't have industry standards. Just like we update standards in education and in the world, you've got to have very basic standards that things talk to one another. Especially in physical security, things don't talk to each other by design, and that's a problem. We need industry standards that force organizations and companies to say, "look you need to be able to talk based on this protocol." So, then I can take this information and use it in another system. Going

back to data and physical security, the most important part is protecting the entrance of a building and ensuring there is no unwanted person or thing coming through a building. Access control technology and simple things like badging and turning off alarms have all grown. In schools, a lot of them are not there yet. You've got schools built in the '50s and up. The cost to redo all of this even from a cabling standpoint is a lot. Standards are the number one thing. Just build it to an industry standard that's then safe and secure."

*Planning, and planning early is of the utmost importance when considering upgrades in security. Storage upgrade requirements and yearly pricing increases in subscription-based software are limited by the strict budgets of K-12 schools. Avoid getting caught up in buying software that can cost more money than originally budgeted for. Although many*

*improvements have been made, more efforts should be made to push for industry standards in physical security that would benefit everyone.*

*Schools have always been the place where members of the community come together to collectively educate and protect children, and their futures. Having a plan for creating a safe school starts with designing and building out a security plan. Planning should involve communities coming together from local school districts, law enforcement agencies and security integrators alike. When these groups can have vulnerable, productive conversations, real changes can be made for everyone's benefit. Involving voices from many spheres to share their successes, and more importantly, failures will only strengthen security in schools to protect our future generations to come. Now go, be vulnerable and reach out; build the security program your school needs. ❧*



The world is growing increasingly unsafe and incidents at schools are rapidly on the rise. If you are responsible for the safety of your students, faculty, staff, and visitors, now is the time to familiarize yourself with the benefits of transforming your physical security screening.

**Learn how Evolv is helping schools take a proactive stance against the threat of violence and ensure a safe learning environment.**

**evolvtechnology.com**

Request information: [www.SecurityInfoWatch.com/21214371](http://www.SecurityInfoWatch.com/21214371)

**evolv™**



# How Dangerous School Active-Shooter Myths **Can Increase** **CASUALTIES**

Schools must be able to identify and implement proper training procedures and policy to make security work

By Michael Dorn

*Poor active shooter training programs have thus far been a contributing factor in school shootings where more than \$130 million in out-of-court settlements have been paid by school systems and law enforcement agencies*



Upon hearing the instructions to lock down, a teacher and students move briskly to place chairs, desks and tables in front of the door to their classroom to prevent an active shooter from forcing entry to their classroom. Next, the students and teacher arm themselves with books and other objects to throw at the attacker's face and prepare to "swarm" the attacker. Sadly, this is not just a hypothetical example of how some schools with the best of intentions are spending precious time, energy and budget to increase rather than decrease the risk of harm to students and staff.

The various active shooter training programs that teach these types of approaches that have increased casualties in multiple school shootings provide but one example of the types of popular but dangerous approaches that are causing increased fatalities in U.S. K-12 schools. In fact, these types of active shooter training programs have thus far been a contributing factor in school shootings where more than \$130 million in out-of-court settlements have been paid by school systems and law enforcement agencies – in just a few of the school shootings our center's analysts have worked with litigation for other shootings ongoing.

Unfortunately, our experience providing official post-incident assistance for 23 active assailant and targeted shootings in K-12 schools in three countries, show that actions such as these clearly increase rather than decrease the danger to students and staff in most K-12 school shootings. But how could these alleged "best practice" approaches increase rather than decrease danger?

### **Know The Drill!**

For starters, having timed well-practiced teachers and high school students who barricade in this fashion, we have found that it takes an average of more than 120 seconds to accomplish the above actions, which keeps occupants in an exposed position for longer periods than it took the attacker at Marjorie-Stoneman Douglas High School to shoot his first 24 victims

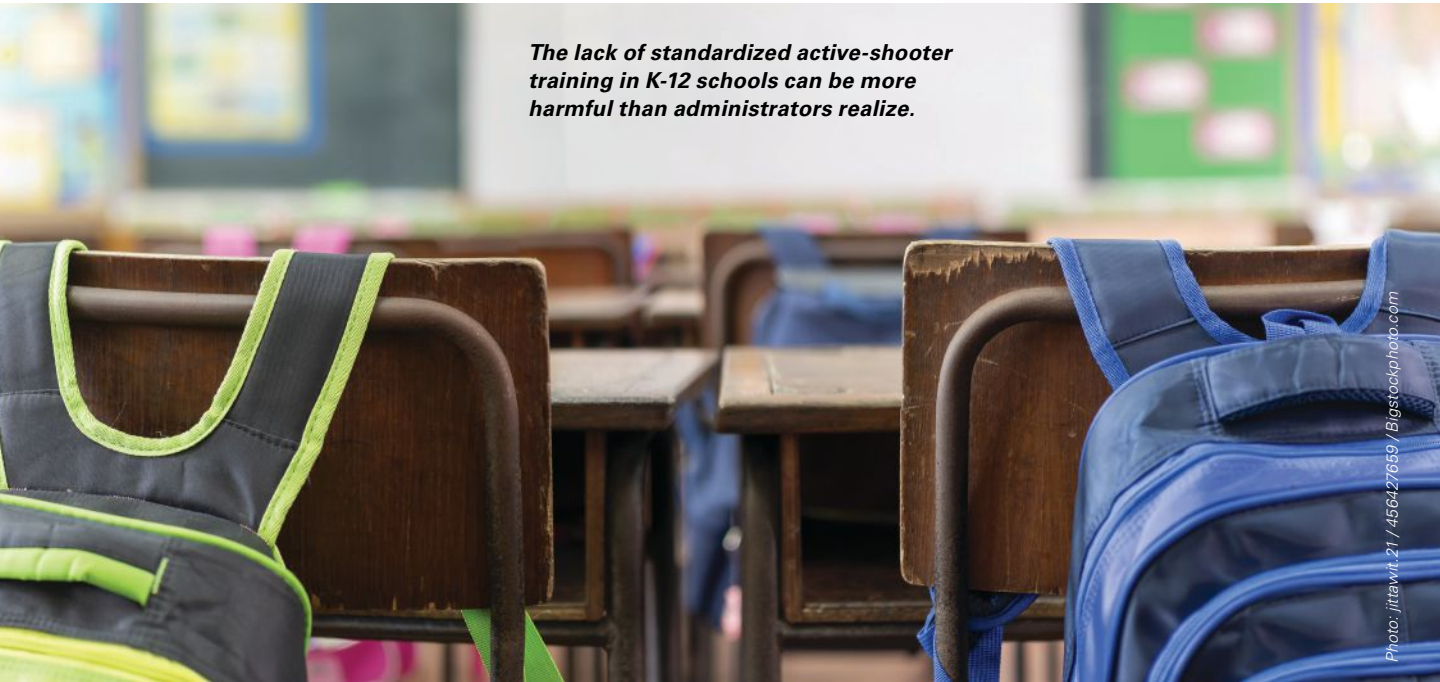


Photo: jittawit.21 / 456427659 / Bigstockphoto.com

***The lack of standardized active-shooter training in K-12 schools can be more harmful than administrators realize.***

worked on were shot in less than 90 seconds with many victims shot within the first seven to 43 seconds of a gun being observed.

The reality is that there has only been one K-12 school shooting in the United States where an attacker has forced entry into a locked classroom and subsequently killed occupants. In fact, the approaches taught in several of the more popular active shooter training programs fail to mitigate predominant attack patterns. Even though the “mega study” of school shootings recently conducted by the National Institute of Justice found that more than 50% of the people shot on K-12 school campuses around the country in the last 25 years, more than 650 that occurred were *outdoors* when they were shot, these training programs fail to address the far more important reverse evacuation tactics.

This severe training disconnect resulted in a catastrophic failure in a shooting on an elementary playground that personnel from our center observed as an expert witnesses. The litigation following this tragedy resulted in five sizeable out-of-court settlements in state and

federal jurisdictions. There are no easy answers to this complex problem in a nation with more students in school each day than the combined populations of Canada and Australia. Continuing to seek simple solutions to complex and challenging societal problems that lead to on-campus shooting ensure that more tragedies will occur unless realistic active-shooter strategies are embraced.

### **Misguided Active Shooter Training and Security Technology Implementation**

Flawed active shooter training programs are not the only critical problem seen from well-intentioned, but misguided school safety efforts. Oversimplified and canned emergency preparedness plans, unreliable emergency phone apps, dangerous emergency door locking devices, gun detection systems that do not work as advertised, incredibly expensive wearable panic buttons that are prone to malfunction and an array of other unsafe solutions have created havoc on school safety as fear-based mitigation methods have become more popular.

Our staff has also noticed school officials who are implementing security technologies that exceed the fiscal and staff resources over the long term. One extremely expensive and unreliable wearable duress button system incurs a yearly cost close to the initial installation cost. Most school districts or non-public schools will be unable to maintain the system over time. Many schools are less safe because precious limited time, energy and budget are being expended on solutions that are unreliable or fail to provide a viable benefit in relation to cost and staff time.

The time, energy and budget wasted on marginal types of security and safety solutions may also lead to preventable serious injuries and fatalities. Technology solutions that don't work are increasingly being used as powerful objective evidence against school officials in litigation. Common examples of solutions that fail to address significant risks are as simple as improving student supervision with training and electronic hall-pass systems or enhanced pre-employment screening and properly confronting traffic safety in parking lots. Other



boxes that can be checked include proper implementation of student threat assessment and management processes, use of effective self-harm prevention measures, upgrades to facilitate more rapid reverse evacuation from outdoor areas (if it is not safer to move away from the school in a particular event) and improving internal and internal public address capabilities.

### Misconceptions

One of the most critical observations derived from our more than seven decades working full-time in the field is that many of the perceptions surrounding school safety are seriously out of balance with reality. These misconceptions have been systemic since the tragic shooting at Columbine High School in 1999 and have become even more pervasive with every inaccurately publicized mass casualty attack.

Much too often, the severe disconnect between perceptions and facts that have given birth to the common refrain that there is an “epidemic of school shootings” in the United States, is an objectively false descriptor that can have serious ramifications in litigation if relied upon for determining school safety priorities. An “epidemic” is a public health term that defines a dramatic and rapid increase in a public safety threat over a short period of time. To be historically accurate, we would require an increase of thousands of school shootings in one or two school years to be truly considered a health crisis. This is not the case and among the reasons, the public health community has not declared school shootings to be an epidemic.

Much of the discussion and debate about reducing school violence oversimplifies complex societal problems. Comprehensive, locally tailored, assessment based and data-driven solutions to school safety may not make good media sound bites or be easy to implement but they are the most efficient way to create safe, welcoming and

The reality is that there has only been one K-12 school shooting in the United States where an attacker has forced entry into a locked classroom and subsequently killed occupants.

effective schools. In a nation with more quality free training, assessment and school safety planning tools than any place on earth, American school and public safety officials should not be negligent in utilizing them to develop practical and sustainable school safety strategies. «



**About the author:** The author of 28 books in his field, Michael Dorn serves as the Executive Director of Safe Havens International, the world’s largest K12 school safety center. Michael’s work has taken him to eleven countries during his 41-year career in the campus safety field.

**HALO SMART SENSOR**

**The Award Winning HALO 3C Device Protects Schools with Advanced Health, Safety & Vape Detection.**

- Chemical and Gas Detection
- Gunshot Detection
- Emergency Escape Lighting
- Air Quality Monitoring
- Aggression Detection and Calls for Help
- Disease Prevention with Health Index
- Motion & Occupancy Detection
- Vape and THC Detection
- Panic Button

**HALO SMART SENSOR**

[www.halodetect.com](http://www.halodetect.com)  
[info@ipvideocorp.com](mailto:info@ipvideocorp.com) | 631.969.2601

Request information: [www.SecurityInfoWatch.com/10239527](http://www.SecurityInfoWatch.com/10239527)



By Steve Lasky

# What Can We Do to Fix a Broken School Security Blueprint?

I have been writing about school shootings for more than two decades. As heinous and bone-crushing as each of them are, the most recent (up until this writing that is) in Uvalde, Texas seems to have shaken most security professionals to the core. Count me among them. The epic failure of local and state law enforcement during and after the shooting to address the threat, the utter confusion of school administrators to assess and react, combined with the shocking lack of basic security technology countermeasures created the perfect storm of chaos, coverup and carnage.

Over the years there has evolved a dual path of thinking related to school shootings, active-shooter protocols and preemptive security. One is couched in training and response and the other embraces technology implementation. My assessment is that both are critical to mitigating campus crime and violence, but there must be a symbiotic relationship between policy and hardware.

In the wake of the Uvalde shootings, this past June, Carnegie Mellon University's Biometrics Center hosted an online forum of experts in school security, law and technology for a special "School Safety Emergency Summit." (<https://vimeo.com/723133604/3e34e1c42c>). While one of the technology sponsors discussed the benefits of facial recognition as a lead element in a burgeoning AI-based technology environment for school and campus security solutions, veteran security professionals like Guy Grace, Vice-Chairman of the Partner Alliance for Safer Schools and a Unified K12 Life Safety consultant, was a bit more holistic.

"There is tremendous aftermath for years after a shooting. Uvalde is going to be dealing with this for the rest of their life. It's a cascading effect and it's all about how we mitigate that. Our mitigation is an all-hazards-type response [including] technologies that we use to support the response but also to support the aftermath of how we deal with these situations. Technology that empowers, it's a tool that we use to deal with the aftermath of these situations. It's multi-faceted when we're dealing with these emergencies. The technology measures... are there to detect, deter and deny... there are other security components that we need to have in place to nullify the effects or impact of a failure of one component. We have to be comprehensive when we're putting in these technologies not to just address an active threat situation, so we have to be thinking in an all-hazards sense in schools," stresses Grace.

Michael Matranga, the CEO of M6 Global security consultancy, a former U.S. Secret Service agent and a past director of security for Texas City ISD was adamant that the first responder to these types of events is not necessarily the law enforcement officer or the medical professional

"It's the person in the classroom right next door or in the hallway; we have to empower them for self-sustainability because we know that seconds matter in all of these things, whether it be in a school, whether it be in a grocery store, or in a shopping mall," he says.

Grace continues: "Everything we implement and purchase for schools, they are tools. They are going to be a unified life and safety system. The most important piece is going to be

the people and how do the people use those tools that we as security practitioners provide to our school districts and our communities to protect them."

Carnegie Mellon Bossa Nova Robotics Professor of Artificial Intelligence, Electrical and Computer Engineering Director Marios Savvides, Ph.D., provided an insight into the value of video surveillance used to help the FBI apprehend the Boston Marathon terrorist bombers. He laments that the data supplied was after-the-fact information and that today's goals are to prevent such incidents before they occur.

"While the killings are unacceptable no matter what you term them and are an unspeakable tragedy for the impacted families and communities, we have yet to acknowledge and clearly state: the senseless murder of Americans going about their daily lives should be addressed with the same focused and coordinated determination that our national security enterprise exhibits in preventing transnational and domestic terrorist attacks on the homeland. Let us not forget, the whole concept of homeland security gained prominence after 9/11 because of the need to protect Americans against the terror of attack as we went to work, traveled, and lived our lives," says Dr. Savvides.

He concludes: "It has been 10 years since the carnage at Sandy Hook elementary school. Following that mass shooting... we were part of the interagency team working at the White House, contributing to the President's plan to protect our children and our communities by reducing gun violence. Sadly, a decade later, mass shootings have increased exponentially. We have reached a point where this epidemic needs to be addressed as a significant risk to the homeland." «



# Safeguarding Moments for K-12 & Higher Education Campuses

Milestone Systems open video technology platform empowers administrators, security professionals, and IT leaders in our schools and universities to safeguard joyous moments, major turning points, and everything in between.



Scan here to  
learn more

**MAKE THE  
WORLD SEE**



Request information: [www.SecurityInfoWatch.com/10214397](http://www.SecurityInfoWatch.com/10214397)

© 2022 Genetec Inc. Genetec and the Genetec logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.



# Unified security, unlimited possibilities.

Securing your organization requires more than video surveillance. To be successful, you need access control, intercom, analytics, and other systems too. This is why our Security Center platform excels. It delivers a cohesive operating picture through modules that were built as one system. So, whether you're securing an airport, a parking structure, a multi-site enterprise, public transit, or an entire city, you can access all the information you need in one place.



To learn about the benefits of unifying your security operations visit [genetec.com](https://www.genetec.com)



Request information: [www.SecurityInfoWatch.com/10213771](https://www.SecurityInfoWatch.com/10213771)