

SECURITY DIRECTOR'S REPORT

ISSUE 07-06

WWW.IOMA.COM/SECURE

JUNE 2007

16 Mistakes That Can Turn 'Smart' Video Into a Dumb Move

Smart video has a powerful allure. Video systems that can alert to trouble—rather than just observe or record it—is a great leap forward in technology. But when you take a leap, you risk falling, and there are hurdles to consider with intelligent video, according to SDR interviews and presenters at the ISC West conference in Las Vegas.

Take a look at 16 mistakes that can turn an investment in smart video into a dumb move.

1. Focus on what analytics are capable of doing. "Don't let analytics drive the debate," warned Buddy Flerl, executive vice president at Agent Video Intelligence (www.aspectusvi.com). Instead, focus on the security needs of the facility and then "figure out how analytics can benefit your security posture," he said.

2. Purchase the best analytic system instead of the system that is best for you. Security executives often make the mistake of looking for the best cameras and most advanced behavior algorithms, said Flerl. The reality is that there is not—and will never be—one "best" system. There is, however, one system that is the best at detecting the behaviors you need to detect under the conditions that you need to detect them.

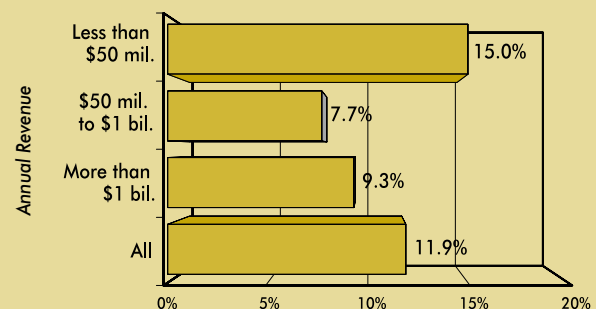
3. Don't do a complete and accurate site survey. Video analytic systems require security teams to balance the probability of system detection against the rate of nuisance alarms, Flerl warned. And unless you do a detailed assessment of the environment in

which a system is going to operate and thoroughly vet systems under its most extreme conditions, you won't get the balance right and may even select the wrong system. "I can't stress enough how important detailed site surveys are—per behavior, per camera."

4. Only worry about the algorithm, not video quality. Better video quality allows for superior video content analysis, which is why higher resolution network cameras are better than analog cameras and why a camera with built-in content analysis may be the best choice in specific applications, noted Pete DeAngelis, CEO of IQinVision (www.iqeye.com), a maker of Megapixel network cameras. "Analytics can do a better job running on raw video information than on encoded images."

5. Fall in love with a particular system's user-friendliness. Customers should look for an analytic

Combined IT/Physical Security Dept., 2007



(Source: IOMA)

system that is intuitive to operate and makes it easy to create and change video rules, but they should not think that such features separate one product from the rest of the pack. User-friendliness is now an increasingly universal selling point of video analytic systems. It's now more rare to find a system that *isn't* user-friendly.

Be wary of plug-and-play promises. Calibration per camera requires work, and there is no way to get around it.

6. Believe the hype about edge devices. A lot of today's tech talk is on pushing analytics to the edge, but "understand what those edge devices are capable of doing and what they're not capable of doing," said Flerl. "Smart cameras have arrived but you may want to wait 12 to 18 months for cameras with more horsepower."

7. Ignore what happens after systems spot suspicious behavior. The goal of deploying video analytics isn't to spot possible trouble—it is to get the information to the right people, at the right time, over the right medium, warned Steve Volz from systems integrator Adesta (www.adeitagroup.com). He said end-users frequently focus on system capabilities over the practicalities of delivering the information—and that is a mistake.

8. Don't worry about software integration. End-users are running into trouble with intelligent video systems supporting other features of their security system. "You want to make sure an analytic system adheres to as many software systems as possible," advised Flerl.

9. Forget traditional rules about video coverage. Volz said he sometimes sees end-users—in a rush of excitement over the capabilities of intelligent video systems—forget the tenants of Surveillance Video 101. "IVS [Intelligent video systems] can't detect what the camera system doesn't cover. Basic CCTV rules still apply, and an IVS is only as good as the CCTV system it's on."

10. Don't develop a test plan. All rules and behaviors on each camera must be tested over time and conditions, said Volz. Without a test plan that considers changing conditions up front, an intelligent video system that provides valuable alerts in summer may create nuisance alarms when snow is on the ground.

11. Underestimate the complexity of set-up. Be wary of plug-and-play promises. Calibration per camera requires work, and there is no way to get around it. "It's crucial," said Flerl.

12. Don't compare analytics for yourself. If you want to see if a certain system's analytics match your security needs and application, "take video clips and run raw video through each of three systems to measure them against latency of detection, failure of detection, and nuisance alarms," advised Flerl.

13. Don't tie video content analysis into the bigger security picture. "Some people act like analytics systems can do everything for you. You go home, and it will call you when you're needed," said James Chong, chief technology officer at VidSys (www.vidsys.com), a security software company. He warned that individual technology strengths don't necessarily add up to an effective enterprise security solution and that security departments should focus their planning around the common operating platform that will bring together all the disparate elements of the security operation.

14. Assume that scalability and cost-effectiveness are the same thing. "All analytic systems are scalable, but at what cost?" said Flerl. In a typical system configuration, a server may only support 16 cameras. Security departments must understand the threshold of cameras per server that makes it cost-effective for them.

15. Rely on labor savings to provide a return-on-investment (ROI). The practical experience of security departments suggests that it's unwise to expect video content analysis to result in a dramatic reduction in the number of security personnel. Yes, analytics do the job of watching video—something

staff used to do—but since algorithms are better at spotting possible problems that need checking out, you may find staff is just as necessary as ever (just more for response). This may help prevent losses, which can lead to ROI, but it may only provide greater security assurance and piece of mind—something that is valuable but a little squishy on the bottom line.

16. Just throw everything on the existing network. Smart video is only as effective as the network system that it is part of, and many companies mistakenly think it is as simple as putting video on the network. It's against this misconception that companies such as Steelbox Networks Inc. (steelbox.com) are fighting.

In one way, the company has a tough sell: It wants security departments to pay \$20,000 for something they already think they have. The company's Digital Matrix Storage Switch (DMSS), one of the stand-out products at the recent ISC West show, supports hundreds of concurrent video

streams for watching or recording at any number of surveillance stations. But some companies wonder why—since they can already put video on the network—should they pay extra for an appliance that sits between them?

The truth is that you can't just route vast amounts of video over your existing network if you really want it to be reliable and work as intended. By load balancing and routing data requests, appliances such as the DMSS provide the foundation that is necessary for making IP video work.

Because there is no guarantee of direct financial benefit, it's important to leverage the value of video content analysis. In addition to alerting when a scene violates a security rule, configure its capabilities to provide business information. Depending on the system and environment, systems could calculate customer conversion rates, measure transaction times, improve customer flow, validate advertising expenditures, reduce customer wait time, improve customer service, and so on. □

This article was originally published in IOMA's monthly newsletter *Security Director's Report* and is republished here with the express written permission of IOMA. © 2007. It is a violation of federal copyright law to reproduce all or part of this publication or its contents by any means. The Copyright Act imposes liability of up to \$150,000 per issue for such infringement. Information concerning illicit duplication will be gratefully received. To ensure compliance with all copyright regulations or to acquire a license for multi-subscriber distribution within a company or for permission to republish, please contact **Lou Klein** at IOMA's corporate licensing department, 646-424-3885, or e-mail lklein@ioma.com. For more information about IOMA or to subscribe to any IOMA publication, go to www.ioma.com.