Michael Dell invests in VMS provider Eagle Eye

Enrique Salem of Symantec, Austin Ventures also participate in round

By Martha Entwistle

AUSTIN, Texas—In his first personal investment in physical security, Michael Dell, founder and CEO of Dell Inc., on July 31 announced a “multi-million dollar” investment in VMS provider Eagle Eye Networks. “Eagle Eye is the first company in physical security where I have personally led with the investment decision,” Dell told Security Systems News in an email interview.

Eagle Eye, a cloud-managed video management system launched in January by Dean Drako, an entrepreneur who co-founded Barracuda Networks in 2003, will use most of the funding to build infrastructure, namely data centers, Drako told SSN.

Both Eagle Eye and Dell are based here in Austin.

Dell said the “major reason I invested in Eagle Eye is because I believe in Dean Drako’s execution as founder and long-time CEO of Barracuda Networks.”

The Series B Funding came from MSD Capital L.P., Michael Dell’s private investment firm. Also participating in the round were Austin Ventures and Enrique Salem, former CEO of Symantec and current board member at FireEye.

Drako declined to tell SSN the exact amount of the investment. “Michael and a few other folks... learned about Eagle Eye and had a strong interest in contributing and assisting in its growth,” Drako said.

Dell “is not on our board or [working with us] in any official capacity; but he has offered to do whatever he can to assist when we need help, or where he can help.”

“Michael has been selling IT products for a long time. He... learned about Eagle Eye and had a strong interest in contributing and assisting in its growth,” Drako said.

Lowe’s takes look at install option

By Tess Nacelewicz

MOOREVILLE, N.C.—In the two years since Lowe’s launched InS, the new do-it-yourself home automation/home security product is doing so well it’s offered in Lowe’s stores nationwide and the company is trialing a professional

LOWE’S see page 38

A POLICE CHIEF’S PERSPECTIVE

Video verification benefits assessed

By Leif Kothe

HIGHLAND PARK, Texas— Law enforcement is taking an increasingly active role in shaping video verification alarm policies. Testament to this are the best practices recently completed by the Partnership for Priority Video Alarm Response, which made law enforcement feedback a defining feature of the process.

While verified alarm proponents tout the technology’s ability to foil criminals and reduce false alarms, one police chief closely involved with that process warns that if jurisdictions do not follow best practices, the benefits of video verification may not be maximized.

Chris Vinson is the newly appointed head of the Texas Police Chiefs Association Alarm Committee, one of 12 law enforcement agencies closely involved in PPVARS best practices development process. Speaking to Security Systems News, he expressed optimism regarding the best practices and what kind of benefits law enforcement could reap from their adoption—particularly when it comes to stopping crimes in progress and apprehending criminals.

He said the key thing for the industry to understand about law enforcement’s perspective

POLICE CHIEF see page 36
Chief Vinson on video verification

Continued from page 1

of video verification is that the alarms have to “maintain a level of confidence if they want to keep that level of priority.”

The best practices can help, Vinson says. “If [video verified alarms] don’t all adhere to that type of practice then pretty soon, if we start responding to video alarms that are not an offense in progress, or something a reasonable person believed presented an immediate danger, every alarm gets relegated back to a low priority response,” he said. “The industry doesn’t want that, law enforcement doesn’t want that, and the customers out there don’t want that.”

Vinson, who is director of public safety for the town of Highland Park, Texas, near Dallas, acknowledged that while education efforts could spur broader adoption of PPVAR’s best practices, those involved had to be realistic for the time being, given that the decision to adopt or not would come down to the discretion of individual jurisdictions.

Vinson said efforts such as informing its membership that the Texas Police Chiefs Association stands in favor of the practices, or writing a position paper on why adopting the best practices could be a sound solution, are just a few good measures the organization can take on behalf of the cause.

When it comes to verification, Vinson believes there are still important discussions to be had between stakeholder groups over what qualifies as verification technology. Disagreements tend to be connected to the question of whether enhanced call verification (ECV) and cross-zoning should fall under the umbrella of verified technology.

Vinson says ECV methods and cross-zoning have proven effective at scaling back false alarms. But

“...A FUTURE.

With Keyscan’s full complement of feature-rich 1, 2, 4 and 8-reader door and elevator floor access control units and our renowned software, we can provide a simple solution to upgrading your aged or failing access control system.

Keyscan’s ‘hybrid’ approach to access control mixes network appliance-based hardware architecture as well as our ‘At-the-Edge’ solution. It simplifies system design by utilizing some, if not all, of your existing readers, credentials, network and power cables.

Keyscan’s approach helps you breathe new life into your aged or failing system by providing the latest in access control technology and making it easy for you to upgrade.

Visit us at ASIS 2014 - Booth 3811 or call us today to find out how we can assist you.

1 888 KEYSCAN (539-7226) toll free Canada or USA
www.keyscan.ca

“...I think there’s a huge distinction between false alarm reduction and verification.”

—Chris Vinson, Texas Police Chiefs Association

he doesn’t believe they qualify as verification technology. “I think there’s a huge distinction between false alarm reduction and verification,” he said. “There’s a lot of things you can do to reduce false alarms, from enhanced call verification to cross-zoning, but when it comes down to actual verification, it’s really difficult to call anything else verification of an actual offense unless we have a witness on the scene or video an operator can see.”

According to Vinson, there’s a building consensus forming around that idea in the law enforcement community, and the distinction isn’t just a matter of semantics. “It’s not mere words,” he said. “There’s true meaning when we talk about verification.”

He added: “With verification, it gives law enforcement the confidence to respond at a higher priority. That makes all the difference in world between just going to an alarm where there’s a break in here and we’re too late to do anything, versus showing up in time to catch somebody.”

GIS

Continued from page 32

The aging population, and the subsequent rise in demand for PERS, is a “big driver” behind why mapped information could become important for monitoring companies.

“Everything that you could imagine that you’d be thinking about when you’re mobile, you’d want to have information for,” Auen told SSN. “If someone is mobile, they’re going to want to know where they’re at and what resources they have available.” SSN