IT Intelligence

MORE ANALYTICS CAPABILITIES BREEDS MORE POTENTIAL CONCERNS

by Bob Stockwell

Bob Stockwell is Chief Technology Officer for STANLEY Security. From 1997-2012, he was Niscayah's Director of Systems Operations.

bob.stockwell@sbdinc.com

Twenty-five years ago, the most advanced video analytic present in almost any environment — whether it be health care, retail, financial or educational institutions — was motion-based detection accompanied by some point-of-sale (POS) information; this was based on pixel changes in a camera. The event was local to the DVR, and the only notification was an alert on the DVR or possibly a relay closure. Fast-forward to the modern networks of today, and almost every device incorporates some level of intelligence designed and deployed for the hyper-connected, Internet-dependent world.

As new security devices reach the marketplace, they incorporate modern open protocols designed to interact in concert with other business intelligence offerings, such as POS. Today's systems can now be monitored in real-time, using cloud-based, custom analytic dashboards that send alerts based on predetermined business rules.

CUSTOMERS DON'T REALIZE SECURITY RISKS

There are both benefits and drawbacks in this new age of business intelligence. For example, real-time monitoring allows for much more immediate responses to events as they happen, allowing for more controlled and, ultimately, better outcomes. Additionally, increased interoperability and standardized protocols allow security officers to more readily build a detailed picture of an event in order to administer an appropriate response or preventative measures for the future.

The downside is that all of these devices create large amounts of transactional data, information that can be gathered and saved to create detailed images of routine workflows within a business. Many cable companies offer self-monitoring solutions that integrate alarm, video and automation devices into one package. Every time a customer disarms his or her alarm or captures a video, this information is immediately stored. However, in the wrong hands, this information might place a business or customer at risk for a massive data and privacy breach.

Customers should be aware that oftentimes the service provider owns the recorded information and the customer has little or no control over its usage, or with whom it is shared. Many users have strong opinions about this fact, and where to draw the delicate line between information necessary to business functions and personal data. Though all clients are required to sign end-user license agreements very rarely do the majority of customers read them in their entirety.

All too often, customers are not completely knowledgeable of these agreements and the kind of information gathering, storage and usage they've agreed to when entering into a partnership with service providers. Though the level of connectivity and intelligence provided to the business is invaluable, encourage your customers to be mindful of the security-related information being stored and the potential threats it poses.

END-USER BENEFITS VS. PRIVACY ISSUES

The new era of business intelligence, information sharing and connectivity, users are forced to consider whether the benefits outweigh the privacy concerns and risks posed by new technologies. With the high level of integration and increase in interoperability connections, people are much more aware of their surroundings and can respond much more quickly and aptly to situations.

For example, hospitals can incorporate video analytics, such as facial recognition, direction and tripwire traffic patterns, to increase workflow and enable security processes to be more efficient. Banks and retailers can verify fraud more immediately, or simply accumulate better business intelligence on their customers to drive greater revenue opportunities.

Too often, customers are not completely knowledgeable of the kind of information gathering, storage and usage they've agreed to when entering into a partnership with service providers.

In educational facilities, connected devices can offer a great advantage as well. With people-counting features or through identity recognition programs, instructors can more easily take attendance in a classroom, or locate a missing student or staff member quickly. Security can be immediately notified if an unidentified individual is on campus. Smart cards allow students to pay for lunch, check out library books or attend functions without having to carry cash or additional identification.

A process should be cultivated to ensure that any new security-sourced business intelligence tools and interconnected devices are vetted to best serve as business tools, still placing the protection of individuals and personal information at the forefront. Only by keeping privacy concerns and protection of the end-users' data in mind can these devices remain secure against intrusion and the legal issues that would ensue. SSI