

SECURITY INTELLIGENCE

INDIA
Executive Briefing

MAY 2010

SECURITY INDUSTRY COMING OF AGE

- Drawing Lessons From Mumbai Episode
- Indian Firms Enhancing IT Security
- Video Surveillance Emerging As A Service



Mumbai Terrorist
Kasab Awarded Death

But when will it be executed is
the question?



Should You Jump to
IP Surveillance?

Think strategically and
plan ahead



India Blips On The
Cybercrime Radar

Hackers have moved to
sophisticated campaigns



when using video for investigations or for sharing with internal business units or external law enforcement.

Trying to do it all at once has its own hazards. There are the obstacles in justifying a very significant investment while discarding what is usefully in place. Overreaching IP-based security could overwhelm the enterprise's network either perceived or in real-time.

For our CSO, Terry, the best bet – and one his team chose – was to do something, with emphasis on coexistence of existing analog with introduction, where it makes security and business sense, of IP video surveillance.

Whatever the plan, however, it does not have to be a go-it-alone proposition for the security department. There are security systems integrators, consultants and architecture and engineering firms that boast a track record of help and advice.

Case Study: University of South Florida's IP Jump

Infinova has worked with Nate Rice, USF's engineer for video surveillance, and his team, performing site surveys to analyze where new IP cameras can provide the greatest coverage and the best return on investment.

"There are several reasons why it is important that we begin to migrate to an IP solution," Rice reports. "First of

all, we must reduce costs. We have over 200 buildings on campus. Any one of them may request surveillance coverage and, when they do, our team visits them, analyzes their needs and designs a system.

"In too many cases, we end up with a need for only one camera and there is no way to connect it to another head-in running fibre. So, all too often, that means we need to include a dedicated DVR. Even when we use a 10-port DVR, the cost of that one-camera solution is ridiculous. With an IP camera, we can simply plug it into the network and allocate storage for that camera.

"In addition," Rice adds, "we have many departments who have created their own 'big box retailer' surveillance system with 'no-name' DIY residential type cameras and DVRs. Then, they want us to service and manage it. In almost every case, we decline. With our new system, we want a single solution for all video surveillance used throughout the campus. We will be using the VMS and IP cameras we select to set our standard. Equally as important, we also want to take advantage of the higher resolution that an IP surveillance solution provides. We want to have the availability of megapixel images when needed and that is very difficult to provide in a DVR environment." USF also gained an ability to integrate systems through its IP migration.

Railways Take Measures for Security

Policing on Railways is the responsibility of the Government Railway Police (GRP), which functions under the control of state government concerned. Whenever any specific information is received regarding Terrorist/Militant/Maoist activities, local -police/government railway police and civil authorities provide security to the railway track, railway passengers and railway infrastructure to avoid any untoward incident.

According to the Minister of State for Railways, K H Muniyappa, "In addition to action taken by civil and police authorities, Railways have taken up further measures for security of passenger." The measures are listed below.

1. Integrated Security scheme consisting of CCTV surveillance system, access control system, personal and baggage screening system and bomb detection and disposal system has been finalized for 202 important stations and the same is under implementation.
2. Commando training is being imparted to selected Railway Protection Force (RPF) staff to deal with insurgent attacks.
3. Sniffer dog squads in divisions and zones are being augmented.
4. Under modernization scheme, security gadgets are being procured and the weaponry is being upgraded.
5. Strength of RPF is being augmented. Altogether 5,134 posts have been sanctioned. In addition to it, three RPSF battalions. One commando training centre and

12 Mahila companies have been approved in Budget 2010-11.

Mock drills are conducted by the RPF in all the zonal railways at regular intervals to test security preparedness and to ensure corrective measures. Two Mock drills were conducted at New Delhi during January to March 2010.

The Railway committee has identified security equipment needed for rail security and adequate fund has been released to ensure procurement of these equipments.

Over 2200 important trains are being escorted by Government Railway Police and about 1275 trains are being escorted by Railway Protection Force on daily basis for providing safety and security of passengers in vulnerable sections.

Also, access control is ensured at important railway stations. An All-India Railway Protection Force help-line has been approved in works programme 2010-11 at an anticipated cost of US\$ 50 million.

Networking of security control rooms and Railway Protection Force posts at divisions/zones and Railway Board, to improve response to passengers and to ensure better crime control, has been approved in works programme 2010-11 at an anticipated cost of US\$ 44 million.

An integrated security system has been sanctioned for 202 sensitive stations of the country at an estimated cost of US\$ 3530 million.

Deploying Effective Solutions

Nuisance alarms are the bane of the security industry. Whether false alarms come from burglar alarms, outdoor sensors or some other system component, they can undermine security effectiveness and cause security teams to lose trust in their systems. Repeated false alarms can eventually condition security operators to ignore valid alerts. Nuisance alarms can become part of the "background noise" of a dysfunctional security system and can negatively impact accountability of the entire security organization.

Some facilities are plagued with hundreds of nuisance alarms every week. Outdoor detection systems, which must operate in an uncontrolled environment subject to weather changes, random movements from trees, shadows from clouds, and small animals that can inappropriately trigger alerts, are especially prone to nuisance alarms. One cause of these nuisance alerts in outdoor systems comes from deploying intelligent video systems originally designed for static indoor environments.

When these indoor systems are misapplied to protect a facility's perimeter or buffer zone, the recurrence of nuisance alarms can undermine the important mission of perimeter security to serve as the first line of defense. Often the only option left in such cases is to decrease the system's detection sensitivity in order to decrease the number of nuisance alerts. As a result, there is a high likelihood that such systems will never detect the threats that they were intended to stop.

Intelligence Surveillance Systems

For these reasons, providing effective outdoor security systems without nuisance alarms or misdetects requires intelligent surveillance systems designed for outdoor applications. A number of camera features engineered specifically for outdoor surveillance enables such a system to provide accurate detection in the outdoor environment, despite uncontrolled factors. For example, sufficient on-board image processing can be used to discriminate legitimate targets from extraneous surrounding motion and clutter.

Such processing power within the camera can be used to stabilize the image electronically, before video content analysis takes place. This removes camera motion as a source of nuisance alarms or misdetects, since video analytics software cannot detect an object entering into view if the whole scene is moving from wind. Sufficient in-camera processing can also eliminate water reflections and tree motion as sources of nuisance alarms, and dynamically correct lighting to detect events that would otherwise be



JOHN ROMANOWICH
CEO, SIGHTLOGIX, INC.

missed. Additional environmental factors that need to be addressed in the outdoors include the sun moving across the sky, clouds constantly in motion and shadows moving through a scene, all of which must be filtered so as not to appear to the camera as targets on which to alarm.

Protecting Large Outdoor Access

When sufficient processing is placed directly within the camera, 100 percent of the raw scene data is available to make accurate determinations, data that would otherwise be stripped away for transmission over the network for external analysis. Such extra processing can also be used to georegister the camera's field-of-view to GPS coordinates and provide operators with accurate determination of target location, size, bearing and speed, information which is not needed for indoor surveillance but becomes critical when protecting large outdoor areas.

The economics of covering large outdoor areas is also different. Outdoor surveillance involves additional infrastructure costs, including engineering design, construction, trenching, camera poles, network connectivity, video display and storage. By providing the appropriate level of computational power, such outdoor cameras are able to cover great distances, as much as three to five times the distance (more than ten times the area) of indoor surveillance cameras, reducing the number of cameras, infrastructure and associated costs. While outdoor cameras may have a higher cost per unit, their extended range from extra processing leads to an overall reduction in deployment cost. Applying outdoor solutions to outdoor problems is the key to eliminating nuisance alarms. Using appropriate tools designed for the task enables the full realization of the long-promised benefits of intelligent video – and delivers new levels of efficiency for the \$100 billion security guard market.