

# *HCL Infosystems Ltd.*

*Media Coverage*

*Dataquest*

*Thought Leadership - Security Beyond Devices*

*Industry Expertise - The Answers are here...*

**HCL**

Publication: Dataquest; Issue -December 15<sup>th</sup> 2009

Green IT, 75 Follow Dataquest on [www.twitter.com/dataquest\\_india](http://www.twitter.com/dataquest_india) | INR 25

# DATAQUEST

Vol XXXVIII No 23 - 1 December 15, 2009  
A CYBER MEDIA publication

USA: Marc Benoit, Chairman & CEO, Microsoft Corp.

## DISJOINTED

It's one year after 26/11 and we are still as vulnerable to terror. The efforts are visible but in desperate need of an integrated approach

**'Use of IT in police is not a movement yet'**  
—Dr Kiran Bedi

**Solving Copenhagen**  
With the UN Climate Change Summit in Copenhagen kicking closer, and controversies around it heating up, it's time to explore the chances of the event becoming a success /78

**Time for Convergence**  
BBT's new vision 2009-12 for payment systems is a drive to create a converged patch for all kinds of payments to be processed within the country /18

## Burnt and Broken...

...was Mumbai one year back, and there have not been many changes in security setups one year after the horrifying 26/11 attacks. The saving grace perhaps is the great awakening that we have had as a country—though it is yet to translate into decisive steps /34

### The Answers are Here...

...and they lie with the vendors. It's the right questions that seem to be missing /48

### Eyeing Security Solutions

Increases in security threats have helped the video surveillance industry gain momentum even during the slowdown /46

### 'Use of IT in police is not a movement yet'

—Dr Kiran Bedi /48

### 'Network video surveillance is 80% IT'

—Ray Maritzson, president and global CEO, Axis Communications /48

### Security Beyond Devices

The Mumbai terror attacks have grown to become a sort of knee-jerk, all-purpose examples for all scenarios. Lessons from it? We are still learning /50

Cover Story

Column

## Security Beyond Devices

The Mumbai terror attacks have grown to become a sort of knee-jerk, all-purpose examples for all seasons. Lessons from it? We are still learning

**W**e are a young nation, and as we grow, our nation will come across new challenges and yes, we will learn how to overcome them. But what does not need to be learnt the difficult way is the realization that even we as a nation are today vulnerable to the new face of terrorism. The attack on the Parliament, or potential attack on sensitive government installations is a *pané*. Today militant organizations with sleeper cells across cities, assaults with arms and hi-tech equipment that our policemen are not equipped with—target soft, vulnerable public areas like hotels, hospitals, office complexes, railway stations, etc. Their only goal is to cause maximum mayhem and damage. The siege of South Mumbai by a handful of men brought that fact home. Chillingly.

The need of the hour is not only to neutralize those men with guns but also to build a security blanket that detects, preempts and prevents such threats at every sensitive government installation, tourist spot, public-office area, be it private or government.

### Are We Doing Enough?

We don't need research to prove that the adoption of technology in the security architecture helps reduce vulnerability and minimize risks. We see some of it around in every day—at home, or at work. CCTV surveillance, for example, helps monitor activities in designated zones, metal detectors trace all things concealed, baggage screeners help detect explosives and weapons, access control to secure admission in premises, and intrusion

detection systems to identify and bar intrusion, among others.

The CCTV grab in Mumbai helped cops in identifying Ajmal Kasab, and I am sure it will help the authorities in establishing...but what did it do beyond that? Did it aid authorities in ceasing or minimizing the mayhem caused? There is more technology can do than to merely identify terrorists after a strike. It can help detect and deter the terrorists, and also enable the rapid deployment of relief and rescue operations.

### Managing Risk

Managing security is all about managing risk. Risk is a function of the threats we face; how vulnerable are we to those threats; and finally, what the consequences may be if those threats are successful. Risk does not remain constant, however, a baseline risk profiling can be used for design and implementation of a security system, but it must be understood that risk profile will change both from the baseline level as well as in real-time. The security system must be able to adapt to this dynamically changing risk profile.

It is critical that it is realized by all involved in our system for security that there is no single solution. Mere deployment of CCTV surveillance, baggage screeners or explosive detectors alone will not help minimize threats. Yes they deter, but they just land up being isolated islands of checks, with false alarms going like promotional calls on our cellphones.

To adequately secure an environment, we need an integrated approach to synchronize policy with

process, technology, intelligence, and on ground policing. The key is 'convergence' of information, communication and security technologies. This 'convergence' and integration allows for the coordination and adaptation of the security system to meet the threat at hand in the fastest and most efficient manner. Such a convergence and integration would offer actionable intelligence.

The key is to build a security cover that has the ability to trigger 'actionable intelligence' which enables authorities to act, and react, in a security threat situation, in a focused manner so as to prevent an attack or minimize the impact of an attack. Convergence of information, communication, and security technologies allows coordination and adaptation within a security system to meet the threat in the quickest and the most efficient manner.

### Beyond Cameras

Note that the system has offered more than just 'monitoring', it has collected inputs from panic buttons and responded by activating CCTV cameras over the alert zone. When multiple alerts were generated, the system automatically responded and communicated the issue to the authorities and ground police. Besides alerting people in the premises, the system pro-actively engaged a pre-mediated response mechanism to contain damage. This is 'actionable intelligence'. It is not only about terminal devices, but also managing information to minimize risks, and its impact.

Cover Story

### Actualize Actionable Intelligence

This is exactly what P Chidambaram did after taking over as the Union Home Minister after the Mumbai terror attack on November 26 last year. He set in motion a quick overhaul of homeland security. This includes training maritime protection, borders, airports, mass-transport networks, and critical infrastructure security.

Besides immediately operationalizing the multi-agency center, which enables analysis of intelligence inputs on a real-time basis and sharing of information among intelligence agencies and police forces, Chidambaram has also talked of legislative actions like strengthening the Prevention of Unlawful Activities Act and creation of the National Investigative Agency.

What we need is not mere tinkering of institutional mechanisms but a total overhaul of the security system. A report prepared by a FICCI taskforce on national security and terrorism, which charts out what went wrong during the Mumbai attacks that killed over 180 people, recommends: a) A compelling need to improve the country's capabilities with respect to terrorist related intelligence; b) Better coordination between various government agencies in connection with the information they have access to; c) Need to convert such information to actionable intelligence, and to communicate it to the concerned operational agencies in the fastest way possible.

What is required is to take a lesson from the US post 9/11. The need of the hour is to put in place a comprehensive national security policy framework and enable investigative agencies, on ground policing, prosecution and the courts, to foil terror plots internally as well as externally.

### What Needs to be Done?

On the first anniversary to that black blot on the calendar, what we need is a change in mindset. Securing our borders alone will not help, as unfor-

### A Case Scenario

Various sensors with varied functions are installed in a building, including CCTV cameras, panic buttons, public address systems, and gunshot detectors, among others. These components are connected to a command and control center (C&C) and the latter, in turn, is connected to a master C&C that operates at a central level across multiple centers. Now, the panic button is pressed. What happens?

- CCTV focused on the panic button focuses on to the spot where the panic button is pressed.
- A signal from the panic button reaches the zonal C&C through a secure connection; the system directs other cameras in the region towards the identified spot with operator's assistance.
- The display module simultaneously displays feeds from all those cameras onto the video wall.
- The control module will flash check points to facilitate operator through the decision making process and decide on further course of action.
- The system, besides performing these activities, can automatically communicate feeds to nearby ground police and

- headquarters.
- The ground police locations will be triggered with the help of GIS modules, which are an integral component of the C&C center architecture.
- Access control systems can be activated to prevent entry into the core area of the alert zone.
- The public address system will be automatically activated to alert and guide people to evacuate the area.
- Similar address systems in nearby areas will alert people to avoid getting close to the 'hotspot'.
- Training and drills can be periodically carried out to hone the skills, reduce response times in the event of an actual crisis.

tunately the threat is closer home than we often perceive.

Post 26/11, there have been talks about proper training for private security guards since they are the first line of defense in homeland security. What is also required is to make it mandatory for the custodians of private and public places to deploy proper integrated security system. Further, evacuation and disaster management plans also needs to be built in. These cannot be the responsibility of the government alone. It is critical to bring in professional security companies in the design and deployment of such systems, further their needs to be an integration with local law enforcement agencies in the form of regular meeting to establish rapport, ensure readiness, share advance intelligence and enable coordinated responses.

It is also imperative to create awareness among citizens to take on security responsibilities on themselves. In the West, every household invests in the basic CCTV, alarm monitoring and response, gas detection systems, fire

detection systems, and guarding services. In India, hi-tech security is still an area of the privileged. Though the cost of such equipment could be a barrier, creating awareness, linking insurance to security cover enabled, legislation, etc, will help enable this transition. It will also help create standards and competition. Therefore, mass adoption will control costs automatically.

As a nation we are on the threshold of a wave of growth that can transform the lives of millions in our country. To achieve this, and if we are to be a destination of choice for global investments, it is imperative that we secure our society and nation. A legislation to make security mandatory for every Indian will go a long way in securing our homes and society.

As citizens, a right to be secured must be made a fundamental right.



—Ajai Chowdhry, chairman & CEO, HCL Infosystems and chairman, HCL Security

Authored by – Mr. Ajai Chowdhry Chairman & CEO, HCL Infosystems Ltd.



Publication: Dataquest; Issue -December 15<sup>th</sup> 2009

Cover Story



# The Answers are Here...

...and they lie with the vendors. It's the right questions that seem to be missing

**T**he 26/11 terror attacks tipped the balance. In favor of security, in favor of an integrated set up and in favor of vendors. For they now had many more motivations to secure. The theater of terror had moved beyond the government buildings and shifted to private areas with large

footfalls. And that's quite good news, for the private players were not only willing to do more, they were willing to do it quickly. However, it's not to be assumed that the government has been sitting with its hands folded. It too is taking this wake up call seriously and building up its security toolbox,

even though at a very slow pace. And while it is assembling its tools, the vendors have leaped far ahead. From advanced biometrics to integration with analytical softwares, they have thought of and indeed developed an array of advanced security solutions. But are we up to such advancement yet? What is it



“There is a big hesitancy because of the capex factor. And then, there is a problem of legacy infrastructure”



“There is a big hesitancy because of the capex factor. And then, there is the problem of legacy infrastructure”

—Rohan Bhattacharyya, CEO, HCL Security

that the Indian market holds for security vendors and integrators? And will their leap of faith in India's potential bear fruit? We try to find out...

**Beyond Image Capture**  
And there is a lot to be seen behind the camera glasses as well. The problem is that only a very select group of people have been able to see this far.

According to Rohan Bhattacharyya, CEO, HCL Security, there is a lot that can be done with camera surveillance. “There is scope for biometrics, face recognition, number plate recognition, forensics and storage coming out of surveillance through the use of technology,” he says. If so much is possible then why is it that we are still stuck with an isolated camera, good only for post incident footage?

The reason, says Bhattacharyya, are many. For one, “There is a big hesitancy because of the capex factor.” And then, there is the problem of legacy infra-



“Regulation will be the most healthy thing for the security industry”

—Sandeep Lugani, practice head, BMS and physical security, Wipro Infotech

structure. While the first problem can be overcome through reasonable amount of convincing and case building, the second is something that is prevalent across our country in many forms.

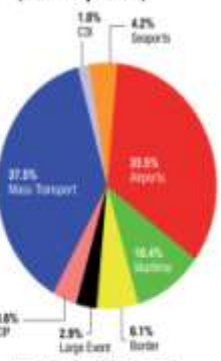
However, the market dynamics have figured an answer to that one as well—and they are the integrators. People who can take under their umbrella anything from any vendor and integrate the threads together.

However, that too is somewhat of a pressure on the pockets, but is certainly not as painstaking as replacing everything old. The two major names in the integration space today—HCL and Wipro—prove that integration is nothing small, and has a lot to offer.

Moreover, all the vendors and network providers are also increasingly recognizing that a key element of architecture is to integrate legacy infrastructure with new technologies. As Bhattacharyya puts it, “The key to being successful in this market, is to be ‘product agnostic.’”

So it's time to make that timely camera happen by finding it a partner, albeit of a different breed.

**The Future of Indian Homeland Security Market (2016 Projections)**



CB: Command, Control, Communications and Intelligence  
CIP: Critical Infrastructures Protection  
Source: Frost & Sullivan

**The maximum security focus will center around mass transport like railways and airports in the coming decade**

**Is Need Recognition Enough?**

“I anticipate this market to be at a stage where the need is recognized...,” says Subodh Varshan, country head and director, sales, government and public safety, Motorola India. Although that is half the job done, there are a lot of impediments to be yet surpassed. As Varshan says in his next utterance, “The biggest challenge now is the coming together of various parties and procuring the required and suitable technology.”

Most vendors tend to agree that at least the need for security has been well accepted and while private industry seems to be reacting a little faster, the government too is at its job. And well, the vendors aren't complaining because so far

**Cover Story**



“Vendors are trying to bring integration technologies, but there is no adoption. All we have is still a very rudimentary set-up”

—Asoen Kumar, GM, marketing, IT Outsourcing Services

they are getting their models. The analysts, however, are critical. While they agree that the government and private parties are both buying stuff, it's their proper deployment that is becoming a matter of concern. A standalone camera in a market, perhaps integrated to a police chowki, is no doubt creating a security market but is it resulting in a host of broad security solution? Perhaps not.

And that is where the crux in our security landscape is that though there is awareness, it is not necessarily being addressed in the right manner. The efforts so far have been isolated and disjointed. The right technology answers seem to be coming with the vendors but not many seem to have an ear to hear them out.

As Asoen Kumar, GM, marketing, IT Outsourcing Services puts it, “Vendors are trying to bring integration technologies, but there is no adoption. All we have is still a very rudimentary set-up.”



“The biggest challenge now is the coming together of various parties and procuring the required and suitable technology”

—Subodh Varshan, country head in director, sales, government and public safety, Motorola India

**The IP Backbone**

Yes, IP is the spine that the security structure is assuming gradually. And airports seem to be the ones in this regard. Free of late, every agency from police forces to state governments seems to be waking up to the IP movement. Devices are fast shifting modes from analog to IP. And in that lies some great news for the vendors.

According to Sandeep Lugani, practice head, BMS and physical security, Wipro Infotech, “As IP becomes more popular, reactions is going to be more organized as there will be more knowledge available.” With IP gaining ground, software analytics is another thing that the vendors are banking on big time.

As people begin to understand that hardware is just the beginning, security is becoming more and more software driven. And what's come as a big surprise to everyone is that it is the police that is driving the software adoption for intelligence purposes.

**To Each his Own**

That's the mantra of this market as of now. Everyone is doing their own bit, without bothering about any other part of the set up. The problem that glares us in the face is the lack of standardization.

And this disparity is something that even the vendors haven't been able to handle that well. In fact, many vendor issues are only feeling the differences.

It is nothing new that the government's efforts are detached and disjointed. However, vendors can't be given a clean chit either. While some like Honeywell have created their own integrating arms (separate companies) some like Bosch don't have any integrating set up of their own. Thus they tie up with independent integrators and that sort of apparatus doesn't work across the country. Besides, with different vendors following different protocols one is forced to ask: “Where is the standardization?”

Moreover, in tier-2 and -3 cities integrating and maintenance projects are a problem with most vendors. Also, what India is clearly missing is a local vendor. Maybe that will indeed help in addressing some of the local issues that we are facing today. Sturmung Systems is one such name that is coming up...let's keep our fingers crossed!

**The Security Hygiene**

That perhaps is the last leg for establishing a security regimen. The crying need to introduce a security certification and insurance. As long as we don't have set parameters we are going to have unsecured security set ups against untested threats.

And the vendors and the integrators are unanimous on this one, as Lugani puts it, “Regulation will be the most healthy thing for the security industry.”

—Mehak Chavla, mehac@cybermedia.co.in

