"How to Maximize Security with Existing Infrastructure"

Capt SB Tyagi

The environment, in which the Security operates, has changed beyond recognition. The ease of travel, more open borders and digital technologies have globalized criminality, making it far harder to contain and prosecute. Terrorism, of course, is notoriously borderless. But globalization has also massively expanded opportunities for organized crime. And technology, by spawning new kinds of crime while facilitating the traditional variety, is helping lawbreakers become ever bolder and more difficult to track down.

The shelf-life of security technology and the functional life of security systems have been severely challenged by fast paced innovations and newer technology. Today's technology is on the verge of obsolescence and yesterday's technology is obsolete already! The investment on security systems and measures are directly linked to ROI and the operational life of the security systems.

One of the biggest challenges enterprise and public sector organizations face is in leveraging existing infrastructure like video surveillance to deliver more value, better situational awareness, and faster threat recognition and response. We need to gain a better understanding of today's challenges and best practices in video surveillance and physical security, and how they can maximize existing security assets while minimizing risk.

We need to learn how the combination of PSIM, behaviour recognition technology and video surveillance can improve existing security infrastructure as well as gain insight on how data can be analysed for dramatic improvements in situational awareness, response and resolution.

To maximise the security with existing infrastructure, following are the essential ingredients -

- Thinking out-of-the-box!
- Innovation and application
- Know your inventory
- Know your technology
- PSIM
- Predict and improve through analytics
- Data storage – cloud computing
- Trust the team
- Optimize ways of working
- Enhance collaboration
- Proactively manage changes

Physical security information management (PSIM) is a category of software that provides a platform and applications created by middleware developers, designed to integrate multiple unconnected security applications and devices and control them through one comprehensive user interface. It collects and correlates events from existing disparate security devices and

information systems (video, access control, sensors, analytics, networks, building systems, etc.) to empower personnel to identify and proactively resolve situations. PSIM integration enables numerous organisational benefits, including increased control, improved situation awareness and management reporting. Ultimately, these solutions allow organisations to reduce costs through improved efficiency and to improve security through increased intelligence.

A complete PSIM software system has six key capabilities:

- **Collection:** Device management independent software collects data from any number of disparate security devices or systems.
- **Analysis:** The system analyses and correlates the data, events, and alarms, to identify the real situations and their priority.
- **Verification:** PSIM software presents the relevant situation information in a quick and easily-digestible format for an operator to verify the situation.
- **Resolution:** The system provides Standard Operating Procedures (SOPs), step-by-step instructions based on best practices and an organization's policies, and tools to resolve the situation.
- **Reporting:** The PSIM software tracks all the information and steps for compliance reporting, training and potentially, in-depth investigative analysis.
- **Audit trail:** The PSIM also monitors how each operator interacts with the system, tracks any manual changes to security systems and calculates reaction times for each event.

A key differential between PSIM based integration and other forms of physical security system integration is the ability for a PSIM platform to connect systems at a data level, contrasting other forms of integration which interface a limited number of products. PSIM allows use of open technologies which are compatible with a large number of manufacturers. These PSIM products offer more opportunities for expansion and can reduce implementation costs through greater use of existing equipment. PSIM solutions in general are deployed to centralize information to single or multiple control hubs. These are referred to as control rooms or command and control centres. Security systems typically integrated into a PSIM solution include;

- Access control systems
- CCTV
- Fire detection
- Video wall
- Intrusion detection system
- Perimeter Intrusion detection system
- Radar based detection
- GIS mapping systems
- Intercom
- Automated barriers & bollards
- Building management systems
- Lighting control system
- Power Monitoring System

Behavioral Recognition Systems: It is Behavioural Analytics technology that analyses video content by imitating learning and memory processes of the human brain. This fully automated scalable surveillance technology is different from all Video Analytics systems since it is able to autonomously detect abnormal behaviour in real time, without the need of human intervention. The computer software utilizes the behavioural Analytics technology, which monitors a scene through each camera separately and learns on behaviour. This system combines computer vision with cognitive machine learning processes, and it develops patterns for different classes of objects. These patterns later become rules for the system that autonomously detaches normal situations from those that can be possible threats.

Functionality

- **Reason-based system:** Unlike the traditional, rule-based system, Behavioral Analytics is the reason-based system that enables a machine to learn what is abnormal, without human pre-programing. By decreasing the number of alerts, it helps security officers to perceive more threats in real time.
- **The Entire Field of View Analysis:** BRS analyses the total field of view through each video camera in closed-circuit television system, despite certain difficulties, types of equipment or specific conditions on a scene.
- **Continuous Learning and Modifying:** Unlike the traditional video surveillance rules-based technology, BRS permanently learns and registers when some changes occur, so any on-going programing is not necessary.
- **Open Standards:** It is the "open standards" system which enables it to cooperate easily with different infrastructures, both the existing ones and the new ones. This video surveillance technology has been deployed globally across critical infrastructure facilities, intelligence agency applications, urban areas, seaports, financial institutions and others.
- **Easy Installation:** BRS needs maximum of a few days for the complete hardware and software installation, regardless of the number of cameras that need to be connected into the system and without any changes on the client's site.

Moving your Infrastructure to the Cloud:

In all probability, the CCTV system needs largest storage space. The need increases with advent of HD cameras. A typical CCTV System with 140 cameras of fixed focal and 10 DH cameras, the storage needed for 30 days recording with reduced frame rate is 20 TB approximately. With the number of HD cameras and the types of video analytics increase, the storage space goes for quantum leap! In such scenario the cloud computing is better alternative.

With Cloud Computing becoming more widely utilized, it is important for organizations to understand ways to maximize benefits and minimize risks of a move to the cloud. Buyers need to appreciate that assessing individual providers is critical to the success of Cloud Computing programs.